

Gestion des risques de sécurité humanitaire

Revue des bonnes pratiques 8
Troisième édition



**Le Réseau
de Pratiques
Humanitaires**

Humanitarian Practice Network (HPN)

ODI Global
4 Millbank
London SW1P 3JA
Royaume-Uni

E-mail : hpn@odi.org.uk
Site Web : www.odihpn.org

Imprimée et reliée au Royaume-Uni par Formara Print and
Marketing
Mise en page et production : Jessica Rennoldson

Cette édition a été traduite avec le soutien de CLEAR Global
(clearglobal.org/).
Traductrices : Safinaz Iris Soliman, Emilie Rigault Fourcadier,
Anne-Marie Luigi. Réviseurs : Katy Lebrun, Mariana Duque-Díez

© ODI Global, Londres, 2025
ISBN : 978-1-0682923-1-6

Les lecteurs sont encouragés à reproduire le contenu pour
leurs propres publications, à condition qu'elles ne soient pas
vendues à des fins commerciales. ODI Global demande à être
dûment cité et à recevoir un exemplaire de la publication.

Les demandes de reproduction commerciale du contenu
du HPN doivent être adressées à ODI Global en tant que
détenteur des droits d'auteur. Le coordinateur du réseau
HPN apprécierait de recevoir des informations détaillées sur
l'utilisation de ce contenu dans le cadre de formations, de
recherches ou de la conception, de la mise en œuvre ou de
l'évaluation de programmes.

Les opinions exprimées dans ce document sont celles des
auteurs et ne reflètent pas nécessairement celles de ODI
Global ou de nos partenaires.

Cette œuvre est placée sous licence CC BY-NC-ND 4.0.

Revue des bonnes pratiques

**Gestion des risques de sécurité
humanitaire**

Juin 2025

Troisième édition

Table des matières

Auteurs et remerciements	7
Déclaration de non-responsabilité	11
Glossaire des termes de sécurité	12
Avant-propos	19
Introduction	21

Partie 1 Fondements de la gestion des risques de sécurité humanitaire 27

- 1.1 Concepts et principes clés
- 1.2 Approche de sécurité centrée sur la personne

Partie 2 Les écosystèmes de la gestion des risques de sécurité 61

- 2.1 Les réseaux de sécurité et la collaboration entre les acteurs
- 2.2 Plaidoyer et sécurité

Partie 3 Éléments organisationnels : structures et instruments politiques 85

- 3.1 Le système de gestion des risques de sécurité humanitaire
- 3.2 Accès et sécurité
- 3.3 Financement de la gestion des risques de sécurité
- 3.4 Suivi de la conformité, de l'efficacité et de l'impact
- 3.5 Gestion des risques de sécurité dans les partenariats

Partie 4 Éléments opérationnels : processus et outils 147

- 4.1 Éléments analytiques
- 4.2 Élaboration d'une stratégie de sécurité
- 4.3 Plans et dispositions de sécurité
- 4.4 Réponse aux incidents et gestion de crise

Partie 5 Les personnes engagées dans la gestion des risques de sécurité **249**

- 5.1 Ressources humaines
- 5.2 Formation à la sécurité
- 5.3 Communication sur la sécurité au sein de l'organisation
- 5.4 Bien-être du personnel
- 5.5 Considérations médicales et de santé

Partie 6 Technologie et sécurité **331**

- 6.1 Gestion de la sécurité de l'information et des communications
- 6.2 La sécurité dans un monde numérique

Partie 7 Gestion des menaces et des situations à risque spécifiques **383**

- 7.1 Sécurité des déplacements
- 7.2 Sécurité du site
- 7.3 Sécurité des fonds en espèces
- 7.4 Criminalité
- 7.5 Surveillance hostile
- 7.6 Troubles civils
- 7.7 Violence sexuelle
- 7.8 Détention et arrestation
- 7.9 Enlèvement, enlèvement contre rançon et situation d'otages
- 7.10 Menaces liées aux combats et vestiges de guerre

Postface **526**

Auteurs et remerciements

Cette édition révisée de la *Revue des bonnes pratiques* (RBP) est dédiée aux nombreux spécialistes de la sécurité humanitaire qui travaillent sans relâche pour soutenir leurs collègues et leurs organisations. Elle est dédiée à ceux qui ne sont plus parmi nous, mais dont les contributions et le dévouement dans ce domaine resteront à jamais gravés dans nos mémoires.

Cette troisième édition a été co-éditée par Adelicia Fairbanks et Abby Stoddard de Humanitarian Outcomes. Elles ont été aidées par Monica Czwarno et Meriah-Jo Breckenridge, également de Humanitarian Outcomes. Samiha Ahmed a coordonné le processus de production pour HPN, et Matthew Foley, rédacteur à ODI Global, a édité le manuscrit. Cette RBP s'appuie sur le travail des éditions précédentes, dirigées par Koenraad Van Brabant, Adele Harmer, Abby Stoddard et Katherine Haver.

Les contributeurs à cette RBP ont généreusement donné de leur temps pour réviser le contenu, fournir des ressources, partager leurs connaissances et leurs conseils, et contribuer à la rédaction. La présente RBP est le fruit d'un véritable travail collectif, auquel ont contribué les personnes suivantes :

Banu Altunbas

Tara Arthur, Collective Security Group

Javeria Ayaz Malik, ActionAid et INSSA

Petro Babyak, Mercy Corps Ukraine

Shaun Bickley, Tricky Locations

Awil Bihi, CARE

Tamsin Blake, Medair

Donald S. Bosch, Ph.D., Psya.D., Humanitarian Psychological Services

Phil Candy, Medair

Araba Cole

Amaury T. Cooper

Gonzalo de Palacios, Oxfam

Steve Dennis, Proper Support Recovery Consulting

Catherine Deseure-Plumridge, UNDSS

Gurpreet Dhoot, Fauna & Flora

Neil Elliot, MSyl, Oxfam International

Daniel Elliott, CAFOD

Shannon Fariel-Mureithi, ChildFund International

Anthony Val Flynn, Direction générale des partenariats internationaux de la Commission européenne

Alexandra Godoi, Oxfam GB et Oxfam International

Paul Herridge, Itad

Henrieke Hommes, ZOA

Heather Hughes, Global Interagency Security Forum (GISF)

Stephen Ingram, Mines Advisory Group

Rafael K. Khusnutdinov, RTI International

Jean-Philippe Kiehl, Comité International de la Croix-Rouge

Sarah Kilani, Centre on Armed Groups

Jenna Kuokkanen, World Vision International

Elodie Leroy-Le Moigne, Plan International

Armstrong Maina, Project HOPE

Steven A. Mercer, Samaritan's Purse International Relief

Alan Mordaunt, Trócaire

Robert Muggah, Institut Igarapé

Noemi Muñoz Zamora, International Rescue Committee (IRC)

Michael O'Neill, INSSA

Kevin Pedone, Clements Worldwide

Carina Peña, Programme Alimentaire Mondial

Christine Persaud, Université du Québec, Montréal

William Plowright, Université de Durham

Adrian Powell, Proelium Law LLP

Pegah Rajabi, International NGO Safety Organisation (INSO)

Jeremy Reeves

Lisa Reilly

Jochen Riegg, Norwegian Refugee Council

Scott Ruddick, Cowater International

Rod Slip, Oxfam

Craig Spencer, M.D., M.P.H., Brown University School of Public Health

Barry Steyn, International Rescue Committee (IRC)

Matt Stockton, Global Interagency Security Forum (GISF)

Sandrine Tiller, Médecins Sans Frontières

Marieke van Weerden

Julian Visser, ZOA

Ron Waldman, MD, MPH, Milken Institute School of Public Health, George
Washington University

Benjamin Whelan, Access Now

Christina Wille, Insecurity Insight

Chris Williams, CARE

Christine Williamson, Duty of Care International

Ian Woodmansey, Crucial Safety

Tara Yip-Bannicq Ward, Plan International

Hannah Zitner, International Rescue Committee (IRC)

Déclaration de non-responsabilité concernant la présente Revue des bonnes pratiques (« RBP »)

ODI Global, dans toute la mesure permise par la loi :

1. Ne fera ni ne laissera entendre aucune déclaration, promesse ou garantie quant aux recommandations ou conseils fournis dans la présente RBP.
2. Ne fera ni ne laissera entendre aucune déclaration, promesse ou garantie quant à la qualité, la durée de vie ou l'usure de la présente RBP publiée en 2025, ni quant à son adéquation à un usage particulier ou à une utilisation dans des conditions spécifiques.
3. N'assumera aucune responsabilité pour toute perte, tout dommage ou tout inconvénient résultant de l'utilisation, de l'impossibilité d'utiliser ou de l'interprétation des informations contenues dans la présente RBP.
4. N'assumera aucun devoir de diligence, aucune responsabilité et ne sera pas responsable envers vous ou toute autre personne pour tout dommage quel qu'il soit résultant de toute décision prise ou action entreprise à la lumière des informations fournies dans la présente RBP.

Toutes les informations contenues dans la présente RBP sont présentées par ODI Global ou ses collaborateurs tiers qui ont contribué à cette RBP, conformément à leur compréhension au moment de la publication des recommandations générales en matière de gestion des risques de sécurité. La présente RBP ne doit pas être considérée comme une déclaration adéquate ou valide concernant les procédures opérationnelles standards, les types de menaces dans un pays particulier ou la gestion des risques de sécurité d'une ou plusieurs agences.

Bien que ODI Global se soit efforcé de garantir l'exactitude et la qualité des informations présentées dans cette RBP, ODI Global ne peut garantir l'exactitude ou la qualité des informations présentées dans cette RBP. Vous devez évaluer vous-même les risques et le comportement à adopter dans des environnements à haut risque, violents ou potentiellement à haut risque ou violents, même dans les conditions décrites dans la présente RBP. La présente RBP ne peut en aucun cas remplacer votre obligation de faire preuve de diligence raisonnable ou de procéder à votre propre évaluation avant d'intervenir dans un environnement violent, à haut risque ou potentiellement violent ou à haut risque. La présente RBP est rendue publique à titre indicatif uniquement.

La présente RBP peut inclure les opinions ou recommandations de tiers et ne reflète pas nécessairement les opinions de ODI Global ni n'indique un engagement envers une ligne de conduite particulière.

Glossaire des termes de sécurité

Le glossaire suivant contient des termes et des concepts clés relatifs à la présente *Revue des bonnes pratiques*.¹

Accès humanitaire Capacités des acteurs humanitaires à atteindre les populations touchées, et capacités des personnes touchées à accéder à l'aide et aux services.

Analyse/cartographie des acteurs Exercice visant à identifier et à analyser les acteurs/parties prenantes dans un environnement donné qui sont essentiels à la compréhension du contexte et qui peuvent avoir une incidence sur la sécurité d'une organisation.

Analyse/évaluation des risques Processus analytique en plusieurs étapes par lequel les organisations identifient les risques pour leur personnel, leurs actifs, leurs programmes et leur réputation, et les évaluent en fonction de leur probabilité et de leur impact afin d'en déterminer la gravité.

Analyse d'acceptation Processus d'évaluation des niveaux d'acceptation dont bénéficie l'organisation auprès des différentes parties prenantes dans son environnement.

Analyse du contexte Processus visant à comprendre l'environnement dans lequel une organisation évolue, comme première étape pour identifier les menaces potentielles pour la sécurité et les vulnérabilités.

Anti-surveillance Pratique consistant à détecter la surveillance, par exemple pour déterminer si les déplacements du personnel ou les installations font l'objet d'une surveillance malveillante.

Approche centrée sur les personnes survivantes Priorité accordée aux besoins, aux droits et à la sûreté des personnes touchées par des événements traumatisants. Elle met l'accent sur le respect, la confidentialité et l'autonomie, permettant aux personnes survivantes de prendre des décisions éclairées tout en reconnaissant leur besoin potentiel de soutien tout au long du processus de rétablissement.

Approche de dissuasion Approche de sécurité qui consiste à réduire ou à éliminer les menaces en opposant une contre-menace susceptible de dissuader ou d'influencer les agresseurs potentiels.

Approche de protection Approche de sécurité visant à réduire l'exposition du personnel à certaines menaces au moyen de mécanismes et de procédures de protection.

¹ Ce glossaire est adapté et aligné sur le glossaire du Global Interagency Security Forum (GISF) : <https://gisf.ngo/glossary-french/>

Approche de sécurité centrée sur la personne Approche de gestion des risques de sécurité qui place les individus au cœur des activités de gestion des risques de sécurité et tient compte de leur profil de risque personnel. Elle reconnaît les risques spécifiques auxquels les individus sont exposés en raison de leur identité intersectionnelle, de leur comportement, de leur rôle et de leur organisation, ainsi que du contexte dans lequel ils travaillent.

Approche par acceptation Approche de gestion des risques de sécurité qui vise à réduire ou à éliminer les menaces en établissant des relations avec les communautés locales et les parties prenantes concernées dans la zone d'opération et en obtenant leur bonne volonté et/ou leur consentement à la présence et au travail de l'organisation.

Appétence au risque Compréhension commune du niveau et du type de risque qu'une organisation est prête à accepter pour atteindre ses objectifs.

Arrestation L'arrestation et la détention d'une personne par une autorité officielle (police ou armée) en lien avec un crime, un délit ou une infraction.

Atténuation des risques Actions visant à réduire les risques en diminuant la probabilité et l'impact potentiel des dommages.

Audit de sécurité Examen interne ou externe fondé sur des preuves qui évalue l'efficacité de la gestion des risques de sécurité de l'organisation et qui détermine si celle-ci s'acquitte de son devoir de diligence envers son personnel.

Cadre de gestion du risque de sécurité Ensemble de politiques, protocoles, plans, mécanismes et responsabilités visant à réduire les risques de sécurité du personnel.

CBRN Menaces/armes chimiques, biologiques, radiologiques et nucléaires.

Chaîne de communication Système hiérarchique utilisé pour diffuser rapidement des informations à un grand groupe par téléphone, SMS, e-mail ou tout autre moyen.

Collaboration en matière de sécurité Organisations agissant ensemble pour répondre à des préoccupations communes en matière de sécurité et d'accès, partager des informations sur les incidents et les risques et renforcer leurs capacités collectives de gestion de risque.

Convoi Groupe de véhicules (ou de navires) voyageant ensemble de manière organisée afin d'apporter soutien et protection mutuels.

Coordination civilo-militaire Interaction entre les forces militaires et les organisations humanitaires/acteurs civils nécessaire pour promouvoir les principes humanitaires, garantir l'accès et protéger les travailleurs humanitaires et autres civils.

Crise Événement ou série d'événements qui perturbe considérablement le fonctionnement normal d'une organisation et a de graves conséquences pour le personnel ou l'organisation, nécessitant des mesures extraordinaires et une action immédiate de la part de l'encadrement supérieur.

Criticité des programmes Mesure de la dépendance des populations à l'égard de la poursuite de l'aide humanitaire pour leur survie ou pour éviter des souffrances extrêmes.

Culture de la sécurité Hypothèses, valeurs et croyances communes qui façonnent les comportements en matière de sécurité au sein des organisations. Elles peuvent être positives ou négatives.

Devoir de diligence Obligation (morale et juridique) d'une organisation d'assurer la sécurité, la sûreté et le bien-être des personnes qui effectuent son travail.

Discours de haine Contenu écrit ou oral qui cible un groupe ou un individu en fonction de ses caractéristiques intrinsèques, telles que l'ethnicité, la religion ou le genre.

Déconfliction Échange d'informations entre les acteurs humanitaires et les forces militaires afin de prévenir les attaques contre les installations, le personnel et les opérations, en informant les parties au conflit de l'emplacement et des déplacements du personnel et des activités humanitaires.

Détention Rétention d'une personne contre son gré par une personne ou un groupe, sans inculpation formelle, sans calendrier précis ni conditions de libération.

Enlèvement contre rançon Capture par la force d'une personne ou d'un groupe de personnes qui sont retenues contre leur gré dans un lieu inconnu jusqu'à ce que les demandes de rançon ou d'autres concessions soient satisfaites.

Enlèvement Toute capture illégale et forcée d'une personne ou d'un groupe.

Entreprise de sécurité privée/ETS Entité privée fournissant des services de sécurité rémunérés à des particuliers ou à des organisations.

Exigences minimales de sécurité Protocoles que l'organisation attend de tous ses employés qu'ils respectent afin d'assurer la sûreté et sécurité des biens, du personnel et des informations.

Extorsion Recours à la coercition, aux menaces ou à l'intimidation pour obtenir de l'argent, des biens ou des actions de la part de la cible.

Évacuation Retrait du personnel pour des raisons de sécurité vers un lieu de sûreté situé au-delà des frontières internationales d'un pays.

Évaluation de la menace Processus d'identification et d'analyse des sources potentielles de préjudice dans un environnement opérationnel.

Évaluation de la vulnérabilité Processus d'analyse du degré d'exposition du personnel, des biens et des actifs d'une organisation aux menaces.

Formation «Sensibilisation en milieu hostile» (HEAT) Formation en sécurité personnelle conçue pour le personnel travaillant dans des environnements à haut risque, impliquant généralement une formation basée sur des scénarios.

Gestion de l'information en cas d'incident de sécurité Processus de collecte et d'utilisation des informations relatives aux incidents de sûreté et sécurité afin de suivre les tendances et d'éclairer la prise de décision.

Gestion des risques de l'entreprise Processus organisationnel visant à identifier et à gérer tous les risques, y compris, mais sans s'y limiter, les risques de sécurité, qui pourraient avoir une incidence sur ses objectifs, ses activités et ses parties prenantes.

Gestion des risques de sécurité Système organisationnel permettant d'évaluer et d'atténuer les risques et de répondre aux incidents.

Harcèlement Comportement abusif ou indésirable répété à l'égard d'une personne, qui cause de la détresse ou de l'inconfort.

Hibernation Suspension temporaire des activités régulières du projet tout en maintenant le personnel au bureau, à domicile ou dans un autre lieu sûr afin d'éviter une menace émergente, ou jusqu'à ce que les conditions s'améliorent.

Identité intersectionnelle Les multiples facteurs identitaires interconnectés des individus qui façonnent leur profil de risque personnel.

Incident critique Événement ou série d'événements qui menacent gravement le bien-être du personnel, pouvant entraîner la mort, des blessures ou des maladies mettant la vie en danger. Un incident critique peut être trop grave pour être géré par les structures de gestion standard et nécessite un soutien et des capacités supplémentaires.

Incident Événement indésirable relatif à la sécurité qui entraîne ou pourrait entraîner un préjudice pour le personnel, une perturbation des programmes et des activités, ou une perte ou une atteinte aux biens ou à la réputation de l'organisation.

Informations erronées, désinformation et mauvaise information Les informations erronées désignent des informations inexacts ou fausses qui sont diffusées sans intention de tromper. La désinformation est une information délibérément fausse ou trompeuse. La mauvaise information est une information vraie qui est sortie de son contexte d'origine ou manipulée de manière à induire en erreur ou à causer un préjudice.

MEDEVAC Evacuation médicale. Le transport d'un patient par voie terrestre, maritime ou aérienne à bord d'un moyen de transport médical spécialisé, avec des soins prodigués pendant le trajet, dans le but de lui faire bénéficier d'un traitement médical dans un autre lieu.

Menace Tout événement, action ou entité susceptible de porter préjudice au personnel, aux programmes ou aux biens, ou d'entraver la réalisation des objectifs de l'aide.

Niveaux de sécurité Système utilisé pour classer et communiquer le niveau de risque au personnel dans un contexte ou un lieu spécifique, et pour orienter les décisions, les actions et les mesures de gestion des risques de sécurité en réponse à l'insécurité croissante (également appelé «phases de sécurité»).

Partage du risque Partage équitable des responsabilités entre les partenaires organisationnels des risques qui les concernent tous les deux.

Partenariat Toute relation de travail formalisée entre deux ou plusieurs organisations visant à atteindre des objectifs convenus, comme dans le cadre de la mise en œuvre d'un programme d'aide.

Personnel de sécurité/point focal Membre du personnel responsable de la sûreté et sécurité dans le cadre de ses fonctions.

Plan d'urgence Ensemble de procédures et de mesures préétablies, adaptées au contexte local, qui guident le personnel dans la coordination d'une réponse rapide et efficace à des incidents de sécurité ou à des perturbations spécifiques.

Plan de sécurité Document ou ensemble de documents spécifiques à un lieu, décrivant les mesures et les procédures en place pour gérer la sécurité, ainsi que les responsabilités et les ressources nécessaires à leur mise en œuvre.

Politique de sécurité Document de gouvernance qui énonce l'approche de l'organisation en matière de risques de sécurité et de sûreté, les principes clés qui sous-tendent cette approche, ainsi que les rôles et responsabilités de tous les membres du personnel dans la gestion des risques.

Premiers secours Fourniture d'une aide immédiate à une personne malade, blessée ou en détresse émotionnelle («premiers secours psychologiques») jusqu'à ce qu'une aide professionnelle soit obtenue.

Procédures opérationnelles standards (standard operating procedures, SOP) Ensemble d'instructions détaillées destinées à aider le personnel à effectuer les opérations courantes ou à répondre à des situations spécifiques de manière à optimiser la sûreté et sécurité.

Profil de risque personnel Ensemble unique de risques auxquels une personne est confrontée en raison de son identité intersectionnelle, qui est en partie façonnée par la manière dont ses caractéristiques personnelles sont perçues par les autres.

Rançon Argent, biens ou services exigés ou versés en échange de la libération en toute sécurité des personnes enlevées.

Relocalisation Retrait du personnel et des biens des zones dangereuses vers des zones plus sûres à l'intérieur du pays, jusqu'à ce que la situation se stabilise.

Risque La probabilité qu'un événement préjudiciable se produise et l'ampleur du préjudice s'il se produit.

Risque résiduel Le niveau de risque restant après la mise en œuvre de toutes les mesures d'atténuation des risques appropriées.

Risques liés à l'identité Risques encourus par le personnel en raison de ses caractéristiques personnelles et de la manière dont celles-ci sont perçues.

Sauver des vies ensemble (Saving Lives Together, SLT) Cadre de collaboration en matière de sécurité entre le système de gestion de la sécurité des Nations unies (UNSMS), les organisations non gouvernementales internationales et d'autres organisations internationales dans le monde entier, ainsi que dans les contextes de réponse humanitaire partagée.

Seuil de risque La limite du risque acceptable, au-delà de laquelle l'organisation ou un individu n'est pas disposé à aller.

Situation d'otages Le fait de retenir une personne ou un groupe par la force dans un lieu connu, comme dans une situation de siège, jusqu'à ce que des demandes spécifiques soient satisfaites.

Soutien psychosocial Approche qui intègre à la fois les aspects psychologiques et sociaux du bien-être, en tenant compte de l'impact des relations, de l'environnement et de la communauté sur la santé mentale.

Stratégie de sécurité Approche adoptée par une organisation pour gérer la sécurité en fonction de l'environnement opérationnel et des risques présents sur le site, influencée par les principes et les valeurs de l'organisation.

Stress Réaction émotionnelle, cognitive, physique ou comportementale face à des pressions et à des situations difficiles.

Surveillance hostile Observation attentive d'individus, d'actifs ou de biens dans une intention malveillante, telle que la planification d'une attaque.

Sécurité Absence de risque ou de préjudice résultant de la violence ou d'autres actes intentionnels.

Sécurité de l'information Pratique consistant à protéger les informations contre tout accès non autorisé, vol, révélation, perturbation, modification ou destruction.

Sécurité numérique Mesures, stratégies et processus visant à atténuer les risques liés à l'utilisation des technologies numériques et à la présence et aux comportements numériques d'un individu et/ou d'une organisation.

Sûreté Absence de risque ou de préjudice résultant d'actes involontaires (accidents, phénomènes naturels ou maladies).

Taux/niveaux de risque Risques évalués, classés selon leur degré de gravité en termes de probabilité et d'impact.

Transfert du risque La création, la transformation ou le transfert intentionnel ou non de risques d'un acteur à un autre.

Traumatisme Expérience pénible ou perturbante qui dépasse les capacités d'adaptation d'un individu et qui a des effets négatifs durables sur son fonctionnement et son bien-être.

Violence sexuelle Tout acte sexuel forcé, imposé ou sans consentement.

Avant-propos

La première édition de cette *Revue des bonnes pratiques* représentait les connaissances collectives du personnel humanitaire et des organisations non gouvernementales (ONG) qui s'étaient réunis en 1998, d'abord aux États-Unis d'Amérique (USA), puis au Royaume-Uni (RU), pour une formation à la sécurité d'une semaine. Elle reflétait la prise de conscience croissante que notre communauté devait collaborer si nous voulions améliorer notre approche de la gestion de la sécurité institutionnelle. Fruit d'un effort collectif, la préparation et l'élaboration de la «RBP8» ont mobilisé du personnel humanitaire et du développement, des artisans de la paix, des ingénieurs, des formateurs, des démineurs, des théoriciens et une poignée de professionnels de la gestion de la sécurité dans les ONG qui s'efforçaient de relever les défis actuels en matière de gestion de la sécurité. La RBP8 est devenue l'ouvrage de référence incontournable, proposant des modèles et des recommandations à toute une génération de responsables de la sécurité et de points focaux pour les questions de sécurité au sein des ONG et des organisations humanitaires.

L'édition révisée de la RBP8 en 2010 a reconnu la précieuse contribution d'une multitude de professionnels de la gestion de la sécurité dans le domaine humanitaire et les ONG, dont beaucoup n'occupaient pas encore ces fonctions lors de la publication de la première édition en 2000. Leur expérience de l'application des principes et des recommandations présentés dans le texte original a renforcé les bonnes pratiques et a permis d'améliorer les approches et de perfectionner les outils. Parmi les thèmes mis en avant figuraient l'amélioration des évaluations des risques, la mise en œuvre d'une approche par «acceptation active», l'exploration des dimensions de sécurité de la programmation de «gestion à distance», la promotion de la coordination interagences en matière de sécurité et la gestion des incidents critiques.

S'appuyant sur les éditions précédentes, cette troisième édition de la RBP8 tire parti des connaissances et de l'expérience acquises au cours des 15 dernières années, en intégrant les conclusions des recherches récentes sur les approches existantes et émergentes en matière de gestion des risques de sécurité. Elle reflète également les nombreux changements importants qui ont marqué le paysage humanitaire au sens large au cours de cette période. L'un des plus importants est la reconnaissance tardive du rôle essentiel des acteurs nationaux dans les écosystèmes de réponse humanitaire et de gestion des risques de sécurité humanitaires, ainsi que des défis spécifiques auxquels ils sont confrontés.

Cette version souligne clairement qu'une bonne gestion des risques de sécurité est nécessaire dans tous les contextes de réponse humanitaire – et pas seulement dans les environnements les plus violents – et encourage les lecteurs à réfléchir de manière critique à l'origine et à la nature des menaces et des risques, ainsi qu'aux personnes considérées comme menaçantes et aux raisons de cette perception. Pour cela, il est essentiel de reconnaître que les frontières entre les lieux de programmation et d'autres espaces supposés sûrs, tels que le domicile, le siège social, les succursales et les complexes, sont poreuses. Un nouvel élément important de cette édition concerne le concept et l'application d'une approche centrée sur la personne dans la gestion des risques de sécurité. Cette approche encourage les professionnels de la gestion des risques de sécurité à se concentrer autant sur «qui est en sécurité» que sur «où est-on en sécurité», ce qui permet de mieux comprendre l'importance des risques liés à l'identité.

La nouvelle édition aborde également les thèmes suivants : la gestion des risques de sécurité dans le cadre des partenariats de mise en œuvre et des opérations gérées à distance ; la pertinence des nouvelles technologies pour la gestion des risques de sécurité ; les besoins, les types et les sources de formation ; et la manière dont la gestion des risques de sécurité peut être influencée par le travail de plaidoyer externe et, à son tour, contribuer à celui-ci.

Nous espérons que cette version actualisée et enrichie de la RBP8 aidera les intervenants humanitaires à identifier et à gérer plus efficacement les risques de sécurité. La nature dynamique de l'environnement opérationnel, aggravée par des phénomènes mondiaux qui risquent de déplacer des millions de personnes dans les années à venir, nous oblige à réfléchir et à réévaluer en permanence les principes fondamentaux d'une gestion des risques de sécurité efficace et les moyens de les mettre en pratique.

Wendy Fenton

Ancienne coordinatrice du HPN

Michael O'Neill

International NGO Safety and Security Association (INSSA)

Introduction

Publiée en 2000, la *Revue des bonnes pratiques sur la Gestion opérationnelle de la sécurité dans des contextes violents*, ou « RBP8 », est rapidement devenu une référence dans le domaine naissant de la gestion des risques de sécurité des opérations humanitaires. À l'époque, très peu d'organisations disposaient d'un personnel dédié ou avaient mis en place des mécanismes de sécurité, et cette publication a servi à la fois de signal d'alarme sur la nécessité de mieux gérer les risques et de modèle pour les premiers efforts de nombreuses organisations.

Une édition révisée en 2010 a vu l'ajout d'exemples actualisés, reflétant les changements dans le secteur humanitaire et les menaces auxquelles les humanitaires étaient confrontés dans le contexte des conflits et des crises post-11 septembre.

Bien que les concepts et principes présentés dans ces deux premières éditions restent valables, quinze années supplémentaires se sont écoulées, les capacités humanitaires et les environnements de sécurité continuent d'évoluer, et les nouvelles réflexions en matière de gestion des risques de sécurité méritent une nouvelle révision. Même si elle n'est plus la seule ressource indispensable qu'elle était lors de sa première publication, la RBP8 peut servir de texte de référence et de recueil utile de principes et de pratiques pour les experts en gestion des risques de sécurité humanitaire comme pour les nouveaux venus dans le domaine.

Contexte de la nouvelle édition

Comme pour les deux éditions précédentes, cette version de la RBP8 est le fruit des efforts conjoints d'un grand nombre de praticiens-experts. Fruit d'une collaboration entre Humanitarian Outcomes, le Global Interagency Security Forum (GISF) et le Réseau des pratiques humanitaires (Humanitarian Practice Network - HPN), le projet de mise à jour de cet ouvrage a débuté en 2022, grâce au financement du Bureau de l'aide humanitaire de l'Agence des États-Unis pour le développement international (US Agency for International Development's Bureau for Humanitarian Assistance - USAID/BHA).

Dans un premier temps, l'équipe éditoriale a mené une enquête mondiale auprès de professionnels de la gestion des risques de sécurité humanitaire afin d'évaluer l'utilisation actuelle et la pertinence de la RBP8. L'enquête a révélé que la plupart du personnel de sécurité connaissaient bien cette publication, plus d'un quart d'entre eux continuant à l'inclure dans les documents d'information destinés au personnel. Il y a également eu un soutien en faveur d'une troisième édition. Cependant, l'enquête a confirmé qu'avec la prolifération des guides techniques et des documents pratiques

sur la gestion des risques de sécurité, la RBP8 est désormais davantage considérée comme une référence faisant autorité pour le personnel de sécurité et un manuel d'introduction aux concepts et principes clés pour les nouveaux venus dans le domaine, plutôt que comme un manuel pratique.

Dans cette optique, l'équipe s'est lancée dans une étude approfondie des pratiques actuelles et des nouvelles réflexions en matière de gestion des risques de sécurité en contextes humanitaires. La recherche s'est appuyée sur des études de cas dans cinq contextes humanitaires (République centrafricaine, Colombie, Éthiopie, Irak et Ukraine) et sur des consultations avec plus de 250 praticiens de l'humanitaire dans le monde entier. Les conclusions, publiées dans un rapport distinct par le GISF et Humanitarian Outcomes en 2024, ont largement inspiré le nouveau contenu de cet ouvrage, ainsi que les contributions distinctes et les analyses critiques fournies par les experts participants.¹ Dès le début, le projet a été guidé par un groupe consultatif composé des principales parties prenantes et des leaders d'opinion dans le domaine de la gestion des risques de sécurité. Chaque chapitre a été revu et corrigé par les rédacteurs, puis soumis à un groupe d'experts en la matière afin d'obtenir leur avis sur le fond. De plus, certains nouveaux chapitres ont été rédigés par des experts participants et ont fait l'objet du même processus de révision par les pairs. Après avoir intégré les commentaires, les versions révisées ont été examinées afin d'en vérifier le contenu général, la structure, l'exactitude technique et la sensibilité du langage et du ton.

Nouveautés

Outre un titre raccourci, qui couvre les aspects non opérationnels de la gestion des risques de sécurité et reflète la réalité selon laquelle les risques de sécurité peuvent exister dans toutes sortes d'environnements, cette édition actualise le contenu des versions précédentes et introduit de nouveaux thèmes, s'appuyant sur les dernières recherches et réflexions dans le secteur. Elle introduit et applique notamment le concept d'une « approche centrée sur la personne » à la gestion des risques de sécurité, qui place l'individu au centre de la gestion des risques de sécurité. La nouvelle édition met également l'accent sur le travail essentiel et la charge disproportionnée des risques assumés par les acteurs humanitaires nationaux et locaux, et examine le fonctionnement de la gestion des risques de sécurité dans le cadre des partenariats nationaux-internationaux.

Parmi les nouveaux thèmes abordés figurent les dimensions de sécurité des efforts d'accès et de déconfliction, ainsi que tous les nouveaux risques numériques auxquels sont confrontées les organisations humanitaires sous la forme d'informations erronées et de désinformation, de vol de données, de surveillance et de cybercrime.

1 GISF et Humanitarian Outcomes (2024) *State of practice: the evolution of security risk management in the humanitarian space* (en anglais, « État des lieux: l'évolution de la gestion des risques de sécurité dans le domaine humanitaire ») (https://humanitarianoutcomes.org/security_risk_mgmt_humanitarian_space_2024).

Il y a également un nouveau contenu relatif à la criminalité en général, ainsi que des contenus supplémentaires sur la formation, le financement, la conformité et le devoir de diligence. La structure révisée du volume reconnaît que la gestion des risques de sécurité s'inscrit dans différents écosystèmes – l'organisation, le système humanitaire, le domaine de l'aide humanitaire au sens large et la sphère politique –, chacun ayant ses propres considérations et défis.

Cette édition de la RBP8 met l'accent sur les bonnes pratiques et les principes directeurs plutôt que sur des instructions détaillées concernant les procédures techniques. L'abondance de nouvelles ressources, principalement en ligne, dans le domaine humanitaire, qui fournissent des recommandations détaillées, répond largement à ce besoin, et tenter de les reproduire rendrait cet ouvrage superflu et rapidement obsolète. Il se concentre plutôt sur la présentation d'idées et de concepts visant à encourager la réflexion et à éclairer les discussions politiques de haut niveau, ainsi que sur le partage des bonnes pratiques d'experts, tout en orientant le lecteur vers des ressources pertinentes pour des exemples concrets, des modèles et des recommandations pratiques.

Enfin, les éditeurs et les contributeurs à cette révision ont cherché à décentrer autant que possible l'organisation internationale occidentale en tant que perspective principale et public cible de ce document, afin de garantir que le langage et l'approche du contenu soient pertinents et inclusifs pour tous les prestataires d'aide humanitaire.

Public cible

La RBP8 originale était principalement destinée aux cadres supérieurs des organisations humanitaires supervisant des opérations dans des environnements hostiles. Cette édition cible un public un peu plus large. Tout d'abord, elle veille à inclure toutes les organisations humanitaires - locales, nationales et internationales, de la plus petite à la plus grande. Cependant, étant donné que les organisations de tailles et de budgets différents ont des besoins et des capacités différents, certaines des bonnes pratiques décrites pour les grandes organisations comportant plusieurs départements et bureaux peuvent être moins pertinentes ou moins faciles à mettre en œuvre pour les petites organisations. Dans la mesure du possible, cela est indiqué dans le texte, accompagné d'un rappel des principes fondamentaux qui sous-tendent ces pratiques, lesquels sont universellement applicables.

Outre le personnel humanitaire chargé de la sécurité (ci-après dénommé « personnel de sécurité »), la RBP peut également intéresser les hauts responsables et les conseils d'administration des organisations humanitaires, ainsi que les étudiants, les journalistes, les chercheurs et toute personne souhaitant en savoir plus sur la gestion des risques de sécurité dans le cadre des opérations humanitaires. D'autres organisations opérant dans des conditions à risque peuvent également la trouver utile.

Les bonnes pratiques décrites ici concernent la gestion des risques de sécurité au niveau organisationnel et sont destinées à être prises en considération par le personnel chargé d'améliorer la sécurité de tous les membres du personnel. La RBP n'est pas destinée aux membres du personnel à titre individuel en ce qui concerne leur sûreté personnelle ou les mesures à prendre en cas d'incident. Cela ne diminue en rien l'importance de l'action individuelle en matière de sécurité, mais reflète simplement la portée des recommandations.

Le terme « personnel » désigne toute personne travaillant pour le compte de l'organisation, y compris les bénévoles. Le terme générique « organisations » englobe toutes les organisations humanitaires, des agences des Nations Unies (ONU) et du Mouvement international de la Croix-Rouge et du Croissant-Rouge aux ONG et aux organisations communautaires. La diversité des acteurs humanitaires signifie que, parfois, certains contenus peuvent être plus ou moins pertinents pour un type d'organisation particulier. Une fois encore, en mettant l'accent sur les principes fondamentaux et la réflexion, nous espérons que ce guide pourra être utile à tous.

À retenir

Le thème central de cet ouvrage est la « sécurité », qui concerne les actes délibérés visant à causer un préjudice (tels que la violence et la criminalité), par opposition à la « sûreté », qui implique des accidents ou d'autres circonstances entraînant un préjudice involontaire (tels que les incendies et les dangers environnementaux). Bien que dans la pratique, ces deux notions se recoupent souvent, cet ouvrage n'aborde pas en profondeur les aspects liés à la sûreté dans le cadre de l'action humanitaire.

La RBP utilise délibérément un langage non normatif, proposant des bonnes pratiques à prendre en compte par le personnel chargé de la sécurité, plutôt que d'établir des normes ou des exigences. Toutes les pratiques décrites sont destinées à être adaptées aux besoins spécifiques et au contexte opérationnel de chaque organisation.

Dans les crises humanitaires, le grand public est souvent exposé à un risque de violence égal ou supérieur à celui du personnel humanitaire, et a besoin d'une aide et d'une protection importantes. Cependant, les stratégies utilisées pour protéger les personnes touchées sont souvent très différentes de celles utilisées pour protéger le personnel humanitaire, et relèvent également de la responsabilité de services distincts de ceux chargés de la gestion des risques de sécurité au sein de la plupart des organisations.

Enfin, il est important de reconnaître et de renforcer l'idée que la mise en place d'une gestion des risques de sécurité efficace n'est pas une fin en soi. Il s'agit plutôt d'un moyen d'atteindre l'objectif plus large qui consiste à répondre aux besoins humanitaires des personnes en situation de crise.

Structure de la revue

Nous commencerons par les grands principes fondamentaux de la gestion des risques de sécurité humanitaire, puis nous aborderons les domaines de pratique plus spécifiques. Les novices en gestion des risques de sécurité peuvent suivre l'ordre des chapitres pour obtenir une introduction complète au sujet, mais chaque section est autonome et peut être lue indépendamment.

La partie 1 explique des concepts clés tels que la menace, le risque, le devoir de diligence et la criticité des programmes, et présente les dernières réflexions sur l'approche de sécurité centrée sur la personne. **La partie 2** décrit les « écosystèmes » dans lesquels s'inscrit la gestion des risques de sécurité : le contexte opérationnel, la communauté interagences et les mécanismes conjoints, le cercle plus large des acteurs tels que les gouvernements et les forces armées, et l'interaction avec d'autres objectifs organisationnels tels que le plaidoyer. **Les parties 3 et 4** abordent ensuite les principaux éléments stratégiques, politiques et opérationnels liés à l'élaboration et à la mise en œuvre d'un système de gestion des risques de sécurité organisationnelle. **La partie 5** traite des questions liées aux ressources humaines, aux bonnes pratiques en matière de communication, à la formation et au bien-être du personnel. **La partie 6** est consacrée à la gestion des risques de sécurité dans le domaine des technologies de l'information et de la communication, y compris les informations préjudiciables. Enfin, la **partie 7** fournit des exemples d'atténuation des risques pour des situations et des types de menaces spécifiques. Celles-ci ont été révisées et mises à jour afin de refléter les tendances récentes en matière d'insécurité et les contextes opérationnels actuels.

1 Fondements de la gestion des risques de sécurité humanitaire

1.1 Concepts et principes clés

Ce chapitre présente les principes fondamentaux de la gestion des risques de sécurité dans le cadre de l'action humanitaire. Il aborde notamment les concepts de base que sont la menace et le risque, le devoir de diligence et les seuils de risque, ainsi que la manière dont ils correspondent à la criticité des programmes. Le chapitre décrit également les principes fondamentaux de l'action humanitaire et leur lien avec la sécurité, ainsi que les bonnes pratiques pour créer une culture de la sécurité organisationnelle.

1.1.1 Qu'entend-on par risques de sécurité et que signifie « gérer » ces risques ?

L'action humanitaire, qui se déroule souvent dans un contexte d'instabilité, de conflit et de crise, comporte inévitablement des risques de sécurité. Bien que ces risques ne puissent jamais être totalement éliminés, leur gestion efficace peut faire la différence entre le fait que les populations reçoivent ou non une aide vitale.

L'insécurité n'est qu'un type de risque parmi d'autres auxquels les personnes et les organisations peuvent être confrontées. Il en existe beaucoup d'autres, notamment les risques financiers, opérationnels, fiduciaires et réputationnels, qui peuvent tous être liés entre eux et au risque de sécurité. Selon la norme *ISO 31000*, la définition plus large du risque est « l'effet de l'incertitude sur les objectifs ». ² Cette définition implique deux distinctions importantes : un risque n'est pas la même chose qu'une menace et, bien que la gestion des risques soit liée aux objectifs, elle n'est pas synonyme de ceux-ci. En contexte humanitaire, la gestion des risques de sécurité est donc au service des objectifs humanitaires ; éviter les dommages et les pertes est un moyen, et non une fin en soi. Cela est important car, lorsque « assurer la sécurité des personnes » devient l'objectif primordial, l'aversion au risque est inévitable.

Les concepts clés à comprendre sont les suivants :

- Menace
- Vulnérabilité
- Risque
- Réduction/atténuation des risques.

2 Organisation internationale de normalisation (2018) *ISO 31000:2018: Risk management – Guidelines (en anglais, « Gestion de risque - Directives »)* (www.iso.org/standard/65694.html).

Dans un environnement opérationnel, une menace est tout ce qui peut causer un préjudice ou une perte, tandis que la vulnérabilité désigne la probabilité d'être confronté à une menace et l'impact qui en résulterait. La combinaison d'une menace pour la sécurité et de la vulnérabilité d'une personne à cette menace constitue un risque de sécurité. En d'autres termes, le risque de sécurité concerne le potentiel de préjudice : la probabilité qu'un événement préjudiciable se produise et l'ampleur de ce préjudice s'il se produit.

Une organisation peut choisir d'éviter complètement certains risques (par exemple, en décidant de ne pas travailler dans une zone donnée) ou de les transférer à quelqu'un d'autre, comme un sous-traitant ou un partenaire de mise en œuvre – nous y reviendrons plus tard. Mais lorsqu'elle met en œuvre une programmation directe et cherche à réduire et à atténuer les risques pour son personnel, une organisation peut prendre trois types de mesures principales, qui ne s'excluent pas mutuellement :

- Neutraliser la menace – réduire la menace elle-même (par exemple en négociant des accords d'accès sécurisé avec un groupe armé afin de réduire l'hostilité).
- Réduire la probabilité - réduire l'exposition à la menace.
- Réduire l'impact - prendre des mesures pour s'assurer que, face à la menace, l'impact sera limité.

Depuis l'an 2000, le secteur humanitaire a développé et rendu opérationnel un ensemble de connaissances, de politiques et de pratiques connues sous le nom de « gestion des risques de sécurité », qui fait l'objet du présent ouvrage. La gestion des risques de sécurité est un système organisationnel permettant d'identifier, d'évaluer et de se préparer aux risques afin de prévenir les incidents de sécurité et d'en minimiser l'impact lorsqu'ils se produisent, en y répondant efficacement. En prenant des mesures actives pour réduire les risques de sécurité, une organisation humanitaire maximise ses capacités à atteindre ses objectifs programmatiques tout en respectant son devoir de diligence envers les personnes qui fournissent l'aide.

Fondamentalement, la gestion des risques de sécurité dans l'espace humanitaire est un moyen d'assurer la sécurité de l'accès. Il ne peut y avoir d'accès sans un certain degré de protection pour les membres du personnel qui leur permette de travailler dans des seuils de risque raisonnables et convenus. Lorsque la gestion des risques de sécurité est efficace, elle garantit que le personnel aide les personnes dans le besoin et qu'il se sent en sécurité et en confiance dans l'exercice de ses fonctions. Cela peut, en retour, permettre à l'organisation de s'acquitter de ses responsabilités envers le personnel, de renforcer sa réputation de partenaire légitime auprès des donateurs, de limiter les pertes et d'élargir son champ d'action et son avantage concurrentiel. En d'autres termes, la gestion des risques de sécurité devient un puissant catalyseur des objectifs stratégiques et programmatiques globaux de l'organisation.

1.1.2 Devoir de diligence

Le devoir de diligence fait référence à l'obligation d'une organisation d'assurer la sûreté, la sécurité et le bien-être des personnes qui effectuent son travail. Ce concept a d'importantes implications juridiques et morales pour les organisations humanitaires. Au sens juridique strict, le devoir de diligence est l'obligation pour les organisations de prendre toutes les mesures raisonnables et appropriées pour renforcer la sûreté et sécurité de leur personnel. De nombreux pays ont intégré le devoir de diligence dans leur droit du travail et dans d'autres textes législatifs. Le fait de ne pas informer pleinement le personnel des risques et de ne pas prendre de mesures d'atténuation des risques raisonnables peut exposer une organisation à des poursuites pour négligence et à une responsabilité juridique. Plus important encore, le non-respect de cette obligation peut avoir des conséquences dévastatrices, voire fatales, pour les individus.

Bien qu'il n'existe pas d'ensemble unique et standard d'actions définissant une politique de devoir de diligence, il existe des éléments communs de bonne pratique :

- Évaluer les risques que présentent pour le personnel toute nouvelle condition, tout nouveau lieu ou toute nouvelle activité dans lesquels il sera amené à travailler.
- Informer le personnel des risques auxquels il peut être confronté, des mesures mises en place par l'organisation pour y faire face et des mesures que chaque individu est censé prendre (y compris les comportements attendus).
- Travailler à la prévention des incidents, par exemple en mettant en place des mesures d'atténuation des risques basées sur les risques évalués.
- Suivre la mise en œuvre et la pertinence des mesures de gestion des risques de sécurité.
- Intervenir en cas d'incident afin d'en réduire les conséquences négatives, par exemple en mettant en place des équipes de gestion de crise et en proposant une prise en charge post-incident au personnel touché.

Comme nous le verrons en détail dans les chapitres suivants, les éléments ci-dessus sont étroitement liés aux activités indispensables à une bonne gestion des risques de sécurité. Il est important de noter que le devoir de diligence peut également s'étendre au-delà de la relation employeur-employé officiellement établie. Les organisations font appel à des consultants, à des bénévoles et divers prestataires de services qui ne sont pas automatiquement soumis au devoir de diligence, mais à l'égard desquels elles peuvent néanmoins avoir une certaine responsabilité. La responsabilité juridique d'une organisation peut être comprise, selon la juridiction, comme étant relative au degré de maîtrise du risque qu'elle exerce sur une personne dans un environnement donné, tel que son logement, son emplacement et le choix de son moyen de transport.³

3 Kemp, E. et Merkelbach, M. (2011) *Can you get sued? Legal liability of international humanitarian aid agencies toward their staff*. Initiative de gestion de la sécurité (en anglais, « Pouvez-vous être poursuivi en justice ? Responsabilité juridique des agences d'aide humanitaire internationale envers leur personnel. ») (www.gisf.ngo/resource/can-you-get-sued-legal-liability-of-international-humanitarian-aid-organisations-towards-their-staff/).

De plus en plus, les organisations élaborent des politiques et des cadres relatifs au devoir de diligence afin d'orienter stratégiquement ces différents aspects du bien-être du personnel et de communiquer à celui-ci l'engagement de l'organisation en faveur de son bien-être général. Cela implique notamment d'adapter les politiques en matière de devoir de diligence afin de répondre aux besoins d'une main-d'œuvre diversifiée, en tenant compte des différents contextes personnels et culturels qui peuvent avoir une incidence sur les risques de sécurité. Ces politiques peuvent être régulièrement révisées afin de tenir compte des nouveaux défis et des nouvelles circonstances.

Exemple de cadre de devoir de diligence

Plusieurs processus soutiennent le devoir de diligence, et un cadre peut aider à communiquer visuellement ce que sont ces processus. Une organisation a structuré son cadre de devoir de diligence en plaçant la « culture » (valeurs communes et objectifs de bien-être) au centre, et la sécurité opérationnelle comme l'un des nombreux éléments de soutien, parmi lesquels la gouvernance, la formation, la communication et la gestion de crise.

La figure 1 est un exemple de cadre de devoir de diligence élaboré pour aider à définir et à transmettre l'intention du devoir de diligence, avec la sûreté et sécurité comme éléments distincts.

Figure 1 Visualisation du cadre de devoir de diligence



Culture - valeurs, méthodes de travail, engagement et inclusion, bien-être.

Gouvernance, leadership et redevabilité - définir une politique, préciser l'appétence au risque et le seuil de risque, et mettre en place des structures de contrôle, de redevabilité, de transparence et d'apprentissage.

Sûreté et sécurité opérationnelles - évaluations des risques et plans de sécurité spécifiques aux lieux et aux activités, gestion de risque liée aux déplacements, y compris les risques liés à l'identité personnelle et les engagements envers les sources, les partenaires et les interlocuteurs.

Gestion de crise - personnel, plans, assurances et consultants, formation, communication, soutien avant et après l'incident, et examens a posteriori.

Ressources - financement, dotation en personnel et soutien en matière de conseil.

Communication - méthodes, protocoles, sécurité de l'information, appareils, licences, formation et exercices.

Formation - intégration, sûreté et sécurité des personnes et des équipes, et gestion des risques de sécurité.

Au cœur du devoir de diligence se trouvent une bonne communication et l'information du personnel sur les risques. Les organisations ont la responsabilité d'informer le personnel et le personnel potentiel (y compris les bénévoles et les consultants) des risques de sécurité auxquels ils peuvent être confrontés et des mesures d'atténuation qui seront utilisées. Un engagement total sur ces questions permet à chacun de prendre une décision explicite, réfléchie et éclairée quant à l'acceptation ou non des risques identifiés.

Pour garantir la communication et l'engagement du personnel, les mesures suivantes peuvent être prises:

- **Révélation complète des informations.** Cela comprend des détails sur la nature spécifique des risques, les mesures de sécurité mises en place, les rôles et responsabilités de chacun, ainsi que toute implication potentielle en matière de santé et de sûreté. Il peut également être utile d'indiquer les informations manquantes ou insuffisantes.

- **Discussion explicite et acceptation du risque.** Une décision libre et pleinement éclairée du personnel d'accepter les risques liés au travail découle d'une compréhension claire des risques et des mesures d'atténuation, sans aucune pression ni crainte de conséquences négatives en cas de refus. Le fait de rendre cette décision explicite permet de garantir que l'organisation et le personnel sont engagés et conscients de la gravité de la situation.
- **Documentation.** Il peut être judicieux que la compréhension et l'acceptation du risque par les membres du personnel soient explicites et documentées, en particulier lorsque les conditions de sécurité changent ou lorsque le personnel commence à travailler dans de nouveaux lieux. Il est important de comprendre que ce processus vise à garantir que la discussion ait lieu et que le personnel soit pleinement informé et engagé. Il ne s'agit pas d'une protection contre une éventuelle responsabilité juridique. Certaines organisations demandent à leur personnel de signer des documents de « consentement éclairé » ou autres décharges de responsabilité, mais ceux-ci ne sont pas reconnus de la même manière dans toutes les juridictions et n'empêchent pas nécessairement les personnes qui les ont signés d'intenter des poursuites pour négligence.
- **Communication continue.** Les organisations doivent s'efforcer de fournir des mises à jour sur tout changement dans l'évaluation des risques, en informant le personnel des nouveaux risques dès qu'ils apparaissent.
- **Droit de rétractation.** Il convient de rappeler régulièrement au personnel qu'il a le droit de changer d'avis et de mettre fin à sa participation à tout moment s'il se sent en danger ou si les conditions changent de manière significative.

La gestion des risques de sécurité consiste souvent à trouver un équilibre entre les objectifs humanitaires de l'organisation et son devoir de diligence. Dans le même temps, une bonne gestion des risques de sécurité est essentielle pour remplir le devoir de diligence, et un bon devoir de diligence peut également renforcer la gestion des risques de sécurité en créant des conditions dans lesquelles le personnel est bien informé des risques et se sent valorisé et soutenu. Pour cela, l'organisation doit considérer et communiquer son devoir de diligence comme une valeur fondamentale, et non comme un moyen d'éviter les poursuites judiciaires et les atteintes à sa réputation. Les poursuites judiciaires sont néanmoins une réalité. L'affaire historique Dennis contre Le Norwegian Refugee Council (NRC) a confirmé la responsabilité juridique des organisations humanitaires envers leur personnel en matière de sécurité (voir exemple ci-dessous).

Exemple de cas : Devoir de diligence légal – enseignements tirés de l'arrêt Dennis contre le NRC

En 2012, plusieurs travailleurs humanitaires ont été attaqués lors d'une visite dans un camp de réfugiés à Dadaab, au Kenya, alors qu'ils travaillaient pour le NRC. Un membre du personnel est décédé et quatre autres ont été enlevés. Les personnes enlevées ont été secourues quatre jours plus tard. En 2015, Steve Dennis, qui faisait partie des personnes enlevées et blessées lors de l'attaque, a poursuivi le NRC en justice pour obtenir une indemnisation. Le tribunal de district d'Oslo a jugé que le NRC avait fait preuve de négligence grave et a accordé des dommages-intérêts à M. Dennis.

Cette affaire a été qualifiée de décision historique et beaucoup l'ont considérée comme un tournant décisif, qui a conduit de nombreuses organisations humanitaires à renforcer leurs systèmes de gestion des risques de sécurité. Bien que le devoir de diligence puisse varier d'une juridiction à l'autre, les enseignements tirés de cette affaire peuvent néanmoins guider les organisations qui cherchent à améliorer leurs processus de gestion des risques de sécurité et de devoir de diligence.

Voici quelques-uns des principaux enseignements tirés de la décision du tribunal d'Oslo.

- **Étendue du devoir de diligence :** Le devoir de diligence est une obligation légale qui s'applique autant aux organisations humanitaires qu'à tout autre employeur, et qui exige que les mesures d'atténuation soient proportionnées au risque.
- **Prévisibilité du risque et mesures d'atténuation raisonnables :** Le NRC n'a pas correctement évalué les risques prévisibles d'enlèvement, n'a pas atténué les risques identifiés, n'a pas suivi les recommandations de sécurité (internes et externes) et n'a pas consulté de spécialistes de la sécurité pour éclairer les décisions clés.
- **Consentement éclairé :** Le personnel n'a pas été informé des risques, n'a pas été invité à donner son consentement et n'a pas pu se rétracter lorsque les plans de sécurité ont été modifiés.
- **Pratique communautaire :** En l'absence de normes de sécurité concrètes et universellement applicables dans le secteur humanitaire, le tribunal s'est penché sur les pratiques communautaires à Dadaab afin de déterminer si et en quoi les décisions et les pratiques du NRC différaient de celles de ses pairs. Si le fait de s'écarter des pratiques communément acceptées n'est pas en soi un échec, tout écart de ce type doit être justifié par une décision mûrement réfléchie, fondée sur un raisonnement solide et des informations factuelles.

En résumé, la décision du tribunal de district d'Oslo a souligné la nécessité pour les organisations humanitaires de procéder à des évaluations des risques rigoureuses et de prendre des mesures de sécurité raisonnables dans le cadre de leur devoir de diligence légal.

Sources : Hoppe, K. et Williamson, C. (2016) 'Dennis vs Norwegian Refugee Council: implications for duty of care' (en anglais, « Dennis contre le Norwegian Refugee Council : implications pour le devoir de diligence »). Humanitarian Practice Network (<https://odihpn.org/publication/dennis-vs-norwegian-refugee-council-implications-for-duty-of-care/>) ; et Merkelbach, M. et Kemp, E. (2016) *Duty of care : a review of the Dennis v Norwegian Refugee Council ruling and its implications* (en anglais, « Devoir de diligence : examen de l'arrêt Dennis contre Norwegian Refugee Council et de ses implications »). European Interagency Security Forum (EISF) (www.gisf.ngo/resource/review-of-the-dennis-v-norwegian-refugee-council-ruling/).

Le respect rigoureux du devoir de diligence est lié à la réussite globale de l'organisation. Plus généralement, le devoir de diligence peut contribuer à la satisfaction et à la fidélisation des employés ainsi qu'à la réputation de l'organisation, ce qui peut à son tour soutenir les objectifs plus larges de l'organisation. Il est important de souligner que la plupart des incidents graves dans le secteur humanitaire ne donnent pas lieu à des poursuites judiciaires ; l'affaire Dennis contre le NRC est bien connue parce qu'elle est exceptionnelle. Il est prouvé que l'une des principales raisons qui ont motivé la demande de réparation judiciaire dans l'affaire Dennis contre le NRC était le manque d'attention accordée au personnel après l'incident, notamment le manque d'informations et de transparence sur ce qui s'était passé et sur les mesures de suivi. Bien qu'il soit impossible d'éliminer tous les risques, les organisations ont la maîtrise du risque sur la manière dont le personnel est pris en charge après un incident, et ce soutien post-incident est un aspect important du devoir de diligence.

► Pour plus d'informations sur la prise en charge post-incident, voir le chapitre 5.4 – Bien-être du personnel.

Ces dernières années, le terme « devoir de diligence » a été appliqué aux obligations éthiques que les organisations internationales ont envers leurs partenaires locaux et leurs sous-bénéficiaires. Même si une organisation ne peut être tenue légalement responsable des personnes employées par d'autres entités, il est clair que ces partenariats impliquent souvent un transfert de risque important, ce qui oblige les organisations à fournir tout le soutien approprié possible à leurs partenaires pour la prise en charge de leur personnel.

► Pour en savoir plus sur le transfert du risque et les partenariats, voir le chapitre 3.5.

1.1.3 Risque résiduel, seuils de risque et criticité des programmes

Participer aux efforts de réponse humanitaire implique d'être prêt à prendre certains risques. L'appétence au risque d'une organisation dépendra de ses objectifs stratégiques, de sa mission et de sa culture, et se traduira par une compréhension commune du niveau de risque approprié pour atteindre les objectifs de l'organisation. Le seuil de risque est une compréhension commune de la limite au-delà de laquelle l'organisation n'est pas disposée à aller. Pour déterminer ce seuil, il est nécessaire de comprendre le risque résiduel. Il s'agit du niveau de risque qui subsiste après la mise en œuvre de toutes les mesures d'atténuation des risques appropriées – un concept qui implique de reconnaître qu'il restera toujours un certain niveau de risque. Fixer le seuil de risque acceptable de manière explicite et transparente peut aider à orienter toutes les autres décisions de gestion concernant la conduite à tenir face au risque. Il existe trois moments importants où il convient de discuter du seuil de risque acceptable :

- Lorsqu'il s'agit de décider d'entrer ou de se développer dans un environnement à risque.
- Pour déterminer les seuils de risque acceptable individuels.
- Pour tracer des lignes rouges (limites ou seuils clairs) lorsque la situation se détériore.

Dans le premier cas, déterminer ce qui constitue un risque acceptable pour une organisation nécessite des critères et des conditions explicites afin de garantir un processus décisionnel rigoureux et transparent.

Dans le second cas, lorsqu'il s'agit de déterminer les seuils de risque individuels, il est important de ne pas supposer que tous les employés actuels et potentiels ont le même seuil de ce qu'ils considèrent comme un risque acceptable. Un climat de confiance au sein de l'organisation peut aider les personnes à se sentir capables d'exprimer leur malaise si une situation dépasse leur tolérance du risque, et les personnes qui entrent dans un environnement à haut risque doivent le faire en étant informées des risques qui y existent. Il est également important d'être conscient des incitations économiques ou de la pression des pairs qui peuvent conduire les personnes à prendre des risques au-delà de leur niveau de confort. Les seuils de risque acceptable individuels seront inévitablement influencés par les profils de risque personnel.

► *Les profils de risque personnel sont abordés plus en détail au chapitre 1.2 – Approche de sécurité centrée sur la personne.*

Le but des lignes rouges est d'éviter le syndrome de la « grenouille dans la marmite ». Lorsque le risque augmente progressivement, il n'est pas rare que les travailleurs humanitaires développent une sorte d'« accoutumance au danger ». Même s'ils sont

conscients que la situation se détériore, les membres du personnel peuvent ne pas se retirer ou renforcer leurs mesures de sécurité avant qu'un incident ne se produise. Définir clairement les événements déclencheurs ou les « lignes rouges » peut aider à déterminer quand la sécurité s'est détériorée de manière significative et si les activités du programme justifient clairement un risque plus élevé. Cela introduit un autre concept clé dans la gestion des risques de sécurité : la criticité des programmes. La criticité des programmes est une mesure de la dépendance des populations à l'égard de la poursuite de l'aide humanitaire pour leur survie ou pour éviter des souffrances extrêmes. Plus le programme est essentiel ou vital, plus une organisation peut être prête à accepter des risques pour le maintenir.

1.1.4 Principes fondamentaux de l'action humanitaire

Il devrait désormais être clair que la gestion des risques de sécurité n'est pas une formulation statique ou un ensemble de règles à suivre, mais plutôt un processus souple dans lequel les décisions impliquent de mettre en balance différents enjeux dont l'importance relative évolue. La gestion des risques de sécurité dans le cadre des opérations humanitaires diffère également d'autres secteurs à d'autres égards importants, liés aux principes humanitaires fondamentaux et au statut des travailleurs humanitaires en vertu du droit international humanitaire. Dans les conflits armés, par exemple, en vertu des Conventions de Genève et des Protocoles additionnels, les organisations humanitaires ont le droit de fournir une aide, et les parties belligérantes sont tenues de faciliter leurs opérations, de protéger leur personnel et de leur permettre de se déplacer sans entrave.⁴ La condition corollaire est que les organisations humanitaires opèrent en tant qu'entités neutres et fournissent une aide impartiale, indépendamment de tout agenda politique ou autre, et uniquement en fonction des besoins.

Les principes humanitaires de neutralité, d'impartialité et d'indépendance ont un lien direct avec la sécurité, car ils influencent la manière dont les communautés locales et les parties belligérantes perçoivent les organisations humanitaires et leur personnel. Ces perceptions peuvent déterminer l'acceptation ou le rejet d'une organisation (mesurée par sa notoriété dans une zone donnée et par l'appréciation ou, à tout le moins, la tolérance dont bénéficie son travail). Cela peut à son tour avoir une incidence sur son niveau d'accès aux lieux où son aide est nécessaire. C'est principalement en établissant son acceptation qu'une organisation humanitaire peut obtenir et maintenir un accès sûr pour travailler dans des zones à haut risque.

Le principe « Ne pas nuire »⁵ souligne que les organisations humanitaires doivent veiller à ne pas exacerber les conflits existants ni créer de nouvelles formes de préjudice. Cela signifie qu'elles doivent agir de manière à minimiser les conséquences

4 Pour plus de détails, voir : www.icrc.org/en/document/geneva-conventions-1949-additional-protocols.

5 Anderson, M.B. (1999) *Do no harm: How aid can support peace – or war* (en anglais, « Ne pas nuire : comment l'aide peut soutenir la paix – ou la guerre »). Lynne Rienner Publishers.

négligentes involontaires sur les communautés servies et s'assurer que leur programmation – et, par extension, les mesures de sécurité mises en place – ne contribue pas à créer des tensions, de la violence ou de l'inégalité.

Les concepts et principes directeurs susmentionnés sont spécifiques à la gestion des risques de sécurité humanitaire et ne sont généralement pas appliqués par les acteurs du secteur privé, de l'armée et de la diplomatie qui peuvent partager les mêmes espaces. Ces principes fondamentaux doivent souvent être expliqués et répétés, tant au personnel qu'aux interlocuteurs extérieurs.

► *Pour en savoir plus sur l'approche par acceptation, voir le chapitre 4.2.*

1.1.5 Développer une culture de la sécurité positive

Fondamentalement, la gestion des risques de sécurité consiste pour le personnel à prendre des décisions éclairées qui protègent leur bien-être et celui des autres. Cela peut être facilité par des systèmes et des outils appropriés, mais repose avant tout sur des valeurs, des convictions et des comportements communs en matière de sécurité. Une organisation dont le personnel est très conscient des risques de sécurité et convaincu que la sécurité est essentielle à la réalisation de ses objectifs humanitaires peut être considérée comme dotée d'une « culture de la sécurité » forte ou positive. Bien que la culture ne puisse être conçue ou imposée, elle peut être nourrie et façonnée de manière significative par le leadership et l'exemple. Une organisation peut mettre en place toutes sortes de politiques et de procédures, mais la majeure partie de la gestion des risques de sécurité consiste à faire en sorte que le personnel les comprenne et les accepte.

Pour instaurer une culture de la sécurité positive, il faut commencer par s'assurer que tous les membres du personnel connaissent l'organisation et sa mission. Idéalement, toute personne travaillant pour l'organisation devrait être en mesure de répondre à des questions sur l'objectif et les activités de l'organisation, sur ses sources de financement et sur son indépendance vis-à-vis de tout intérêt politique.

Les organisations doivent considérer la sécurité comme une priorité pour l'ensemble du personnel, et non comme une question sensible réservée à quelques membres du personnel qui en discutent à huis clos. Les cadres supérieurs doivent faire comprendre l'importance qu'ils accordent à la gestion des risques de sécurité s'ils veulent que les autres suivent leur exemple. Plus précisément, les organisations peuvent:

- Mettre l'accent sur l'information et la communication, en faisant de la sécurité un point permanent de l'ordre du jour de chaque réunion de la direction et du personnel, et veiller à ce que la sécurité soit un élément clé dans toute planification de programme.

Partie 1 Fondements de la gestion des risques de sécurité humanitaire

- Souligner l'importance du signalement et du suivi de tous les incidents, car cela est essentiel à la sensibilisation, et non pas un moyen de blâmer ou de prendre des mesures disciplinaires.
 - S'assurer que tous les membres du personnel connaissent clairement leurs responsabilités individuelles en matière de gestion des risques de sécurité et que celles-ci sont incluses dans les descriptions de poste et les évaluations de performance.
 - Reconnaître et renforcer les bonnes pratiques, en mettant en avant les exemples de sensibilisation et de comportements exemplaires en matière de sécurité, ainsi que les cas où des stratégies efficaces de gestion des risques de sécurité ont contribué à la réussite des opérations.
- Voir le chapitre 5.1 pour des recommandations plus détaillées sur les compétences en communication permettant d'améliorer la collaboration entre les services.
- Voir le chapitre 5.3 - Communication sur la sécurité au sein de l'organisation.

Intégrer une culture de la sécurité positive, tant au niveau des membres du personnel qu'au niveau de l'organisation, signifie prendre en compte les implications en matière de sécurité de toutes les actions (ou inactions) de l'organisation, qu'il s'agisse de discussions sur la conception des programmes, de messages publics, de décisions de financement ou du recrutement de prestataires de services externes. Une culture de la sécurité positive signifie que les personnes prennent en compte les risques de sécurité et les implications en matière de sécurité dans tous les aspects de leur travail, car elles en comprennent l'importance et sont respectées pour cela.

Informations complémentaires

Généralités

Anderson, M.B. (1999) *Do no harm: How aid can support peace – or war (en anglais, «Ne pas nuire: comment l'aide peut soutenir la paix – ou la guerre»)*. Lynne Rienner Publishers.

Bickley, S. (2017) *Gestion du risque sécurité: manuel de référence à l'attention des petites ONG*. European Interagency Security Forum (EISF). (<https://gisf.ngo/resource/security-risk-management-a-basic-guide-for-smaller-ngos/>).

Comité international de la Croix-Rouge (CICR) (n.d.) *Les conventions de Genève de 1949 et leurs Protocoles additionnels* (www.icrc.org/en/document/geneva-conventions-1949-additional-protocols).

Organisation internationale de normalisation (2018) *ISO 31000:2018: Risk management – Guidelines (en anglais, «Gestion de risque - Directives»)* (www.iso.org/standard/65694.html).

Devoir de diligence

CHS Alliance (2019) *Introduction to duty of care* (en anglais, « Introduction au devoir de diligence ») (www.chsalliance.org/get-support/article/introduction-duty-care/).

Duty of Care International (n.d.) *Why duty of care?* (en anglais, « Pourquoi le devoir de diligence? ») (<https://dutyofcareinternational.co.uk/why-duty-of-care/>).

GISF (n.d.) *What is humanitarian security risk management?* (en anglais, « Qu'est-ce que la gestion des risques de sécurité humanitaire? ») (www.gisf.ngo/about/what-is-humanitarian-security-risk-management/).

Hoppe, K. et Williamson, C. (2016) 'Dennis vs Norwegian Refugee Council: implications for duty of care' (en anglais, « Dennis contre le Norwegian Refugee Council: implications pour le devoir de diligence »). Humanitarian Practice Network (<https://odihpn.org/publication/dennis-vs-norwegian-refugee-council-implications-for-duty-of-care/>).

Kemp, E. et Merkelbach, M. (2011) *Can you get sued? Legal liability of international humanitarian aid agencies toward their staff*. Initiative de gestion de la sécurité (en anglais, « Pouvez-vous être poursuivi en justice? Responsabilité juridique des agences d'aide humanitaire internationale envers leur personnel. ») (www.gisf.ngo/resource/can-you-get-sued-legal-liability-of-international-humanitarian-aid-organisations-towards-their-staff/).

Le Centre suisse de compétences pour la coopération internationale (n.d.) *Duty of care under Swiss law*. cinfo (en anglais, « Le devoir de diligence en droit suisse ») (www.cinfo.ch/en/publications/duty-of-care-under-swiss-law).

Merkelbach, M. et Kemp, E. (2016) *Duty of Care: A review of the Dennis v Norwegian Refugee Council ruling and its implications* (en anglais, « Devoir de diligence: examen de l'arrêt Dennis contre Norwegian Refugee Council et de ses implications »). European Interagency Security Forum (EISF) (www.gisf.ngo/resource/review-of-the-dennis-v-norwegian-refugee-council-ruling/).

1.2 Approche de sécurité centrée sur la personne

Une approche de sécurité centrée sur la personne reconnaît que la prise en compte des caractéristiques d'identité intersectionnelle est essentielle pour gérer efficacement les risques de sécurité. Plutôt que de traiter les travailleurs humanitaires comme un groupe homogène, également vulnérable aux mêmes menaces, cette approche encourage l'inclusion, la réflexion et la prise en compte de la manière dont les défis et les besoins en sécurité des individus sont influencés par leur profil personnel. Ce chapitre traite des risques liés à l'identité et des raisons justifiant l'adoption d'une approche centrée sur la personne. Tout au long de cette RBP, vous trouverez des rappels et des exemples illustrant comment adopter une approche de sécurité centrée sur la personne. Ce chapitre doit être considéré comme une introduction à ce concept.

1.2.1 Risques liés à l'identité

Les organisations humanitaires tirent un grand bénéfice de la diversité de leur personnel, qui leur donne les capacités de mieux comprendre les différentes communautés cibles et de mieux interagir avec elles, garantissant ainsi que leurs interventions tiennent compte des spécificités culturelles et sont bien accueillies. En apportant des points de vue, des expériences et des compétences variées, des équipes diversifiées peuvent également contribuer à une analyse plus complète et à une résolution innovante des problèmes, permettant ainsi aux organisations d'être mieux armées pour gérer les crises et s'adapter au changement. Les organisations qui accordent la priorité à la diversité peuvent également constater des niveaux plus élevés d'engagement et de fidélisation du personnel. Il est donc impératif de veiller à ce que les organisations disposent d'une diversité et d'une inclusion adéquates, ce qui implique notamment de garantir la sécurité de cette main-d'œuvre diversifiée. Pour ce faire, il est essentiel de comprendre comment l'identité peut influencer le risque.

Il est important de souligner que chaque individu a à la fois des vulnérabilités et des points forts. Une approche inclusive de la gestion des risques de sécurité implique de remettre en question les stéréotypes qui suggèrent que certains profils sont intrinsèquement plus vulnérables. Ces hypothèses ne sont pas toujours exactes et négligent les contributions précieuses qu'une plus grande diversité de profils et d'horizons professionnels peut apporter à la gestion des risques de sécurité et au travail humanitaire dans son ensemble. En se concentrant à la fois sur les vulnérabilités et les points forts, les organisations peuvent adopter une approche plus équilibrée et plus efficace.

Risques liés à l'identité

Les risques de sécurité auxquels le personnel est confronté dépendent de son identité, qui n'est jamais univoque, et, plus important encore, de la manière dont la combinaison de ses caractéristiques personnelles – son « identité intersectionnelle » – est perçue par les autres.

L'intersectionnalité décrit comment divers facteurs sociaux (genre, ethnicité, orientation sexuelle, statut socio-économique, handicap) interagissent et se recoupent pour créer des expériences uniques de discrimination et de privilège. Ici, nous faisons référence à l'« identité intersectionnelle », qui reconnaît que les personnes ont plusieurs identités interconnectées qui ne peuvent être comprises isolément. Les aspects intersectionnels de l'identité d'un individu créent un profil de risque unique qui nécessite une approche de sécurité nuancée et globale.

Bien qu'il ne soit pas possible de couvrir tous les profils de risque personnel, les exemples suivants illustrent certaines considérations liées à l'identité.

- **Race, ethnicité et nationalité.**⁶ Les perceptions relatives à la race, à l'ethnicité et à la nationalité peuvent influencer la manière dont le personnel est traité au sein et à l'extérieur d'une organisation. Les perceptions et les préjugés peuvent entraîner un risque accru de violence ciblée, de discrimination, d'exclusion, de profilage et d'autres expressions du racisme et de la xénophobie, selon le contexte et sa dynamique sociale.⁷
- **Handicap et accessibilité.** Les membres du personnel en situation de handicap peuvent être confrontés à des difficultés supplémentaires, telles qu'une mobilité réduite ou un accès limité aux prestations et services médicaux, en particulier dans les situations d'urgence. Ils peuvent également être plus vulnérables à la violence et à l'exploitation, ainsi qu'à l'isolement social.
- **Facteurs culturels et religieux.** La langue, la culture et la religion peuvent avoir un impact sur la communication, l'intégration et la sécurité. Le personnel peut être confronté à des risques spécifiques liés à ses croyances religieuses ou à ses différences culturelles dans les régions où les tensions religieuses ou autres sont vives.
- **Genre, sexualité et identité.** Les risques liés au genre et à la sexualité concernent tous les individus, mais peuvent être plus prononcés pour les membres du personnel dont l'orientation sexuelle, l'identité et l'expression du genre sont stigmatisées, restreintes, marginalisées, sous-représentées ou criminalisées dans le lieu concerné. Le genre peut influencer la nature et la gravité des menaces auxquelles le personnel est confronté, y compris dans les relations interpersonnelles, au-delà de simples risques différents pour les hommes et les femmes.
- **Autres considérations.** Le statut socio-économique, les fonctions exercées, l'âge et l'expérience professionnelle antérieure sont autant d'éléments qui peuvent influencer la manière dont le personnel est perçu et traité et, par conséquent, sur les risques

6 Nous reconnaissons que les facteurs d'identité tels que le genre, la nationalité, l'ethnicité et la race sont des concepts socialement construits. Tout en reconnaissant leur caractère artificiel, nous les mentionnons ici pour souligner que la perception de ces facteurs d'identité peut avoir des conséquences réelles et parfois graves sur la sécurité des personnes.

7 Pour une analyse plus détaillée, voir Arthur, T. et Moutard, L. (2022) *Toward inclusive security: The impact of 'race', ethnicity, and nationality on aid workers' security* (en anglais, « Vers une sécurité inclusive: l'impact de la « race », de l'ethnicité et de la nationalité sur la sécurité des travailleurs humanitaires »). GISF (www.gisf.ngo/resource/toward-inclusive-security-the-impact-of-race-ethnicity-and-nationality-on-aid-workers-security/).

auxquels il peut être exposé. La perception de la hiérarchie peut également jouer un rôle (au sein de la société comme au sein d'une organisation), les employés moins bien rémunérés ou occupant des postes plus vulnérables (tels que les chauffeurs, les agents d'entretien ou les stagiaires) étant potentiellement plus exposés au danger, mais disposant souvent de moins de ressources et d'une protection moindre. En raison des perceptions et des préjugés, les personnes issues de groupes sous-représentés et marginalisés peuvent également ne pas bénéficier d'une attention suffisante au sein de leur organisation, ce qui peut se traduire par un soutien insuffisant en matière de sécurité pour ces employés.

Exemple de cas : Échecs dans la gestion des risques liés à l'identité

Dans un contexte où la population est majoritairement blanche, une employée internationale au teint plus foncé a été victime de harcèlement de rue à un niveau plus élevé que certaines de ses collègues féminines au sein de l'organisation. Cela a non seulement affecté ses capacités à se déplacer librement entre son domicile et son lieu de travail, mais a également eu un impact sur sa santé mentale et sa vie sociale en dehors du travail.

Lorsqu'elle a fait part de ses préoccupations, le bureau les a minimisées, suggérant que ce type de harcèlement était normal. Cette réponse l'a empêchée de signaler le harcèlement continu et croissant dont elle était victime, et la lourdeur de la procédure à suivre pour obtenir un véhicule afin de se déplacer en toute sécurité l'a encore plus dissuadée de chercher de l'aide. Finalement, cette personne a choisi de partir. Une stratégie d'atténuation peu coûteuse, telle que l'amélioration des procédures administratives pour demander un trajet sécurisé et la sensibilisation accrue aux expériences individuelles, aurait pu améliorer sa situation et potentiellement la retenir au sein de l'organisation.

Il est essentiel de souligner que la façon dont une personne est perçue est souvent une considération de sécurité plus importante que la façon dont elle s'identifie elle-même. Ces perceptions sont souvent ancrées dans des préjugés que le changement de comportement ne peut pas nécessairement corriger. Il est important de prendre en compte la manière dont les traits d'identité intersectionnelle du personnel peuvent contribuer, exacerber ou influencer la réponse et le comportement des différents acteurs, tant internes qu'externes à l'organisation, à l'égard de cette personne.

Considérations supplémentaires

- **Visibilité.** Toutes les caractéristiques liées à l'identité ne sont pas visibles ou immédiatement apparentes (par exemple, l'orientation sexuelle et certains handicaps). Cela démontre la nécessité d'une approche de gestion des risques de sécurité inclusive qui, par défaut, part du principe que le personnel a des besoins divers en matière de sécurité et tient compte de cette diversité dans la mesure du possible au moyen de processus d'orientation et de consultation. Cela signifie également créer un environnement organisationnel qui permet au personnel d'exprimer ses préoccupations et de demander des conseils sur les risques liés à son profil d'identité.
 - **Lieu.** De nombreuses approches de gestion des risques de sécurité se concentrent sur les risques liés au lieu, en tenant compte des menaces générales dans la zone. Bien que ces risques soient indéniablement importants, ils ne sont pas les seuls à prendre en considération, ni nécessairement les plus importants dans tous les cas. À quelques exceptions près (telles que les zones de combat actif ou d'autres contextes où la violence est aveugle), le fait qu'un lieu soit « sûr » pour un membre du personnel dépend souvent davantage de la personne et de la façon dont elle est perçue que de l'endroit où elle se trouve.⁸ Même dans les cas exceptionnels mentionnés, certains profils, tels que les travailleurs humanitaires nationaux, sont plus susceptibles de se trouver dans ces lieux et sont donc exposés à un risque accru en raison d'une plus grande visibilité. La montée des menaces numériques et la résurgence de conflits majeurs en Europe ces dernières années sont une preuve supplémentaire de la nécessité de faire évoluer le débat sur la sécurité, en passant de la question « où est-on en sécurité ? » à « qui est en sécurité ? ».
- *Voir le chapitre 6.2 pour plus de détails sur la manière dont les aspects liés à l'identité affectent la sécurité numérique.*
- **Menaces internes et externes.** De nombreux systèmes de gestion des risques de sécurité se concentrent sur les menaces externes. Cependant, il existe de plus en plus de preuves que les menaces à la sécurité du personnel proviennent des collègues eux-mêmes. Les travailleurs humanitaires qui s'identifient comme lesbiennes, gays, bisexuels, transgenres, queer/en questionnement, intersexués plus (LGBTQI+) ou comme personnes en situation de handicap ont déclaré qu'ils étaient plus préoccupés par les menaces internes que par les menaces externes.⁹ Les menaces internes peuvent inclure les abus verbaux et physiques, le chantage, le harcèlement, la discrimination et la violence. Les comportements et les environnements contribuent à créer des cultures de travail hostiles, et les cas mineurs d'hostilité peuvent évoluer vers des formes plus graves d'agression. Cette

8 Pour une illustration détaillée de ce point, voir Hoppe, K. (2017) *Where is safe?* TEDxBristol, 19 décembre (en anglais, « Où est-on en sécurité ? ») (www.youtube.com/watch?v=Q9RxE9p9T3w).

9 European Interagency Security Forum (2018) *Gérer la sécurité des travailleurs humanitaires aux profils diversifiés* (www.gisf.ngo/resource/managing-the-security-of-aid-workers-with-diverse-profiles/).

escalade est souvent décrite comme un « continuum » ou une « pyramide » de violence, où des incidents apparemment insignifiants de harcèlement, d'incivilité et d'exclusion non seulement deviennent normaux, mais ouvrent également la voie à des abus plus graves.¹⁰ Une culture qui tolère ces agressions mineures augmente le risque d'escalade de ces incidents.

- **Classification du personnel.** Les plans de sécurité ont toujours accordé une grande importance à la manière dont le personnel est classé au sein d'une organisation (par exemple, national, international, résident ou mobile). Cela peut s'avérer problématique, car la classification peut être complexe et ne pas tenir compte de facteurs d'identité importants, tels que la double nationalité, ou le fait que le « personnel national » soit originaire de la zone ou non. Cela peut également conduire à des hypothèses erronées sur la vulnérabilité des membres du personnel face aux menaces et sur leur connaissance des contextes de sécurité. Il est souvent plus efficace de prendre en compte la situation spécifique de chaque individu ainsi que les besoins et les circonstances contextuels, plutôt que de se fier à des classifications générales. Les efforts visant à localiser les postes au sein des organisations internationales doivent également être soigneusement examinés en fonction des profils de risque personnel et des points forts et vulnérabilités individuelles.

► Pour une analyse plus détaillée de la dotation en personnel, voir le chapitre 5.1 sur les ressources humaines.

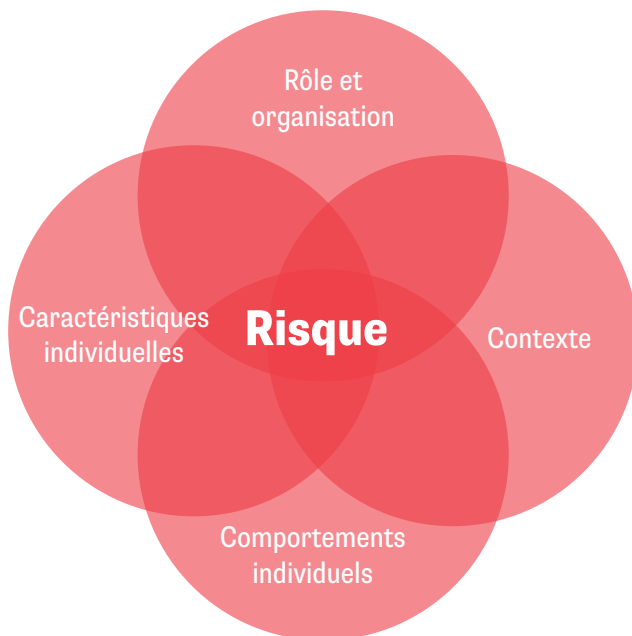
1.2.2 Approche centrée sur la personne

Historiquement, lorsque les systèmes de gestion des risques de sécurité ont pris en compte l'identité, ils se sont principalement concentrés sur les questions liées au genre, à l'ethnicité et à la nationalité, et souvent de manière ad hoc. Au fil des ans, cette approche s'est élargie pour inclure un éventail plus large de caractéristiques liées à l'identité.¹¹ Cette évolution, motivée par la nécessité d'une culture de la sécurité plus inclusive dans le secteur, a conduit à l'introduction d'une approche de gestion des risques de sécurité centrée sur la personne. Celle-ci intègre des considérations fondées sur l'identité et place les individus au centre des activités de gestion des risques de sécurité. Dans la pratique, cela implique de reconnaître les risques spécifiques à chaque profil résultant de l'intersection entre les caractéristiques individuelles (identité intersectionnelle) et le comportement, les facteurs organisationnels et le contexte dans lequel le personnel travaille (tant dans la sphère physique que numérique) (voir la figure 2).

¹⁰ Pour en savoir plus sur la pyramide de la violence, voir European Interagency Security Forum (2019) *Gérer la violence sexuelle à l'encontre du personnel humanitaire : prévention, préparation, réponse et suivi* (<https://gispprod.wpengine.com/resource/managing-sexual-violence-against-aid-workers/>).

¹¹ GISP et Humanitarian Outcomes (2024) *State of practice: the evolution of security risk management in the humanitarian space* (en anglais, « État des lieux : l'évolution de la gestion des risques de sécurité dans le domaine humanitaire ») (https://humanitarianoutcomes.org/security_risk_mgmt_humanitarian_space_2024).

Figure 2 Approche des risques de sécurité centrée sur la personne



Adaptée de Arthur, T. et Moutard, L. (2022) *Toward inclusive security risk management: the impact of 'race', ethnicity and nationality on aid workers' security*. (en anglais, «Vers une gestion des risques de sécurité inclusive : l'impact de la « race », de l'ethnicité et de la nationalité sur la sécurité des travailleurs humanitaires.») GISF (www.gisf.ngo/resource/toward-inclusive-security-the-impact-of-race-ethnicity-and-nationality-on-aid-workers-security/).

Une approche de gestion des risques de sécurité centrée sur la personne consiste à adapter les mesures de sécurité aux besoins et vulnérabilités spécifiques de chaque travailleur humanitaire, plutôt que d'appliquer un modèle unique. Elle favorise une atténuation des risques équitable en tenant compte des identités intersectionnelles uniques des travailleurs humanitaires.

Efforts en matière de sécurité et de décolonisation

En plus d'améliorer la gestion des risques de sécurité, une approche de sécurité centrée sur la personne peut soutenir les efforts de « décolonisation » déployés par un nombre croissant d'organisations internationales. Le personnel de sécurité peut promouvoir ces deux objectifs en s'engageant dans les actions pratiques suivantes.

- **Réflexion critique.** S'engager dans une réflexion critique sur les facteurs historiques et structurels qui influencent les risques de sécurité. Les inégalités historiques, contextuelles et structurelles peuvent exposer certaines personnes à des risques plus importants que d'autres, souvent sans qu'elles bénéficient des mesures de sécurité adéquates pour les protéger, du pouvoir nécessaire pour faire entendre et satisfaire leurs besoins en matière de sécurité ou des capacités à consentir véritablement aux risques auxquels elles sont exposées.
- **Dialogue inclusif.** Favoriser un dialogue inclusif pour comprendre la diversité des points de vue et des expériences. Cela peut aider à identifier et à traiter les préjugés et les inégalités dans les pratiques de sécurité et à garantir que les mesures de gestion des risques de sécurité sont inclusives. Il s'agit notamment d'être ouvert aux connaissances et aux bonnes pratiques de personnes ayant des points de vue différents.
- **Soutien équitable.** Veiller à ce que les ressources soient réparties équitablement afin d'assurer la sécurité de tous les membres du personnel, quelle que soit leur identité. Cela peut impliquer d'adopter une approche de sécurité centrée sur la personne et peut nécessiter une redistribution des ressources afin de remédier aux disparités et de garantir un soutien équitable en matière de sécurité aux groupes marginalisés ou sous-représentés. La question du soutien équitable est également pertinente dans le cadre du travail avec les partenaires (*voir le chapitre 3.5 pour une analyse plus détaillée*).
- **Autonomisation et représentation.** Promouvoir la représentation du personnel marginalisé et sous-représenté dans les processus de prise de décision, y compris l'évaluation des risques et la planification de la sécurité. Le personnel de sécurité peut jouer un rôle important en facilitant les discussions et en apportant son expertise et son expérience, ce qui peut se traduire par des cadres organisationnels plus inclusifs. Cela peut également inclure la recherche d'une plus grande diversité parmi les professionnels de la sécurité à tous les niveaux d'une organisation. Les équipes dirigeantes peuvent également faire savoir que la diversité des identités et des expériences est un atout dans les opérations humanitaires et les efforts de gestion des risques de sécurité.

1.2.3 Considérations relatives aux bonnes pratiques

Culture organisationnelle

Les normes culturelles et les tabous locaux peuvent rendre particulièrement difficiles les discussions sur des caractéristiques spécifiques liées à l'identité, telles que l'ethnicité et l'orientation sexuelle. Cette résistance culturelle peut entraver la mise en œuvre d'efforts de gestion des risques de sécurité inclusive, qui peuvent nécessiter des discussions ouvertes et sensibles sur ces sujets. Certains dirigeants d'organisations peuvent également craindre que le fait d'enquêter sur les expériences des membres du personnel issus de minorités attire l'attention sur d'éventuelles lacunes organisationnelles, au risque de nuire à leur réputation.

La création et la mise en œuvre systématiques de politiques favorisant une approche centrée sur la personne nécessitent un engagement et un soutien institutionnels. Cela peut inclure l'élaboration de directives exhaustives, l'allocation de ressources pour la formation et la garantie que ces politiques sont intégrées dans la culture organisationnelle au sens large. De nombreuses organisations ont encore du mal à intégrer de manière cohérente des considérations et un langage inclusifs dans leurs politiques, leurs formations et leurs communications quotidiennes.

Les équipes dirigeantes peuvent s'attacher à donner aux points focaux pour les questions de sécurité les moyens d'adopter une approche centrée sur la personne dans tous les aspects de leur travail, notamment en élaborant en collaboration un cadre de gestion du risque de sécurité inclusive. Le personnel de sécurité peut jouer un rôle important dans la promotion d'une culture de la confidentialité, de la collaboration, de l'inclusion et de la confiance, et il doit s'efforcer d'être perçu au sein de l'organisation comme accessible et fiable. Certaines organisations ont mis en place dans chaque bureau des points focaux pour les questions de sécurité, qui sont des femmes et/ou des personnes originaires de la zone, afin d'améliorer le signalement des questions sensibles.

L'un des principaux défis consiste à trouver le juste équilibre entre la responsabilité individuelle et le devoir de diligence de l'organisation. Il est conseillé aux équipes dirigeantes de mener des recherches approfondies et de bien comprendre leurs responsabilités dans l'accomplissement de ce devoir, en particulier lorsqu'elles tiennent compte des profils diversifiés de leur personnel. Ne pas traiter de manière adéquate les risques liés à l'identité pourrait entraîner un manquement à ce devoir de diligence, d'autant plus que la grande majorité du personnel humanitaire est composée de personnes issues de milieux divers. Un système de gestion des risques de sécurité qui tient compte des divers besoins du personnel en matière de sécurité contribue non seulement à atténuer ces risques, mais peut également améliorer le bien-être et la fidélisation du personnel ainsi que les résultats des programmes. Les organisations doivent être claires quant au niveau de soutien qu'elles apportent pour gérer les risques liés à l'identité, tout en encourageant les individus à demander des conseils et un soutien pour leurs besoins spécifiques.

Lutte contre la discrimination

Les préoccupations en matière de discrimination constituent un obstacle majeur pour les organisations qui s'attaquent aux risques liés à l'identité. Les organisations ne veulent pas être perçues comme s'immisçant dans la vie privée du personnel ou prenant des décisions en matière d'emploi sur la base de ses caractéristiques personnelles, et elles peuvent à juste titre s'inquiéter des implications juridiques d'une telle démarche. Cela a conduit certaines organisations à adopter une approche «ne rien demander, ne rien dire», dans laquelle les décisions en matière de sécurité fondées sur des aspects liés à l'identité ne sont pas communiquées de manière transparente ni discutées ouvertement. Cependant, traiter tous les membres du personnel comme s'ils avaient un profil de risque unique et commun peut conduire à une protection inadéquate, à une vulnérabilité accrue et à des risques organisationnels encore plus importants. Une étude récente a montré que les travailleurs humanitaires souhaiteraient que les risques liés à l'identité soient traités de manière plus transparente et plus ouverte dans les mesures de sécurité.¹²

Dans certaines circonstances et certains contextes, les personnes présentant certains profils peuvent être amenées à suivre des mesures de sécurité distinctes ou à bénéficier d'un soutien supplémentaire en matière de sécurité. La justification des mesures et des ressources imposées dépendra de la légitimité et de la proportionnalité de ces actions par rapport au risque, ou de l'existence d'autres solutions moins radicales. Toutes les décisions doivent être fondées sur des preuves documentées plutôt que sur des hypothèses ou des perceptions individuelles.¹³ En effet, ces mesures seraient injustifiables si elles étaient arbitraires et si les différences qu'elles entraînent conduisaient à un traitement injuste ou à une inégalité.

Pour mieux comprendre cela, il est utile de faire la distinction entre traitement équitable et égalité de traitement. L'égalité de traitement implique de fournir les mêmes ressources et mesures à chacun, quelle que soit sa situation. Cependant, cette approche peut négliger certaines vulnérabilités spécifiques et ne pas offrir une protection adéquate. Le traitement équitable consiste à fournir des ressources et des mesures adaptées pour garantir à tous les individus le même niveau de sécurité et de soutien, en tenant compte de leurs besoins et risques spécifiques. L'objectif est de veiller à ce que le niveau de risque qui en résulte soit acceptable pour tous. Cette approche n'est pas discriminatoire, mais constitue plutôt un ajustement nécessaire pour faire face efficacement à des menaces réelles et variées.

Pour garantir que les mesures ne soient pas discriminatoires et soient plus facilement acceptées par le personnel, il est possible de recourir aux moyens suivants :

- **Développement conjoint de politiques et de pratiques.** La participation d'un personnel diversifié au développement et à la révision des politiques et pratiques de sécurité garantit que l'approche de l'organisation reflète un large éventail de points

12 European Interagency Security Forum (2018).

13 Pour une analyse plus détaillée des considérations juridiques en matière de lutte contre la discrimination, voir European Interagency Security Forum (2018), chapitre 2 : Devoir de diligence légal et lutte contre la discrimination.

de vue et tient compte des préoccupations et des risques spécifiques auxquels sont confrontés différentes identités. Les organisations peuvent créer des espaces de consultation, des comités consultatifs ou des groupes de travail comprenant des représentants de diverses identités afin de contribuer au développement ou à la révision des mesures de sécurité.

- **Communication claire et en temps utile.** Informer le personnel des risques et communiquer clairement les raisons des mesures de sécurité adaptées en temps utile (par exemple, avant un déplacement ou pendant le recrutement) permet de s'assurer que chacun comprend la nécessité et l'équité de ces mesures.
- **Mécanismes de rétroaction.** La mise en place de canaux permettant au personnel de donner son feedback sur les mesures de sécurité, ainsi que la sollicitation régulière et la prise en compte de ce feedback, contribuent à identifier les problèmes de discrimination perçue et permettent d'adapter et d'améliorer en permanence les pratiques de sécurité à mesure que l'environnement et les risques évoluent.

Systèmes, politiques et pratiques de sécurité inclusive

L'introduction d'une nouvelle méthode de travail peut être décourageante. Le personnel de sécurité travaille souvent dans des délais serrés et avec une charge de travail importante, ce qui rend difficile de consacrer du temps à réfléchir à une nouvelle approche et à adopter des méthodes de travail centrées sur la personne. Le personnel de sécurité peut également se sentir incapable d'engager des conversations sur les risques liés à l'identité en raison d'un manque d'expertise. Malgré ces difficultés, certaines organisations ont fait des progrès significatifs dans l'adoption d'une approche de sécurité centrée sur la personne, souvent sous l'impulsion de la direction, qui a pris les premières mesures, notamment en encourageant et en donnant les moyens à son personnel d'adopter cette approche. Pour certaines organisations, cela s'est traduit par des consultations avec le personnel afin de comprendre les risques liés à l'identité auxquels il est confronté ; pour d'autres, cela a impliqué le recrutement d'équipes de sécurité plus diversifiées, et pour une organisation internationale, cela a consisté à évaluer tous les aspects de ses systèmes de sécurité afin d'identifier les moyens de les rendre plus inclusifs (voir l'exemple de cas ci-dessous).

De nombreuses initiatives ont commencé modestement, avec des changements ciblés dans des domaines particuliers, qui ont ensuite fait boule de neige. La mise en place d'une approche centrée sur la personne ne nécessite pas nécessairement un investissement important en termes d'argent ou de temps, mais peut commencer par un changement de perspective, par exemple en demandant simplement au personnel de sécurité comment une situation ou un programme peut avoir un impact sur la sécurité de collègues ayant des profils et des besoins différents.

Exemple de cas : Adopter une approche de sécurité centrée sur la personne systématique

L'équipe de sécurité mondiale d'une organisation internationale a lancé un projet visant à établir un cadre d'orientation pour une approche de gestion des risques de sécurité centrée sur la personne. L'objectif principal du projet était d'identifier les lacunes en matière de diversité et d'inclusion dans la gestion des risques de sécurité (au moyen de recherches et de consultations du personnel), puis de formuler des recommandations pratiques.

La plupart des membres du personnel consultés dans le cadre du projet ont estimé que les profils personnels constituaient un facteur important dans la détermination du niveau et du type de risques de sécurité auxquels ils étaient confrontés, mais que l'organisation, et en particulier les responsables, devaient faire davantage pour traiter les risques spécifiques à chaque profil.

L'étude a révélé que les principaux défis de sécurité liés aux profils étaient le manque d'accès aux informations pertinentes, la discrimination interne/l'inégalité de traitement et les préjugés/l'hostilité externes dans l'environnement local. Les facteurs qui contribuent à renforcer le sentiment de sécurité du personnel comprennent une communication ouverte de la part de la direction sur les questions liées à la sécurité, des politiques et procédures de sécurité clairement définies par écrit, ainsi que des mécanismes permettant le signalement des incidents ou toute information pertinente afin de mieux comprendre l'environnement de travail dans son ensemble et de traiter les plaintes.

L'étude a montré la nécessité d'une approche plus systématique et inclusive de la gestion des risques de sécurité, ainsi que d'une culture du management plus proactive et inclusive. À la suite du projet, l'organisation a pris des mesures pour mettre en œuvre les recommandations identifiées, ce qui a nécessité la contribution de plusieurs groupes de travail internes et décideurs différents. Compte tenu des changements requis à l'échelle de l'organisation, il était important de veiller à ce que la mise en œuvre soit la responsabilité partagée des différentes parties prenantes, notamment les services de sécurité, les ressources humaines et d'autres départements impliqués dans la formation, le développement des politiques et la collecte de données.

Les considérations relatives à la diversité peuvent être prises en compte dans l'ensemble du cadre de gestion du risque de sécurité.

- **Évaluations des risques inclusives.** Processus complet d'évaluation des risques intégrant les facteurs de risque individuels (identité intersectionnelle et comportements), organisationnels et externes, tenant compte à la fois des menaces internes et externes et de leurs interrelations. Un autre facteur à prendre en compte peut être le temps (certaines périodes, comme les élections, pouvant être plus instables que d'autres). Les petites organisations, ou celles qui connaissent moins de mouvements de personnel, peuvent être mieux à même de procéder à des évaluations des risques individualisées pour chaque membre du personnel lorsqu'il rejoint l'organisation, démarre un nouveau projet ou effectue un déplacement (c'est l'approche adoptée, par exemple, par certaines organisations de défense des droits humains). Les grandes organisations qui auraient des difficultés à le faire pourraient trouver utile de veiller à ce que les évaluations des risques impliquent la plus grande diversité possible de membres du personnel, afin de garantir la prise en compte d'un large éventail de points de vue, et de fournir au personnel les outils et la formation nécessaires pour effectuer leurs propres évaluations des risques individuelles et demander des conseils si nécessaire.
- **Plans de sécurité et mesures de réponse.** Veiller à ce que les mesures d'atténuation des risques, les plans de sécurité et les mécanismes de réponse tiennent compte des besoins divers du personnel. Il peut s'agir, par exemple, de veiller à ce que le personnel en situation de handicap soit dûment pris en compte dans les plans d'évacuation et de sécurité du site, ou que les nationalités du personnel soient prises en compte dans les plans d'urgence (par exemple, l'évacuation de certaines nationalités vers un pays particulier peut les exposer à un risque plus élevé). Pour le personnel résident, qu'il soit national ou étranger, il peut être judicieux d'intégrer les considérations familiales dans les plans d'urgence. Cela peut être réalisé grâce aux approches collaboratives détaillées dans différentes parties de ce chapitre.¹⁴
- **Outils de sécurité.** Intégrer des questions et des informations sur les risques liés à l'identité dans les outils de sécurité existants. Il peut s'agir d'options permettant de sélectionner des qualificatifs fondés sur l'identité dans les formulaires de compte rendu d'incident afin de permettre une meilleure analyse d'incident, ce qui peut aider à déterminer si les incidents peuvent être le résultat d'une discrimination, d'homophobie, de ciblage à caractère ethnique ou d'autres facteurs.
- **Recommandations.** Fournir des recommandations afin que les membres du personnel qui ne souhaitent pas divulguer des informations relatives à leur identité aient accès à des informations leur permettant de prendre des décisions éclairées en matière de sécurité. Il est essentiel que les informations relatives aux risques spécifiques à chaque profil soient systématiquement communiquées à l'ensemble du personnel, quel que soit leur profil personnel. Cela peut inclure l'intégration d'informations sur les risques liés à l'identité dans les documents de sécurité communiqués au personnel et la mise à disposition de points focaux auxquels les membres du personnel peuvent s'adresser de manière confidentielle et individuelle. Les organisations peuvent collaborer avec des groupes spécialisés et des initiatives afin d'intégrer leur expertise et leurs ressources

¹⁴ Pour des exemples détaillés de mesures d'atténuation des risques inclusives, voir European Interagency Security Forum (2018).

dans leurs recommandations internes. Cela pourrait inclure la collaboration avec des organisations qui luttent contre la violence fondée sur le genre ou qui soutiennent les personnes LGBTQI+. Le personnel peut disposer de ses propres ressources et recommandations, mais la manière dont une organisation met l'information à disposition et le type de boucle de rétroaction peuvent faire une grande différence dans la manière dont le personnel interagit avec les recommandations qui lui sont données. Cela peut également améliorer le contenu des recommandations développées et mises à jour par l'organisation.

- **Culture de la sécurité.** Instaurer une culture de la sécurité positive et inclusive au sein de l'organisation en communiquant avec le personnel sur les risques liés à l'identité, en déstigmatisant les discussions et en combattant les «mythes» autour de la vulnérabilité personnelle dans le cadre de réunions de groupe, telles que des séances d'information et des formations. Ce type de communication peut permettre au personnel d'exprimer ses préoccupations et de prendre des décisions plus éclairées en matière de sécurité, tant pour lui-même que pour les autres.
- **Composition du personnel de sécurité.** Recruter un personnel de sécurité diversifié. De plus en plus d'organisations visent une plus grande diversité dans le personnel en général, mais aussi dans les postes de sécurité. L'identité des points focaux pour les questions de sécurité peut influencer considérablement la perception qu'ont les employés des mesures de sécurité et leur engagement à cet égard.¹⁵ Dans la pratique, cela peut signifier qu'il faut tenir compte des exigences du poste. Par exemple, dans les pays où les femmes ne peuvent pas occuper de fonctions policières ou militaires, le fait d'exiger cette expérience pour les postes de sécurité exclura les candidates nationales.

Rôles et profils de risque personnels

Dans certains contextes, certains visiteurs peuvent avoir un profil de risque élevé en raison de leur visibilité ou de leur rôle (par exemple, les visiteurs VIP). Il peut s'agir de dirigeants d'organisations, d'experts, de donateurs, de fonctionnaires et d'auditeurs, dont la présence peut attirer une attention non désirée ou susciter des agressions (au sein et à l'extérieur d'une organisation). Le ciblage de ces personnes peut avoir de graves répercussions sur leur sécurité et sur l'organisation dans son ensemble. Cela peut également accroître les risques de sécurité du personnel, soulevant d'importantes questions quant au caractère essentiel de telles visites. Si la visite justifie le risque encouru par le visiteur et les autres membres du personnel, les organisations peuvent mettre en œuvre des mesures de sécurité appropriées, qui peuvent inclure des détails de sécurité discrets, un logement sécurisé, des protocoles de déplacement spéciaux, des mesures de sécurité de l'information (telles que la non-divulgaration publique des informations relatives au lieu) et des plans d'urgence en cas de situation critique. Dans les organisations où les visites de personnalités sont fréquentes, il est utile de former régulièrement ces personnes et celles qui sont en contact avec elles à la sensibilisation à la sécurité personnelle et au comportement à adopter dans les environnements à haut risque.

¹⁵ Pour en savoir plus, voir : GISF et Humanitarian Outcomes (2024).

Recommandations sur les risques liés à l'identité

Les membres du personnel ont droit au respect de leur vie privée, ce qui signifie que les organisations ne peuvent pas les obliger à divulguer des informations sur leur profil personnel qu'ils ne souhaitent pas partager. En donnant des recommandations générales sur les risques liés à l'identité, les organisations évitent de faire pression sur le personnel pour qu'il divulgue des informations sensibles ou de l'isoler directement en raison d'hypothèses concernant son identité. Cela contribue également à instaurer une culture de la sécurité qui permet à chacun de poser des questions et de réfléchir à ses propres besoins en matière de sécurité.

Les exemples de questions suivants peuvent aider les organisations à déterminer les recommandations à donner :

- Quelle est la composition du personnel? Les informations agrégées et anonymes provenant des ressources humaines (RH) peuvent être utiles à cet égard. En utilisant ces données parallèlement à des facteurs contextuels, quels profils de personnel pourraient nécessiter des recommandations supplémentaires?
- Le personnel comprend-il le devoir de diligence de l'organisation à son égard? Y a-t-il un domaine spécifique dans lequel il a besoin de plus d'informations, et cela pourrait-il être résolu par des recommandations supplémentaires?
- À quelles ressources le personnel a-t-il accès en matière de risques liés à l'identité (externes et internes)? Comment l'organisation peut-elle l'aider à accéder plus facilement à ces informations?
- Le personnel peut-il accéder facilement et en toute confidentialité aux ressources relatives aux risques liés à l'identité?
- Existe-t-il un point focal auquel le personnel peut s'adresser en toute confidentialité pour discuter de ses préoccupations?

Une organisation a veillé à ce que, dans le cadre de ses procédures de déplacement, des liens vers des ressources externes et internes soient fournis sur les risques et les recommandations pertinentes pour le personnel LGBTQI+. Le site intranet de l'organisation dispose également d'une page dédiée donnant des recommandations.

Rendre inclusives les pratiques organisationnelles plus générales

Il peut être utile d'adopter une approche centrée sur la personne pour les pratiques organisationnelles plus générales qui peuvent avoir une incidence sur la sécurité du personnel.

- **Examens du système.** Réaliser des examens organisationnels afin de déterminer si tous les membres du personnel ont un accès adéquat au soutien et aux ressources (y compris en matière de sécurité), quel que soit leur profil personnel, et de remédier à tout obstacle ou inégalité structurelle identifié. Dans toute organisation, en particulier les organisations internationales, il est conseillé d'adapter la communication et les interactions au public cible. Un exemple simple consiste à veiller à ce que le personnel puisse accéder aux communications pertinentes dans sa langue maternelle. Dans de nombreuses organisations internationales, le personnel international et national peut bénéficier de différents niveaux de soutien, notamment en matière d'assurance. Dans certaines circonstances, ces services de soutien supplémentaires sont justifiés et nécessaires, mais cela peut également révéler des inégalités entre les membres du personnel. Il est également important de noter que ces distinctions ne sont pas nécessairement dues à des préjugés ou à un manque d'attention, mais peuvent résulter de facteurs indépendants de la maîtrise du risque de l'organisation, tels que des obstacles juridiques à l'évacuation du personnel national et des restrictions dans les polices d'assurance.
- **Recrutement général et déploiement.** Intégrer les considérations relatives à la sécurité fondée sur l'identité dans les procédures de recrutement et, le cas échéant, dans les discussions avec le personnel avant l'attribution de nouvelles missions.¹⁶ Dans la pratique, cela peut signifier être ouvert à différentes expériences et veiller à ce que les exigences du poste n'excluent pas indûment certains profils (voir l'encadré ci-dessous).

¹⁶ Pour une analyse plus approfondie de la prise en compte des risques liés à l'identité dans le recrutement, voir European Interagency Security Forum (2018).

Problèmes liés à l'identité dans le recrutement et le déploiement

Le recrutement ou le déploiement du personnel dans le secteur humanitaire est plus complexe que dans de nombreux autres domaines professionnels. Certaines personnes peuvent être exposées à un risque accru dans de nouveaux lieux ou de nouvelles fonctions en raison de leur profil de risque personnel. Il est conseillé d'encourager la discussion dans la mesure du possible plutôt que d'interdire purement et simplement certains profils spécifiques. Cela dit, dans certains cas, il peut être judicieux d'indiquer dans la description de poste que certaines fonctions ne sont pas accessibles à des profils d'identité spécifiques en raison de la situation en matière de sécurité. La légalité de ce type de discrimination indirecte dépend du pays ; les mesures doivent toujours viser à être justifiables, proportionnées et légitimes. Un exemple serait de ne pas recruter d'hommes pour travailler dans un refuge ou un centre d'accueil pour femmes.

Le fait d'impliquer les points focaux pour les questions de sécurité dans le recrutement et le déploiement, et d'être clair dans les descriptions de poste et lors des entretiens sur les risques accrus auxquels sont exposés certains profils, permet de garantir que ces préoccupations sont discutées et décidées ouvertement en collaboration avec le personnel concerné.

Formation

Aborder les risques liés à l'identité dans le cadre de la formation à la sécurité peut améliorer les résultats pour l'ensemble du personnel, qu'il s'agisse de la manière dont les membres de l'équipe peuvent aider leurs collègues en situation de handicap en cas d'urgence ou du maintien de la confidentialité de l'orientation sexuelle d'un collègue à la suite d'un incident de sécurité, en particulier si la révélation de cette information peut présenter un risque de sécurité pour le membre du personnel ou l'organisation.

Bien que les formateurs aient rencontré une certaine résistance à aborder ces sujets, traiter la question de la diversité dans ces cours peut être l'occasion d'engager le dialogue et de partager les expériences vécues par les profils sous-représentés parmi les membres de l'équipe, qui, sans cela, n'auraient peut-être jamais été entendues ou comprises par leurs collègues. Si l'on ne peut pas attendre des formateurs qu'ils aient toutes les réponses à toutes les questions concernant les risques liés à l'identité,

ils peuvent toutefois créer un espace permettant aux participants d'examiner les questions pour eux-mêmes et leurs profils individuels, tout en tirant parti des expériences communes des autres.

L'identité du formateur peut également jouer un rôle dans le niveau de confort des participants à la formation lorsqu'il s'agit d'aborder des questions relatives à leur profil individuel. S'il est essentiel d'augmenter le nombre de formateurs issus de groupes sous-représentés, il est tout aussi important que tous les formateurs, quel que soit leur profil, aient les capacités de créer un environnement propice à l'expression des préoccupations et à leur prise en compte en toute sécurité.

► *Pour plus de détails sur la formation et les considérations relatives à l'inclusion, voir le chapitre 5.2.*

Considérations relatives à la formation ciblée

Au-delà de veiller à ce que la formation à la sécurité tienne davantage compte des différents profils de risque, les organisations peuvent également proposer à leur personnel, y compris au personnel de sécurité, des formations sur les préjugés inconscients, le pouvoir, les privilèges, l'intersectionnalité et le rôle des témoins actifs, pour n'en citer que quelques-unes. Certaines organisations ont intégré ces aspects dans leur formation à la sécurité existante. Ces domaines d'apprentissage peuvent contribuer à sensibiliser aux risques encourus par différentes identités et à promouvoir une culture d'inclusion et de respect. Lorsque le personnel comprend la raison d'être des mesures de sécurité adaptées, il est plus enclin à les considérer comme justes et nécessaires, ce qui réduit la résistance et le sentiment de discrimination. Pour le personnel de sécurité, une formation dans ces domaines peut permettre de déconstruire les idées reçues sur les profils de risque individuels, de développer l'empathie et de promouvoir des compétences pratiques pour gérer les risques liés à l'identité.

Il est conseillé de former le personnel de sécurité et les autres collègues concernés (comme les RH) à l'adoption d'une approche centrée sur la personne, par exemple à la manière de mener une évaluation des risques relatifs à la sécurité inclusive. Cela permet de s'assurer que le personnel responsable est en mesure de traiter les risques liés à l'identité et se sent à l'aise pour discuter de ces questions avec le personnel.

Exemple de cas : Sauvegarde opérationnelle des Nations Unies

Le Département de la sûreté et sécurité des Nations Unies (UNDSS) a développé un concept de «sauvegarde opérationnelle», qui s'applique aux politiques, procédures, mesures et formations mises en œuvre au sein de l'ONU pour protéger son personnel, ses biens et ses opérations contre les préjudices interpersonnels. Il se concentre à la fois sur les menaces internes et externes pesant sur le personnel et reconnaît que les efforts visant à lutter contre les menaces internes à l'encontre du personnel de l'ONU vont de pair avec les efforts visant à lutter contre l'exploitation et les abus sexuels commis par le personnel de l'ONU.

La sauvegarde opérationnelle favorise une approche de sécurité centrée sur la personne par la mise en œuvre d'outils de sécurité inclusive et en se concentrant sur les auteurs (connus et inconnus), leurs alliés, l'environnement opérationnel et les vulnérabilités personnelles et situationnelles des cibles potentielles.

Les éléments clés de cette approche sont les suivants:

- Reconnaître que certains comportements et environnements peuvent conduire à des abus de pouvoir, et que des manifestations mineures d'hostilité peuvent dégénérer en formes plus graves de préjudice (la «pyramide de la violence»). Tolérer le harcèlement, l'incivilité et l'exclusion augmente le risque d'incidents plus graves, notamment les agressions sexuelles.
- Reconnaître que toutes les formes d'agression interpersonnelle concernent le personnel de sécurité, car elles constituent un problème transversal grave qui nécessite la collaboration de tous les services en contact avec le personnel.
- Veiller à ce que chaque membre du personnel soit informé de toutes les menaces potentielles, et pas seulement de celles qui semblent pertinentes à chaque individu. En dotant l'ensemble de son personnel des connaissances et des outils nécessaires pour atténuer les risques de manière universelle, l'ONU vise à renforcer la sécurité de tous. En substance, la sécurité collective n'est assurée que lorsque chaque membre est en sécurité: personne n'est vraiment en sécurité tant que tout le monde ne l'est pas.
- Promouvoir l'approche «Upstander» («Défenseur») de l'ONU, en encourageant le personnel formé à devenir des témoins actifs en cas d'incident et à promouvoir la sauvegarde opérationnelle dans le cadre de leur travail.

L'ONU a mis en place une formation mixte sur la sauvegarde opérationnelle. Cette formation interactive vise à sensibiliser le personnel à la mise en œuvre de cette approche et à lui donner les moyens de devenir des « UN Upstanders » (« Défenseurs de l'ONU »). Outre la sensibilisation et la responsabilisation du personnel, la formation vise à dissuader de manière significative les auteurs potentiels d'actes répréhensibles.

Informations complémentaires

Recherche et analyse

Arthur, T. et Moutard, L. (2022) *Toward inclusive security: The impact of 'race', ethnicity, and nationality on aid workers' security* (en anglais, « Vers une sécurité inclusive: l'impact de la « race », de l'ethnicité et de la nationalité sur la sécurité des travailleurs humanitaires »). GISF (www.gisf.ngo/resource/toward-inclusive-security-the-impact-of-race-ethnicity-and-nationality-on-aid-workers-security/).

European Interagency Security Forum (2018) *Gérer la sécurité des travailleurs humanitaires aux profils diversifiés* (www.gisf.ngo/resource/managing-the-security-of-aid-workers-with-diverse-profiles/).

GISF et Humanitarian Outcomes (2024) *State of practice: The evolution of security risk management in the humanitarian space* (en anglais, « État des lieux: l'évolution de la gestion des risques de sécurité dans le domaine humanitaire ») (www.humanitarianoutcomes.org/security_risk_mgmt_humanitarian_space_2024).

Hoppe, K. (2017) *Where is safe?* TEDxBristol (en anglais, « Où est-on en sécurité? ») (www.youtube.com/watch?v=Q9RxE9pT3w).

Recommandations et outils

Bond (2022) *Becoming locally led as an anti-racist practice: a guide to support INGOs* (en anglais, « Devenir une organisation dirigée localement en tant que pratique antiraciste: guide pour soutenir les ONG internationales ») (www.bond.org.uk/resources/becoming-locally-led-as-an-anti-racist-practice-a-guide/).

CICR (2021). « 3.3. Le risque est-il le même pour tous? » dans *SAFE: Manuel de sécurité pour les humanitaires* (www.icrc.org/en/publication/4425-safe-manuel-de-securite-pour-les-humanitaires).

European Interagency Security Forum (2019a) *Gérer la violence sexuelle à l'encontre du personnel humanitaire : prévention, préparation, réponse et suivi* (<https://gisfprod.wpengine.com/resource/managing-sexual-violence-against-aid-workers/>).

European Interagency Security Forum (2019b) *Beyond the tick box: Developing a person-centred and inclusive approach to security risk management* (en anglais, «Au-delà des cases à cocher : développer une approche inclusive et centrée sur la personne de la gestion des risques de sécurité»). 16 décembre (www.gisf.ngo/blogs/beyond-the-tick-box-developing-a-person-centred-and-inclusive-approach-to-security-risk-management/).

GISF (2021) *HNPW | A person-centred approach to security risk management | Resources* (en anglais, «HNPW | Approche centrée sur la personne de la gestion des risques de sécurité | Ressources») (<https://gisf.ngo/resource/hnpw-a-person-centred-approach-to-security-risk-management-resources/>).

GISF (n.d.) 1. *Plans de sécurité*. Guide interfonctionnel sur la sécurité des ONG (<https://gisf.ngo/toolbox-pwa-fr/resource/1-plans-de-securite/>).

Nations Unies (n.d.) *Gender & security* (en anglais, «Genre et sécurité») (www.un.org/en/safety-and-security/gender-and-security).

Persaud, C. (2012) *Genre et sécurité: Orientations pour l'intégration du genre à la gestion des risques de sécurité*. European Interagency Security Forum (<https://gisf.ngo/resource/gender-and-security/>).

RedR UK et European Interagency Security Forum (2016) *Workshop report: Inclusion and security of LGBTI aid workers* (en anglais, «Rapport d'atelier: Inclusion et sécurité des travailleurs humanitaires LGBTI») (<https://gisf.ngo/resource/report-inclusion-and-security-of-lgbti-aid-workers-workshop-22012016/>).

2 Les écosystèmes de la gestion des risques de sécurité

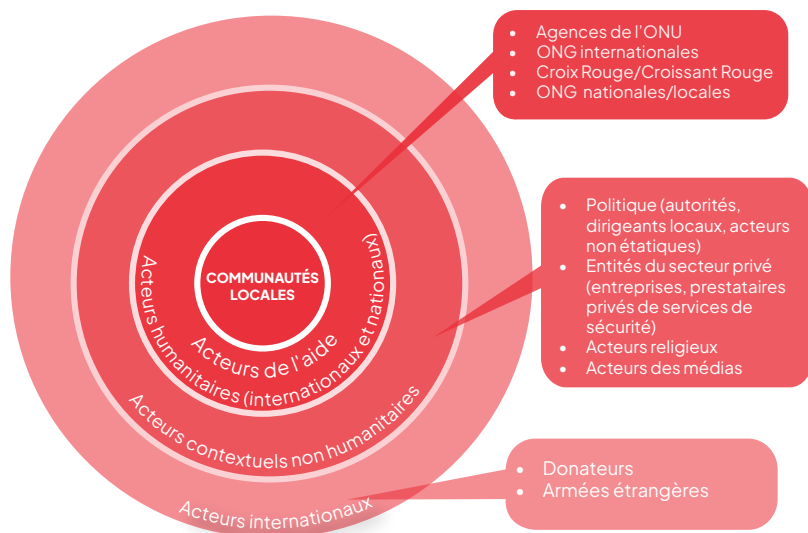
2.1 Les réseaux de sécurité et la collaboration entre les acteurs

Les organisations humanitaires n'opèrent pas dans le vide. Au quotidien, elles interagissent avec des acteurs amis, ennemis ou neutres à différents niveaux. Le nombre d'interlocuteurs n'a cessé d'augmenter ces dernières années, car de plus en plus d'acteurs humanitaires, d'entités du secteur privé et de groupes armés non étatiques opèrent dans les mêmes espaces. Ce chapitre présente les principaux acteurs et les relations qui influencent la gestion des risques de sécurité humanitaire et explore comment le personnel de sécurité peut approfondir sa compréhension et améliorer la coordination et la collaboration afin de renforcer la sécurité tout en faisant progresser les objectifs humanitaires.

2.1.1 Comprendre l'écosystème externe

Lorsqu'une crise humanitaire survient, divers acteurs locaux, nationaux - et souvent internationaux - interviennent pour répondre aux besoins des personnes et des communautés touchées. Ces acteurs humanitaires, tant formels qu'informels, sont divers, chacun ayant son propre statut juridique, ses propres objectifs et ses propres politiques. Dans cet espace humanitaire complexe et souvent encombré, la coordination est indispensable pour poursuivre des objectifs humanitaires communs. En dehors de la sphère humanitaire, les organisations évoluent dans un écosystème encore plus vaste composé d'organisations publiques et privées, d'entités politiques, de groupes militaires et d'institutions financières (figure 3).

Figure 3 L'écosystème externe



Chacun de ces acteurs peut représenter une menace potentielle ou une opportunité pour la gestion des risques de sécurité.

2.1.2 Coordination et collaboration en matière de sécurité

Collaboration en matière de sécurité interagences

À mesure que la gestion des risques de sécurité s'est développée au sein des organisations humanitaires, les structures, les moyens et les pratiques permettant aux organisations opérant dans le même environnement de coopérer entre elles en matière de sécurité se sont également développés. Une collaboration efficace entre les organisations permet à chaque participant d'améliorer considérablement l'efficacité de ses propres systèmes de gestion des risques de sécurité de la manière suivante.

- **Un meilleur système d'alerte.** En partageant leurs informations, les organisations obtiennent une image plus complète des menaces ou alertes de sécurité réelles ou possibles dans leur environnement, ce qui améliore la planification de la réponse et augmente les chances d'éviter un incident.

- **Une meilleure évaluation des risques.** Une compilation centralisée de tous les incidents et quasi-incidents de sécurité impliquant des travailleurs humanitaires dans un environnement opérationnel donné constitue une meilleure base pour l'évaluation des risques relatifs à la sécurité qu'un registre partiel d'une seule organisation.
- **Capacités supplémentaires à moindre coût.** Au lieu que chaque organisation supporte individuellement les coûts liés aux intrants supplémentaires, ceux-ci peuvent être pris en charge sur la base d'un partage des coûts. Par exemple, les coûts liés aux consultations de spécialistes ou à une formation en sécurité peuvent être partagés entre plusieurs organisations.
- **Plaidoyer collectif et négociation avec les autorités.** Plutôt que de s'engager individuellement sur des questions relatives à la sécurité, les organisations peuvent potentiellement présenter des arguments plus convaincants aux gouvernements et aux autres parties prenantes en tant que groupe.
- **Plaidoyer auprès des donateurs pour le financement.** Si la sécurité se détériore et que plusieurs organisations concluent qu'elles ont besoin de ressources financières supplémentaires pour mettre en place des mesures d'atténuation supplémentaires, elles pourraient être en mesure de présenter des arguments plus convaincants auprès des donateurs en agissant collectivement.
- **Assistance directe et comblement des lacunes.** Si une organisation a la capacité d'accueillir du personnel supplémentaire pendant un confinement, ou d'assurer le transport pour relocaliser ou évacuer du personnel alors que d'autres n'en ont pas les moyens, une coordination et une planification préalables peuvent garantir une utilisation efficace de ces ressources.
- **Offre de services communs.** Les mécanismes de coordination établis peuvent tirer parti des économies d'échelle pour offrir des services tels que la centralisation des informations et des analyses en matière de sécurité, ainsi que la formation.
- **Partage des bonnes pratiques.** Les organisations peuvent apprendre les unes des autres lorsqu'elles collaborent et partagent des informations, des conseils et des bonnes pratiques sur la manière de gérer les risques dans un domaine d'activité spécifique.
- **Gestion des risques interdépendants.** Les mesures de sécurité (ou leur absence) mises en place par une organisation peuvent avoir des répercussions sur d'autres. Par exemple, si une organisation fait appel à des escortes de sécurité armées ou verse des « frais de facilitation » aux postes de contrôle, cela peut créer des problèmes pour celles qui ne le font pas. La coopération permet d'identifier et de résoudre ces incohérences.

Mécanismes interagences de coordination en matière de sécurité

Il existe des mécanismes interagences de coordination en matière de sécurité aux niveaux mondial, régional, national et local. Ils peuvent être formels ou informels.¹⁷

17 Pour plus d'informations sur la collaboration en matière de sécurité, voir GISF (2022) *NGO security collaboration guide (en anglais, « Guide de collaboration en matière de sécurité des ONG »)* (<https://gisf.ngo/long-read/ngo-security-collaboration-guide/>).

Les mécanismes officiels destinés aux ONG, tels que l'International NGO Safety Organisation (INSO), l'Opération de sécurité en liaison avec les partenaires (PLSO) de USAID et les services de sécurité des organismes de coordination des ONG, peuvent fournir des produits analytiques, tels que des rapports réguliers sur la sécurité et des analyses des tendances en matière de sécurité. Ces mécanismes offrent également un espace de discussion et peuvent organiser des forums et des formations à la sécurité.

Les organismes de sécurité des ONG collaborent souvent avec les agences de l'ONU sur les questions de sécurité par l'intermédiaire de l'équipe de pays pour l'action humanitaire de l'ONU et du Département de la sûreté et de la sécurité de l'ONU (UNDSS). La coordination et la collaboration entre les ONG et les agences de l'ONU peuvent aider à mener des évaluations conjointes de l'accès et à élaborer des stratégies d'accès sécurisé, à coordonner la planification d'urgence et à gérer le plaidoyer et la liaison avec les autorités gouvernementales, les organismes de l'ONU, les forces militaires et les acteurs privés de la sécurité.

En l'absence d'organisme de coordination officiel, les points focaux pour les questions de sécurité de différentes organisations établissent souvent un réseau informel pour partager des informations, des alertes et des conseils, souvent à l'aide de plateformes en ligne ou par SMS. La participation à ces groupes est généralement volontaire et ponctuelle, et repose sur la représentation des individus plutôt que celle des organisations.¹⁸ À l'heure où nous écrivons ces lignes, il existe des réseaux informels pour le personnel de sécurité régionale en Afrique de l'Ouest, en Amérique latine et dans les Caraïbes.

Historiquement, les mécanismes de coordination en matière de sécurité en contextes humanitaires ont été créés par des organisations internationales et sont centrés sur celles-ci, les organisations locales et nationales étant moins représentées. Cette situation évolue lentement, car on comprend de plus en plus que la valeur de la coordination augmente avec le nombre d'acteurs qui y participent, en particulier ceux qui apportent une connaissance approfondie du contexte et des sources d'information diversifiées.

Au niveau mondial, la coordination entre les ONG - et entre les ONG et l'ONU - a également progressé ces dernières années. Le Global Interagency Security Forum (GISF) est une plateforme interagences destinée au partage d'informations et de bonnes pratiques en matière de gestion des risques de sécurité humanitaire. Le GISF sert de centre d'expertise, développe des recommandations et mène des recherches originales. L'International NGO Safety Organisation (INSO) joue également un rôle au niveau mondial, en proposant des analyses, des produits de formation et des données sur la sécurité. L'International NGO Safety & Security Association (INSSA) est une organisation associative qui propose une certification professionnelle aux responsables des risques

18 Pour une analyse plus approfondie, voir GISF et Humanitarian Outcomes (2024) *State of practice: The evolution of security risk management in the humanitarian space* (en anglais, « État des lieux : l'évolution de la gestion des risques de sécurité dans le domaine humanitaire ») (https://humanitarianoutcomes.org/security_risk_mgmt_humanitarian_space_2024).

de sécurité au niveau national et régional dans le secteur humanitaire. Les groupes de travail mondiaux se concentrent sur des thèmes particuliers liés à la gestion des risques de sécurité, tels que la sauvegarde et l'accès humanitaire.

Plusieurs pays disposent de réseaux de coordination en matière de sécurité pour les organisations dont le siège social est situé sur leur territoire, par exemple le Danish Interagency Security Network (Réseau de sécurité interagences danois) et le UK NGO Security Focal Point Group (Groupe des points focaux pour les questions de sécurité des ONG britanniques). La coordination en matière de sécurité peut également faire partie d'un mécanisme de coordination plus large, tel que InterAction aux États-Unis et La Coordinadora en Espagne. À mesure que le domaine de la sécurité humanitaire s'est développé, des rôles plus spécialisés ont vu le jour et un nombre croissant de plateformes de coordination ont été créées spécifiquement pour ces professionnels.

Saving Lives Together (Sauver des vies ensemble)

Depuis 2001, la coordination et la collaboration en matière de sécurité entre l'ONU et les ONG internationales sont structurées par un cadre écrit connu aujourd'hui sous le nom de « Saving Lives Together » (SLT, Sauver des vies ensemble).¹⁹ « SLT » a connu plusieurs itérations au fil des ans, mais dès le début, il a eu pour objectif de fournir une compréhension commune des possibilités de collaboration entre les ONG, les agences de l'ONU et le Mouvement International de la Croix-Rouge et du Croissant-Rouge face aux défis communs en matière de sécurité. Son objectif est de renforcer les capacités des partenaires à prendre des décisions éclairées et à gérer les risques grâce au partage d'informations et de ressources.

Les participants à « SLT » s'engagent à respecter six objectifs/exigences principaux:

- mettre en place des dispositifs et des forums de coordination en matière de sécurité ;
- partager les informations en matière de sécurité pertinentes ;
- coopérer dans le domaine de la formation à la sécurité ;
- coopérer dans le domaine des dispositifs opérationnels et logistiques, lorsque cela est possible ;
- identifier les ressources nécessaires pour renforcer la coordination en matière de sécurité entre l'ONU, les ONG internationales et les organisations internationales, et plaider en faveur d'un financement ; et
- se consulter sur des règles de base communes en matière d'action humanitaire.

Le comité de surveillance de « SLT », coprésidé par l'UNDSS et des représentants d'ONG internationales, veille à l'efficacité de la mise en œuvre et de la coordination. Toutes les ONG internationales opérant dans un pays peuvent y participer gratuitement, mais certains services peuvent faire l'objet d'un recouvrement des coûts. Si les organisations

¹⁹ La première incarnation de « SLT » a été un protocole d'accord (MoU) appelé « Menu of Options » (Menu d'options), établi par le Comité permanent interorganisations (IASC) avec le Coordonnateur de la sécurité des Nations Unies (UNSECOORD, le précurseur de l'UNDSS).

locales ne peuvent pas obtenir le statut de partenaire de «SLT», elles peuvent toutefois bénéficier des réseaux de sécurité existants des ONG.²⁰

Bien que le cadre de «SLT» ait été révisé et relancé, sa mise en œuvre au niveau national s'est avérée difficile, limitée et lente. La connaissance de l'existence et de l'objectif de ce cadre reste limitée parmi les ONG et le personnel de l'ONU, et dans certaines régions, le manque de confiance entre l'ONU et les ONG entrave encore davantage les progrès.²¹ Malgré tout, «Saving Lives Together» a connu des succès dans des contextes où le leadership de l'UNDSS et des équipes de pays pour l'action humanitaire est fort et efficace, et où les ONG mènent des actions de sensibilisation coordonnées et proactives.

Entreprises de sécurité privée

La sécurité commerciale privée s'est considérablement développée au cours des deux dernières décennies. Le terme «entreprise de sécurité privée» (ETS) peut désigner à la fois des entreprises officiellement enregistrées et des groupes non enregistrés, tels que des milices mercenaires, qui fournissent des services similaires. Les organisations humanitaires ont principalement recours à des sociétés privées pour assurer la sécurité de leurs locaux et de leurs programmes.

Les ETS offrent une large gamme de services, notamment la protection statique (sécurisation des bureaux et des résidences), la protection mobile (escortes), la protection rapprochée (gardes du corps), l'évaluation des menaces, l'analyse des risques, les audits de sécurité, la formation, le conseil, la gestion des incidents critiques, le soutien en cas de crise, la logistique (telle que la sécurité des transports de fonds) et la fourniture d'équipements.

Bien que le recours à la protection armée par les ETS soit peu fréquent, les organisations humanitaires ont parfois fait appel à elles pour assurer une garde non armée et d'autres services de soutien, y compris des travaux d'analyse. Les décisions d'embaucher des ETS reposent souvent sur des hypothèses concernant leur expertise, leur efficacité et leur rentabilité, mais ces hypothèses doivent être examinées avec soin. Si l'externalisation de la sécurité peut sembler moins coûteuse au départ, elle peut entraîner des coûts cachés, notamment l'incapacité à développer des compétences en interne, une atteinte potentielle à la réputation, des responsabilités juridiques et le risque de dépendre d'une approche de sécurité fondée sur la dissuasion qui pourrait s'avérer plus coûteuse à long terme.

Lorsqu'elles font appel à des entreprises de sécurité privée (ETS), les organisations doivent réfléchir attentivement aux personnes qu'elles embauchent et à la manière dont elles seront employées. Les gardes dans les bureaux, les maisons d'hôtes et les entrepôts sont souvent le visage public de l'organisation, ce qui les rend essentiels à la sécurité globale au-delà de leurs fonctions de surveillance de base. Il est également crucial d'évaluer les liens potentiels entre les ETS et les acteurs militaires ou politiques, car ils

20 Pour en savoir plus sur «Saving Lives Together», voir <https://gisf.ngo/themes/coordination-for-hsrm/saving-lives-together/>.

21 Pour en savoir plus sur ces défis, voir GISF et Humanitarian Outcomes (2024).

peuvent être liés aux forces de sécurité de l'État, à la police ou à des individus ayant des antécédents de comportements illégaux ou abusifs, notamment des violations des droits humains. L'évaluation des pratiques générales d'une ETS peut s'avérer difficile en raison de la confidentialité et de la complexité des structures de propriété de certaines entreprises.

L'International Code of Conduct Association (ICoCA), créée à la suite du Document de Montreux sur les obligations légales et les bonnes pratiques des sociétés militaires et de sécurité privée, constitue une ressource utile qui fournit des normes de bonnes pratiques aux ETS. L'ICoCA agit en tant qu'organe directeur et de surveillance du Code de conduite international pour les ETS, qui vise à garantir le respect des droits humains, la conformité avec le droit international et la redevabilité en cas de faute professionnelle. Déterminer si une ETS est enregistrée auprès de l'ICoCA peut constituer un élément précieux du processus de diligence raisonnable, car l'association promeut la bonne gouvernance, les droits humains, le droit international humanitaire et des normes professionnelles élevées au sein du secteur de la sécurité privée.

Lorsque l'on envisage de recourir à des ETS, plusieurs facteurs stratégiques, opérationnels et juridiques doivent être pris en compte. Une expertise externe, telle que les conseils d'organismes comme l'ICoCA, peut également s'avérer utile, en particulier si les capacités internes sont limitées. Les organisations peuvent évaluer si le recours à une ETS est conforme à leur mandat et à leur stratégie de sécurité, s'il réduit les risques à long terme et comment il pourrait affecter leur réputation, tant au niveau local qu'international, ainsi qu'évaluer leur capacité à gérer ces prestataires. Il est également important de déterminer si le recours à des ETS pourrait créer un précédent ou contribuer à l'inflation du marché, ce qui pourrait affecter les communautés locales et d'autres acteurs humanitaires. La manière dont les ETS peuvent renforcer la sécurité publique et garantir le respect des réglementations gouvernementales applicables est également un élément important à prendre en considération.

Lors de la vérification des antécédents et du processus de recrutement, il peut être utile de mettre en place des procédures de diligence raisonnable rigoureuses, de disposer de modèles de contrats clairs et de conserver des registres détaillés des performances. Vérifier qu'une entreprise de sécurité privée (ETS) fonctionne selon un code de conduite clair, dispose d'un personnel bien formé avec des règles d'engagement définies et respecte les normes légales peut garantir sa fiabilité. Il est également important de tenir compte des engagements éthiques, des programmes de formation et des mesures anticorruption du prestataire. Les contrats pourraient préciser les exigences en matière de contrôle des performances et de conformité. Il est fortement recommandé de s'assurer que les ETS disposent de mécanismes internes pour traiter les cas de mauvaise conduite et d'abus.

Une surveillance et un contrôle continus des ETS peuvent aider les organisations à s'assurer que les prestataires respectent des normes élevées et protègent à la fois leurs intérêts et ceux du public. Cela peut également contribuer à atténuer les risques cachés, tels que la dépendance excessive à l'égard de prestataires externes, qui pourrait nuire aux

capacités d'une organisation à développer une expertise interne en matière de gestion des risques de sécurité.²²

► Pour une analyse sur le recours à des escortes armées, voir le chapitre 4.2.

2.1.3 Interaction avec les autorités

Le gouvernement d'un pays touché par une crise a certaines responsabilités en matière de sécurité et de protection des organisations humanitaires, qui sont reflétées dans la législation nationale, le droit international humanitaire et les accords conclus entre l'ONU et les pays hôtes. En principe, ces responsabilités sont les suivantes.

- **Assurer la sûreté et sécurité.** En tant que « détenteurs de responsabilités » au premier chef, les gouvernements sont chargés de maintenir l'ordre public, de garantir un environnement sûr et de protéger toutes les personnes et entités contre la violence et la criminalité.
- **Faciliter un accès sécurisé.** Les gouvernements ont la responsabilité de faciliter l'accès humanitaire aux zones qui ont besoin d'aide, en veillant à ce que les travailleurs humanitaires puissent opérer sans restrictions, ingérences ou menaces injustifiées. Cela comprend la délivrance de visas, de permis et de licences.
- **Fournir un cadre juridique et réglementaire.** Adopter et appliquer des lois qui protègent les organisations humanitaires contre le harcèlement, les attaques ou autres menaces visant leur personnel, leurs opérations et leurs biens.
- **Coordination et communication.** Les gouvernements sont tenus de coordonner leurs actions avec les organisations humanitaires, de partager les informations relatives aux menaces, aux risques ou aux incidents en matière de sécurité, et de collaborer à la mise en place de mesures de sûreté.
- **Enquêter et poursuivre les auteurs d'attaques.** En cas d'attaques ou d'incidents impliquant des organisations humanitaires, le gouvernement est chargé d'enquêter, d'appréhender et de poursuivre les auteurs afin de garantir leur redevabilité.
- **Respecter les principes humanitaires.** La neutralité, l'indépendance et l'impartialité des opérations humanitaires doivent être respectées, en évitant toute action susceptible de compromettre ces principes ou de nuire à l'image des organisations humanitaires dans des environnements conflictuels.

En réalité, le gouvernement peut être plus ou moins capable d'assurer un environnement sûr et peut être partie prenante au conflit qui a provoqué la crise humanitaire. Dans de rares cas, tels que les livraisons transfrontalières d'aide humanitaire à la Syrie pendant la guerre civile syrienne sanctionnées par le Conseil de sécurité de l'ONU et les opérations d'aide secrètes pour le Myanmar à la frontière thaïlandaise, les organisations peuvent

22 Pour plus de recommandations sur les bonnes pratiques, voir Davis, J. et al. (2020) 'Module 14, Contracting private security providers' in *Security to go: a risk management toolkit for humanitarian aid agencies*, 4th edition (en anglais, « Module 14, Recrutement d'entreprises de sécurité privée » dans *La sécurité en pratique: boîte à outils de gestion des risques à l'attention des agences humanitaires*, 4e édition). GISF (<https://gisf.ngo/resource/contracting-private-security-providers/>).

opérer sans l'accord ou l'engagement du gouvernement. Les gouvernements varient également dans la mesure où ils dirigent, soutiennent ou participent à la coordination de la réponse humanitaire. Parfois, ils peuvent politiser, entraver, attaquer ou interférer avec l'acheminement de l'aide. Cela peut également être le cas pour les gouvernements étrangers ayant des intérêts militaires ou autres dans le pays en question.

Pour leur part, les organisations humanitaires sont tenues de consulter les autorités gouvernementales et d'obtenir leur accord et leur soutien pour pouvoir intervenir, en expliquant la finalité et les objectifs de leurs activités, même lorsque le gouvernement est partie prenante au conflit ou entrave activement les efforts humanitaires. Un échange continu avec les homologues gouvernementaux concernés, y compris, parfois, les autorités étrangères, est souvent essentiel pour garantir l'action humanitaire, et les organisations peuvent entretenir des relations et des liens durables avec leurs homologues gouvernementaux grâce à des contacts réguliers, des réunions et des visites de courtoisie.

Dans le même temps, il est conseillé au personnel de sécurité de faire preuve de prudence lorsqu'il interagit avec ses homologues gouvernementaux, en particulier dans les contextes où les autorités peuvent être hostiles aux efforts d'aide. Parfois, le simple fait d'utiliser un terme tel que « sécurité » peut éveiller la suspicion ou susciter une attention particulière, ce qui peut entraîner des restrictions sur les opérations ou une surveillance accrue de l'organisation. Il est utile d'aborder ces interactions avec tact, en définissant clairement les objectifs afin d'éviter tout malentendu, tout en restant vigilant face à toute tentative du gouvernement d'exploiter ces interactions à des fins de collecte d'informations ou de nuire aux activités de l'organisation. La coordination avec d'autres acteurs humanitaires, par le biais de réseaux de collaboration établis, peut faciliter ces interactions.

Lorsqu'elles interviennent dans des situations de crise, les organisations humanitaires peuvent également avoir besoin de se mettre en relation avec des acteurs infranationaux, tels que les autorités régionales ou locales. Bien qu'ils ne disposent pas de la même autorité que les gouvernements nationaux, ces acteurs exercent souvent une influence considérable dans des zones spécifiques. Établir des relations avec les autorités infranationales peut être essentiel pour garantir l'accès humanitaire, en particulier dans les régions où l'influence du gouvernement central est limitée ou lorsqu'il est nécessaire de collaborer avec plusieurs autorités de facto différentes. Une communication claire du mandat humanitaire de l'organisation, mettant l'accent sur la neutralité et l'impartialité, peut contribuer à apaiser les tensions et à instaurer la confiance. Les acteurs infranationaux peuvent avoir leurs propres intérêts, ce qui pourrait avoir une incidence sur la sécurité et la perception des efforts d'aide. Il peut être bénéfique d'engager un dialogue constant et de travailler en coordination avec d'autres acteurs de l'aide, ainsi qu'avec des dirigeants communautaires de confiance.

Acteurs armés non étatiques

Dans les zones de conflit où des groupes armés non étatiques contrôlent le territoire, les organisations humanitaires peuvent être amenées à établir un dialogue afin de négocier l'accès et d'assurer la sûreté de leur personnel. Les acteurs non étatiques peuvent avoir des approches très différentes en matière d'aide humanitaire : certains reconnaissent et facilitent l'accès, tandis que d'autres peuvent se montrer plus hostiles.

Le dialogue avec ces acteurs nécessite une préparation minutieuse, notamment une bonne compréhension de leurs motivations, de leurs affiliations politiques et de leurs relations avec les autres parties au conflit, ainsi qu'avec les communautés locales. Même les interactions quotidiennes peuvent être difficiles et, outre les risques de sécurité, peuvent créer des dilemmes concernant les principes humanitaires et les lignes rouges propres à l'organisation. Le Centre of Competence on Humanitarian Negotiation (CCHN, Centre de compétence sur les négociations humanitaires) a été créé par le Comité international de la Croix-Rouge (CICR) et d'autres organisations afin d'apporter un soutien, d'assurer la coordination et de renforcer les capacités en matière de négociations humanitaires. Il peut constituer une ressource importante.¹

Avant d'entamer tout dialogue avec des acteurs armés non étatiques, il est recommandé aux organisations :

- De définir la portée et les objectifs de l'interaction.
- D'analyser le contexte spécifique dans lequel le dialogue va se dérouler.
- De cartographier les différents acteurs et de comprendre les motivations et les intérêts (déclarés et cachés) de chacun d'entre eux.
- De comprendre les groupes que ces acteurs représentent (le cas échéant).
- D'élaborer et de convenir d'une stratégie d'accès adaptée au contexte.
- De s'accorder sur ce qui est négociable et ce qui ne l'est pas en termes de politiques, de principes, de mandats et de ressources.
- De se concerter/coordonner avec d'autres organisations travaillant dans le même espace afin de comprendre leur position en matière d'accès et de partager leurs expériences.
- De comprendre le statut juridique (au niveau local et international) de ces acteurs.

¹ Voir <https://frontline-negotiations.org/home/discover/about-us/>

- *Pour plus d'informations sur les interactions avec les acteurs armés, voir le chapitre 4.2 – Élaboration d'une stratégie de sécurité.*

2.1.4 Interaction avec les armées

Coordination civilo-militaire

Les militaires sont souvent des acteurs clés dans les contextes de crise, soit parce qu'ils sont engagés dans des conflits armés, soit parce que les gouvernements touchés par une crise font parfois appel aux forces militaires nationales et internationales et à leurs ressources pour apporter des secours dans des situations d'urgence complexes. Dans les deux cas, la coordination entre les acteurs militaires et humanitaires est souvent essentielle pour faciliter la sécurité des opérations humanitaires.

Les principales entités de coordination entre les organisations humanitaires et les armées sont les suivantes.

- **Coordination civilo-militaire humanitaire des Nations Unies (UN-CMCoord)** sous l'égide du Bureau de la coordination des affaires humanitaires des Nations Unies (OCHA). L'UN-CMCoord maintient le dialogue avec l'armée et les autres acteurs armés, y compris les groupes armés non étatiques, afin de promouvoir l'interaction et la coopération entre tous les acteurs, conformément à la résolution 46/182 de l'Assemblée générale des Nations Unies et aux directives existantes en matière de coordination civilo-militaire.
 - **Centres d'opérations civilo-militaires (CMOC).** Les CMOC sont des centres de coordination physique établis dans des zones de conflit ou de catastrophe, où les organisations militaires, gouvernementales et humanitaires peuvent partager des informations et coordonner leurs activités. Ils servent souvent de plaque tournante pour la communication et la planification.
 - **Groupes de travail sur l'accès humanitaire.** À l'initiative de l'OCHA, les organisations humanitaires ont collaboré dans des environnements instables et difficiles d'accès au moyen de groupes de travail sur l'accès humanitaire. Ces groupes peuvent servir de point d'entrée pour le dialogue avec les acteurs militaires, permettant aux organisations humanitaires de communiquer leurs priorités, de négocier un passage sûr et de plaider en faveur du respect des principes humanitaires.
- *Pour en savoir plus sur les groupes de travail et les négociations sur l'accès, voir le chapitre 3.2 – Accès et sécurité.*

Il est important de noter que les mécanismes de coordination spécifiques utilisés peuvent varier en fonction du contexte et de la nature de la crise. Le cadre de coordination civilo-militaire des Nations Unies offre une certaine souplesse dans l'adaptation des stratégies de coordination, allant de la coopération à la coexistence,

en fonction de la situation spécifique. Les accords de liaison et la formation commune jouent un rôle crucial dans la facilitation d'une coordination efficace entre les acteurs humanitaires et militaires. Le *Manuel de terrain de la coordination civilo-militaire des Nations Unies* décrit divers éléments et tâches de coordination, notamment l'établissement d'un dialogue, le partage d'informations et le suivi des activités militaires afin de s'assurer qu'elles n'ont pas d'impact négatif sur l'action humanitaire.²³

Les activités de coordination civilo-militaire peuvent être particulièrement délicates dans les situations de conflit où l'interaction avec les acteurs militaires peut être perçue comme compromettant la neutralité, l'impartialité et l'indépendance opérationnelle des acteurs humanitaires. Dans de telles situations, les organisations humanitaires s'efforcent souvent de maintenir une distance opérationnelle et d'éviter de dépendre excessivement des moyens et des services militaires pour leur protection et leur soutien logistique.

Système de notification humanitaire

Le système de notification humanitaire pour la déconfliction (HNS4D) vise à renforcer la sécurité des opérations humanitaires en informant les acteurs militaires de l'emplacement des installations, des déplacements et des activités humanitaires dans les zones de conflit. Son objectif est de minimiser le risque d'attaques accidentelles contre le personnel et les infrastructures humanitaires en veillant à ce que les forces militaires soient informées de l'existence de ces sites protégés.

Le HNS4D exige des organisations qu'elles soumettent des informations détaillées sur leurs installations, leur personnel et leurs déplacements prévus à un intermédiaire, généralement l'OCHA. Ces informations comprennent souvent les coordonnées GPS, la description des installations et la nature de leurs activités. L'OCHA consolide ensuite ces informations et les partage avec les acteurs militaires concernés afin de s'assurer qu'ils disposent de données actualisées et précises sur les opérations humanitaires dans la zone. Le processus vise à fournir un niveau de protection, avec des mises à jour régulières afin de maintenir l'exactitude des informations à mesure que les opérations évoluent.

Il est arrivé que des organisations humanitaires perdent confiance dans le HNS4D en raison d'échecs répétés et d'un manque de garanties de la part de leurs homologues militaires. En Syrie, en Afghanistan et à Gaza, l'armée internationale a bombardé des installations gérées par des ONG, alors même que les organisations humanitaires avaient fourni à plusieurs reprises des informations et les coordonnées de ces sites. Une compréhension réaliste des capacités et des limites du HNS4D devrait guider les décisions des organisations en matière d'interaction.²⁴

23 UN-CMCoord (2018) *Manuel de terrain de la coordination civilo-militaire des Nations Unies*. Version 2.0. OCHA (<https://gisf.ngo/wp-content/uploads/2021/11/E-Version-UNCMCoord-Field-Handbook-2.0-2018.pdf>).

24 Pour en savoir plus, voir GISF et Humanitarian Outcomes (2024).

2.1.5 Autres acteurs non humanitaires

Un large éventail d'autres acteurs peut également être présent, notamment des entreprises, des institutions financières locales et des groupes communautaires, qui peuvent apporter un soutien logistique et opérationnel. Les acteurs du développement, les organisations de la société civile locales et les groupes de défense des droits humains ont souvent des engagements à long terme dans de nombreuses zones et peuvent apporter des informations et un soutien précieux. En interagissant avec ces entités, les humanitaires peuvent également s'assurer que leurs interventions complètent les efforts existants, en évitant ainsi de perturber le travail en cours de ces groupes et en favorisant une réponse plus durable et ancrée localement.

Informations complémentaires

Recherche et analyse

Bebbington, C. et al. (2022) *Reviewing guidance and perspectives on humanitarian notification systems for deconfliction* (en anglais, « Examen des orientations et des perspectives relatives aux systèmes de notification humanitaire pour la déconfliction »). Centre pour les droits humains et les études humanitaires, Institut Watson pour les affaires internationales et publiques, Université Brown, et Programme de réponse humanitaire, Collège de guerre maritime opérationnelle, Collège de guerre navale des États-Unis (<https://watson.brown.edu/chrhs/files/chrhs/imce/research/2022%20HNS4D%20Research%20Paper%20-%20CHRHS%20%26%20HRP.pdf>).

GISF et Humanitarian Outcomes (2024) *State of practice: The evolution of security risk management in the humanitarian space* (en anglais, « État des lieux: l'évolution de la gestion des risques de sécurité dans le domaine humanitaire ») (https://humanitarianoutcomes.org/security_risk_mgmt_humanitarian_space_2024).

GISF (2023) 'Humanitarian notification systems: Unpacking the complexities and possibilities (No. 3)' [Podcast] in *Evolving NGO security risk management* (en anglais « Systèmes de notification humanitaire: décrypter les complexités et les possibilités (n° 3) » [Podcast] dans *Évolution de la gestion des risques de sécurité des ONG*) (<https://gisf.ngo/resource/evolving-ngo-security-risk-management-ep3-humanitarian-notification-systems-unpacking-the-complexities-and-possibilities-gisf-podcast/>).

ONU OCHA (2021) *Concept note on humanitarian notification in support of access and protection in Syria* (en anglais et en arabe, « Note conceptuelle sur la notification humanitaire à l'appui de l'accès et de la protection en Syrie ») (<https://reliefweb.int/report/syrian-arab-republic/concept-note-humanitarian-notification-support-access-and-protection>).

Recommandations et ressources

Comité permanent interorganisations (IASC) (2013) *IASC non-binding guidelines on the use of armed escorts for humanitarian convoys* (en anglais, « Directives non contraignantes du IASC relatives à l'utilisation d'escortes armées pour les convois humanitaires ») (<https://reliefweb.int/report/world/iasc-non-binding-guidelines-use-armed-escorts-humanitarian-convoys>).

Davis et al. (2020) 'Module 14, Contracting private security providers' in *Security to go: a risk management toolkit for humanitarian aid agencies*, 4th edition. (en anglais, « Module 14, Recrutement d'entreprises de sécurité privée » dans *La sécurité en pratique: boîte à outils de gestion des risques à l'attention des agences humanitaires*, 4e édition). GISF (<https://gisf.ngo/resource/contracting-private-security-providers/>).

GISF (2022) *NGO security collaboration guide* (en anglais, « Guide de collaboration en matière de sécurité des ONG ») (<https://gisf.ngo/long-read/ngo-security-collaboration-guide/>).

GISF (n.d.a) 1. *Collaboration des ONG en matière de sécurité*. NGO Security Toolbox (<https://gisf.ngo/toolbox-pwa-fr/resource/1-collaboration-des-ong-en-matiere-de-securite/>).

GISF (n.d.b) « Saving Lives Together » (<https://gisf.ngo/themes/coordination-for-hsrm/saving-lives-together/>).

Haut-Commissariat des Nations Unies pour les réfugiés (HCR) (2020) *Manuel d'urgence: Coordination civilo-militaire* (<https://emergency.unhcr.org/coordination-and-communication/working-others/civil-military-coordination>).

International Code of Conduct Association (2021), « Le code de conduite international des prestataires de services de sécurité privée » (<https://icoca.ch/the-code/>).

ONU OCHA (n.d.) 'Civil-military coordination' (en anglais, « Coordination civilo-militaire ») (www.unocha.org/es/node/62).

UN-CMCoord (2018), *Manuel de terrain de la coordination civilo-militaire des Nations Unies*. Version 2.0 (<https://gisf.ngo/wp-content/uploads/2021/11/E-Version-UNCMCoord-Field-Handbook-2.0-2018.pdf>).

2.2 Plaidoyer et sécurité

La relation entre le plaidoyer et la sécurité dans le secteur humanitaire peut être complexe, le plaidoyer présentant à la fois des risques et des opportunités pour la sécurité des travailleurs humanitaires. Le personnel de sécurité peut jouer un rôle crucial en veillant à ce que les efforts de plaidoyer ne compromettent pas les efforts de gestion des risques de sécurité, mais renforcent plutôt les mesures de sécurité.

2.2.1 Plaidoyer dans le secteur humanitaire

Le plaidoyer humanitaire vise à influencer les politiques et le comportement des acteurs puissants au profit des personnes touchées par une crise. Il s'agit notamment de sensibiliser aux besoins humanitaires, d'appeler à la protection des civils dans les conflits et de faire pression pour que les activités humanitaires bénéficient d'un accès sûr et sans entrave. Le plaidoyer recoupe souvent les efforts visant à garantir l'accès et s'appuie également sur le droit international humanitaire et les droits humains. Les organisations humanitaires peuvent également mener des actions de plaidoyer afin de promouvoir des changements sociaux, économiques ou politiques spécifiques visant à améliorer les conditions de vie des personnes marginalisées ou défavorisées.

Les organisations peuvent mener ces actions de plaidoyer par divers moyens, tant en public qu'en coulisses.

- **Le plaidoyer public** consiste à s'exprimer ouvertement sur des questions, souvent au moyen de campagnes médiatiques et de déclarations publiques. Il vise à sensibiliser l'opinion publique, à mobiliser le soutien et à faire pression sur les décideurs en attirant l'attention sur les injustices ou les besoins humanitaires.
- **Le plaidoyer privé** peut impliquer des négociations en coulisses, des appels directs et des discussions confidentielles avec des représentants du gouvernement, des groupes armés et d'autres détenteurs de pouvoir ou d'influence. L'objectif peut être d'assurer un accès sûr aux travailleurs humanitaires, d'influencer discrètement les politiques ou de résoudre des problèmes spécifiques sans attirer l'attention du public.

Les organisations doivent souvent trouver un équilibre entre ces différentes approches, en choisissant la méthode la plus appropriée en fonction du contexte, des risques potentiels et des résultats souhaités. Cependant, quelle que soit la structure et l'approche d'une organisation, l'efficacité du plaidoyer peut dépendre de la manière dont celui-ci s'aligne sur les objectifs stratégiques globaux et dont il est soutenu par des mesures de gestion des risques de sécurité visant à atténuer les impacts négatifs potentiels.²⁵

25 Humanitarian Outcomes (2024) *Aid worker security report 2024: balancing advocacy and security in humanitarian action*.

Au sein de certaines organisations à mandats multiples, il existe une tension entre les activités humanitaires traditionnelles et le travail de plaidoyer. Alors que le travail humanitaire est exposé à des menaces telles que la criminalité, le travail de plaidoyer présente différents types de risques, tels que le harcèlement par les autorités, l'emprisonnement, l'expulsion du pays, la fermeture d'activités ou la saisie de documents et d'ordinateurs.

Dans de nombreux contextes, les gouvernements adoptent des positions plus extrêmes, faisant des ONG ayant des programmes politiques des cibles privilégiées, et ciblant même les organisations dont le mandat est davantage axé sur la prestation de services que sur le plaidoyer. La mise en œuvre de mesures d'atténuation efficaces dans ces cas peut s'avérer difficile, car les organisations humanitaires sont confrontées à toute la puissance de l'appareil gouvernemental qui s'oppose à elles. Établir des contacts au sein du gouvernement et faire appel à des experts juridiques spécialisés peut contribuer à réduire ces risques. Si les acteurs de l'aide nationale et internationale sont touchés, le personnel des organisations nationales est susceptible d'être plus vulnérable.

2.2.2 Plaidoyer et sécurité

Le plaidoyer peut avoir des répercussions tant positives que négatives sur la sécurité des travailleurs humanitaires et sur l'environnement général de sécurité dans lequel ils opèrent.

Interactions négatives potentielles

- **Risques accrus.** Le plaidoyer, en particulier lorsqu'il implique de remettre en question des acteurs puissants ou des politiques gouvernementales, peut provoquer des réactions négatives, notamment du harcèlement, des arrestations, des expulsions et même des attaques violentes contre les travailleurs humanitaires. Dans les pays où l'espace civique se réduit, comme le Nicaragua et le Myanmar, les efforts de plaidoyer ont conduit à des mesures répressives de la part du gouvernement, notamment l'expulsion d'organisations et le personnel pris pour cible.
- **Accès compromis.** Les campagnes de plaidoyer public peuvent entraîner des restrictions d'accès aux populations touchées lorsque les gouvernements ou les acteurs non étatiques perçoivent ces efforts comme hostiles ou comme portant atteinte à leur autorité.
- **Risque d'être pris pour cible.** Le fait de s'exprimer sur des questions sensibles, telles que les violations des droits humains, peut exposer les organisations humanitaires et leur personnel à des actes de violence, les actions de plaidoyer pouvant entraîner des attaques directes contre les travailleurs humanitaires.

Exemple de cas : Restriction de l'espace civique

En 2022, le gouvernement nicaraguayen a promulgué des lois et des résolutions qui ont entraîné l'annulation de l'enregistrement légal de plus de 770 ONG et fondations, les contraignant de fait à fermer leurs portes. Ces actions ont eu un impact sur un large éventail d'organisations, notamment celles qui se consacrent aux services médicaux, à la protection de l'enfance, aux droits des femmes et au changement climatique. Depuis 2018, le gouvernement a révoqué l'enregistrement de plus de 950 organisations, restreignant considérablement l'espace civique et entravant les capacités des ONG à fonctionner et à défendre les groupes marginalisés.

Interactions positives potentielles

- **Le plaidoyer comme outil de protection.** Lorsqu'il s'inscrit dans le cadre des efforts de gestion des risques de sécurité, le plaidoyer peut contribuer à renforcer la protection des travailleurs humanitaires en encourageant le respect du droit international humanitaire et en sensibilisant à la nécessité de protéger les opérations humanitaires. Des campagnes telles que #NotATarget («#PasuneCible») ont pour but de sensibiliser le public afin de réduire la violence à l'encontre des travailleurs humanitaires.
- **Tirer parti du plaidoyer pour la sécurité.** Le personnel de sécurité peut utiliser des outils de plaidoyer pour favoriser l'acceptation et le soutien des opérations d'aide au sein des communautés locales, réduisant ainsi le risque d'attaques.
- **Plaidoyer en matière de justice.** Le plaidoyer en faveur de la justice pour les travailleurs humanitaires peut inclure des efforts visant à tenir les auteurs d'attaques, de harcèlement et de violations à l'encontre du personnel humanitaire pour redevables. Les organisations ont tout intérêt à établir des protocoles clairs précisant quand et comment mener des actions de plaidoyer en matière de la justice, en veillant à ce que toute action de plaidoyer s'appuie sur un processus solide d'évaluation des risques.
- **Plaidoyer collaboratif.** La formation d'alliances avec d'autres organisations, des experts juridiques et des organismes internationaux peut amplifier le message tout en partageant les risques associés.

Le plaidoyer présente des limites importantes. Bien qu'il ait permis d'obtenir certains changements politiques, tels que les résolutions du Conseil de sécurité sur la protection des travailleurs humanitaires,²⁶ il s'est révélé largement inefficace dans la pratique pour influencer les acteurs étatiques impliqués dans des conflits armés : voir,

26 Par exemple, la résolution 2730 (2024) du Conseil de sécurité de l'ONU sur la protection du personnel humanitaire et du personnel de l'ONU et associé dans les conflits armés ([https://docs.un.org/en/S/RES/2730\(2024\)](https://docs.un.org/en/S/RES/2730(2024))).

par exemple, les conflits à Gaza et au Soudan, où les acteurs étatiques ont continué à entraver et à mettre en danger les opérations humanitaires malgré d'importants efforts de plaidoyer.²⁷

2.2.3 Impliquer le personnel de sécurité dans le plaidoyer

Le personnel de sécurité peut jouer un rôle important en veillant à ce que les initiatives de plaidoyer améliorent les résultats en matière de sécurité et ne compromettent pas la sécurité des travailleurs humanitaires.

Soutenir le plaidoyer pour renforcer la sécurité

- **Utiliser les données sur la sécurité pour mener le plaidoyer.** Le personnel de sécurité peut fournir des données précieuses sur les incidents, les menaces et le contexte local afin de soutenir les efforts de plaidoyer. Par exemple, les données sur les incidents peuvent mettre en évidence les zones où les travailleurs humanitaires sont le plus à risque, ce qui peut ensuite être utilisé pour plaider en faveur de meilleures mesures de protection auprès des gouvernements et des groupes armés.
- **Soutenir les campagnes de plaidoyer public.** Les équipes de sécurité peuvent contribuer à l'élaboration de campagnes de plaidoyer public en fournissant des informations sur les implications des différents messages et stratégies en matière de sécurité. Cela permet de garantir que les campagnes sont non seulement efficaces pour sensibiliser le public, mais aussi pour assurer la sécurité du personnel.

Veiller à ce que les efforts de plaidoyer ne compromettent pas la sécurité

- **Directives internes.** Une approche structurée avec des directives claires qui intègrent les considérations de sécurité dans les efforts de plaidoyer est bénéfique. Cela peut inclure des protocoles pour s'exprimer, déterminer quand et comment communiquer avec les médias et veiller à ce que toute déclaration publique soit soigneusement examinée afin de ne pas mettre en danger le personnel. Une bonne politique organisationnelle pourrait consister à évaluer d'abord l'impact probable sur le personnel et les opérations, et à solliciter l'avis du personnel de sécurité et des membres du personnel les plus susceptibles d'être touchés, avant de faire une déclaration publique sur une situation particulière.
- **Approche équilibrée.** Le maintien d'un équilibre entre le plaidoyer public et privé peut contribuer à garantir que les efforts déployés n'exposent pas involontairement le personnel à des risques supplémentaires ou n'entravent pas les activités humanitaires en cours.
- **Évaluation des risques et coordination.** Avant de lancer toute initiative de plaidoyer, il peut être utile de procéder à une évaluation des risques potentiels pour le personnel et les opérations en raison des activités de plaidoyer. Cela peut impliquer d'analyser l'environnement politique, de comprendre le potentiel de réactions négatives et d'évaluer la manière dont les messages de plaidoyer pourraient être perçus par différents acteurs. L'évaluation des risques devrait idéalement inclure la prise en compte des impacts à court et à long terme sur les

27 Humanitarian Outcomes (2024) *Aid worker security report 2024: balancing advocacy and security in humanitarian action*

travailleurs humanitaires nationaux et les organisations partenaires, le cas échéant.

- **Mesures d'atténuation.** Le personnel de sécurité peut aider à concevoir et à mettre en œuvre des mesures d'atténuation afin de protéger le personnel pendant les campagnes de plaidoyer.
- **Analyse risques-avantages.** Les organisations ont souvent du mal à trouver un équilibre entre les risques immédiats du plaidoyer et les avantages potentiels à long terme, en raison du manque de données mesurables et de cadres permettant d'évaluer les risques. Pour remédier à cela, les organisations pourraient mettre en place un cadre d'analyse risques-avantages qui compare les conséquences négatives potentielles aux impacts positifs attendus du plaidoyer. Ce cadre pourrait consister à identifier et à classer les risques potentiels, à évaluer les avantages attendus des activités et à utiliser un système de notation pour les comparer entre eux. La planification de scénario peut aider à explorer les résultats possibles, et des mesures d'atténuation peuvent être élaborées pour faire face aux risques identifiés. Un suivi et une réévaluation continus permettraient d'apporter des ajustements en fonction de l'évolution de la situation, et la documentation des résultats peut aider à constituer un ensemble de preuves qui serviront de base aux futurs efforts de plaidoyer.

Checklist des bonnes pratiques

- **Mettre à profit les outils existants.** Utiliser et diffuser des outils éprouvés d'évaluation des risques du plaidoyer, tels que l'outil de suivi de l'espace civique d'Oxfam.
- **Promouvoir le plaidoyer collectif.** Encourager les différents acteurs (forums d'ONG, OCHA, autorités du pays donateur) à mener un plaidoyer collectif, en faisant appel à des acteurs non opérationnels pour instaurer un dialogue plus ferme avec les autorités.
- **Intégrer la sécurité dans la planification du plaidoyer.** Intégrer la gestion des risques de sécurité dans les activités de plaidoyer, en veillant à ce que toutes les activités soient fondées sur des évaluations des risques complètes et mises en œuvre avec des mesures d'atténuation des risques.
- **Plaidoyer privé en premier lieu.** Partager les messages de plaidoyer en privé avec les acteurs ciblés avant de les rendre publics.

- **Faire appel aux hauts responsables et à des messagers externes.** Faire appel aux hauts responsables, à du personnel basé à l'étranger ou à des organisations tierces pour diffuser des messages de plaidoyer (les informations relatives aux abus peuvent par exemple être discrètement communiquées à des organisations de défense des droits humains).
- **Identifier les voies de progression.** Établir des voies claires pour faire progresser les messages de plaidoyer, en tenant informées les autres organisations et les parties prenantes concernées.
- **Plan d'urgence en cas d'opposition.** Se préparer à une éventuelle opposition, notamment sous forme de harcèlement ou de violence, en établissant des contacts et en s'assurant un soutien juridique.
- **Suivre l'impact du plaidoyer.** Mettre en place des mécanismes permettant de suivre les impacts positifs et négatifs des efforts de plaidoyer, notamment sur la sécurité des travailleurs humanitaires.
- **Suivre et exploiter les données sur les incidents.** Suivre les incidents de violence ou de harcèlement et utiliser ces données pour plaider en faveur de la protection des travailleurs humanitaires.
- **Évaluer les stratégies de plaidoyer pour la protection des travailleurs humanitaires.** Développer des outils permettant d'évaluer systématiquement les avantages et les inconvénients des différentes approches de plaidoyer dans la lutte contre la violence à l'encontre des travailleurs humanitaires.

Source: Humanitarian Outcomes (2024) *Aid Worker Security Report 2024: balancing advocacy and security in humanitarian action* (en anglais, «Rapport 2024 sur la sécurité des travailleurs humanitaires: trouver un équilibre entre plaidoyer et sécurité dans l'action humanitaire») (www.humanitarianoutcomes.org/AWSR_2024).

2.2.4 Conséquences des relations avec les médias sur la sécurité

Les organisations humanitaires font appel aux médias pour diverses raisons, notamment pour le plaidoyer, ce qui peut avoir des conséquences sur la sécurité. Une déclaration mal formulée, inexacte ou incendiaire peut mettre le personnel en danger direct et même entraîner son expulsion d'un pays. Il arrive parfois que les objectifs du service communication basé au siège et ceux du personnel sur le terrain soient contradictoires. Ce qui renforce la visibilité d'une organisation à l'échelle internationale peut ne pas contribuer à instaurer la confiance auprès des communautés et des autorités locales. Un système clair peut être mis en place pour éviter les incidents négatifs.

- **Contact avec les médias.** Définir clairement qui est responsable des contacts avec les médias, de la rédaction des communiqués de presse et des déclarations publiques (y compris sur les médias sociaux).
 - **Approbation des déclarations publiques.** Pour des raisons de sécurité, il est conseillé que le responsable de l'organisation dans le pays ait autorité finale sur les messages destinés aux médias, en impliquant le personnel de sécurité, le personnel régional et le personnel du siège social, selon le cas.
 - **Porte-paroles autorisés.** Identifier et former le personnel autorisé à mener des entretiens, en veillant à ce qu'il soit bien préparé. Cela peut se limiter aux hauts responsables dans le pays ou à des personnes ayant des qualifications similaires.
 - **Planification d'une stratégie médiatique en cas de crise.** Une approche peut être élaborée et convenue avant que la crise ne survienne, avec des déclarations préparées à l'avance pour différents scénarios. L'engagement doit être opportun et pertinent, en se concentrant sur les événements actuels afin de maximiser l'impact et d'éviter les retards.
- *Pour en savoir plus sur la communication en cas de crise ou d'incident critique, voir le chapitre 6.1.*

Définir les objectifs et formuler le message

Quel que soit l'objectif du travail médiatique – par exemple, faire avancer les objectifs de plaidoyer ou améliorer la visibilité publique pour la collecte de fonds –, les organisations devront trouver un équilibre entre cet objectif et les préoccupations en matière de sécurité. Par exemple, un communiqué de presse accusant un groupe armé particulier de violence contre des civils pourrait provoquer la colère de ce groupe et mettre le personnel à risque. Il peut être utile de préparer une liste de questions et de réponses possibles avant une interview afin de garder les messages ciblés, en gardant à l'esprit la façon dont les réponses pourraient être reçues compte tenu du contexte et de l'environnement de sécurité.

Fixer des règles de base

Les interviews avec les médias requièrent de la pratique et de l'expertise. Il est facile de se laisser déstabiliser par une question provocante et de dire quelque chose d'imprévu.

- **Faire attention à ne pas attribuer la responsabilité d'une crise.** Dans de nombreuses situations d'urgence politique complexes, il n'est pas toujours possible de déterminer sans équivoque qui est responsable. Il est important de convenir à l'avance d'une réponse institutionnelle à donner aux médias. Le personnel doit faire preuve de prudence lorsqu'il transmet des informations et s'assurer qu'elles ont été vérifiées par une source fiable ; si ce n'est pas le cas, il doit le dire clairement. La propagation de rumeurs inexacts pourrait exacerber les tensions.

- **Veiller à ce qu'il y ait une compréhension mutuelle des commentaires «officiels».** Le personnel doit s'efforcer d'être clair avec les journalistes lorsqu'il fait des commentaires officiels et vérifier comment les différents éléments de son interview seront imputables. Certaines formes courantes de dissimulation légère dans les reportages des médias, telles que «une source haut placée à l'ONU» ou «des agences d'aide humanitaire opérant dans la zone de conflit», peuvent ne pas être très efficaces. Il se peut qu'il n'y ait que quelques organisations humanitaires de ce type et que l'identité de la source soit évidente.

Enfin, comme mentionné précédemment, toutes les questions ne nécessitent pas l'attention des médias, et il peut être approprié de discuter à l'avance des préoccupations éventuelles avec les acteurs cibles afin de voir si les problèmes peuvent être résolus par d'autres moyens.

Informations complémentaires

Recherche et analyse

Humanitarian Outcomes (2024) *Aid worker security report 2024: balancing advocacy and security in humanitarian action* (en anglais, «Rapport 2024 sur la sécurité des travailleurs humanitaires: trouver un équilibre entre plaidoyer et sécurité dans l'action humanitaire») (www.humanitarianoutcomes.org/AWSR_2024).

Legal Action Worldwide (2024) *Justice and accountability for attacks on aid workers: What are the barriers and how to overcome them?* (en anglais, «Justice et redevabilité pour les attaques contre les travailleurs humanitaires : quels sont les obstacles et comment les surmonter ? ») (<https://legalactionworldwide.org/accountability-rule-of-law/report-justice-and-accountability-for-attacks-on-aid-workers-what-are-the-barriers-and-how-to-overcome-them/>).

Magone, C., Neuman, M. et Weissman, F. (2012) *Agir à tout prix? Négociations humanitaires: l'expérience de MSF*. Centre de réflexion sur l'action et les savoirs humanitaires (CRASH) (<https://msf-crash.org/en/war-and-humanitarianism/humanitarian-negotiations-revealed-msf-experience>).

Rubenstein, L. et Fairbanks, A. (2018) *Evidence based advocacy: how incident information can help* (en anglais, «Plaidoyer fondé sur des données probantes: comment les informations sur les incidents peuvent aider»). GISF (www.gisf.ngo/evidence-based-advocacy-how-incident-information-can-help/).

Slim, H. (2022) *La résistance humanitaire: son importance éthique et opérationnelle*. Network Paper 87. Humanitarian Practice Network (<https://odihpn.org/publication/humanitarian-resistance-its-ethical-and-operational-importance/>).

Recommandations

CARE International (2014) *Manuel de plaidoyer de CARE International* (www.care-international.org/resources/care-international-global-advocacy-handbook).

Davidson, S. (2013) *Gérer le message: gestion de la communication et des médias en cas de crise de sécurité*. EISF (<https://gisfprod.wpengine.com/resource/managing-the-message/>).

GISF (2021) *Partenariats et gestion du risque sécurité: guide d'action conjointe pour les organisations humanitaires locales et internationales* (<https://gisf.ngo/resource/partnerships-and-security-risk-management-a-joint-action-guide-for-local-and-international-aid-organisations/>).

ICVA – International Council of Voluntary Agencies (Conseil international des agences bénévoles, 2017) *Guide de plaidoyer pour forum ONG* (www.icvanetwork.org/resource/ngo-fora-advocay-guide-delivering-joint-advocay/).

Tactical Tech (n.d.) *Holistic security manual (en anglais, « Manuel de sécurité holistique »)* (<https://holistic-security.tacticaltech.org/>).

Outils

Groupe de travail sur la protection de l'action humanitaire (2018) *Boîte à outils: répondre à la violence contre l'action humanitaire au niveau politique* (<https://alnap.org/help-library/resources/toolkit-responding-to-violence-against-humanitarian-action-on-the-policy-level/>).

Oxfam (2019) *Outil pour suivi de l'espace civique* (<https://policy-practice.oxfam.org/resources/civic-space-monitoring-tool-understanding-what-is-happening-in-civic-space-at-a-620874/>).

3 Éléments organisationnels : structures et instruments politiques

3.1 Le système de gestion des risques de sécurité humanitaire

Ce chapitre décrit certains des éléments clés du système de gestion des risques de sécurité d'une organisation, à savoir les instruments politiques organisationnels, les structures, les rôles et les responsabilités impliqués dans la réduction des risques pour le personnel et l'accomplissement du devoir de diligence.

3.1.1 Cadre de gestion du risque de sécurité

La gestion des risques de sécurité implique de nombreux processus et recoupe différents domaines de travail et fonctions. Pour faciliter la planification et la mise en œuvre de la gestion des risques de sécurité, il peut être utile de visualiser un cadre reflétant l'architecture, les structures, les processus et les dispositifs de gestion des risques de sécurité de l'ensemble d'une organisation, qui reposent tous sur l'objectif fondamental d'assurer un accès plus sûr et de remplir le devoir de diligence au moyen d'une approche centrée sur la personne (voir la figure 4).

Les différents éléments de ce cadre sont examinés plus en détail dans divers chapitres de la présente RBP.

Figure 4 Exemple de cadre de gestion du risque de sécurité



3.1.2 Politique de sécurité

Aperçu

Une politique de sécurité est un document de gouvernance essentiel qui est généralement approuvé par le conseil d'administration de l'organisation ou un organe similaire faisant autorité. Cette politique reflète la culture et les valeurs de l'organisation, et décrit comment celle-ci entend respecter son devoir de diligence tout en poursuivant ses objectifs stratégiques. Une politique de sécurité bien définie permet non seulement de traiter les risques opérationnels, mais aussi de promouvoir une culture de la vigilance

et de la responsabilité. La politique de sécurité doit être élaborée en fonction des objectifs et des modalités opérationnelles de l'organisation. Dans le contexte du cadre de gouvernance d'une organisation, la politique de sécurité sert de document fondamental qui soutient son orientation stratégique globale et son intégrité opérationnelle. Idéalement, cette politique ne devrait pas être élaborée de manière isolée, mais être reliée à d'autres documents de gouvernance afin de garantir une approche cohérente dans l'ensemble de l'organisation.²⁸

Éléments d'une politique de sécurité

Les documents relatifs à la politique de sécurité peuvent comprendre les éléments suivants.

- **Déclaration d'approche.** Elle décrit l'approche générale de l'organisation en matière de sécurité, y compris sa structure de gouvernance. La déclaration peut également indiquer si l'organisation adopte une approche centrée sur la personne (*voir chapitre 1.2*). Elle peut préciser le champ d'application de la politique et les personnes auxquelles elle s'applique, notamment le personnel, les bénévoles, les consultants, les travailleurs occasionnels et les partenaires organisationnels. Elle aide tous les membres de l'organisation à comprendre leur rôle et les attentes en matière de sécurité qui leur sont imposées.
- **Rôles et responsabilités.** Les rôles et responsabilités spécifiques liés à la gestion des risques de sécurité au sein de l'organisation. Cela définit la hiérarchie et les mécanismes de redevabilité, en veillant à ce que chacun, de la direction générale au personnel opérationnel, comprenne le rôle qu'il joue dans le maintien de la sécurité.
- **Exigences minimales de sécurité.** Les exigences minimales de sécurité que l'organisation attend de son personnel sur chaque site opérationnel. Elles peuvent être utiles pour standardiser les pratiques de sécurité et garantir une approche cohérente dans l'ensemble de l'organisation. (Voir ci-dessous pour plus d'informations.)
- **Intégration avec d'autres politiques.** La politique de sécurité doit être liée à d'autres documents politiques pertinents de l'organisation, tels que ceux relatifs à la coordination civilo-militaire, à l'exploitation, les abus et le harcèlement sexuels, ainsi qu'au devoir de diligence. Cette intégration contribue à assurer la cohésion et peut renforcer l'engagement de l'organisation en faveur d'une gestion de risque globale et d'une conduite éthique. En harmonisant ces politiques, l'organisation veille à ce que les considérations de sécurité soient intégrées dans tous les domaines d'activité et de gouvernance.
- **Principes et culture.** La politique doit définir le seuil de risque de l'organisation, sa culture de la sécurité et les autres principes directeurs qui façonnent son approche en matière de gestion des risques de sécurité. Elle peut également souligner

²⁸ Alors qu'une politique de sécurité fournit des directives pratiques pour la mise en œuvre de mesures de sécurité, une stratégie de gestion des risques de sécurité définit les objectifs à long terme et l'approche de l'organisation en matière de gestion des risques de sécurité. Pour plus d'informations sur la manière d'élaborer et de mettre en œuvre une stratégie de gestion des risques de sécurité, voir GISF (2024) *Développement de la stratégie et de la politique de gestion des risques de sécurité (GRS): Un guide interfonctionnel* (<https://gisf.ngo/resource/srm-strategy-and-policy-guide/>).

l’engagement de l’organisation à maintenir une approche de sécurité conforme aux principes, valeurs et normes éthiques pertinents (voir les exemples du tableau 1). Le fait d’énoncer clairement le seuil de risque de l’organisation permet au personnel de prendre des décisions conformes à l’attitude face au risque de l’organisation.²⁹

Tableau 1 Principes, valeurs et normes éthiques en matière de sécurité

Terme	Définition
Principes humanitaires	Respect des principes humanitaires fondamentaux d’humanité, de neutralité, d’impartialité et d’indépendance, qui guident l’action humanitaire en soulignant la nécessité de soulager la souffrance humaine, de rester neutre dans les conflits, de fournir une aide fondée uniquement sur les besoins, sans discrimination, et de conserver son autonomie par rapport aux objectifs politiques ou autres objectifs non humanitaires.
Ne pas nuire	Les organisations évitent d’exacerber les conflits existants ou de créer de nouvelles formes de préjudice par leur présence et leur travail.
Responsabilité partagée en matière de sécurité	La sécurité est une responsabilité partagée entre l’organisation et son personnel à tous les niveaux.
Primauté de la vie	Principe selon lequel la vie et le bien-être humains doivent bénéficier de la plus haute priorité et de la plus grande importance. Ce principe est étroitement lié au concept de criticité des programmes.
Criticité des programmes (ou risque proportionné)	Les activités du programme justifient le niveau de risque que le personnel est appelé à prendre. Plus le programme est essentiel ou vital, plus une organisation peut être prête à accepter des risques pour le maintenir.
Obligation d’informer	Les mesures de sécurité réduisent les risques, mais ne les éliminent pas complètement. Le personnel doit être informé du niveau de risque qui subsiste après la mise en place des mesures d’atténuation et avoir la possibilité de discuter de ce risque résiduel et de faire un choix éclairé en fonction de son seuil de risque personnel.
Droit de retrait	Le personnel a le droit de se retirer d’un lieu ou d’une activité pour des raisons de sécurité.
Interdiction de rester	Le personnel n’a pas le droit de rester dans un lieu si la direction de l’organisation a décidé de suspendre ses activités en raison de l’insécurité.
Utilisation d’armes/de moyens armés	Une organisation doit disposer d’un principe organisationnel clair sur le moment et la manière dont les armes et autres moyens armés (tels que les escortes) peuvent être utilisés par le personnel dans le cadre de son travail.

29 Voir GISF (2024) pour un exemple de déclaration d’appétence au risque.

Sécurité équitable	Les mesures de sécurité sont appliquées de manière équitable à l'ensemble du personnel, en fonction des besoins individuels de chacun. Équitable ne signifie pas toujours égal, mais consiste plutôt à tenir compte des circonstances individuelles afin d'adapter les mesures de sécurité en fonction des besoins. Il s'agit là d'un principe fondamental de l'approche de sécurité centrée sur la personne.
Approche centrée sur la personne	Approche qui place les individus au cœur des activités de gestion des risques de sécurité. Cela implique notamment de reconnaître les risques spécifiques auxquels les individus sont exposés en raison de leur identité intersectionnelle, de leur rôle et de leur organisation, ainsi que du contexte dans lequel ils travaillent.
Partenariats équitables	Approche qui vise à établir des méthodes collaboratives pour traiter conjointement les problèmes de sécurité auxquels sont confrontées toutes les organisations partenaires, partageant ainsi les risques entre les partenaires.

Adapté de Bickley, S. (2017) *Gestion du risque sécurité: manuel de référence à l'attention des petites ONG*. European Interagency Security Forum (<https://gisf.ngo/resource/security-risk-management-a-basic-guide-for-smaller-ngos/>).

Une évaluation régulière du cadre de gouvernance de l'organisation est nécessaire pour maintenir son efficacité. L'amélioration continue – par exemple grâce au feedback, au suivi, aux examens a posteriori et aux enseignements tirés – peut contribuer à affiner les politiques de sécurité au fil du temps.

Exigences de sécurité

Les exigences minimales de sécurité sont des protocoles que l'organisation attend de tous ses employés qu'ils respectent afin d'assurer la sûreté et sécurité des biens, du personnel et des informations. Ces exigences peuvent constituer la base d'un système de sécurité solide, adapté pour répondre aux menaces et vulnérabilités spécifiques inhérentes à chaque lieu, à chaque membre du personnel (en tenant compte des profils de risque individuels) et à chaque axe de travail. Un exemple d'exigence minimale de sécurité pourrait être un plan de sécurité pour chaque bureau ou site de programme.

Les exigences de sécurité sont parfois structurées en niveaux, sur la base des niveaux de sécurité ou des cotes de risque attribués aux différents lieux (par exemple, élevé, moyen et faible). En tenant compte des facteurs de risque et de vulnérabilité propres à chaque lieu, les mesures de sécurité peuvent être adaptées en conséquence, ce qui garantit une allocation appropriée des ressources et une attention adéquate à la gestion des risques de sécurité.

Ce qui constitue un risque élevé, moyen ou faible varie selon les organisations et devrait idéalement être déterminé à l'issue d'une évaluation approfondie, tenant compte de la composition du personnel et des vulnérabilités individuelles et organisationnelles face à des menaces spécifiques.

- **Lieux à haut risque.** Ces zones requièrent généralement les mesures de sécurité les plus strictes, qui peuvent inclure des systèmes de surveillance avancés, des mécanismes de maîtrise du risque d'accès étendus et une protection armée.
- **Lieux à risque moyen.** Ces lieux nécessitent généralement des mesures solides mais moins intensives, notamment des barrières physiques renforcées, des audits de sécurité réguliers et des plans de réponse aux incidents détaillés.
- **Lieux à faible risque.** Ces sites exigent généralement des protocoles de sécurité de base, axés sur la sensibilisation générale et les mesures préventives.

Pour de nombreuses organisations internationales, il est courant que le personnel se rendant dans un lieu à haut risque suive une formation «Sensibilisation en milieu hostile» (Hostile Environment Awareness Training, HEAT).

► Voir le chapitre 5.2 pour plus d'informations sur les formations «Sensibilisation en milieu hostile» (HEAT).

Des exigences de base spécifiques peuvent également s'appliquer à d'autres facteurs, notamment les postes occupés par le personnel et certains projets particuliers. Les profils de risque personnel jouent également un rôle dans la détermination du niveau de risque d'un lieu. Il est donc conseillé aux organisations d'en tenir compte lorsqu'elles définissent leurs exigences de sécurité.

Suivi de la conformité et de l'efficacité

Les exigences de sécurité peuvent jouer un rôle important dans le suivi de la conformité et de l'efficacité en :

- Établissant une base de référence pour les pratiques de sécurité dans tous les lieux, garantissant ainsi leur cohérence et leur comparabilité.
- Fournissant des critères clairs pour les audits de sécurité internes et externes, aidant ainsi à identifier les lacunes et les domaines à améliorer.
- Permettant la révision et la mise à jour régulières des mesures de sécurité en fonction des résultats des audits et de l'évolution des menaces.
- Garantissant le respect des lois, réglementations et bonnes pratiques sectorielles applicables.
- Attribuant la responsabilité des mesures de sécurité, en favorisant une culture de la redevabilité et de la vigilance.

- Voir le chapitre 3.4 pour plus d'informations sur le suivi de la conformité et les audits de sécurité.

Bonnes pratiques de mise en œuvre

La mise en œuvre des aspects pratiques d'une politique de sécurité peut s'avérer difficile. L'une des principales difficultés réside dans l'allocation des ressources, qui implique de garantir un financement et un personnel suffisants pour une mise en œuvre efficace. Un autre défi est celui de l'adaptabilité : les mesures de sécurité doivent être continuellement ajustées pour répondre aux risques et aux besoins opérationnels des différents sites et du personnel. La conformité et l'application des règles constituent également un défi. Suivre l'évolution des technologies de sécurité et les intégrer dans les systèmes existants nécessite des efforts et des investissements continus. Les différences culturelles et régionales doivent également être prises en compte avec soin. Il est essentiel de respecter les lois, les coutumes et les pratiques commerciales locales tout en maintenant des attentes cohérentes en matière de sécurité dans les différents lieux.

Compte tenu de ces défis, les éléments suivants peuvent faciliter la mise en œuvre.

- **Leadership et redevabilité.** Garantir l'engagement des hauts responsables, en intégrant la sécurité dans la structure globale de gouvernance de l'organisation.
- **Affectation des ressources.** Garantir des ressources suffisantes en termes financiers et humains pour mettre en œuvre la politique de sécurité.
- **Intégration interfonctionnelle.** Viser à intégrer la sécurité dans toutes les fonctions, telles que les ressources humaines, les finances, les technologies de l'information (TI) et les programmes.
- **Adaptation contextuelle.** Veiller à ce que la politique soit suffisamment souple dans son application pour permettre une adaptation aux contextes locaux ou à d'autres circonstances, en tenant compte, par exemple, des facteurs d'identité, culturels, linguistiques, technologiques et environnementaux.
- **Suivi continu.** Suivre, examiner et adapter régulièrement l'approche de l'organisation grâce au feedback et au signalement des incidents.
- **Diffusion.** Veiller à ce que la politique soit communiquée à l'ensemble du personnel dans un format accessible et pertinent.

3.1.3 Gouvernance et redevabilité

En tant qu'employeurs et personnes morales, les organisations ont une responsabilité formelle envers l'ensemble de leur personnel, conformément à leur devoir de diligence. Le devoir de diligence d'une organisation envers son personnel devrait idéalement être défini dans sa politique de sécurité ainsi que dans des documents tels que les contrats de travail. Si la sécurité est une responsabilité partagée entre l'organisation et son personnel, il incombe aux organisations de mettre en place des

structures de gouvernance efficaces et de veiller à ce que le personnel connaisse et comprenne son rôle et ses responsabilités au sein de cette structure.

► Voir le chapitre 1.1 pour une analyse plus détaillée sur le devoir de diligence.

Rôles et responsabilités

Pour bien positionner la gestion des risques de sécurité au sein de la structure de gouvernance de l'organisation, il faut définir clairement les responsabilités de chacun. L'adoption d'une matrice RACI peut s'avérer utile.³⁰

► Voir le chapitre 5.1 pour plus d'informations sur la matrice RACI.

Direction exécutive

La redevabilité ultime en matière de sécurité incombe généralement au directeur exécutif (ou son équivalent) de l'organisation ou, dans certains cas, au conseil d'administration. Dans la plupart des organisations, l'exécutif donne le ton en matière de tolérance du risque, veille au respect des obligations légales (telles que le devoir de diligence) et alloue les ressources nécessaires à la mise en œuvre des mesures de sécurité. Cette redevabilité comprend souvent la supervision des politiques, la gestion des crises et l'intégration de la sécurité dans la planification de la continuité des activités. Le conseil d'administration peut également jouer un rôle clé dans la surveillance stratégique et la gouvernance des risques. Cela garantit que la sécurité n'est pas seulement une préoccupation technique ou opérationnelle, mais un aspect fondamental de la gouvernance et de la résilience de l'organisation.

La gestion opérationnelle de la sécurité est liée aux pratiques de gestion et de prise de décision à l'échelle de l'organisation, et la plupart des organisations décentralisent les décisions en matière de sécurité au niveau d'autorité pertinent le plus proche. La décision de lancer ou non des opérations dans un nouveau lieu et le type de programme à mettre en œuvre relèvent généralement de la responsabilité de l'exécutif. L'organisation peut également exiger que les cadres supérieurs contribuent aux décisions importantes en matière de sécurité (par exemple, la décision de déplacer ou d'évacuer le personnel) ou donnent des conseils à ce sujet. Les questions relatives aux médias, à la communication et à la collecte de fonds, ainsi que les questions relatives aux ressources humaines, telles que la mise en place de polices d'assurance, sont généralement décidées et gérées au niveau du siège social. Certaines décisions peuvent également nécessiter l'approbation formelle de l'exécutif, notamment :

- augmenter ou réduire le niveau de risque d'un lieu ;
- réintégrer une zone dont le personnel a été évacué en raison des risques de sécurité ;

30 Pour un exemple détaillé d'une matrice RACI concernant les responsabilités en matière de sécurité, voir GISF (2024).

- adopter une approche « discrète » et retirer les logos et drapeaux des bureaux et véhicules ;³¹
- recourir à une protection armée ; et
- faire appel à une entreprise de sécurité privée.

Personnel de sécurité

De nombreuses organisations emploient du personnel de sécurité afin d'apporter son expertise et ses conseils aux managers (qui sont généralement les derniers responsables des décisions liées à la sécurité). Ces points focaux pour les questions de sécurité sont souvent chargés de mener des actions liées à la sécurité, telles que l'élaboration de plans de sécurité et le partage de leurs connaissances et de leur expertise avec leurs collègues qui ne travaillent pas dans le domaine de la sécurité. La plupart des organisations disposent de points focaux pour les questions de sécurité entièrement dédiés ou polyvalents à différents niveaux, depuis le siège jusqu'aux responsables de projets locaux, les sites les plus à risque bénéficiant souvent de l'investissement le plus important en termes de personnel. Dans certaines organisations, la sécurité est gérée par plusieurs équipes, comités ou groupes de travail, où les tâches et les décisions relatives à la gestion des risques de sécurité sont partagées entre plusieurs membres clés du personnel. Dans d'autres organisations, la gestion des risques de sécurité est intégrée à la gestion hiérarchique et il n'existe aucune fonction distincte dédiée à la sécurité (voir ci-dessous pour une analyse plus détaillée de ces types de structures de gouvernance).

► Voir le chapitre 5.1 pour plus de détails sur les rôles de sécurité.

Leadership au niveau du pays (pour les organisations internationales)

Au niveau du pays, il incombe généralement au représentant principal (c'est-à-dire le directeur de pays ou le chef de mission) de veiller à ce que les politiques et procédures organisationnelles soient mises en œuvre et respectées, la plupart des tâches de gestion des risques de sécurité étant déléguées à un point focal pour les questions de sécurité.

Managers

Les managers à tous les niveaux d'une organisation ont une responsabilité envers leur personnel, qui consiste notamment à veiller à leur sécurité. Dans la pratique, cela peut varier d'une organisation à l'autre, mais cela peut inclure de s'assurer que le personnel assiste aux réunions d'information et aux formations à la sécurité, d'apporter un soutien aux points focaux pour les questions de sécurité et de contribuer à l'évaluation des risques et à la planification de la sécurité.

31 Les donateurs gouvernementaux peuvent imposer des obligations contractuelles concernant la visibilité (« image de marque ») de l'aide qu'ils financent, auquel cas l'organisation peut être amenée à demander leur accord formel pour déroger à cette exigence.

Personnel

Tous les membres du personnel, des responsables de programme seniors aux stagiaires, sont responsables de leur propre sécurité, ainsi que de celle de l'équipe dans son ensemble et de l'organisation. Idéalement, tous les membres du personnel devraient participer à des discussions et à des activités régulières sur la sécurité, y compris à des formations.

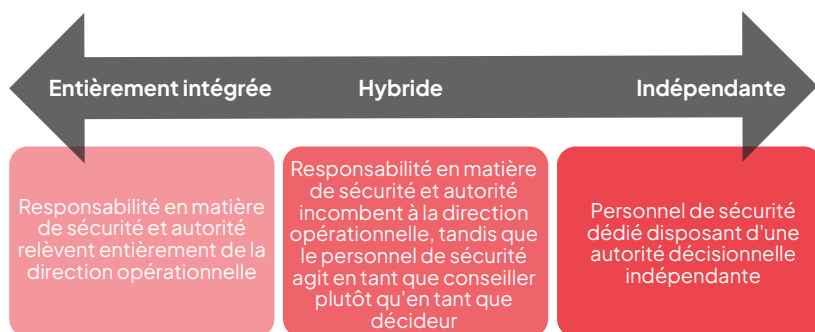
Types de structures de gouvernance de la sécurité

Les structures de gouvernance de la sécurité peuvent varier en fonction de l'approche globale de l'organisation. Cela peut être conçu comme un continuum avec, à une extrémité, une gestion des risques de sécurité entièrement intégrée et, à l'autre extrémité, une structure de sécurité indépendante et dotée de ressources importantes (voir la figure 5).

- **Entièrement intégrée.** La responsabilité en matière de sécurité et l'autorité relèvent entièrement de la direction opérationnelle. Il n'y a généralement pas de personnel de sécurité dédié.
- **Hybride.** La responsabilité en matière de sécurité et l'autorité incombent à la direction opérationnelle, mais les tâches liées à la sécurité, telles que la réalisation d'évaluations des risques et l'élaboration de plans, incombent au personnel de sécurité dédié. Le personnel de sécurité dans ces organisations agit généralement à titre de conseiller, mais n'est pas décisionnaire.
- **Indépendante.** Les organisations qui adoptent cette structure disposent d'un personnel de sécurité dédié à plusieurs niveaux, habilité à prendre des décisions en matière de gestion des risques de sécurité indépendamment des autres fonctions de gestion. Cette structure est plus courante dans les environnements d'entreprise et est parfois décrite comme un modèle de «sécurité d'entreprise».

La plupart des organisations se situent généralement quelque part sur ce continuum, en fonction de leur approche de la gestion des risques de sécurité, de leurs ressources et de leurs préférences. Par exemple, une organisation peut employer un grand nombre de personnel de sécurité professionnel tout en conservant l'intégralité de l'autorité décisionnelle en matière de sécurité au sein de la direction. Certaines organisations peuvent également employer des structures différentes selon les lieux, par exemple des postes de conseillers en sécurité plus spécialisés dans les contextes à haut risque et une approche plus intégrée dans les contextes à faible risque. L'important est d'assurer la cohérence et une communication claire sur les personnes qui ont la responsabilité finale des décisions en matière de sécurité aux différents niveaux de l'organisation.

Figure 5 Types de structures de gouvernance de la sécurité



Toutes ces structures ont leurs points forts et leurs points faibles.

Dans le cadre de l'approche intégrée, les managers sont pleinement responsables de la sécurité du personnel, ce qui peut contribuer à faire en sorte que la sécurité soit considérée comme faisant partie intégrante du processus décisionnel opérationnel, ce qui augmente les chances que la sécurité soit alignée sur les objectifs du programme. Cependant, les managers chargés de la sécurité peuvent manquer d'expertise dans ce domaine et ne pas avoir le temps nécessaire pour s'acquitter correctement de leurs tâches en matière de sécurité en plus de leurs autres responsabilités. Dans ces circonstances, le recours à des services de sécurité externalisés peut être plus important (mais pas nécessairement).

La structure hybride permet aux organisations de bénéficier d'une expertise dédiée en matière de sécurité tout en conservant le pouvoir décisionnel au sein de la direction opérationnelle. Cela offre une approche équilibrée, avec des conseils en matière de sécurité intégrés au processus de planification sans compromettre les objectifs du programme. La flexibilité de cette structure lui permet de s'adapter aux différents besoins organisationnels. Cependant, le rôle consultatif du personnel de sécurité peut limiter ses capacités à faire respecter les mesures de sécurité. Cette dépendance vis-à-vis de la direction opérationnelle pour les décisions finales peut entraîner des retards dans les actions ou une mise en œuvre incohérente des mesures de sécurité, en particulier si les responsables de programme ne donnent pas la priorité aux questions de sécurité.

La structure indépendante de la fonction sécurité fournit le plus de ressources et d'autorité au personnel de sécurité. Le personnel de sécurité peut prendre des mesures directes, ce qui permet d'améliorer l'atténuation des risques, la formation du personnel et la conformité. Cependant, cette structure peut conduire à un cloisonnement de

la sécurité par rapport aux autres fonctions. La sécurité peut être perçue comme un obstacle aux activités du programme, en particulier si les décisions prises par le personnel de sécurité sont en contradiction avec les objectifs du programme. Cela peut nuire à la flexibilité et à la réactivité nécessaires dans certains contextes opérationnels et compromettre l'adhésion du personnel aux mesures de sécurité.

En résumé, les structures entièrement intégrées peuvent offrir une meilleure harmonisation avec les programmes, mais peuvent manquer d'expertise ; les approches hybrides peuvent offrir un équilibre, mais peuvent rencontrer des difficultés en matière de cohérence et de mise en œuvre ; et les structures indépendantes peuvent offrir une sécurité solide, mais peuvent être considérées comme restrictives. Beaucoup dépendra de la manière dont le personnel de sécurité interagit avec ses collègues. Par exemple, dans une structure indépendante, même si le personnel de sécurité a le pouvoir d'appliquer des mesures strictes, il peut choisir de ne le faire que dans des cas extrêmes, préférant collaborer avec d'autres équipes pour prendre des décisions équilibrées. En fin de compte, si les modèles de gouvernance peuvent façonner l'approche globale de l'organisation en matière de sécurité, les attitudes et les approches des individus peuvent également jouer un rôle important dans la manière dont la sécurité est gérée et perçue.

- *Ce sujet est abordé plus en détail dans la partie 5 – Les personnes engagées dans la gestion des risques de sécurité.*

Prestataires de services externes

Certaines organisations engagent des conseillers externes en sécurité, soit comme seuls fournisseurs d'expertise et de ressources en matière de sécurité, soit pour soutenir des fonctions internes qui ne disposent pas des capacités, des compétences ou du temps nécessaires. Si les prestataires externes offrent une vaste expérience, des perspectives impartiales et une connaissance des bonnes pratiques, ils peuvent toutefois manquer d'une compréhension approfondie de la culture et des relations internes de l'organisation, ou ne pas s'y investir suffisamment. Une dépendance excessive à leur égard peut affaiblir les capacités internes et les connaissances institutionnelles.

- *Voir le chapitre 2.1 pour plus d'informations sur les entreprises de sécurité privée.*

Intégrer la sécurité aux autres fonctions organisationnelles

Au sein d'une organisation, la gestion des risques de sécurité touche à de nombreux domaines d'activité. La fonction de gestion des risques de sécurité dans une organisation peut être rattachée à la fonction globale de « gestion de risque », aux

opérations ou à un autre domaine fonctionnel, selon la structure de l'organisation. Quel que soit le domaine dans lequel s'inscrit la sécurité, la collaboration à l'échelle de l'ensemble de l'organisation et d'autres mesures pertinentes de gestion de risque sont essentielles, et constituent souvent le plus grand défi.

Le personnel de sécurité peut améliorer la collaboration en comprenant l'écosystème interne de l'organisation et le rôle que joue la fonction sécurité au sein de celui-ci. Cela implique notamment de comprendre la dynamique organisationnelle interne et les environnements externes, d'anticiper les tendances en matière de risques et d'y répondre, de saisir les opportunités pour développer et améliorer les méthodes de travail, et de favoriser les relations qui profitent à l'organisation dans son ensemble. Cette approche holistique favorise la résilience et l'adaptabilité organisationnelle.

Le personnel chargé de la gestion des risques de sécurité peut bénéficier des éléments suivants :

- **Promotion d'une vision globale de la dynamique interne de l'organisation, des influences externes et des interactions interfonctionnelles.** Cette approche aide les professionnels et les responsables de la sécurité à identifier les risques de sécurité dans tous les services, processus et systèmes, plutôt que de les traiter de manière isolée. Elle s'aligne également sur les principes de la gestion des risques de l'entreprise (voir ci-dessous).
- **Collaboration interdisciplinaire active.** La complexité d'une organisation nécessite souvent une collaboration avec d'autres services et domaines d'expertise. L'intégration de la gestion des risques de sécurité dans les domaines de travail existants permet de réunir des perspectives, des expériences et des connaissances diverses afin de traiter la nature multiforme des risques.
- **Intégrer la pensée systémique.** Cela permet aux organisations de mieux identifier, comprendre et atténuer les risques grâce à l'analyse des interactions dynamiques et des boucles de rétroaction au sein de l'ensemble de l'organisation. La pensée systémique pour une gestion des risques de sécurité efficace implique de comprendre les interdépendances entre les différentes fonctions organisationnelles et les facteurs externes, de favoriser la collaboration interfonctionnelle pour des évaluations des risques complètes et d'élaborer des stratégies de gestion adaptatives et dynamiques.

Comprendre comment la sécurité interagit avec les autres fonctions organisationnelles

Questions pour le personnel de sécurité :

- Comment la gestion des risques de sécurité s'intègre-t-elle dans les autres fonctions de l'organisation, influençant ainsi sa résilience et son adaptabilité globales ?
- La stratégie de gestion des risques de sécurité de votre organisation permet-elle à chacun d'atteindre ses objectifs et ses buts de manière efficace, favorisant ainsi une culture de la réussite et de la collaboration ?
- La vision et l'objectif de l'équipe de sécurité sont-ils adaptés pour soutenir la résilience ?
- Afin de favoriser une plus grande collaboration, existe-t-il des personnes ou des équipes clés dans d'autres fonctions organisationnelles qui devraient être contactées en priorité ?

Certaines grandes organisations internationales ont adopté une approche de « gestion des risques de l'entreprise », qui consiste à identifier, évaluer et gérer tous les risques au sein d'une organisation. La sécurité est un type de risque que les organisations gèrent au quotidien. Les autres risques sont les risques stratégiques, fiduciaires et financiers, cybernétiques, de sûreté, juridiques, d'information, de réputation et opérationnels. Ces types de risques se recoupent souvent et peuvent avoir un impact sur la sécurité, ou être impactés par celle-ci. Les organisations qui adoptent une approche de gestion des risques de l'entreprise visent à intégrer les pratiques de gestion de risque dans leur stratégie globale et leurs processus décisionnels afin de garantir une approche coordonnée et systématique. En situant les risques de sécurité dans le cadre global de gestion de risque d'une organisation, les décideurs peuvent trouver un équilibre entre les considérations de sécurité et d'autres risques, tels que les risques financiers ou réputationnels, en veillant à ce que les mesures de sécurité n'entravent pas involontairement les opérations ou les objectifs stratégiques de l'organisation.

Les bonnes pratiques en matière de gestion des risques de l'entreprise consistent notamment à définir clairement les tolérances, les seuils et les attitudes face au risque, ce qui aide à orienter la prise de décision dans tous les services. Il est conseillé de lier les efforts de gestion des risques de l'entreprise à la continuité des activités et à la gestion de crise, en veillant à ce que la gestion des risques de

sécurité soutienne la résilience organisationnelle au sens large. La mise en œuvre d'une approche de gestion des risques de l'entreprise implique l'engagement des cadres supérieurs, une collaboration interfonctionnelle et un suivi et une évaluation réguliers afin d'adapter la stratégie aux risques émergents. L'intégration interfonctionnelle est particulièrement importante. La gestion des risques de sécurité ne doit pas être cloisonnée ou considérée comme un axe de travail distinct ; elle doit au contraire être reliée aux autres services. Des équipes interfonctionnelles peuvent travailler en collaboration pour gérer les risques et garantir la fluidité des échanges d'informations. Une communication régulière, des objectifs communs et une responsabilité collective entre les différentes fonctions favorisent de meilleures pratiques en matière de gestion de risque. Cette intégration permet de faire face à divers risques, qu'ils soient liés à l'accès aux communautés, à la protection des données ou à la continuité des activités, et de promouvoir une culture de la sécurité positive dans toute l'organisation.³²

Informations complémentaires

Recommandations

Bickley, S. (2017) *Gestion du risque sécurité : manuel de référence à l'attention des petites ONG*. European Interagency Security Forum (<https://gisf.ngo/resource/security-risk-management-a-basic-guide-for-smaller-ngos/>).

GISF (2024) *Développement de la stratégie et de la politique de gestion des risques de sécurité (GRS) : Un guide interfonctionnel* (<https://gisf.ngo/resource/srm-strategy-and-policy-guide/>).

32 Pour obtenir davantage de recommandations pratiques sur l'intégration interfonctionnelle, voir GISF (2024).

3.2 Accès et sécurité

L'accès humanitaire, s'il n'est pas une fin en soi, est une condition préalable à l'action humanitaire. L'insécurité constitue souvent un obstacle à l'accès humanitaire et, de même, les efforts visant à améliorer et à élargir cet accès ont des implications importantes en matière de sécurité.

Cette section définit le concept et les multiples défis de l'accès humanitaire en relation avec la gestion des risques de sécurité, tant dans le cadre des efforts externes déployés par les organisations pour obtenir, maintenir et élargir l'accès que dans le cadre des fonctions internes du personnel. Un accès bien établi et négocié est essentiel pour maintenir la sécurité dans des contextes très contestés, tant pour le personnel des organisations humanitaires que pour les personnes qu'elles servent.

3.2.1 Concepts clés

L'accès humanitaire est défini comme « l'accès des acteurs humanitaires aux personnes ayant besoin d'aide et de protection, et l'accès des personnes dans le besoin aux biens et services essentiels à leur survie et à leur santé, dans le respect des principes humanitaires fondamentaux ». ³³

L'accès repose sur deux piliers fondamentaux : les principes humanitaires et le droit international humanitaire (DIH), tels qu'ils sont consacrés dans les Conventions de Genève et leurs Protocoles additionnels. ³⁴ Le principe d'humanité oblige les acteurs humanitaires à s'efforcer d'aider toutes les personnes en situation de crise, en accordant la priorité à celles qui en ont le plus besoin, tandis que le droit international humanitaire stipule que les acteurs et les opérations humanitaires impartiaux doivent être protégés et bénéficier d'un accès sans entrave aux parties au conflit. ³⁵ Les organisations disposent de plusieurs outils pour obtenir un accès humanitaire fondé sur des principes, notamment la diplomatie de haut niveau, la coordination civilo-militaire et les négociations sur l'accès.

La gestion des risques de sécurité et l'optimisation de l'accès sont deux éléments essentiels de l'action humanitaire, mais ils sont souvent considérés comme deux objectifs distincts et incompatibles. De nombreux praticiens estiment qu'il est nécessaire de trouver un « équilibre » entre sécurité et accès dans les contextes dynamiques à haut risque, où une gestion trop conservatrice des risques peut entraver la recherche active d'un accès aux personnes dans le besoin. Plutôt que de présenter cela comme un compromis, une approche plus productive consiste à

33 ONU OCHA (2012) *OCHA on message: humanitarian principles (en anglais et en arabe, « OCHA on message: principes humanitaires »)* (<https://reliefweb.int/report/world/ocha-message-humanitarian-principles-enar>).

34 CICR (2014) *Les conventions de Genève de 1949 et leurs Protocoles additionnels* (www.icrc.org/en/document/geneva-conventions-1949-additional-protocols).

35 CICR (2014), « Questions/réponses du CICR et lexique sur l'accès humanitaire » *Revue internationale de la Croix-Rouge* 96(893) (<https://international-review.icrc.org/articles/icrc-qa-and-lexicon-humanitarian-access>).

utiliser la criticité des programmes pour orienter les objectifs d'accès et à recourir à la gestion des risques de sécurité pour limiter les dangers liés à la poursuite de ces objectifs. Dans un premier temps, il est utile que le personnel de sécurité comprenne les obstacles à l'accès, ainsi que la manière dont les efforts d'accès sont menés dans la pratique et comment la sécurité peut contribuer à ces efforts.

3.2.2 Difficultés d'accès externe

Les obstacles à l'accès humanitaire peuvent prendre différentes formes, intentionnelles ou non. Les organisations humanitaires les classent généralement en trois grandes catégories :

- les conflits et l'insécurité ;
- les obstacles bureaucratiques et administratifs ; et
- les contraintes environnementales et logistiques.

Si la gestion des risques de sécurité concerne plus directement la première catégorie, les trois catégories comportent des dimensions de risques, et les efforts visant à les surmonter et à élargir l'accès pourraient utilement faire appel au personnel de gestion des risques de sécurité.

Conflits actifs et insécurité

Dans les conflits armés, les obstacles à l'accès liés à l'insécurité comprennent :

- les menaces et les actes de violence dirigés contre le personnel et les biens humanitaires par les parties au conflit ;
- les attaques indirectes (violence collatérale) touchant le personnel et les biens ; et
- les dommages collatéraux causés à l'environnement opérationnel, y compris aux infrastructures civiles.

L'insécurité des acteurs humanitaires peut également s'aggraver dans les zones de conflit actif en raison de l'effondrement de l'ordre social, de l'augmentation de la criminalité et de l'activité économique illicite, ainsi que des actes désespérés commis par la population.

Les conflits armés peuvent servir de prétexte à des ingérences politiques visant à restreindre l'accès. En particulier, si le gouvernement est partie au conflit, il peut invoquer la violence et l'insécurité pour refuser ou restreindre l'accès des organisations humanitaires à certaines zones. Les gouvernements et les armées sont connus pour refuser les autorisations de déplacement aux organisations humanitaires, à moins qu'elles ne se déplacent sous escorte militaire (qu'elles doivent souvent payer) – une mesure qui peut nuire à l'image publique et donc créer plus de risques qu'elle n'en atténue.

Les parties au conflit peuvent imposer des blocus dans certaines zones, empêchant ainsi les organisations humanitaires d'acheminer l'aide et les fournitures essentielles aux civils pris au piège. Les blocus peuvent être une tactique de punition collective ou un moyen de faire pression sur les groupes d'opposition, entraînant des pénuries de nourriture, de médicaments et d'autres produits de première nécessité.

Obstacles bureaucratiques et administratifs

Des procédures bureaucratiques lourdes, longues et peu claires, telles que l'obtention d'autorisations de déplacement et de projet, de visas ou de dédouanements, retardent souvent l'acheminement de l'aide humanitaire et augmentent les coûts opérationnels. Au Soudan, par exemple, tant le gouvernement que les forces d'opposition ont retardé la réponse humanitaire en exigeant de multiples autorisations pour les déplacements et ont empêché l'importation d'équipements médicaux et humanitaires essentiels.

Les gouvernements peuvent également recourir à des mesures de harcèlement juridique et d'ingérence à l'encontre des organisations humanitaires, notamment la surveillance, les perquisitions, les détentions, les arrestations et les contestations judiciaires impliquant de longues procédures judiciaires. Dans les cas les plus graves, les organisations peuvent se voir refuser leur enregistrement et être expulsées du pays. Les lois sur la lutte antiterroriste peuvent restreindre l'engagement avec certains groupes et imposer des sanctions sévères ; les contrôles excessifs effectués par les donateurs et les pratiques de réduction des risques mises en place par les banques exacerbent ces difficultés. En Russie, les ONG n'ont pas le droit de procéder au signalement public des informations relatives aux actions du gouvernement ou de l'armée. Qu'elles soient intentionnelles ou non, les barrières financières, telles que les embargos commerciaux, le gel des avoirs et les frais administratifs, peuvent également entraver les opérations humanitaires.

Contraintes environnementales et logistiques

Les obstacles logistiques et environnementaux comprennent le manque d'infrastructures de transport ou les perturbations et les dommages causés par les événements climatiques.

Ce type d'obstacle à l'accès n'est pas toujours entièrement fortuit ou involontaire. Le fait que le gouvernement n'accorde pas la priorité à ces domaines et à ces questions peut constituer une forme indirecte de refus d'accès. Les fermetures sélectives de routes, les couvre-feux et l'interruption des services (par exemple, Internet et les télécommunications) peuvent limiter les capacités des populations dans l'accès à l'information et aux services, et entraver l'action des organisations humanitaires dans les zones sinistrées. Les solutions de contournement peuvent être coûteuses (par exemple, l'utilisation de moyens aériens lorsque les routes sont impraticables) et potentiellement dangereuses (utilisation de véhicules de remplacement et d'itinéraires dangereux).

3.2.3 Obstacles internes à l'accès humanitaire

Toutes les contraintes d'accès ne sont pas externes. Les facteurs internes sont les suivants :

- **Culture organisationnelle et appétence au risque.** Même lorsque la volonté et les incitations à maximiser l'accès existent au niveau de la programmation, si l'appétence au risque et la culture de gestion des risques de sécurité ne sont pas clairs et partagés à tous les niveaux, l'hésitation, l'inertie et les priorités concurrentes peuvent limiter l'action. C'est notamment pour cette raison qu'il est important que les organisations intègrent leurs stratégies d'amélioration de l'accès dans leur système de gestion des risques de sécurité et vice versa.
- **Systèmes et politiques.** Les mandats et les aspirations de l'organisation ne correspondent pas toujours aux procédures et processus organisationnels internes. Les discussions sur l'accès humanitaire se limitent souvent aux équipes chargées des programmes et des politiques. Cependant, les fonctions de soutien - telles que les ressources humaines, les finances, la logistique, la sécurité et la communication - jouent un rôle tout aussi important dans l'élaboration des stratégies d'accès et de programme. Les organisations qui ont mis en œuvre des programmes de manière durable ont utilisé efficacement tous les aspects de leur capacité organisationnelle.
- **Capacités organisationnelles et humaines.** Les défis en matière de ressources humaines touchant l'ensemble du secteur, il peut être difficile de recruter des personnes compétentes dans le domaine de l'accès et des négociations humanitaires. De plus en plus d'organisations se tournent désormais vers la formation sur le terrain pour pallier le manque de compétences.

3.2.4 Considérations et approches pratiques pour l'accès

Les organisations peuvent gérer les contraintes d'accès grâce à des adaptations programmatiques, au plaidoyer, à l'engagement et à la coordination. Les stratégies d'accès combinent souvent ces mesures et diverses approches afin de faire face aux environnements les plus difficiles. Par exemple, en Irak, lors de la réponse à la crise des déplacements en 2016, les organisations ont mis en œuvre une stratégie d'accès multiforme, qui comprenait le renforcement des capacités d'accès autonomes, la négociation directe avec les groupes armés, l'adoption de programmes de gestion à distance et la participation à des groupes de travail opérationnels et de coordination civilo-militaire.

Les éléments d'une stratégie d'accès diversifiée peuvent être les suivants :

- **Diplomatie et plaidoyer de haut niveau.** Engager le dialogue avec les autorités du pays donateur, les autorités nationales, les organisations internationales et régionales et d'autres acteurs influents sur la protection des travailleurs humanitaires et la responsabilité d'assurer une aide humanitaire sans entrave. Cela peut se faire par

l'intermédiaire du Coordonnateur humanitaire de l'ONU ou de consortiums d'ONG axés sur le plaidoyer au nom des agences de l'ONU et/ou des organisations humanitaires.

- **Groupes de travail interagences sur l'accès.** Collaborer avec d'autres organisations humanitaires au moyen de mécanismes d'ensemble afin de partager des informations et d'élaborer des stratégies communes pour améliorer l'accès. Cela peut contribuer à éviter la duplication des efforts tout en atténuant les risques pour chaque organisation. Les groupes de travail sur l'accès sont généralement présidés par l'OCHA et coprésidés par une ONG. Leurs fonctions varient en fonction du contexte, mais en principe, leurs principaux objectifs comprennent le partage d'informations, la mise à disposition d'un espace de discussion sûr, le suivi de l'accès et le renforcement des capacités.
- **Accords à distance ou collaboration avec des partenaires.** Le partenariat avec des organisations locales et des groupes communautaires qui ont établi des réseaux et un climat de confiance au sein des communautés touchées peut faciliter l'accès.
- **Négociations humanitaires.** Engager des discussions avec différents acteurs, y compris les parties au conflit, afin d'obtenir un accès sécurisé aux populations touchées. Cela peut aller de discussions informelles avec les gardes des postes de contrôle à des efforts interagences ou diplomatiques formels, et implique de former le personnel à la négociation, à la désescalade et à la médiation des conflits. Les cadres pour les négociations humanitaires, tels que celui développé par le Centre of Competence on Humanitarian Negotiation (Centre de compétences en négociation humanitaire, CCHN),³⁶, peuvent fournir des outils et des méthodes utiles pour analyser les environnements de négociation, évaluer les positions et les intérêts des parties, construire des réseaux, définir des objectifs et des lignes rouges et mettre en œuvre des accords. Le personnel de sécurité, qui participe à une grande partie de cette analyse, peut être bien placé pour mener ces négociations ou fournir des informations et un soutien. Ces négociations peuvent être menées par des organisations individuelles ou dans le cadre d'efforts collectifs (aux niveaux local, national ou international).
- **Acceptation, engagement communautaire et sensibilisation.** Impliquer les communautés locales et le secteur privé dans les processus de planification et de prise de décision afin de mieux identifier les besoins locaux et les obstacles à l'accès, ainsi que les solutions potentielles. L'adoption d'approches communautaires en matière d'accès et de sécurité, qui impliquent un engagement régulier et intentionnel avec divers acteurs clés, notamment les dirigeants locaux, les anciens et les organisations communautaires, peut contribuer à atténuer les risques de sécurité et à promouvoir l'acceptation de l'aide humanitaire. Cela peut renforcer et élargir le réseau d'une organisation et servir de système d'alerte précoce pour signaler aux organisations les changements dans le contexte.

36 CCHN (2019) *Le manuel de terrain du CCHN sur la négociation humanitaire de première ligne*. Frontline Negotiations (<https://frontline-negotiations.org/home/resources/field-manual/>).

- **Gestion de l'information.** Collecte et analyse de données sur les contraintes d'accès et les risques de sécurité afin d'adapter les stratégies et de prendre des décisions éclairées. Pour dresser un tableau complet de l'environnement d'accès et élaborer des stratégies appropriées, les organisations peuvent intégrer les informations en matière de sécurité dans une analyse plus large (telle que l'analyse politico-économique et l'analyse des conflits) afin de comprendre les causes profondes des difficultés d'accès.
 - **Soutenir un accès sécurisé dans l'ensemble des fonctions organisationnelles.**
 - Administration: Veiller au respect des cadres juridiques et réglementaires afin d'éviter ou de réduire les problèmes juridiques ou bureaucratiques susceptibles d'entraver l'accès.
 - Logistique: Élaborer et mettre en œuvre des plans de secours pour l'acheminement de l'aide, y compris des itinéraires et des moyens de transport alternatifs.
 - Gestion des risques de sécurité: Comprendre le contexte local et les contraintes d'accès potentielles. Former le personnel à prendre des décisions éclairées en matière de sécurité et mettre en place des plans d'urgence pour faire face à l'évolution de la situation.
 - **Technologie.** Utiliser la technologie pour améliorer l'accès, comme l'imagerie satellite pour l'analyse du contexte, les applications mobiles pour les signalements en temps réel et les plateformes numériques pour le suivi et la coordination à distance.
 - **Engagement civilo-militaire.** La coordination civilo-militaire pour l'accès humanitaire trouve son origine dans le droit international humanitaire et dans les directives élaborées par le Comité permanent interorganisations (IASC) et le Service de coordination civilo-militaire de l'OCHA.
- *Pour plus d'informations, voir le chapitre 2.1 sur la collaboration en matière de sécurité et les réseaux.*

3.2.5 Intégrer la sécurité à l'accès pour atteindre les objectifs de programmation

Les fonctions d'accès peuvent couvrir plusieurs postes standard, notamment dans les équipes chargées de la logistique, du plaidoyer, des programmes et de la sécurité. Pour relever ce défi multidisciplinaire, les organisations ont recours à trois modèles différents.

- **Capacités d'accès autonomes.** Peu d'organisations ont investi dans le recrutement de personnel dédié à l'obtention et à l'amélioration de l'accès. Si le fait de disposer d'un poste dédié à l'accès peut souligner l'importance de l'accès en tant que catalyseur de programme, ce modèle peut rapidement devenir coûteux, difficile à reproduire et redondant si la direction n'a pas l'expérience nécessaire pour tirer parti des atouts des fonctions de sécurité et d'accès. Dans ce modèle, il est important que le personnel chargé de la sécurité et de l'accès collabore autant que possible ; par exemple, la prise en compte des questions d'accès dès les phases de conception et de lancement permet d'identifier les risques et de mettre en œuvre des adaptations programmatiques et opérationnelles, notamment en matière de gestion des risques de sécurité.

- **Intégrer des fonctions d'accès à divers postes, y compris les équipes chargées de la sûreté et sécurité.** Certaines organisations ont adopté une approche intégrée de gestion de la sécurité et des accès en combinant les deux fonctions. Si ce modèle nécessite moins de ressources et permet d'éviter toute confusion entre les rôles et les responsabilités, son succès dépend probablement des capacités de l'organisation à élaborer une description de poste qui englobe de manière adéquate les deux fonctions, puis à recruter le profil adéquat. Cela peut s'avérer particulièrement difficile si les spécialistes de la sécurité sont recrutés parmi les forces de police ou l'armée.

Exemple de cas : Le Cadre pour un accès plus sûr – un modèle intégré

Le Cadre pour un accès plus sûr, élaboré par le CICR afin d'aider les Sociétés nationales de la Croix-Rouge et du Croissant-Rouge à obtenir un accès sûr aux populations touchées, comprend huit catégories de mesures visant à améliorer l'acceptation, la sécurité et l'accès. Il s'agit notamment de comprendre le contexte et les risques locaux, de situer l'organisation dans les cadres juridiques et politiques, de renforcer et de maintenir l'acceptation parmi les parties prenantes locales, d'assurer la visibilité de l'organisation, de garantir une communication interne et externe efficace et de mettre en œuvre un système solide de gestion des risques de sécurité opérationnelle.

Cette approche reconnaît les liens entre l'acceptation, la sécurité et l'accès, et fournit des mesures clés pour améliorer ces trois aspects. Dans la pratique, cela s'est traduit, par exemple, par l'intégration de pratiques visant à renforcer la sécurité et l'acceptation dans la formation des bénévoles, le renforcement des équipes de communication afin de suivre la perception du public et de préserver la réputation de l'organisation en ligne, et la mise en place d'équipes de coordination locales qui travaillent avec différents départements et programmes afin de mettre en œuvre les principes et les priorités du Cadre pour un accès plus sûr.

Pour plus d'informations, voir <https://saferaccess.icrc.org>

- **Modèle hybride.** Certaines organisations ont séparé la responsabilité de l'accès opérationnel et le soutien technique. Au niveau du siège social, les experts en accès technique travaillent séparément des équipes de sécurité et fournissent des conseils et des recommandations aux équipes de pays, notamment en matière de formation et d'élaboration de stratégies. Au niveau régional et du pays, l'accès opérationnel quotidien est géré par les équipes de sécurité. Ce modèle permet de disposer de capacités techniques internes en matière d'accès, tout en reconnaissant la difficulté de recruter du personnel supplémentaire dédié au niveau du pays. Cependant, cela ne résout pas le problème lié au fait que les équipes techniques ne disposent pas d'une ligne technique vers le personnel de sécurité au niveau régional ou du pays, ce qui signifie que le contrôle qualité dépend du recrutement de profils adaptés aux fonctions de sécurité et de la solidité des relations entre l'équipe chargée de l'accès et les directeurs de pays.

Informations complémentaires

Recherche et analyse

ACAPS (July 2024) 'Humanitarian access' (en anglais, «Accès humanitaire») (www.acaps.org/en/thematics/all-topics/humanitarian-access).

GISF et Humanitarian Outcomes (2024) *State of practice: the evolution of security risk management in the humanitarian space* (en anglais, «État des lieux: l'évolution de la gestion des risques de sécurité dans le domaine humanitaire») (https://humanitarianoutcomes.org/security_risk_mgmt_humanitarian_space_2024).

Magone, C., Neuman, M. et Weissman, F. (2012) *Agir à tout prix? Négociations humanitaires: l'expérience de MSF*. Centre de réflexion sur l'action et les savoirs humanitaires (CRASH) (<https://msf-crash.org/en/war-and-humanitarianism/humanitarian-negotiations-revealed-msf-experience>).

ONU OCHA (2012) 'OCHA on message: humanitarian principles' (en anglais et en arabe, «OCHA on message: principes humanitaires») (<https://reliefweb.int/report/world/ocha-message-humanitarian-principles-enar>).

Recommandations et ressources

CCHN (2019) *Le manuel de terrain du CCHN sur la négociation humanitaire de première ligne*. Frontline Negotiations (<https://frontline-negotiations.org/home/resources/field-manual/>).

CICR (n.d.) *Les conventions de Genève de 1949 et leurs Protocoles additionnels* (www.icrc.org/en/document/geneva-conventions-1949-additional-protocols).

CICR (2015) «Questions/réponses du CICR et lexique sur l'accès humanitaire» *Revue internationale de la Croix-Rouge* 96(893) (<https://international-review.icrc.org/articles/icrc-qa-and-lexicon-humanitarian-access>).

CICR (n.d.) *Safer access for all national societies. Overview* (en anglais, «Accès plus sûr pour toutes les sociétés nationales. Aperçu») (<https://saferaccess.icrc.org/overview/>).

3.3 Financement de la gestion des risques de sécurité

Quelle que soit la combinaison de mesures de gestion des risques de sécurité mise en place par les organisations humanitaires, celle-ci entraînera inévitablement des coûts. Ces coûts, tout comme les mesures elles-mêmes, doivent être pris en compte dès les premières étapes de la conception du programme et intégrés dans les budgets prévisionnels. Il est essentiel de veiller à ce que les organisations disposent d'un financement suffisant pour pouvoir fonctionner en toute sécurité, et c'est un sujet sur lequel les organisations et leurs donateurs doivent être prêts à avoir des discussions franches. Ce chapitre présente les bonnes pratiques en matière de budgétisation des dépenses liées à la sécurité et met en évidence certaines des questions clés et des évolutions importantes dans les initiatives de financement et de coordination des donateurs.

3.3.1 Coûts et budgétisation

Il n'existe pas de formule budgétaire uniforme ni de définition commune des dépenses pour les intrants et les activités destinés à renforcer la sécurité opérationnelle. Les organisations et les donateurs varient dans leur manière de budgétiser les coûts liés à la sécurité. Certains incluent le financement de la sécurité dans les frais généraux ou les services d'appui, d'autres l'incluent comme un poste distinct ou comme un pourcentage fixe des coûts du programme, ou encore intègrent entièrement les coûts de sécurité dans les coûts de leur programme. Par exemple : les véhicules nécessaires au déplacement du personnel en convoi seraient inscrits dans la ligne « véhicules/transport » ; l'installation de mesures de sécurité physique telles que des portails ou des alarmes serait inscrite dans la ligne « réparation/entretien des installations » ; et les professionnels de la gestion des risques de sécurité pourraient être inscrits dans la ligne « personnel d'appui ». De même, les membres du personnel ayant des compétences en matière de négociation ou de liaison avec les communautés sont souvent essentiels à la mise en œuvre de mesures d'acceptation pour la gestion des risques de sécurité, mais ne sont pas nécessairement considérés comme des coûts liés à la sécurité.

Il est désormais généralement admis qu'une gestion des risques de sécurité efficace est essentielle à la mise en œuvre durable des programmes et ne devrait donc, dans l'idéal, pas être considérée comme des frais indirects. Lorsque les donateurs exigent plutôt des estimations des coûts de sécurité dans les propositions (comme le font certaines grandes autorités du pays donateur), cela permet non seulement aux organisations d'inclure les contributions nécessaires, mais les incite également à réfléchir activement aux besoins en sécurité dans le cadre du processus d'élaboration du budget et de conception des programmes. Comme beaucoup d'autres aspects de la gestion des risques de sécurité, le calcul des coûts et la budgétisation de la sécurité découlent principalement de l'évaluation des risques, qui peut orienter l'affectation de l'attention et des ressources. L'évaluation des risques peut également inclure la prise en compte des risques encourus par les organisations partenaires travaillant sur le programme, et ces coûts peuvent être intégrés

dans toute proposition. En résumé, les coûts liés à la gestion des risques de sécurité peuvent désigner toute dépense visant à réduire les dommages ou pertes potentiels pour l'organisation, son personnel et ses partenaires, ou à répondre et à indemniser les dommages ou pertes réels, tout en maximisant les chances de réussite des opérations.

Pour remplir son devoir de diligence, les mesures de gestion des risques de sécurité d'une organisation doivent être proportionnées au niveau de risque auquel son personnel est exposé dans l'exercice de ses fonctions. Ne pas budgétiser de manière appropriée les risques prévisibles serait une négligence. Cela nécessite une communication ouverte et directe avec les donateurs et les équipes organisationnelles concernées, non seulement au stade de la proposition, mais aussi tout au long du cycle de vie du programme, car les conditions de sécurité peuvent évoluer. Cela exige également que les organisations comprennent et documentent les coûts engagés pour gérer les risques de sécurité, ce qui leur permet ensuite de démontrer aux donateurs qu'elles ont optimisé les ressources en permettant la mise en œuvre de la programmation de l'aide.

La budgétisation de la sécurité au niveau des projets/programmes doit généralement respecter les exigences des donateurs, mais les organisations ont souvent besoin d'une politique générale de budgétisation de la sécurité qui s'applique à l'ensemble de l'organisation et qui ne dépend pas des budgets individuels des projets qui ont une date d'échéance. Le recours à un financement de base, qu'il provienne de frais généraux cumulés, de fonds sans restriction ou de subventions spécifiques, peut permettre de mettre en place des fonctions, des structures et des postes de personnel durables pour la gestion des risques de sécurité, qui couvrent plusieurs projets et plusieurs années. Cela peut être difficile à réaliser pour les organisations locales, qui ont un accès beaucoup plus limité au financement de base que les organisations internationales et se trouvent donc dans une situation structurellement défavorable lorsqu'il s'agit de renforcer leurs capacités organisationnelles.

Budgétisation de la sécurité

Le Risk Management Expense Portfolio (Portefeuille de dépenses de la gestion de risque, RMEP) du GISF est un outil de budgétisation sous forme de tableur qui fournit des indications sur l'ensemble des coûts tangibles et intangibles liés à la sécurité dans des domaines tels que les actifs et les équipements, les salaires et la formation. L'outil présente les catégories budgétaires suivantes, dans lesquelles les dépenses de sécurité peuvent s'inscrire en tant que coûts directs:¹

- salaires
- administration et logistique
- formation, apprentissage et développement
- gestion de l'information et des connaissances

- accès
- gestion des installations
- actifs de communication
- actifs médicaux
- actifs de transport
- actifs de gestion de crise
- assurances
- fonds de réserve généraux (par exemple pour la réponse aux incidents critiques ou les évacuations).

Remarque complémentaire : l'ajout de notes explicatives dans le budget pour chaque poste, renvoyant au texte de la description de la proposition, peut être un outil puissant pour justifier les coûts.

ⁱ Pour plus de détails, voir www.gisf.ngo/resource/the-cost-of-srm-for-ngos/

3.3.2 Processus internes

Une difficulté se pose lorsque le personnel chargé d'élaborer les propositions et les budgets n'a pas une vue d'ensemble des besoins en gestion des risques de sécurité ou ne collabore pas suffisamment avec ceux qui en ont une. Cela augmente le risque que les coûts liés à la sécurité ne soient pas correctement budgétés ou que, en cas de coupes budgétaires, ces coûts soient les premiers à être supprimés.

C'est une erreur de concevoir un programme d'aide et de déterminer ensuite comment le « sécuriser ». Pour véritablement permettre l'action humanitaire, la gestion des risques de sécurité doit être intégrée à toutes les étapes de la programmation. Cela nécessite une collaboration étroite entre les équipes chargées de la programmation, des finances et de la gestion des subventions, de la gestion des risques de sécurité, de la logistique et tout autre personnel concerné, dès les premières étapes de la conception et de l'élaboration des propositions, ainsi qu'à chaque changement, tel que les modifications budgétaires ou les prolongations sans financement. Il est conseillé aux organisations qui disposent de conseillers ou de responsables dédiés à la gestion des risques de sécurité de veiller à ce que ces membres du personnel soient impliqués dès le début, en travaillant de manière collaborative plutôt qu'isolément. En outre, ils peuvent développer des compétences en matière de processus budgétaires afin de collaborer efficacement avec leurs collègues chargés des finances et de la gestion des subventions.

Le personnel des organisations partenaires d'un programme ou d'un projet devrait idéalement participer aux principales réunions de planification et de budgétisation, afin que les besoins de tous les partenaires en gestion des risques de sécurité soient pris en compte dans le processus de budgétisation dès les premiers stades.

► *Pour en savoir plus sur le financement de la sécurité entre partenaires, voir le chapitre 3.5 - Gestion des risques de sécurité dans les partenariats.*

Exemple de cas : Budgétisation de la sécurité

Le personnel de sécurité d'une organisation internationale commence à planifier les coûts de gestion des risques de sécurité des programmes au cours de la phase d'élaboration du budget de fonctionnement pour l'exercice fiscal à venir. Cela permet de s'assurer que les coûts globaux liés à la sécurité, qui ne sont pas spécifiques à un projet, sont pris en compte dans les coûts partagés du programme pour l'exercice fiscal, et réduit le temps nécessaire pour définir et inclure ces coûts dans toute proposition de projet spécifique. Ces coûts peuvent inclure la formation et le développement, les fournitures et l'équipement, ainsi que l'administration et la logistique. Les propositions de coûts liés au projet visent à refléter avec précision les coûts supplémentaires liés au maintien des normes et de la politique de sûreté et sécurité de l'organisation.

L'organisation veille également à ce que la phase d'élaboration du budget implique une coordination avec les collègues concernés des ressources humaines, de l'administration, des finances, de la chaîne d'approvisionnement, des partenariats et autres, afin d'éviter tout doublon ou suppression de coûts pour des éléments qui peuvent être liés à la sûreté et sécurité, mais qui sont gérés par ces départements.

3.3.3 Engagement des donateurs

D'une manière générale, les principaux donateurs humanitaires gouvernementaux sont prêts à financer les dépenses appropriées et justifiées liées à la sûreté et à la sécurité. Les directives relatives aux propositions de quelques organismes donateurs officiels font explicitement référence à la gestion des risques de sécurité et aux dépenses connexes, et un petit nombre de donateurs disposent d'unités ou de points focaux spécifiques chargés de la coordination et la gestion des risques de sécurité, qui peuvent fournir des conseils utiles, en particulier lors de la planification des programmes et des premières étapes de la budgétisation. Certains organismes donateurs ont également organisé des réunions et des ateliers afin de conseiller les organisations humanitaires sur la manière d'inclure les coûts de sécurité dans leurs propositions. Bien que certains donateurs ne demandent pas expressément que les coûts de gestion des risques de sécurité soient inclus dans une proposition, ils peuvent financer ces coûts s'ils sont présentés et justifiés.

Cependant, lorsque des organisations internationales accordent des subventions ou passent des contrats de sous-traitance avec des organisations locales, elles peuvent ne pas proposer ou autoriser l'inclusion des coûts de gestion des risques de sécurité dans le budget. Cela peut créer un danger moral, dans la mesure où l'organisation locale est incitée à prendre des risques et à ne pas inclure les coûts de sécurité dans son budget afin d'être plus compétitive dans la recherche de contrats internationaux. Tout en veillant à ne pas créer de bureaucratie supplémentaire inutile, les organisations internationales peuvent s'efforcer de garantir le même niveau de discussion ouverte, de communication claire des besoins et de planification écrite en matière de gestion des risques de sécurité avec leurs partenaires de mise en œuvre qu'avec leurs donateurs. Idéalement, les partenariats incluront une composante de coûts de base pour permettre à l'organisation locale de développer des capacités durables de gestion des risques de sécurité.

Bien que les donateurs varient dans leurs choix de financement, les domaines de dépenses communs comprennent les équipements de communication, les équipements de sécurité physique et leurs mises à niveau, la formation à la sécurité, les équipements de sûreté, les trousseaux de premiers secours/d'urgence et le personnel de sécurité (partiellement ou entièrement, selon le niveau de risque du contexte et le donateur). Un soutien supplémentaire en matière de sécurité au niveau opérationnel, tel que celui offert par des entreprises de sécurité privée, est généralement envisagé au cas par cas.

Certains organismes d'autorités du pays donateur encouragent activement une plus grande sensibilisation à la sécurité et le renforcement des compétences en sécurité au sein des organisations humanitaires qu'elles financent, et s'attendent à voir figurer les dépenses de sécurité dans les budgets. Les propositions peuvent devoir être accompagnées d'un plan de sécurité détaillé comprenant une analyse du contexte et une évaluation des risques. Afin d'éviter des révisions importantes

des budgets des projets une fois les contrats signés, les évaluations des risques peuvent décrire les scénarios futurs possibles - et les besoins futurs - en cas de détérioration de la sécurité. Au-delà de cela, cependant, les donateurs ont tendance à ne pas imposer de politiques ou de pratiques de sécurité particulières, préférant laisser les organisations déterminer leur propre position en matière de sécurité et exercer leur propre contrôle qualité dans ce domaine. Cela s'explique en partie par le fait que les donateurs ne disposent pas du personnel, des compétences et de la présence opérationnelle nécessaires pour exercer une influence plus directe. Les donateurs craignent également d'être perçus comme imposant un modèle de sécurité particulier aux organisations. S'impliquer formellement dans l'assurance qualité pourrait également exposer les donateurs à des poursuites en responsabilité civile. De nombreux donateurs ne demandent pas explicitement de budget pour la sécurité, et les professionnels de la sécurité en ont rencontré certains qui déclarent ne pas vouloir financer la sécurité. Dans les cas où il n'y a pas de ligne budgétaire explicitement dédiée à la sécurité, les coûts liés à la sécurité peuvent être couverts par d'autres lignes budgétaires.

Implication des donateurs au-delà du financement des besoins opérationnels de sécurité

Bien que les donateurs n'assument jamais la responsabilité de la gestion des risques de sécurité d'une organisation, plusieurs d'entre eux ont fourni des ressources supplémentaires afin de renforcer les efforts déployés par les organisations humanitaires en gestion des risques de sécurité. Par exemple, les donateurs gouvernementaux ont soutenu les capacités et les compétences interagences en finançant le GISF et l'INSO. Les donateurs gouvernementaux ont également financé des recherches visant à examiner l'évolution des défis en matière de gestion des risques de sécurité et à évaluer les pratiques actuelles des organisations humanitaires en matière de sécurité.

Les donateurs versent également des fonds à l'UNDSS pour financer du personnel et des activités supplémentaires, en mettant particulièrement l'accent sur les responsabilités de liaison avec les ONG dans le cadre de l'initiative « Saving Lives Together » (Sauver des vies ensemble) et sur le renforcement de la sécurité à l'échelle du secteur, par exemple pour des formations à la sécurité personnelle et aux premiers secours supplémentaires.

Comme les organisations financent souvent des programmes grâce aux contributions de plusieurs donateurs, la coordination entre ces derniers est importante (mais actuellement limitée) pour garantir la cohérence des exigences et des directives en matière de budgétisation de la sécurité.

Certains donateurs exigent que leur financement soit visible et appliquent des politiques de marque qui imposent l’affichage de leur logo sur les biens qu’ils financent, notamment les bureaux, les véhicules et les articles de secours. Dans certains cas, cette association peut être considérée comme une menace pour la sécurité, en particulier si le donateur en question est impopulaire dans le contexte donné ou si l’organisation tente d’adopter une approche discrète. Dans ce cas, une organisation peut demander officiellement une dérogation à l’obligation de visibilité. Les donateurs peuvent faire preuve de souplesse à l’égard de ces exigences lorsque des considérations de sécurité imposent la prudence.

Informations complémentaires

Recherches et recommandations

European Interagency Security Forum (2013) *The Cost of Security Risk Management for NGOs* (en anglais, « Le coût de la gestion des risques de sécurité pour les ONG ») (www.gisf.ngo/resource/the-cost-of-srm-for-ngos/).

GISF et Humanitarian Outcomes (2024) *State of practice: the evolution of security risk management in the humanitarian space* (en anglais, « État des lieux: l’évolution de la gestion des risques de sécurité dans le domaine humanitaire ») (https://humanitarianoutcomes.org/security_risk_mgmt_humanitarian_space_2024).

Stoddard, A. et Harmer. A. (2010) *Supporting security for humanitarian action: a review of critical issues for the humanitarian community* (en anglais, « Soutenir la sécurité dans le cadre de l’action humanitaire: examen des questions cruciales pour la communauté humanitaire »). Humanitarian Outcomes (www.humanitarianoutcomes.org/publications/supporting-security-humanitarian-action).

Politiques et exemples de financement par les donateurs gouvernementaux

Foreign, Commonwealth & Development Office (FCDO, Bureau des affaires étrangères, du Commonwealth et du développement) (n.d.) *FCDO humanitarian funding guidelines for NGOs applying for CHASE humanitarian response funding* (en anglais, « Directives du FCDO relatives au financement humanitaire des ONG qui sollicitent un financement humanitaire dans le cadre du programme CHASE »). Annexe B : Budget template (en anglais, « Modèle de budget ») (www.gov.uk/guidance/humanitarian-response-funding).

Protection civile et opérations d’aide humanitaire européennes (ECHO) (2023) « Plans de mise en œuvre humanitaire (HIP) ». Thematic policy annex 2024. General considerations: safe and secure provision of aid (en anglais, « Annexe thématique sur les politiques 2024. Considérations générales : fourniture d’une aide sûre et sécurisée ») (https://ec.europa.eu/echo/files/funding/hip2024/thematic_policies_annex_2024.pdf).

3.4 Suivi de la conformité, de l'efficacité et de l'impact

Un élément essentiel de la gestion des risques de sécurité consiste à veiller à ce que les politiques, les plans et les procédures soient régulièrement revus et évalués afin de mesurer leur conformité, leur efficacité et leur impact à l'échelle de l'organisation et au niveau de chaque site.

3.4.1 Mécanismes de suivi

Le suivi de la conformité, de l'efficacité et de l'impact de la gestion des risques de sécurité permet de garantir que la sécurité aide l'organisation à atteindre ses objectifs et soutient efficacement ses programmes. Le suivi est un élément important du respect du devoir de diligence et peut fournir des informations essentielles pour identifier les forces et les faiblesses, ce qui permet aux organisations de concentrer leurs ressources là où elles sont le plus nécessaires.

Cependant, l'un des principaux défis liés aux mécanismes de suivi réside dans le fait qu'ils sont parfois perçus comme des obstacles à la mise en œuvre des programmes, créant des charges supplémentaires et alourdissant la bureaucratie. Une autre préoccupation concerne les approches axées sur la conformité, c'est-à-dire qui visent principalement à garantir le respect des exigences minimales plutôt qu'à évaluer l'efficacité des mesures mises en place. Pour remédier à cela, les mécanismes de suivi doivent être adaptables et évolutifs. Ils ne doivent pas submerger les responsables ni servir à mettre en place un dispositif de sécurité inutile (même si l'intention est louable) qui pourrait entraver la fluidité de la programmation. Il est conseillé de mettre en place des mesures de suivi différentes pour les environnements à faible risque et à haut risque, qui soient proportionnées et adaptées aux besoins et aux capacités. Les mécanismes de suivi peuvent également offrir aux équipes de sécurité l'occasion de prendre du recul et de se demander pourquoi une organisation utilise les outils et les processus qu'elle utilise, si les choses pourraient être simplifiées, et de s'assurer que la sécurité aide l'ensemble du personnel à atteindre les objectifs organisationnels et programmatiques.

Un suivi efficace favorise l'apprentissage organisationnel. Cela peut s'avérer particulièrement difficile lorsqu'il y a beaucoup d'informations à assimiler, et il est particulièrement important que les connaissances et l'apprentissage ne se limitent pas aux équipes de sécurité. Au niveau le plus élémentaire, les conclusions et recommandations des audits de sécurité et autres mécanismes de suivi pertinents doivent être communiquées aux personnes qui y ont participé et, dans la mesure du possible, être accessibles à l'ensemble du personnel. Le partage des résultats de ces processus peut favoriser la transparence et sensibiliser à la manière dont le personnel

de sécurité utilise les informations recueillies pour créer un environnement de travail plus sûr et plus propice.

Les efforts de suivi peuvent être regroupés en trois domaines interdépendants (et se recoupant parfois).

- **Conformité.** Examen régulier de la mise en œuvre des pratiques de gestion des risques de sécurité, y compris la communication régulière de signalements et le suivi des indicateurs clés afin de s'assurer que tout fonctionne correctement et de déterminer si des changements sont nécessaires. Les tableaux de bord jouent un rôle utile à cet égard.
- **Efficacité.** Analyses approfondies périodiques des processus afin de mesurer l'efficacité des pratiques et des systèmes de sécurité, y compris des audits de sécurité formels.
- **Impact.** Analyse approfondie utilisant les informations issues des efforts de suivi et d'autres sources afin de déterminer si le système de gestion des risques de sécurité de l'organisation influence le changement ou y contribue.

Ces points sont abordés plus en détail ci-dessous.

3.4.2 Suivi de la conformité

Pour le suivi la conformité, les organisations peuvent utiliser une combinaison de méthodes, telles que des listes de contrôle et des indicateurs clés de performance (de l'anglais « key performance indicators » ou KPI). L'objectif du suivi de la conformité est avant tout de comprendre les raisons de la non-conformité, et non de sanctionner le personnel. Il se peut que les processus ne soient pas suivis parce qu'ils sont irréalistes ou inadaptés au contexte. La non-conformité peut également révéler des difficultés, telles que des ressources insuffisantes, une perception négative des pratiques de sécurité parmi le personnel et des lacunes dans les connaissances. Un suivi de cette nature peut aider à identifier les lacunes et les défis à relever, notamment en matière de formation, d'orientation, de soutien ou d'autres activités positives visant à instaurer une culture de la sécurité. Le tableau 2 présente quelques exemples de mesures de suivi de la conformité.

Tableau 2 Exemples de mesures de suivi de la conformité

Mesure	Information
Listes de contrôle	Une liste de contrôle aide à évaluer la conformité aux politiques de sécurité et aux exigences minimales, en particulier au niveau du bureau ou du projet. Une liste de contrôle peut aider les responsables à vérifier rapidement que les informations qu'ils reçoivent du personnel sont correctes.
Indicateurs clés de performance (KPI)	Les KPI mesurent et suivent les performances par rapport aux objectifs stratégiques et opérationnels. Ils sont utilisés pour la prise de décision et l'amélioration des performances. Les KPI peuvent remplir plusieurs fonctions dans le cadre du suivi de la conformité. Ils peuvent être liés à des rôles et responsabilités individuels, en particulier ceux des responsables et du personnel, qui sont chargés de veiller au respect des règles de sécurité. Les programmes et les bureaux peuvent également disposer de KPI liés à la sécurité, tels que des pourcentages et des chiffres concernant, par exemple, les plans de sécurité actualisés, les briefings sur la sécurité destinés au personnel en déplacement, le nombre d'employés formés, le pourcentage du budget global consacré à la sécurité, le budget prévisionnel par rapport au budget réel alloué et l'utilisation des fonds consacrés à la sécurité, ainsi que la couverture des besoins. Certains KPI sur la sécurité peuvent également être mondiaux. Les tableaux de bord peuvent être particulièrement utiles pour le suivi des KPI, notamment pour le suivi des indicateurs dans différents bureaux, pays et régions (voir la section ci-dessous pour plus de détails sur les tableaux de bord).
Évaluation des performances du personnel	Les cadres supérieurs et autres personnes responsables de la gestion des risques de sécurité peuvent faire l'objet d'une évaluation des performances afin d'apprécier leurs performances dans les domaines de travail liés à la sécurité. Dans la plupart des cas, tous les membres du personnel, quel que soit leur poste, sont tenus de se conformer aux règles de sécurité et de partager les informations pertinentes avec le personnel de sécurité. Les chefs d'équipe peuvent également faire l'objet d'une évaluation des performances portant sur la manière dont eux-mêmes et leurs équipes se sont conformés au système de gestion des risques de sécurité. À cette fin, des éléments liés à la sécurité devront être inclus dans les processus de recrutement, tels que les descriptions de poste et les questions d'entretien.

Mesure	Information
Signalement régulier en matière de sécurité	Des signalements et analyses quantitatifs et qualitatifs réguliers sur la sécurité peuvent fournir une vue d'ensemble des pratiques de gestion des risques de sécurité et de leur mise en œuvre. Des rapports réguliers peuvent aider le personnel responsable à comprendre si les exigences minimales sont respectées, à identifier les défis et les lacunes et à prendre des mesures correctives. Des signalements et un suivi réguliers peuvent réduire la probabilité de résultats et de conclusions inattendus lors d'audits plus formels. Les indicateurs de signalements réguliers pourraient inclure : • Validité/expiration des plans de sécurité. • Changements dans les niveaux de sécurité. • Nombre et gravité des incidents et des personnes touchées. • Budget disponible pour la sécurité et montant dépensé. • Nombre d'employés formés à la sécurité par rapport aux cibles de l'organisation. Les outils en ligne peuvent faciliter le suivi de certains indicateurs clés. Par exemple, les organisations qui disposent de ressources de formation en ligne peuvent rapidement fournir, si nécessaire, des informations sur la conformité en matière de participation aux formations.
Analyse et signalement des incidents	Le suivi du nombre d'incidents affectant un lieu particulier peut fournir une vue d'ensemble des tendances et signaler les cas où les processus de gestion des risques de sécurité peuvent nécessiter une attention particulière. Cependant, cela peut être trompeur sans valeur de référence ou base de comparaison, car une augmentation peut indiquer une amélioration du signalement plutôt qu'une insécurité accrue. Outre le nombre d'incidents, le suivi de la manière dont les signalements sont gérés (retards dans la soumission, exhaustivité des modèles de signalement, niveaux de sous-signalement, etc.) peut aider à évaluer la conformité aux pratiques de sécurité. L'analyse d'incident permet également de soutenir les personnes touchées et sert d'alerte pour évaluer l'efficacité des évaluations des risques, des mesures d'atténuation et du système global de gestion des risques de sécurité. Elle permet également d'identifier les problèmes de conformité ou les lacunes dans les procédures, le soutien et la formation en analysant le type, la fréquence et les causes des incidents impliquant le personnel. (Voir le chapitre 4.4 pour plus d'informations sur le signalement des incidents.)
Analyses post-incident/post-crise	Tout comme l'analyse d'incident, une évaluation approfondie après un incident critique ou une crise peut fournir une vue d'ensemble de la conformité aux mesures de sécurité, ainsi que de leur pertinence et de leur efficacité.

Les cadres supérieurs doivent fournir un feedback afin d'encourager le signalement et la mise en œuvre d'autres mécanismes de conformité. Les conclusions de ce suivi, y compris les rapports, peuvent être mis à la disposition des responsables et autres membres du personnel concernés et partagées par e-mail, lors de réunions ou via un tableau de bord (voir ci-dessous).

Améliorer la gestion des risques de sécurité grâce au suivi peut parfois signifier tenir le personnel pour redevable du non-respect des politiques et des procédures. Si des preuves de non-conformité justifient une sanction, il est important que la politique de l'organisation à cet égard soit appliquée de manière transparente. La politique de l'organisation à cet égard doit être clairement communiquée au personnel à l'avance. L'objectif doit être de favoriser une culture de la sécurité positive, plutôt que de créer davantage de découragement ou d'animosité à l'égard des processus de sécurité.

Exemple de cas : Établir des relations pour améliorer la conformité

Une ONG internationale a constaté que la conformité et la culture de la sécurité globale s'étaient améliorées à la suite d'une refonte de la manière dont l'équipe de sécurité interagissait avec les autres membres du personnel. Cela a impliqué de supprimer le jargon sur la sécurité des communications et de prendre d'autres mesures pour instaurer la confiance et rendre l'équipe de sécurité plus accessible. Des efforts ont été faits pour recruter du personnel de sécurité issu de divers horizons et pour encourager le personnel à considérer l'équipe de sécurité comme une ressource essentielle et utile. Des activités de sensibilisation ont également été mises en place, notamment des sessions mensuelles sur la sécurité et des réunions avec différentes équipes organisationnelles. Le changement de ton adopté par la direction de l'organisation concernant le rôle de la sécurité en tant que facteur facilitant l'exécution des tâches par le personnel a également joué un rôle fondamental dans cette évolution.

Le personnel de sécurité a également tout intérêt à faire preuve de créativité dans la manière de promouvoir la conformité, notamment en envisageant différents types d'incitations. Les récompenses, ainsi que les mesures visant à dénoncer publiquement les contrevenants, se sont révélées efficaces dans certains cas. Par exemple, certaines organisations internationales utilisent des forums organisationnels pour dresser la liste des bureaux de pays qui ne se conforment pas aux règles ou qui ne respectent pas les principaux indicateurs de performance clés (KPI). Les tableaux de bord peuvent constituer un outil efficace à cet effet, comme l'illustre la section ci-dessous.

3.4.3 Suivi de l'efficacité

Afin de suivre l'efficacité, de plus en plus d'organisations procèdent désormais à des audits, des examens et des consultations en matière de sécurité. Ceux-ci vont au-delà du simple contrôle de la conformité et examinent de manière plus approfondie la mise en œuvre et l'efficacité des systèmes et des mesures de sécurité.

Audits de sécurité

L'objectif principal d'un audit de sécurité est d'examiner si les mesures de gestion des risques de sécurité mises en place par une organisation lui permettent d'atteindre les objectifs du programme sans exposer l'organisation et son personnel à des risques évitables. Le résultat d'un audit de sécurité devrait idéalement être un plan d'action qui aide le personnel à effectuer son travail en toute sécurité (figure 6).

La forme que prend un audit de sécurité, sa fréquence, les personnes qui le réalisent et son niveau de détail varient d'une organisation à l'autre. Cependant, les audits de sécurité peuvent être classés en deux grandes catégories : ceux qui concernent l'ensemble de l'organisation et ceux qui concernent un site spécifique.

Les audits de sécurité, en particulier ceux qui concernent un site spécifique, peuvent être utilisés pour vérifier que les mesures d'atténuation identifiées dans l'évaluation des risques et le plan de sécurité ont été mises en œuvre, et pour évaluer dans quelle mesure les politiques et procédures ont été respectées. Les audits de sécurité peuvent aider à déterminer si les évaluations et les plans initiaux sont toujours pertinents, et peuvent être utilisés pour vérifier l'exactitude des informations en matière de sécurité régulières (par exemple, par le biais de rapports de sécurité) provenant d'un lieu de travail particulier.

Les audits peuvent être ponctuels ou réguliers. Les audits spécifiques à un site sont réalisés conformément aux politiques mises en place au niveau organisationnel. Les audits de sécurité sont généralement annoncés à l'avance, mais ce n'est pas toujours le cas.

Si chaque organisation élabore ses propres processus et outils d'audit, y compris ses indicateurs clés, le Guide des audits de sécurité³⁷ du GISF (anciennement European Interagency Security Forum) et le Duty of Care Maturity Model (en anglais, « Modèle de maturité du devoir de diligence ») du Centre suisse de compétence pour la coopération internationale (CINFO)³⁸ proposent des exemples d'indicateurs pouvant servir de modèles pour évaluer les performances d'une organisation dans le domaine de la sécurité.³⁹ Les organisations ont tout intérêt à mettre en correspondance les indicateurs et les résultats avec les systèmes, cadres ou exigences en matière de sécurité.

37 Finucane, C. (2013) *Évaluations de la sécurité*. European Interagency Security Forum (<https://gisf.ngo/resource/security-audits/>).

38 Voir <https://dutyofcare.cinfo.ch/>

39 European Interagency Security Forum (aujourd'hui GISF) *Gestion du risque sécurité : Manuel de référence à l'attention des petites ONG* fournit un guide de référence rapide sur un certain nombre d'éléments liés à la sécurité qui peuvent être utiles pour planifier un audit ou un examen : <https://gisf.ngo/resource/security-risk-management-a-basic-guide-for-smaller-ngos/>.

Audit par opposition à examen

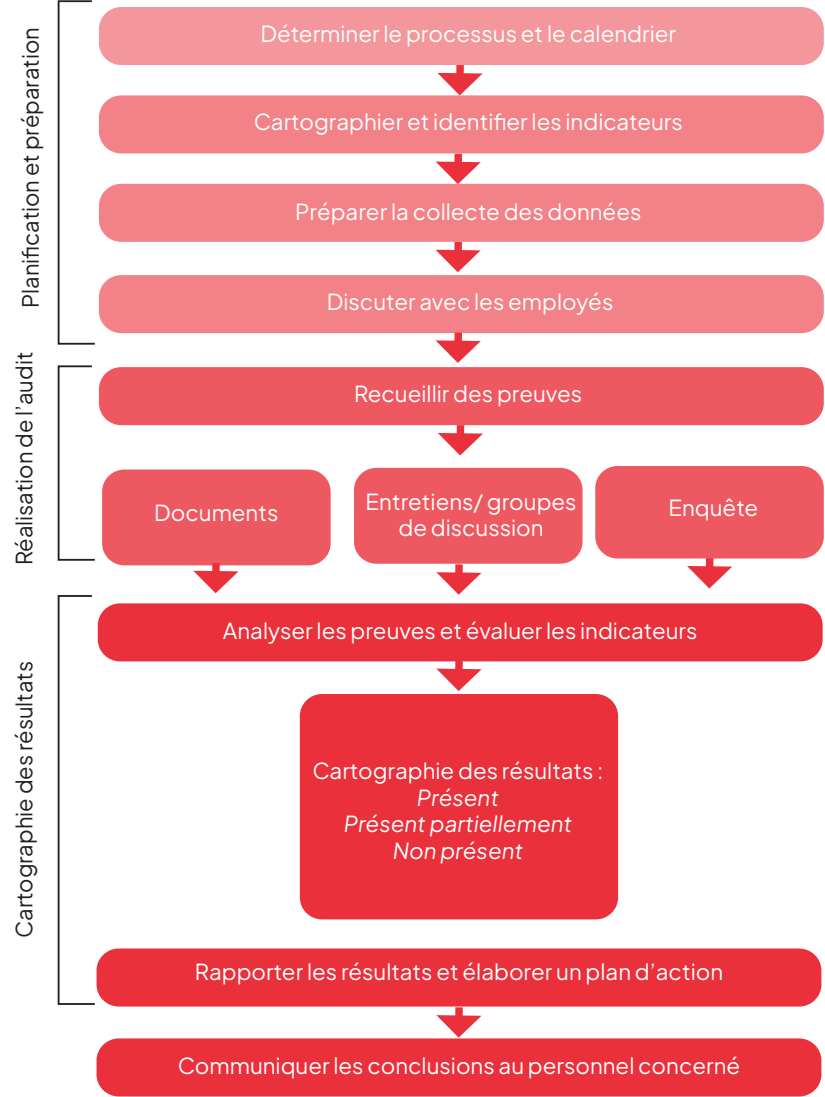
Un audit de sécurité est une évaluation formelle, axée sur la conformité, les politiques, procédures et pratiques de sécurité d'une organisation par rapport aux exigences et indicateurs organisationnels établis. En revanche, un examen de la sécurité est souvent un processus plus souple et informel qui évalue l'efficacité des mesures de sécurité, identifie les faiblesses et formule des recommandations d'amélioration, en mettant l'accent sur le renforcement de la sécurité globale plutôt que sur la seule conformité. Les audits de sécurité sont planifiés, tandis que les examens sont plus susceptibles d'être effectués après un incident critique ou à la suite d'un changement soudain du contexte.

Certaines organisations procèdent également à des examens globaux ou organisationnels des systèmes et approches de sécurité, qui sont des évaluations formelles basées sur des termes de référence spécifiques. Ceux-ci vont souvent au-delà d'une simple évaluation des normes ou exigences internes ; bien qu'ils puissent servir de référence par rapport aux approches courantes et aux bonnes pratiques du secteur, ils ne sont pas soumis à des normes externes spécifiques, c'est pourquoi on les qualifie souvent d'examens et non d'audits.

Certaines organisations ont choisi de ne pas utiliser le terme « audit » en raison de ses connotations négatives, préférant des termes tels que « examens » ou « contrôles » afin de s'éloigner de l'idée selon laquelle les examinateurs évaluent les performances individuelles ou cherchent à trouver des failles dans le travail des membres du personnel. Par conséquent, ce qui est considéré comme un « audit » par opposition à un « examen » varie d'une organisation à l'autre.

Les examens et les audits de sécurité évaluent tous deux la « santé » des systèmes de sécurité ainsi que la sensibilisation et la compréhension du personnel en matière de ressources et de mesures de sécurité. Ces évaluations offrent au personnel l'occasion de mettre en évidence les défis ou les risques de sécurité auxquels ils sont confrontés dans leur vie et leur travail, et qui pourraient ne pas être suffisamment pris en compte par les mesures de sécurité existantes.

Figure 6 Processus d'audit de sécurité



Adapté de Finucane, C. (2013) *Évaluations de la sécurité*. European Interagency Security Forum (www.gisf.ngo/resource/security-audits/).

Les audits peuvent comprendre un examen de la documentation pertinente, des données sur les incidents, des entretiens, des discussions de groupe avec le personnel clé et des enquêtes. Ils peuvent prendre beaucoup de temps.

Idéalement, les audits de sécurité devraient impliquer la consultation d'un large éventail de membres du personnel, et pas seulement ceux qui sont chargés de la gestion des risques de sécurité. La collecte des données pertinentes et l'évaluation des indicateurs clés sont suivies d'une analyse des conclusions, d'une présentation des résultats et d'un plan d'action. Un plan d'action énumère les activités spécifiques à mener, identifie les responsables, établit les priorités, fixe un calendrier et quantifie le budget nécessaire à la mise en œuvre.

Dans certains cas, il peut être judicieux de faire appel à des auditeurs ou à des consultants externes pour réaliser les audits de sécurité. Cela permet d'obtenir des résultats plus objectifs et peut également servir à comparer une organisation à ses pairs en s'appuyant sur les connaissances de l'évaluateur externe. Dans certains cas, un évaluateur externe peut également obtenir des réponses plus franches de la part des membres du personnel sur l'efficacité et les faiblesses du système de gestion des risques de sécurité. Lorsque le coût d'un évaluateur externe peut constituer un obstacle, les organisations collaborent parfois pour réaliser des évaluations par les pairs.

Exemple de cas : Processus d'audit

Une ONG internationale a mis au point un processus complet d'audit de la sûreté et sécurité, qui est en place depuis plusieurs années. Chaque année, plusieurs pays font l'objet d'un audit. Des auditeurs externes sont mandatés pour mener des consultations à la fois en personne et à distance. L'audit est réalisé sur la base de plus de 100 KPI. Les auditeurs produisent un rapport sur les KPI (axé sur la conformité) et un rapport narratif qui examine l'efficacité du système de sécurité dans son ensemble : ce qui fonctionne bien, les lacunes et les recommandations.

Mesure de l'acceptation

Une faiblesse inhérente aux audits de sécurité, et à tous les mécanismes de suivi, est la tendance à se concentrer sur des données faciles à collecter et à analyser, avec un biais particulier en faveur des données quantitatives (telles que le pourcentage de personnel formé et le nombre d'incidents de sécurité). Cela peut conduire à se concentrer sur les activités de protection, qui sont plus tangibles et plus faciles à enregistrer que les mesures d'acceptation.

Les mécanismes de suivi de la sécurité peuvent mesurer l'acceptation et les perceptions en tirant des données des activités de suivi programmatique et des enquêtes de perception, en développant et en mettant en œuvre des outils supplémentaires (tels que des analyses de l'acceptation) ou en intégrant des indicateurs d'acceptation dans les outils existants, tels que la cartographie des acteurs. Les évaluations de programmes peuvent fournir un moyen de suivre les perceptions et l'acceptation, mais elles alimentent rarement les efforts de suivi de la gestion des risques de sécurité.

Le projet « Acceptance Research » (en anglais) et la boîte à outils « Acceptance Toolkit » (en anglais) fournissent quelques conseils utiles sur la manière d'évaluer l'acceptation : <https://acceptanceresearch.wordpress.com>. Voir aussi le chapitre 4.2 - *Élaboration d'une stratégie de sécurité*.

Pour obtenir des outils et des recommandations sur la manière de suivre l'acceptation plus régulièrement, voir, par exemple, le modèle d'analyse de l'acceptation du GISF (<https://gisf.ngo/toolbox-pwa-fr/resource/2-strategie-dacceptation/>) et le chapitre 4 de *Achieving safe operations through acceptance: challenges and opportunities for security risk management* (en anglais, « Assurer la sécurité des opérations grâce à l'acceptation : défis et opportunités pour la gestion des risques de sécurité ») (<https://gisf.ngo/resource/achieving-safe-operations-through-acceptance/>).

Consultations

Les consultations ponctuelles du personnel sur les défis et les faiblesses sont de plus en plus courantes dans le secteur humanitaire. Elles font souvent suite à une plainte ou à des signalements d'inconduite ou de négligence, et peuvent porter sur des questions telles que le racisme, l'exploitation et les abus sexuels, le harcèlement et

les brimades. Les équipes de sécurité peuvent utiliser les enseignements tirés de ces consultations pour améliorer leur travail, et peuvent également bénéficier de la mise en place de leurs propres consultations sur des sujets particuliers liés à la sécurité. Les mécanismes de signalement confidentiel et de lancement d'alertes peuvent aider les organisations à mettre au jour les mauvaises pratiques en matière de sécurité.

Exemple de cas : Consultations

Une ONG internationale a interrogé plus de 2 000 employées dans plusieurs pays afin de comprendre leurs préoccupations en matière de sécurité. Les conclusions ont donné lieu à un rapport mondial et à un plan d'action, ainsi qu'à une évolution vers une approche institutionnelle des risques liés à l'identité. D'autres consultations sont prévues pour aborder d'autres risques et préoccupations liés à l'identité.

3.4.4 Évaluation de l'impact

L'impact désigne les changements, tant intentionnels qu'involontaires, qui résultent des activités d'une organisation. La mesure de l'impact consiste à évaluer ces changements, tant sur le plan qualitatif que quantitatif. Elle permet de déterminer dans quelle mesure les changements observés peuvent être attribués à des actions spécifiques menées par une organisation.

Pour mesurer l'impact, les organisations peuvent appliquer une approche fondée sur la théorie du changement, qui consiste à établir une feuille de route détaillée décrivant les résultats souhaités à long terme, tels que la création d'un environnement de travail plus sûr, et les mesures nécessaires pour les atteindre. Ce processus implique généralement de décomposer l'objectif à long terme en résultats intermédiaires, tels que l'amélioration de la gestion de crise et la réduction du taux d'incidents, qui peuvent être suivis dans le temps et soutenus par des activités spécifiques, telles que des formations à la sécurité et la planification de la gestion de crise. Il est conseillé d'identifier des indicateurs appropriés de changement positif et négatif, en mettant l'accent sur la détermination de la causalité (c'est-à-dire dans quelle mesure le changement est dû à l'influence ou à la contribution des pratiques et des systèmes de gestion des risques de sécurité). Les mécanismes de suivi décrits dans ce chapitre peuvent aider à évaluer l'impact.

Les exercices d'évaluation d'impact ne doivent pas nécessairement viser à trouver des preuves concluantes qu'une intervention a contribué à un changement ou à une série de changements. Le processus peut plutôt se concentrer sur la production d'un récit plausible, fondé sur des preuves, qui indique l'impact. Les questions d'apprentissage basées sur des preuves peuvent être utiles dans cet exercice (voir l'encadré ci-dessous pour des exemples).

Exemples de questions d'apprentissage basées sur des preuves

- Dans quelle mesure les programmes de formation à la sécurité de l'organisation améliorent-ils la sensibilisation et le comportement du personnel en matière de risques de sécurité?
 - Registres de présence à la formation, évaluations avant et après la formation, enquêtes de satisfaction auprès du personnel et changements observés dans le comportement ou la prise de décision.
- Quel impact les incidents de sécurité ont-ils eu sur les capacités de l'organisation à fournir une aide humanitaire?
 - Registres des perturbations opérationnelles, des retards ou des changements dans la mise en œuvre des programmes dus à des incidents de sécurité. Entretiens avec le personnel sur la manière dont les incidents de sécurité ont affecté les opérations.
- Y a-t-il des améliorations observables dans les résultats de la gestion des risques de sécurité par rapport aux périodes précédentes et à d'autres organisations similaires opérant dans les mêmes zones?
 - Données historiques sur les incidents de sécurité, analyses des tendances (par rapport à d'autres organisations) et comparaisons de l'efficacité de la gestion de risque au fil du temps.
- Quels enseignements ont été tirés des incidents de sécurité récents et comment ont-ils été appliqués pour améliorer les pratiques?
 - Examens post-incident, plans d'action, enseignements tirés documentés, modifications apportées aux politiques ou procédures sur la base de ces enseignements et suivi de l'efficacité de ces modifications.
- Quel a été l'impact des mesures de sécurité sur la fidélisation et le recrutement des employés? (Un environnement de travail sûr peut être un facteur clé pour attirer et fidéliser le personnel.)
 - Taux de rotation par site par rapport aux indicateurs de sécurité, feedback résultant des entretiens de départ (raisons du départ), nombre de candidats à un poste et leur feedback sur la réputation de l'entreprise en matière de sécurité.

3.4.5 Visualisation des données et tableaux de bord

Les organisations utilisent de plus en plus les tableaux de bord numériques dans la gestion des risques de sécurité. Un tableau de bord est un ensemble d'indicateurs clés et de points de données affichés en temps réel sur une plateforme unique. Les tableaux de bord facilitent la visualisation des données sous différents formats, tels que des cartes, des KPI, des tableaux et des graphiques. Ces outils sont accessibles à la fois publiquement et en privé, et leur compatibilité avec les appareils mobiles est de plus en plus courante.⁴⁰

Les tableaux de bord prennent en charge de nombreuses applications dans le domaine de la gestion des risques de sécurité, notamment la visualisation des niveaux de sécurité et des restrictions de déplacement par lieu, le stockage et l'accès aux évaluations des risques et aux plans de sécurité, le suivi de la conformité, l'affichage des chiffres relatifs aux incidents et l'aide à l'identification des lacunes afin de hiérarchiser les financements et autres formes de soutien. Ils facilitent également la formation des nouvelles recrues, la préparation des rapports et le suivi des allocations budgétaires. Ces données en temps réel permettent aux organisations de prendre rapidement des mesures correctives, sans avoir à attendre les rapports ou mises à jour périodiques.

Lors de la conception d'un tableau de bord, il est essentiel de définir son objectif, les informations nécessaires à son fonctionnement, les méthodes de collecte des données, les rôles et responsabilités ainsi que les autorisations d'accès. Il existe différentes solutions de visualisation des données disponibles à l'achat, certaines étant gratuites jusqu'à un certain niveau d'utilisation. La compatibilité avec les systèmes existants est un critère essentiel à prendre en compte.

Exemple de cas : Tableaux de bord, conformité et impact

Une grande ONG internationale a investi dans l'amélioration du taux de plans de sécurité valides, la simplification du format et un suivi plus étroit, pour lesquels un tableau de bord s'est avéré essentiel. Le tableau de bord a involontairement créé une « saine concurrence » entre les équipes de pays pour montrer qui répondait le mieux aux exigences en matière de sécurité. Avant l'introduction du tableau de bord, l'organisation avait du mal à améliorer la conformité. Les plans n'étaient pas mis à jour avant leur date d'expiration et la visibilité était faible entre les bureaux de pays, régionaux et mondiaux.

40 Pour un exemple de tableau de bord accessible au public, voir INSO : <https://ngosafety.org/conflict-data-dashboard/#dashboard>

Grâce au tableau de bord, les responsables ont pu voir comment leurs pays et leurs régions se comportaient en matière de conformité, à l'aide d'un simple code couleur inspiré des feux de signalisation. Le tableau de bord a ensuite été publié sur l'intranet de l'équipe de sécurité et partagé avec les décideurs.

Un indicateur clé de performance (KPI) en matière de sécurité a été créé sur la base du nombre de plans de sécurité à jour, visibles par le personnel des bureaux de pays, régionaux et internationaux. Un an après l'introduction du tableau de bord, l'indicateur a atteint 70 %, simplement grâce à la mise à disposition du personnel des données. Au cours de la deuxième année, il a atteint 79 %.

Des tableaux de bord fiables nécessitent des données pertinentes, fiables et accessibles, tant internes qu'externes. Des processus de collecte et de gestion des données doivent être mis en place, avec des garanties de confidentialité. Les tableaux de bord doivent viser à trouver un équilibre entre le besoin de partage d'informations et les exigences de confidentialité et les réglementations en matière de protection des données, en veillant à ce que les informations sensibles soient traitées de manière appropriée.

Les outils de visualisation des données sont conçus pour être présentés et partagés, et pour aider les responsables à prendre des décisions. Tout conflit entre confidentialité et partage d'informations devrait idéalement être résolu lors de la phase de conception et de planification.

Informations complémentaires

Recommandations et recherches

Bickley, S. (2017) *Gestion du risque sécurité : manuel de référence à l'attention des petites ONG*. European Interagency Security Forum (<https://gisf.ngo/resource/security-risk-management-a-basic-guide-for-smaller-ngos/>).

Billaudel, R. (2021) 'Measuring and improving acceptance: ACF's experience and perspectives' (en anglais, « Mesurer et améliorer l'acceptation : l'expérience et les perspectives d'ACF » sur le site du GISF (éd.) *Achieving safe operations through acceptance: challenges and opportunities for security risk management* (en anglais, « Assurer la sécurité des opérations grâce à l'acceptation : défis et opportunités pour la gestion des risques de sécurité ») (<https://gisf.ngo/resource/achieving-safe-operations-through-acceptance/>).

Finucane, C. (2013) *Évaluations de la sécurité*. European Interagency Security Forum (www.gisf.ngo/resource/security-audits/).

GISF (2024) *Développement de la stratégie et de la politique de gestion des risques de sécurité (GRS) : Un guide interfonctionnel* (<https://gisf.ngo/resource/srm-strategy-and-policy-guide/>).

GISF et Humanitarian Outcomes (2024) *State of practice: the evolution of security risk management in the humanitarian space* (en anglais, « État des lieux : l'évolution de la gestion des risques de sécurité dans le domaine humanitaire ») (https://humanitarianoutcomes.org/security_risk_mgmt_humanitarian_space_2024).

Outils

CINFO (n.d.) *Duty of care maturity model* (en anglais, « Modèle de maturité du devoir de diligence ») (<https://dutyofcare.cinfo.ch/model.html>).

Collaborative Learning Approach to NGO Security Management (2011) *Acceptance toolkit* (en anglais, « Approche collaborative de l'apprentissage en matière de gestion de la sécurité des ONG (2011), Boîte à outils sur l'acceptation ») (<https://acceptanceresearch.wordpress.com/acceptance-toolkit/>).

GISF (n.d.) 'Acceptance analysis template - xlsx' (en anglais, « Modèle d'analyse d'acceptation - xlsx »). 2. *Stratégie d'acceptation*. Guide interfonctionnel sur la sécurité des ONG (<https://gisf.ngo/toolbox-pwa-fr/resource/2-strategie-dacceptation/>).

INSO (n.d.) *Conflict data dashboard* (en anglais, « Tableau de bord des données sur les conflits ») (<https://ngosafety.org/conflict-data-dashboard/#dashboard>).

3.5 Gestion des risques de sécurité dans les partenariats

Dans le domaine de l'aide humanitaire, il est courant qu'une partie ou la totalité d'un programme soit conçue et « détenue » par une organisation, mais mise en œuvre en partie ou en totalité par une autre. Travailler avec et par l'intermédiaire d'autres organisations ou associations peut s'avérer plus rentable, plus judicieux sur le plan programmatique ou s'inscrire dans le cadre d'une stratégie délibérée, par exemple pour renforcer les capacités locales ou réduire les risques. Le nombre de partenariats dans le secteur humanitaire a augmenté ces dernières années, en partie grâce aux efforts de localisation et de décolonisation. Ce chapitre examine les partenariats équitables sous l'angle de la sécurité. Tout en reconnaissant la diversité des partenariats dans le secteur humanitaire et en visant une application générale, il se concentre sur les partenariats entre les organisations internationales et les acteurs nationaux et locaux.⁴¹

3.5.1 Principes et considérations stratégiques

Un partenariat est une relation de travail formalisée entre deux ou plusieurs organisations visant à atteindre des objectifs convenus. Les partenariats dans le secteur humanitaire peuvent varier en termes de forme, de durée, de portée et de degré de collaboration ; ils peuvent être stratégiques et à long terme, ou basés sur des projets et à court terme. Ils sont souvent bilatéraux entre des organisations internationales et des acteurs nationaux (par exemple, des ONG locales et des groupes communautaires), mais peuvent également être conclus entre plusieurs organisations (par exemple, par le biais de consortiums et de subventions de tutelle), entre des organisations et des entreprises privées, ainsi qu'entre des ONGN. Pour certaines organisations internationales, la mise en œuvre par l'intermédiaire de partenaires locaux peut constituer leur mode de fonctionnement principal, tandis que pour d'autres, il peut s'agir uniquement d'un écart occasionnel par rapport à la mise en œuvre directe par leur propre personnel.

Les accords ou contrats de partenariat ont tendance à dicter la portée de ce type d'arrangements, les responsabilités en matière de sécurité étant parfois précisées dans les accords comme relevant de chaque entité juridique individuelle. Dans certaines circonstances, les accords peuvent imposer un transfert de soutien, par exemple en cas d'incident critique. Dans de nombreux cas, cependant, les responsabilités ne sont pas clairement définies et la coopération en matière de gestion des risques de sécurité n'est pas précisée, ce qui entraîne de grandes disparités dans la manière dont ces questions sont traitées.

41 Certaines publications font la distinction entre les organisations et les acteurs « nationaux » et « locaux ». La présente Revue des bonnes pratiques (RBP) utilise ces deux termes de manière interchangeable pour désigner tous les types d'organisations qui opèrent exclusivement dans un seul pays, que ce soit dans plusieurs endroits ou dans un seul, y compris les groupes communautaires.

Les appels de plus en plus nombreux en faveur de la « localisation » dans le secteur humanitaire n'ont malheureusement pas donné lieu à un débat équivalent sur la gestion des risques de sécurité et les considérations relatives au devoir de diligence dans les accords de partenariat international-local. Cela se fait souvent au détriment des acteurs locaux, qui sont souvent les plus exposés au risque d'incidents de sécurité graves, mais qui bénéficient du moins de soutien en matière de sécurité (tant au sein de leurs organisations que de la part de leurs partenaires internationaux).⁴² La recherche a également montré que, dans les partenariats internationaux-locaux, les risques les plus discutés et les plus atténués sont les risques fiduciaires, tandis que les risques de sécurité sont souvent traités de manière superficielle. Bien que cela semble changer, des défis subsistent.⁴³

La question de savoir si et comment les accords de partenariat prennent en compte la gestion des risques de sécurité peut souvent refléter :

- dans quelle mesure chaque organisation partenaire examine et traite en interne les risques de sécurité ; et
- les circonstances et les objectifs du partenariat.

Les organisations qui manquent de connaissances ou de capacités, ou qui ne disposent pas de systèmes internes solides de gestion des risques de sécurité, peuvent se sentir incapables d'avoir des discussions sur la sécurité ou d'étendre leur soutien au-delà de leur propre organisation et de leur personnel, ou peuvent ne pas avoir la culture de la sécurité organisationnelle nécessaire pour même envisager de le faire. L'engagement peut également varier au sein d'une même organisation en raison des capacités variables en matière de gestion des risques de sécurité entre les différents bureaux et sites.

L'intentionnalité ou l'objectif d'un partenariat influe également sur la manière dont celui-ci est perçu et géré, ce qui a des conséquences sur la manière dont les partenaires discutent des risques auxquels ils sont confrontés dans l'exercice de leurs activités. Par exemple, la recherche sur les partenariats locaux-internationaux a montré que les modèles de partenariat à court terme, basés sur des projets, ne sont pas propices aux discussions ou au soutien en matière de gestion des risques de sécurité.⁴⁴

42 GISF (2020) *Partnerships and security risk management: from the local partner's perspective* (en anglais et en espagnol, « Partenariats et gestion du risque sécurité: du point de vue du partenaire local ») (<https://gisf.ngo/resource/partnerships-and-security-risk-management-from-the-local-partners-perspective/>) ; GISF et Humanitarian Outcomes (2024) *State of practice: the evolution of security risk management in the humanitarian space* (en anglais, « État des lieux: l'évolution de la gestion des risques de sécurité dans le domaine humanitaire ») (https://humanitarianoutcomes.org/security_risk_mgmt_humanitarian_space_2024).

43 Humanitarian Outcomes (2019) *NGOs & risk: managing uncertainty in local-international partnerships (global report)* (en anglais, « ONG et risques: gérer l'incertitude dans les partenariats locaux-internationaux (rapport mondial) ») (<https://humanitarianoutcomes.org/publications/ngos-risk2-partnerships>) ; GISF et Humanitarian Outcomes (2024).

44 GISF (2020).

3.5.2 Défis

Les partenaires sont confrontés à un certain nombre de défis et d'obstacles lorsqu'ils tentent de s'engager dans une gestion des risques de sécurité mutuellement avantageuse.

Devoir de diligence – considérations juridiques et éthiques

Comme indiqué au chapitre 1.1, « Concepts et principes fondamentaux », le devoir de diligence légal s'applique généralement uniquement aux employés d'une organisation, et non à ceux des organisations partenaires. Il existe néanmoins un devoir éthique de soutenir les partenaires dans la gestion des risques de sécurité et de partager les informations pertinentes, les connaissances et les bonnes pratiques. Certaines organisations internationales craignent qu'en offrant un tel soutien, elles n'assument involontairement une responsabilité légale envers le personnel de leurs partenaires. Pour cette raison, certains membres du personnel de sécurité ont été invités par leur conseiller juridique à s'abstenir de collaborer avec leurs partenaires sur les questions de sécurité.⁴⁵

Bien que l'étendue et la nature de la responsabilité juridique puissent varier considérablement selon la juridiction et les circonstances particulières, ces préoccupations peuvent être exagérées. Comme pour les individus,⁴⁶ la responsabilité juridique d'une organisation envers un partenaire peut dépendre du « degré de maîtrise du risque » qu'elle exerce sur les processus décisionnels de ce dernier.

Bien qu'il soit recommandé de prendre en considération les instruments juridiques pertinents et leurs implications sur la gestion des risques de sécurité dans le cadre des partenariats, ignorer complètement cette question constitue un manquement éthique qui pourrait, potentiellement, entraîner des conséquences juridiques. En général, il est avantageux pour toute organisation qui conclut régulièrement des partenariats d'établir une politique sur le type de soutien qu'elle fournira ou attendra de ses partenaires. En plus de préciser les responsabilités, le soutien apporté aux partenaires en matière de sécurité doit viser à rester collaboratif, sans imposer une approche particulière plutôt qu'une autre, et à laisser clairement la prise de décision à chaque organisation. À cet égard, il est également important d'être conscient de la manière dont les déséquilibres de pouvoir et les incitations financières peuvent faire passer le « soutien et les conseils » pour des directives. Dans certaines juridictions, une personne morale peut être tenue responsable s'il s'avère qu'un accord a porté préjudice à l'une des parties, même si les deux parties l'ont accepté. Cela est particulièrement préoccupant, car les partenaires de mise en œuvre peuvent se sentir contraints d'accepter des risques de sécurité plus importants que ceux qu'ils jugent acceptables afin d'obtenir des contrats. Pour remédier à cette situation, les

45 GISC et Humanitarian Outcomes (2024).

46 La responsabilité juridique d'une organisation envers un individu peut être relative au « degré de maîtrise du risque » que l'organisation exerce sur la situation de cet individu. Par exemple, une organisation qui accueille un visiteur non employé dans un pays donné et qui contrôle entièrement le lieu de séjour du visiteur, ses modalités de déplacement et son itinéraire général, aura probablement un devoir de diligence légal envers cet individu, qu'il existe ou non un accord contractuel. Voir Kemp, E. et Merkelbach, M. (2016) *Duty of care: a review of the Dennis v Norwegian Refugee Council ruling and its implications* (en anglais, « Devoir de diligence : examen de l'arrêt Dennis contre Norwegian Refugee Council et de ses implications »). European Interagency Security Forum (www.gisf.ngo/resource/review-of-the-dennis-v-norwegian-refugee-council-ruling/).

partenaires peuvent donner la priorité à l'établissement d'une relation de confiance entre eux et au développement d'une communication solide autour de ces questions.

Transfert du risque

Parfois, les ONG internationales s'associent à des acteurs locaux afin de réduire les risques encourus par leur propre personnel. Dans ces circonstances, le transfert du risque devient un élément d'une stratégie de gestion de risque opérationnelle dans le cadre de laquelle une organisation cherche quelqu'un d'autre pour mener à bien certaines activités en contexte d'insécurité afin de réduire les risques pour son propre personnel. Cette définition classique du «transfert du risque» a fait l'objet de nombreuses discussions ces dernières années et des efforts sont en cours pour remédier aux manquements inhérents au devoir de diligence éthique qui peuvent en découler, en particulier lorsqu'aucune évaluation claire n'indique que le personnel des organisations locales est moins exposé au risque que celui des organisations internationales.

S'il est parfois plus facile pour les acteurs locaux que pour les organisations internationales de maintenir l'accès dans des environnements instables, cela doit être correctement évalué et convenu par les deux partenaires. Les acteurs internationaux et locaux peuvent être confrontés à des risques et des défis différents selon les contextes, y compris des risques qu'ils peuvent se transférer ou créer les uns aux autres dans le cadre du partenariat. En effet, en concluant un partenariat, les organisations transfèrent automatiquement des risques, de manière intentionnelle ou non. Par exemple, en s'associant à une organisation internationale pour mettre en œuvre un programme très médiatisé, un groupe communautaire peut être exposé à un risque accru en raison de l'attention supplémentaire qu'il peut susciter, notamment de la part des autorités locales et des communautés.

Dans cette optique, le transfert du risque s'entend comme « la formation ou la transformation des risques (augmentation ou diminution) pour un acteur, causée par la présence ou les actions d'un autre ».⁴⁷ Cela peut aller au-delà des partenariats internationaux et locaux et inclure les relations avec les donateurs et d'autres acteurs, tels que les organisations communautaires.

Les bonnes pratiques encouragent les partenaires à réfléchir à l'impact qu'un partenariat peut avoir sur leur exposition respective à certaines menaces et sur la capacité de chaque organisation à faire face aux risques avant de conclure un accord de partenariat.

Déficits de financement

Les organisations nationales reçoivent systématiquement des financements insuffisants, sporadiques et liés à des projets spécifiques, ce qui les empêche de développer les systèmes et les ressources nécessaires pour gérer efficacement les risques de sécurité.⁴⁸ Compte tenu de la pénurie générale de financement et d'un environnement

47 GISF (2021) *Partenariats et gestion du risque sécurité : guide d'action conjointe pour les organisations humanitaires locales et internationales* (<https://gisf.ngo/resource/partnerships-and-security-risk-management-a-joint-action-guide-for-local-and-international-aid-organisations/>).

48 GISF (2020) ; GISF et Humanitarian Outcomes (2024).

extrêmement concurrentiel, les budgets des partenariats peuvent ne pas inclure de lignes budgétaires spécifiques à la sécurité ou de coûts de base adéquats, tandis que les acteurs locaux peuvent être incités à donner la priorité aux coûts des programmes plutôt qu'aux dépenses liées à la sécurité lorsqu'ils concluent des accords de partenariat. Les partenaires locaux peuvent également se sentir obligés d'accepter des niveaux de risque plus élevés pour obtenir un financement. Sachant cela, il est recommandé aux organisations internationales de veiller systématiquement à ce que les budgets des partenaires prévoient des fonds pour la sécurité, soit sous forme de coûts de sécurité évalués, soit sous forme de pourcentage standard du financement global fourni.

Défis en matière de communication et de confiance

Il existe de nombreux obstacles à la communication sur la sécurité au sein des partenariats, mais le principal est l'absence totale de discussion sur la sécurité. La communication sur les questions de sécurité se limite trop souvent à des contrôles de diligence raisonnable des partenaires de mise en œuvre ou à un élément d'un ensemble plus large de mesures de « renforcement des capacités » menées par un partenaire international. Les points focaux pour les questions de sécurité des deux organisations peuvent ne pas être suffisamment impliqués dans ces discussions initiales.

La sécurité peut être un sujet sensible et les acteurs de mise en œuvre peuvent être dissuadés de parler honnêtement de leurs problèmes de sécurité et du soutien dont ils ont besoin, par crainte de répercussions financières et sur leur réputation. Les partenaires financiers peuvent craindre d'engager leur responsabilité juridique s'ils abordent le sujet, comme indiqué ci-dessus. Les discussions sur la sécurité sont également susceptibles de poser des difficultés en raison d'un manque de vocabulaire commun, de différences dans la compréhension de la sécurité, du risque et de l'appétence au risque, ainsi que de déséquilibres de pouvoir. Il faut du temps pour établir et maintenir des relations de confiance, que le financement à court terme et basé sur des projets peut encore compromettre.

3.5.3 Considérations pratiques

Une approche stratégique et axée sur les politiques en matière de partenariats permet aux organisations d'adopter plus facilement une approche équitable de la gestion des risques de sécurité. L'objectif est de faire évoluer les discussions sur la sécurité au sein du partenariat, afin qu'elles ne portent plus uniquement sur les contrôles de diligence raisonnable et le « transfert du risque », mais qu'elles débouchent sur des discussions collaboratives sur la manière de « partager les risques », en impliquant directement les points focaux pour les questions de sécurité et le personnel chargé des programmes concernés de tous les partenaires.

Le guide du GISF intitulé *Partenariats et gestion du risque sécurité* propose une feuille de route pour la mise en œuvre de cette approche, qui est résumée dans les sections suivantes de ce chapitre.⁴⁹

49 GISF (2021).

Avant de conclure un partenariat : approche stratégique et discussions préalables

Bien qu'il existe de nombreux exemples positifs de collaboration informelle entre les points focaux pour les questions de sécurité dans le cadre de partenariats, ceux-ci ne sont souvent pas viables dans la pratique. Sans une approche stratégique claire expliquant pourquoi et quand une organisation peut rechercher des partenaires, ou comment elle abordera la gestion des risques de sécurité au sein des partenariats, les dispositions en matière de sécurité peuvent être soumises aux préférences et aux préjugés individuels des membres du personnel, et les résultats positifs risquent d'être perdus lorsque le personnel change de fonction.

Les organisations qui ont élaboré des politiques relatives à la conclusion d'accords de partenariat et à leurs responsabilités envers leurs partenaires, ainsi que des accords de sécurité clairement énoncés, bénéficient d'accords de partenariat plus stratégiques et mieux équilibrés, qui favorisent davantage les discussions constructives sur la gestion des risques de sécurité et le soutien mutuel. Cette approche stratégique augmente les chances que les deux partenaires tirent profit du partenariat et réduit la probabilité d'un transfert du risque involontaire et non traité.

Dans la pratique, cela implique de veiller à ce que les considérations de sécurité des points focaux soient intégrées dans la documentation stratégique des partenariats et les politiques connexes. Les discussions préalables peuvent être intégrées dans les processus de diligence raisonnable. Si elles sont bien menées, ces discussions offrent aux partenaires l'occasion d'aborder ensemble les préoccupations liées au transfert du risque, d'évaluer les capacités et l'état de préparation en matière de sécurité, et d'explorer les moyens de se soutenir mutuellement sur les questions liées à la sécurité.

Exemple de cas : Au-delà des processus de diligence raisonnable unilatéraux

Une ONG internationale a commencé à impliquer son personnel de sécurité local dans les processus d'identification et de recrutement des partenaires de mise en œuvre locaux. Cela a permis à l'organisation d'aborder les questions de sécurité dès le début d'un partenariat, et a fait en sorte que la sécurité ne se limite plus à un simple « examen des systèmes » dans le cadre du partenariat.

Au cours de cette phase, les partenaires doivent s’efforcer d’évaluer comment les risques sont transférés entre les organisations et trouver ensemble des moyens de relever les défis qui se présentent, y compris les risques liés à l’identité découlant de la perception externe de l’organisation et de son personnel. Par exemple, s’il apparaît qu’une communauté locale a une perception négative de certaines tâches qu’un partenaire de mise en œuvre est censé accomplir pour son partenaire financier, les partenaires peuvent discuter de mesures d’atténuation. Il peut s’agir de réduire la visibilité de ces activités du programme ou de modifier le projet afin de renforcer la sécurité du personnel de mise en œuvre. Voir le tableau 3 pour quelques questions clés.

Début du partenariat : convenir d'une approche de gestion des risques de sécurité

Peu après avoir conclu un partenariat ou, si cela est possible et approprié, avant de finaliser le contrat, les organisations devraient s’efforcer de convenir de la manière dont chaque partenaire peut soutenir l’autre sur les questions liées à la sécurité qui se posent dans le cadre du partenariat et de la mise en œuvre du programme.

Le guide du GISF intitulé *Partenariats et gestion du risque sécurité* fournit une liste de questions pouvant faciliter ces discussions et propose quelques idées sur la gestion conjointe des risques de sécurité entre partenaires. Un résumé des questions clés figure dans le tableau 3.

Tableau 3 Questions préliminaires sur la gestion des risques de sécurité

Zone	Questions
Devoir de diligence	• Quelles sont les obligations légales et éthiques respectives de chaque partenaire en matière de devoir de diligence ? • Ces éléments sont-ils clairement expliqués dans les documents relatifs au partenariat ?
Gouvernance et redevabilité	• Les deux partenaires ont-ils contribué aux décisions clés concernant le programme, le projet, le partenariat et/ou la sécurité ? • Les deux partenaires disposent-ils de structures appropriées de gestion des risques de sécurité (y compris les rôles et responsabilités) pour permettre la réalisation des objectifs du partenariat ? • L’accord de partenariat mentionne-t-il les risques de sécurité et leur gestion ? • Les partenaires peuvent-ils se soutenir mutuellement, par exemple en recrutant du personnel de sécurité dédié ?

Zone	Questions
Transfert du risque	• Comment chaque partenaire est-il perçu par les parties prenantes concernées ? • L'identité organisationnelle d'un partenaire peut-elle avoir un impact sur l'autre partenaire ? • Le partenariat entraîne-t-il de nouvelles menaces pour l'une ou l'autre organisation ? • Le partenariat modifie-t-il l'impact ou la probabilité d'une menace ? Si oui, est-ce positif ou négatif ? • Lors de l'examen des mesures d'atténuation, une organisation peut-elle prendre des mesures particulières pour réduire le risque auquel est confronté son partenaire ? • Dans les environnements conflictuels, comment le partenariat interagit-il avec la dynamique du conflit, et des mesures peuvent-elles être prises pour mieux tenir compte des conflits ?
Politiques et principes	• Le mandat, la mission, les valeurs et les principes de chaque organisation sont-ils compris par les deux partenaires, et les deux organisations sont-elles à l'aise avec le travail et l'approche de l'autre en matière d'opérations et de sécurité (par exemple, les deux parties sont-elles d'accord avec la position de l'autre sur les principes humanitaires et la sauvegarde) ?
Opérations et programmes	• Quels sont les besoins et les attentes de chaque partenaire en matière de sécurité ? • Les partenaires disposent-ils d'un système convenu pour identifier et suivre les risques de sécurité encourus par le personnel ? • Les partenaires ont-ils des points focaux pour les questions de sécurité qui peuvent communiquer entre eux sur les questions de sécurité ? • Les partenaires s'accordent-ils sur les personnes responsables de la gestion des risques identifiés et sur la manière dont ces postes doivent être gérés et financés ? • Existe-t-il un système permettant aux deux partenaires d'être informés des risques de sécurité et des changements dans l'environnement des risques (physiques et en ligne) ? • Chaque partenaire dispose-t-il de ressources suffisantes (par exemple, financement, temps et personnel) pour gérer les risques de sécurité ?
Approches de gestion des risques de sécurité inclusive	• L'approche de gestion des risques de sécurité des deux organisations tient-elle compte de la manière dont l'identité des membres du personnel peut influencer sur leur vulnérabilité aux menaces ? • Comment les partenaires doivent-ils aborder les questions sensibles liées à l'identité, telles que les menaces internes et externes fondées sur l'orientation sexuelle ou le genre ? Quels sont les niveaux de confort (compte tenu des sensibilités culturelles) ? • Comment les partenaires peuvent-ils se soutenir mutuellement pour sortir de leur zone de confort afin de garantir une gestion des risques de sécurité efficace pour l'ensemble du personnel ?

Zone	Questions
Menaces internes et sauvegarde	• Comment les partenaires géreront-ils les menaces à la sécurité pouvant provenir de l'intérieur de leurs propres organisations ? • Comment les questions de sauvegarde sont-elles abordées au sein du partenariat ? • Des mécanismes de signalement appropriés de cas de sauvegarde sont-ils en place ?
Déplacement	• Comment gérer les risques de sécurité résultant des déplacements liés au partenariat ?
Sensibilisation et partage des capacités	• Comment les partenaires identifieront-ils les besoins en matière de sensibilisation à la sécurité et de renforcement des capacités, et comment y répondront-ils conjointement (tant pour la sécurité personnelle que pour la gestion des risques de sûreté et sécurité) ? • Le personnel de sécurité d'un partenaire peut-il fournir des conseils, un encadrement et un soutien technique aux points focaux pour les questions de sécurité de l'autre organisation, si cela s'avère nécessaire ? • Le personnel des partenaires a-t-il accès à une formation à la sécurité appropriée (interne et externe aux organisations partenaires) ?
Suivi des incidents	• Comment les partenaires doivent-ils partager les informations relatives aux incidents, le cas échéant ?
Gestion de crise et d'incident	• Comment les partenaires collaboreront-ils/se coordonneront-ils en cas de crise ou d'incident critique affectant l'une ou l'autre organisation sur le lieu où le partenariat est actif ?
Bien-être du personnel	• Les deux partenaires ont-ils accès à des polices d'assurance pertinentes ? Si ce n'est pas le cas, l'un des partenaires peut-il aider l'autre à souscrire une assurance appropriée ? • Les deux partenaires ont-ils mis en place des politiques et des procédures de bien-être du personnel, notamment en ce qui concerne les soins médicaux, la santé mentale et le soutien post-incident ? • Les partenaires peuvent-ils se soutenir mutuellement en mettant à disposition des ressources et des activités pertinentes pour le bien-être du personnel (notamment en apportant des changements au sein du partenariat afin d'améliorer le bien-être du personnel, tels que la réduction de la charge de travail, la flexibilité des horaires et la réduction des exigences administratives) ?
Les réseaux de sécurité et la collaboration entre les acteurs	• Existe-t-il des plateformes dans le contexte concerné qui traitent des questions de sécurité ? Si oui, les deux partenaires ont-ils accès à ces plateformes et réseaux dans leurs zones opérationnelles, y compris les plateformes de partage d'informations en matière de sécurité, et y ont-ils une voix sur un pied d'égalité ? • L'accès aux mécanismes de coordination existants peut-il être amélioré pour l'un ou l'autre des partenaires ?

Zone	Questions
Suivi de la conformité et de l'efficacité	• Comment les deux partenaires doivent-ils examiner les mesures de gestion des risques de sécurité au cours du partenariat ?
Ressources	• Les partenaires ont-ils partagé leurs ressources respectives en matière de gestion des risques de sécurité ? • L'accès aux ressources existantes peut-il être amélioré pour l'un ou l'autre des partenaires ?
Fin du partenariat	• La fin du partenariat conformément au contrat (et au calendrier financier) aura-t-elle des implications pour la sécurité de l'un ou l'autre des partenaires ? Si oui, comment cela devrait-il être traité ?

Adapté de GISF (2021) *Partenariats et gestion du risque sécurité: guide d'action conjointe pour les organisations humanitaires locales et internationales* (<https://gisf.ngo/resource/partnerships-and-security-risk-management-a-joint-action-guide-for-local-and-international-aid-organisations/>).

Enfin, pour qu'un partenariat soit équitable, il est essentiel que les deux parties aient une compréhension claire de leur attitude respective face au risque et de leur tolérance à celui-ci. Les partenaires ont tout intérêt à discuter ouvertement de leur appétence au risque et à trouver des moyens de s'aligner lorsqu'il existe des différences marquées, qui peuvent être assez frappantes dans de nombreux contextes où sont menés des programmes humanitaires. L'attitude de chaque partenaire à l'égard du risque devrait idéalement être discutée au début du partenariat et régulièrement réexaminée tout au long de la durée du partenariat (ce qui pourrait correspondre au calendrier des étapes importantes du partenariat). Dans certains cas, il peut arriver qu'aucun accord ne soit trouvé sur les seuils de risque ou que les risques ne puissent être atténués de manière appropriée, ce qui peut donner lieu à des discussions plus stratégiques sur l'opportunité de poursuivre le partenariat ou de modifier le travail programmatique.

► Voir le chapitre 1.1 pour plus d'informations sur les seuils de risque et la criticité des programmes.

Au cours des partenariats : identifier et répondre aux besoins, combler les lacunes et relever les défis

Renforcer la communication et mettre en œuvre les principes

Des efforts proactifs peuvent être déployés pour améliorer la communication entre les partenaires. Cela peut impliquer de s'assurer que les bonnes personnes font partie de la chaîne de communication (qui devrait généralement inclure les points focaux pour les questions de sécurité de chaque partenaire) ; que la fréquence et la méthode de communication sont les plus appropriées et les plus pratiques pour les

deux partenaires ; que la communication est transparente, honnête et claire ; et que le personnel adhère aux principes clés visant à traiter et à surmonter les préjugés inhérents et à instaurer la confiance.

Principes de partenariat

Afin de rendre les partenariats plus équitables, efficaces et sûrs, le personnel chargé d'établir et de maintenir des partenariats peut tenir compte de certains principes de bonnes pratiques fondamentaux :

- Équité - les partenaires ont des droits égaux, indépendamment de tout déséquilibre de pouvoir.
- Transparence - les interactions entre les partenaires sont ouvertes et honnêtes.
- Bénéfice mutuel - les deux partenaires doivent tirer profit du partenariat, idéalement au-delà de la simple réalisation des objectifs du partenariat.
- Complémentarité - chaque partenaire apporte ses propres forces et faiblesses au partenariat, les partenaires se complètent mutuellement et reconnaissent que la diversité peut être un atout.
- Orienté vers les résultats - les actions attendues des partenaires doivent être réalistes et axées sur les résultats.
- Responsabilité - les partenaires doivent assumer la responsabilité de leurs actions et éviter de prendre des engagements excessifs ou de faire des promesses excessives.

Source : GISF (2021) *Partenariats et gestion du risque sécurité : guide d'action conjointe pour les organisations humanitaires locales et internationales* (<https://gisf.ngo/resource/partnerships-and-security-risk-management-a-joint-action-guide-for-local-and-international-aid-organisations/>).

Exemple de cas : Le partage du risque en pratique

Une ONG locale nigériane a sollicité ses deux partenaires internationaux afin d'obtenir un financement pour le recrutement d'un agent de sécurité. En plus d'accepter de financer deux nouveaux postes de sécurité au sein de l'ONG locale, le personnel de sécurité des partenaires internationaux a apporté son soutien au processus de recrutement et a proposé aux nouvelles recrues des formations d'intégration, un soutien bihebdomadaire et des réunions mensuelles de suivi. En discutant des avantages et des défis, le personnel de sécurité de l'ONG internationale impliqué dans le processus a convenu que l'adhésion de tous les partenaires était essentielle et a veillé à ce que chaque organisation conserve la maîtrise des rôles et des décisions en matière de sécurité. Ils ont convenu que, pour partager les risques de manière efficace, l'un des principaux défis consistait à s'assurer que le personnel de sécurité de l'ONG internationale avait les capacités d'établir des relations et d'offrir un niveau approprié d'encadrement aux points focaux pour les questions de sécurité de l'ONG locale.

Source: Christian Blind Mission (CBM) et Sight Savers International (SSI) (2022) *Sharing risk – a good practice example in the INGO sector* (en anglais, «Partage des risques – un exemple de bonne pratique dans le secteur des ONG internationales») (www.gisf.ngo/resource/sharing-risk-a-good-practice-example-in-the-ingo-sector/).

Évaluations des risques conjointes et plans de sécurité adaptés

Bien qu'elles soient encore peu répandues dans le secteur humanitaire, les évaluations des risques conjointes liés aux activités du programme permettent aux deux partenaires d'avoir une vision claire des risques potentiels et au partenaire de mise en œuvre (et à son personnel) d'exprimer ses préoccupations avant d'entreprendre le travail. Une évaluation des risques conjointe permet également d'approfondir la discussion sur les mesures d'atténuation possibles et les moyens par lesquels chaque partenaire peut aider l'autre à répondre aux besoins en sécurité et à atteindre les objectifs du programme. Ce processus permet d'avoir des discussions plus claires sur la propriété du risque et les responsabilités au sein du partenariat, ainsi que de définir dès le départ des attentes claires quant à ce que chaque organisation peut apporter au partenariat. Il est également conseillé de procéder à un examen périodique conjoint de l'évolution des risques. Cet exercice peut être l'occasion pour les partenaires de bénéficier de l'échange de leurs points de vue respectifs et aide à identifier les adaptations qui pourraient être nécessaires. Il peut s'agir, par exemple, de concilier l'importance accordée par une

organisation à la documentation et aux politiques écrites avec la préférence d'une autre pour la communication verbale.

Selon les circonstances, cette évaluation des risques conjointe peut aboutir à la mise en place de protocoles de sécurité communs. Au minimum, ces évaluations des risques devraient servir de base aux plans et procédures de sécurité de chaque organisation. Une communication régulière entre les partenaires peut aider à répondre rapidement aux préoccupations en matière de sécurité.

Les partenaires doivent être préparés à faire face aux crises et aux incidents critiques et, dans l'idéal, convenir à l'avance de la meilleure façon de les gérer. Les partenaires peuvent déterminer quelle organisation serait la mieux placée pour intervenir en cas de crise ou d'incident critique (par exemple, en termes de logistique, d'accès et d'expertise). Tout soutien apporté dans ces circonstances devra généralement être décidé à un niveau stratégique, en tenant compte des implications juridiques et financières pertinentes. Cependant, la prudence face au risque n'est pas nécessairement la meilleure option, car le coût en termes de réputation lié à l'absence de soutien lors d'un tel événement (où une intervention serait bénéfique et ne causerait pas plus de tort que de bien) peut être plus préjudiciable que la possibilité d'une responsabilité juridique. Une organisation internationale qui a reconnu ce problème a pris des mesures proactives pour aider ses partenaires locaux à obtenir une assurance appropriée, ce que les organisations locales peuvent avoir du mal à obtenir par elles-mêmes.

Exemple de cas : Gestion des risques de sécurité dans les partenariats

Une organisation internationale a mis en œuvre plusieurs initiatives afin de mieux répondre aux problèmes et aux besoins en gestion des risques de sécurité lorsqu'elle travaille avec des partenaires. Parmi celles-ci, on peut citer :

- Renforcer l'implication du personnel de sécurité dès les premières discussions avec les partenaires.
- Sensibiliser le personnel de sécurité à la signification du partenariat et à la manière de travailler ensemble pour obtenir des résultats communs en toute sécurité.
- Créer (et parfois co-crée) et partager des recommandations, y compris des outils.
- Proposer un « menu » de formation aux partenaires.
- Augmenter le nombre de membres du personnel des partenaires participant aux sessions de formation à la sécurité de l'organisation.
- Soutenir les partenaires dans la gestion des incidents (sous forme de conseils techniques).

Partage des capacités

Les partenaires apportent leurs propres connaissances et points forts au partenariat. Une discussion sur ces derniers, ainsi que sur les points faibles et les lacunes, peut jeter les bases d'un accord plus solide et mutuellement avantageux. Les différences d'approche ne doivent pas être considérées comme un manque de capacités. Les partenaires doivent s'efforcer de s'entendre sur les besoins les plus importants en matière de soutien, par exemple la formation à la sécurité, et sur les formats les plus efficaces. Une organisation internationale a créé un site web auquel ses partenaires peuvent accéder pour suivre des formations sur des sujets particuliers, y compris des contenus liés à la sécurité. D'autres organisations ont promu des plateformes en ligne et des formations avec leurs partenaires. Certaines organisations internationales ont mis au point des formations à la sécurité spécifiques pour leurs partenaires locaux, tandis que d'autres les invitent à participer aux formations qu'elles dispensent à leur propre personnel. Il est important que tout renforcement des capacités soit pertinent et bénéfique pour chaque partenaire, convenus conjointement selon les besoins et durables afin de soutenir les capacités à long terme du personnel et des organisations.

► Voir le chapitre 5.2 pour plus d'informations sur la formation à la sécurité.

Financement

Les partenaires doivent s'efforcer de discuter des coûts de sécurité dès que possible, y compris du financement nécessaire pour renforcer les systèmes de sécurité en arrière-plan. Les budgets des partenariats devraient en règle générale inclure des lignes budgétaires consacrées à la sécurité, tandis que les partenaires peuvent veiller à ce que les coûts de sécurité soient adaptés aux risques de sécurité évalués. Les besoins de financement à plus long terme doivent également être pris en compte et discutés au sein du partenariat, comme le financement de la formation et de la couverture d'assurance médicale et contre les actes de malveillance pour le personnel le plus à risque. Les partenaires internationaux peuvent plaider auprès des donateurs pour un financement adéquat de leurs partenaires de mise en œuvre, tandis que les donateurs eux-mêmes peuvent exiger une meilleure prise en compte des besoins en sécurité des partenaires en aval.

► Voir le chapitre 3.3 pour plus d'informations sur le financement de la sécurité.

Partage des ressources

Les partenaires profitent du partage proactif des ressources et des informations relatives à la gestion des risques de sécurité au sein d'un partenariat. Les partenaires de mise en œuvre peuvent avoir une meilleure connaissance des conditions de sécurité locales, qu'ils peuvent partager, tandis que les partenaires internationaux peuvent avoir un meilleur accès aux mécanismes de coordination et de partage d'informations, dont ils peuvent faciliter l'accès. Bien que cela se fasse souvent de manière informelle, les ressources en matière de sécurité devraient idéalement être partagées activement et régulièrement, être disponibles en ligne et hors ligne (dans divers formats si possible) et être traduites dans les langues pertinentes. Les partenaires peuvent se soutenir mutuellement en

participant à des réseaux de sécurité et à des forums de partage d'informations aux niveaux local, national, régional et international.

Exemple de cas : Mécanismes de coordination en matière de sécurité

Les acteurs locaux sont largement sous-représentés dans les mécanismes de coordination dirigés par les acteurs humanitaires internationaux. Souvent, les acteurs locaux ne connaissent pas bien ces mécanismes ou n'y participent pas en raison d'obstacles tels que la localisation géographique et la langue. Des organisations comme INSO prennent des mesures pour remédier à cette situation en proposant l'adhésion aux ONG nationales enregistrées, permettant ainsi à ces acteurs d'accéder librement au réseautage, au partage d'informations et à la formation. Cependant, les acteurs humanitaires locaux non enregistrés continuent de rencontrer des difficultés importantes pour rejoindre les réseaux.

Plaidoyer et partenariats

Les partenariats présentent à la fois des opportunités et des risques en matière de plaidoyer. Les efforts communs de plaidoyer entre partenaires peuvent permettre de faire entendre une voix amplifiée, ce qui peut être utile pour le plaidoyer sur la gestion des risques de sécurité (par exemple, les partenaires internationaux plaidant auprès des autorités du pays donateur en faveur d'un financement accru de la sécurité pour les acteurs locaux). Cependant, le plaidoyer d'une organisation peut présenter des risques de sécurité pour ses partenaires, par exemple lorsqu'un gouvernement local tient les partenaires locaux dans le pays responsables des efforts de plaidoyer menés à son égard par un partenaire international. Une bonne pratique consiste à examiner l'impact que les efforts de plaidoyer peuvent avoir en dehors de l'organisation, en particulier sur les partenaires, avant de les mettre en œuvre. Une organisation internationale au Myanmar a activement discuté des messages de plaidoyer avec ses partenaires de mise en œuvre avant de passer à l'action, afin de s'assurer que ses partenaires soient non seulement informés, mais aussi en mesure de discuter des conséquences possibles du plaidoyer et des mesures d'atténuation nécessaires.

► Pour en savoir plus, voir le chapitre 2.2 sur le plaidoyer et la sécurité.

Informations complémentaires

Recherche et analyse

CBM et SSI (2022) *Sharing risk – a good practice example in the INGO sector* (en anglais, «Partage des risques – un exemple de bonne pratique dans le secteur des ONG internationales») (www.gisf.ngo/resource/sharing-risk-a-good-practice-example-in-the-ingo-sector/).

European Interagency Security Forum (2012) *Security management and capacity development: international agencies working with local partners* (en anglais, «Gestion de la sécurité et renforcement des capacités: agences internationales travaillant avec des partenaires locaux») (<https://gisfprod.wpengine.com/resource/international-agencies-working-with-local-partners/>).

GISF (2020) *Partnerships and security risk management: from the local partner's perspective* (en anglais et en espagnol, «Partenariats et gestion du risque sécurité: du point de vue du partenaire local») (www.gisf.ngo/resource/partnerships-and-security-risk-management-from-the-local-partners-perspective/).

GISF et Humanitarian Outcomes (2024) *State of practice: the evolution of security risk management in the humanitarian space* (en anglais, «État des lieux: l'évolution de la gestion des risques de sécurité dans le domaine humanitaire») (https://humanitarianoutcomes.org/security_risk_mgmt_humanitarian_space_2024).

Humanitarian Outcomes (2019) *NGOs & risk: managing uncertainty in local-International partnerships (global report)* (en anglais, «ONG et risques: gérer l'incertitude dans les partenariats locaux-internationaux (rapport mondial)») (www.humanitarianoutcomes.org/publications/ngos-risk2-partnerships).

Kemp, E. et Merkelbach, M. (2016) *Duty of care: a review of the Dennis v Norwegian Refugee Council ruling and its implications* (en anglais, «Devoir de diligence: examen de l'arrêt Dennis c. Norwegian Refugee Council et de ses implications»). European Interagency Security Forum (www.gisf.ngo/resource/review-of-the-dennis-v-norwegian-refugee-council-ruling/).

Recommandations et ressources

GISF (2021) *Partenariats et gestion du risque sécurité: guide d'action conjointe pour les organisations humanitaires locales et internationales* (www.gisf.ngo/resource/partnerships-and-security-risk-management-a-joint-action-guide-for-local-and-international-aid-organisations/).

Global Database of Humanitarian Organisations (GDHO, «Base de données mondiale des organisations humanitaires») (n.d.) (<https://humanitarianoutcomes.org/projects/gdho>).

4 Éléments opérationnels : processus et outils

4.1 Éléments analytiques

Une bonne gestion des risques de sécurité repose sur une analyse solide, et les bonnes pratiques montrent que les organisations fonctionnent de manière plus efficace et plus sûre lorsqu'elles évaluent systématiquement les risques. Ce chapitre traite des méthodologies et des outils utilisés pour mener une analyse approfondie des risques, afin de constituer la base d'une prise de décision éclairée et d'une planification stratégique. Il souligne l'importance de la compréhension du contexte, renforcée par une analyse fondée sur des données, dans l'élaboration de mesures d'atténuation des risques de sécurité solides.

Les analyses du contexte et des risques ne sont pas une science exacte. Il s'agit plutôt d'un moyen d'aider les organisations à mieux comprendre la situation et à améliorer leur prise de décision en identifiant les questions clés à se poser.

4.1.1 Aperçu

Vous trouverez ci-dessous les étapes fondamentales d'un processus analytique que le personnel de sécurité et des programmes a trouvé utile (voir également la figure 7). Les activités spécifiques menées à chaque étape, détaillées dans les sections suivantes, peuvent varier en termes de complexité et de sophistication d'une organisation à l'autre, en fonction des capacités et des ressources disponibles. Il est important de garder à l'esprit qu'il n'existe pas de modèle unique et que le modèle le plus approprié est celui qui sera facilement compris et systématiquement utilisé par le personnel à tous les niveaux. En général, les organisations qui privilégient la simplicité à la complexité ont plus de chances de voir leurs outils utilisés par leur personnel.

Étape 1 : Analyse du contexte, des menaces et de la vulnérabilité

- **Analyse du contexte général.** Examiner le contexte général dans lequel la programmation sera mise en œuvre, la dynamique du conflit (le cas échéant) et les principaux acteurs.
- **Analyse interne.** Examiner les objectifs du programme de l'organisation, ses priorités, ses structures, la présence géographique de son personnel, ses capacités de gestion des risques de sécurité et ses modalités de fonctionnement.
- **Identification des menaces.** Identifier les dangers potentiels pour les actifs essentiels de l'organisation (c'est-à-dire les personnes), les programmes, les processus, les biens et la réputation.
- **Vulnérabilités.** Identifier les vulnérabilités (et les points forts) spécifiques de l'organisation et de son personnel en ce qui concerne sa programmation et son niveau d'acceptation dans la zone.

Étape 2 : Identification et examen des risques (évaluation des risques)

- **Identification des risques.** Dresser la liste des risques plausibles liés au travail dans ce contexte, sur la base des menaces identifiées et des vulnérabilités spécifiques de l'organisation et de son personnel.
- **Analyse et examen des risques.** Analyser la probabilité et l'impact potentiel des risques identifiés. Les évaluer en conséquence, de faible à élevé, afin de déterminer les priorités en matière de mesures d'atténuation et de planification de la gestion.

Étape 3 : Atténuation des risques et planification de la gestion

- **Atténuer les risques identifiés.** Déterminer les mesures nécessaires pour réduire la probabilité et/ou l'impact de chacun des risques. Celles-ci seront souvent influencées par la stratégie de sécurité de l'organisation (*abordée au chapitre 4.2*).
- **Traiter le risque résiduel.** Réfléchir à tout risque résiduel qui pourrait subsister après la mise en œuvre de toutes les mesures d'atténuation. Décider s'il convient de l'accepter, de l'éviter ou de le partager. Cette décision sera guidée par les objectifs de l'organisation, son appétence au risque et la criticité des programmes.

Étape 4 : Suivre et réviser

- **Suivre et réviser.** Suivre, réviser et adapter en permanence l'évaluation des risques, si nécessaire, afin de s'assurer qu'elle reste pertinente et efficace.

Ce processus peut être documenté et intégré aux plans de sécurité.

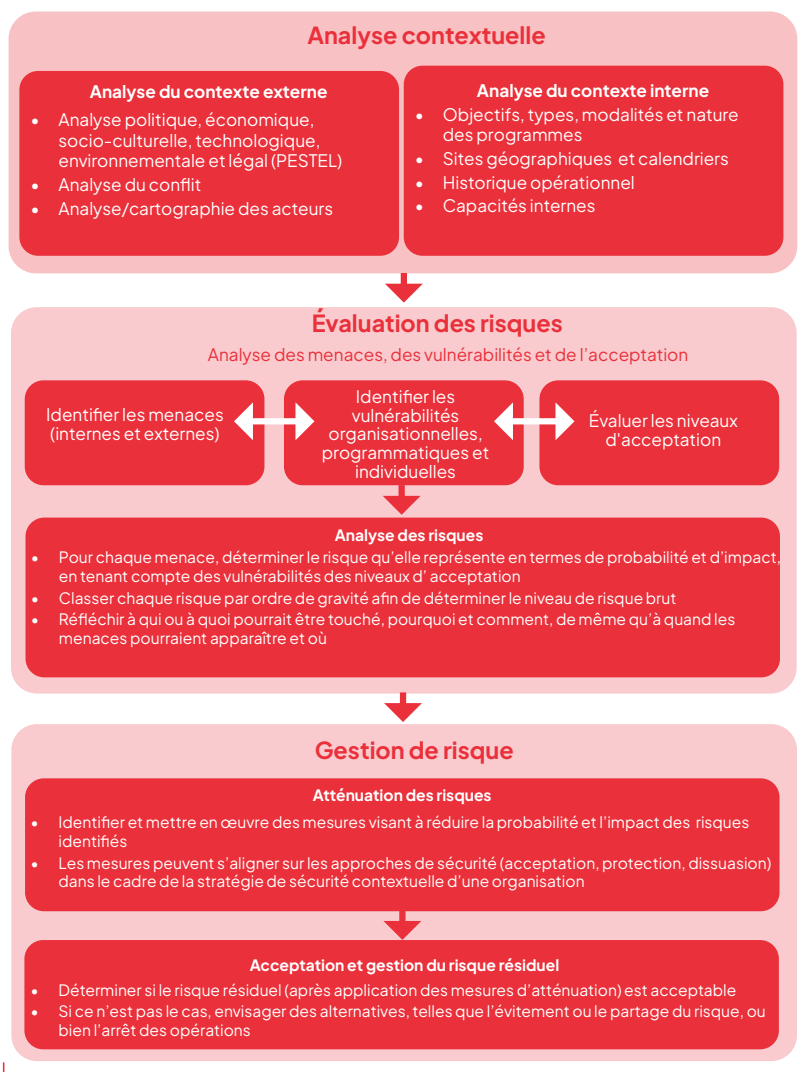
► Voir le chapitre 4.3 pour plus d'informations sur les plans de sécurité.

Pour soutenir ce processus, il est essentiel de communiquer en permanence les risques, les mesures d'atténuation et leur impact opérationnel à toutes les parties prenantes, tout en tenant le personnel informé des changements en matière de sécurité et en sollicitant le feedback des parties prenantes. Il est également important d'évaluer et de mettre à jour régulièrement l'approche de sécurité de l'organisation afin de s'assurer qu'elle reste pertinente, qu'elle reflète les bonnes pratiques et qu'elle soutient les capacités de l'organisation à atteindre ses objectifs dans un contexte en constante évolution.

► Pour en savoir plus sur la communication avec le personnel, voir le chapitre 5.3.

► Pour en savoir plus sur le suivi de l'efficacité, voir le chapitre 3.4.

Figure 7 Processus analytique



Consulter, partager, évaluer, améliorer et mettre à jour si nécessaire

Il est important d'adopter une approche systématique de l'évaluation des risques car, même si l'expérience et l'intuition peuvent jouer un rôle essentiel dans la compréhension et la gestion des risques, il n'est pas conseillé de se fier uniquement à son « instinct ». Les expériences isolées des individus, leurs préjugés invisibles, leurs perceptions personnelles et d'autres facteurs subjectifs peuvent souvent fausser leur vision des choses. Plus précisément, les gens ont tendance à exagérer les risques rares et spectaculaires tout en minimisant ceux qui sont fréquents, à réagir de manière excessive aux menaces immédiates tout en négligeant les dangers à long terme, et à réagir rapidement aux changements dramatiques, mais à s'adapter lentement aux changements progressifs (syndrome de la « grenouille dans l'eau bouillante » ou « grenouille dans la casserole »). Ils peuvent également éprouver des difficultés à évaluer des risques inconnus et surestimer des dangers largement évoqués.

Une approche structurée et rigoureuse peut aider à distinguer les faits des perceptions et des émotions, permettant ainsi à l'analyste d'absorber davantage d'informations pour obtenir une image plus complète. Elle peut également aider les équipes à parvenir à un consensus fondé sur les preuves disponibles. La ou les personnes qui dirigent ou coordonnent le processus d'évaluation des risques, généralement le personnel de sécurité, doivent veiller à garantir l'inclusion. Il s'agit de recueillir les points de vue et les informations de l'ensemble du personnel et d'examiner les risques sous différents angles. Cette approche favorise une compréhension commune des risques et une responsabilité partagée des mesures de sécurité. Un exemple serait un atelier d'évaluation des risques où des personnes aux profils et rôles divers se réunissent pour discuter des menaces et des vulnérabilités qu'elles subissent personnellement.

En plus de permettre une meilleure compréhension des risques comme base pour la prise de décision, une évaluation des risques bien documentée peut servir d'outil de gestion important pour suivre les changements dans l'environnement opérationnel et fournir une justification claire pour les investissements en matière de sécurité. Elle peut également fournir un indicateur de performance clé pour les activités du programme, confirmant que les risques sont identifiés et gérés pendant la mise en œuvre.

4.1.2 Analyse du contexte, des menaces et de la vulnérabilité

Analyse du contexte externe

Cadre PESTEL

L'analyse du contexte externe commence généralement par l'examen des facteurs qui façonnent l'environnement opérationnel. Adopter le cadre PESTEL peut s'avérer utile à cet effet. Dans la pratique, cela implique d'évaluer systématiquement chaque catégorie afin d'identifier les risques et les opportunités pertinents, ainsi que leur impact potentiel sur l'organisation et son personnel. Les catégories sont les suivantes.

- **Politique.** L'environnement politique, la stabilité du gouvernement, la dynamique des conflits, les principaux détenteurs du pouvoir et les opposants, la violence politique et les politiques gouvernementales.
- **Économique.** Pauvreté, inflation, taux d'emploi, stabilité monétaire, croissance économique et inégalités.
- **Socio-culturel.** Tendances démographiques, taux de criminalité, attitudes communautaires, normes, relations de genre et dynamiques intergroupes susceptibles d'influencer l'acceptation et les risques liés à l'identité. Cela peut inclure l'historique de l'aide dans la zone et la manière dont la communauté humanitaire et l'organisation (le cas échéant) ont été perçues par la population locale.
- **Technologique.** Technologie, sécurité numérique et stabilité des infrastructures, y compris la couverture Internet et mobile, la culture numérique et les limites technologiques.
- **Environnemental.** Chocs climatiques et dangers naturels, pénurie et concurrence des ressources, réglementations environnementales.
- **Légal.** Lois et réglementations relatives aux opérations d'aide, y compris le droit du travail et les exigences de conformité. Cela peut inclure l'impact des facteurs juridiques sur les risques liés à l'identité.

En utilisant ce cadre, les équipes peuvent mieux évaluer comment les facteurs externes interagissent et influencent leurs opérations, ce qui conduit à des efforts d'atténuation des risques plus éclairés.

Analyse du conflit

En plus du cadre PESTEL, une analyse plus détaillée des conflits et de la violence peut aider à mettre en lumière les sources de menace dans les zones où des conflits armés ont lieu. Une bonne analyse du conflit ne se concentre pas uniquement sur les endroits où la violence est visible. La violence peut être précédée de tensions moins évidentes : les « divisions profondes » et les « lignes de fracture » au sein d'une société. Celles-ci doivent également être explorées et comprises. Parfois, plusieurs conflits s'entremêlent. Les tensions et les flambées de violence en Irak, par exemple, peuvent être liées aux relations entre sunnites et chiites, à l'influence de l'État islamique, à la concurrence pour les ressources, aux tensions entre Kurdes et Arabes ou à l'héritage de l'invasion américaine. Tous ces facteurs peuvent constituer une source de menace.

Plusieurs cadres peuvent servir à l'analyse du conflit. Cependant, cette analyse ne doit pas nécessairement être trop complexe et peut se concentrer sur la réponse à certaines questions clés, telles que celles qui suivent.

- **Quelles sont les causes visibles et sous-jacentes du conflit ?**
 - Existe-t-il des griefs ou des divisions profondément enracinés qui alimentent les tensions (par exemple, économiques, politiques, sociaux, historiques) ?
 - Comment les structures politiques, les systèmes de gouvernance et les conditions économiques contribuent-ils au conflit ? Existe-t-il des institutions qui perpétuent l'exclusion ou l'inégalité ?
- **Qui sont les principaux acteurs et parties prenantes impliqués, et quels sont leurs intérêts ?**
 - Comment les rapports de force et les relations entre ces acteurs influencent-ils le conflit ?
 - Quel rôle jouent les institutions externes dans la dynamique du conflit (par exemple, les gouvernements étrangers et les agences internationales) ?
- **Quels sont les risques potentiels et les facteurs de division qui contribuent à l'escalade du conflit ?**
 - Existe-t-il des événements ou des déclencheurs spécifiques susceptibles d'aggraver la situation ?
 - Quels sont les signes avant-coureurs d'une escalade potentielle ?
- **Quels sont les liens ou les possibilités de consolidation de la paix qui existent ?**
 - Existe-t-il des intérêts communs, des liens culturels ou des mécanismes locaux susceptibles de réduire les tensions ?
 - Quelles sont les possibilités de consolidation de la paix ou d'atténuation du conflit grâce à la collaboration avec les acteurs locaux ?
- **Quel pourrait être l'impact des interventions de l'organisation sur le conflit ?**
 - Les actions de l'organisation risquent-elles d'alimenter involontairement les tensions, et comment le personnel peut-il garantir la sensibilité au conflit ?
 - Comment l'organisation peut-elle rester flexible et réactive face aux changements dans l'environnement du conflit, tels que de nouvelles alliances ou une violence inattendue ?

Une bonne pratique consiste à mettre régulièrement à jour l'analyse du conflit pour refléter les changements de situation, afin de refléter l'évolution de la situation, en veillant à ce que les stratégies restent pertinentes et adaptées à la dynamique changeante.

Analyse des acteurs

L'analyse des acteurs, ou cartographie des acteurs, se concentre sur les principaux individus et groupes susceptibles d'affecter la sécurité d'une organisation et de son personnel, y compris les membres du personnel eux-mêmes. Pour rester pertinente, cette analyse doit être continue et, au départ, elle suscitera probablement plus de questions que de réponses. Il s'agit d'un exercice exploratoire qui peut se dérouler en trois étapes :

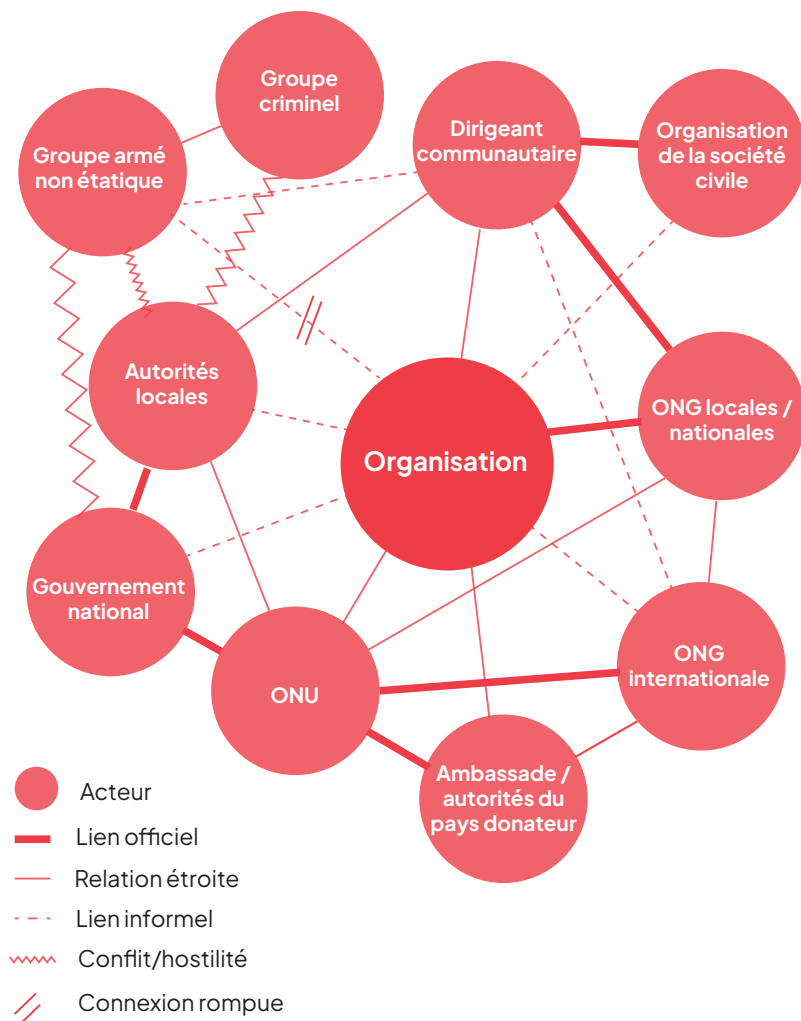
- identifier et répertorier tous les acteurs concernés ;
- comprendre leur identité, leurs motivations, leurs objectifs et leurs positions politiques/sociales ; et
- analyser leurs relations les uns avec les autres.

En contexte de conflit, les acteurs concernés comprennent tous les groupes armés et les acteurs nationaux et internationaux qui participent au conflit ou tentent d'influencer celui-ci (y compris les forces de maintien de la paix). Les acteurs locaux peuvent également inclure les chefs d'entreprise, les groupes d'étudiants, les syndicats, les propriétaires fonciers, les factions religieuses ou nationalistes militantes, les médias locaux, les organisations locales et les dirigeants traditionnels. Les acteurs régionaux et internationaux potentiellement concernés peuvent être les puissances voisines, les organisations intergouvernementales, les sociétés transnationales, les diplomates, les organisations de défense des droits humains et les groupes de la diaspora.

Les interactions entre les différents acteurs peuvent être illustrées par des lignes tracées entre eux, représentant différentes relations – par exemple, qui se bat, coopère ou rivalise avec qui, et quels groupes financent ou dirigent quels autres ? Une matrice peut aider le personnel à visualiser les relations, mises à jour à mesure que la dynamique évolue (voir la figure 8). Les relations peuvent être classées par catégorie, par exemple « allié », « ami », « ennemi », « compliqué » ou « en développement ». Différentes personnes peuvent donner différentes interprétations de ces relations, ce qui doit être pris en compte dans l'élaboration de la matrice. Cet exercice peut également constituer un outil pratique pour informer le nouveau personnel. Au fur et à mesure que l'analyse s'approfondit, il peut apparaître que les groupes ne sont pas aussi homogènes qu'ils le semblaient au premier abord.

Les acteurs constituant une menace potentielle à prendre en compte dans l'analyse comprennent les groupes armés non étatiques, les acteurs criminels, les acteurs économiques et les acteurs gouvernementaux. Il est important de reconnaître que ces étiquettes ne s'appliquent pas toujours avec des distinctions nettes ; les groupes peuvent avoir des objectifs et des motivations qui se recoupent, et les acteurs constituant une menace peuvent changer au fil du temps.

Figure 8 Exemple simplifié de cartographie des acteurs



Groupes armés

Les groupes armés peuvent englober un grand nombre d'entités ayant des identités, des motivations et des intentions différentes, notamment des groupes extrémistes, des groupes criminels organisés et des groupes rebelles à motivation politique luttant contre un gouvernement. Il est essentiel de comprendre les groupes armés pour comprendre comment et pourquoi la présence et les programmes d'une organisation peuvent être manipulés ou menacés. En fonction de leur dynamique de pouvoir et de leur idéologie, les groupes armés peuvent considérer les organisations humanitaires comme des menaces, des cibles de substitution, des outils politiques ou des sources de ressources à exploiter. Là encore, les informations ne peuvent être obtenues que progressivement. Pour chaque groupe armé identifiable, les organisations pourraient évaluer :

- Sa structure de commandement et de contrôle : dans quelle mesure les dirigeants et les combattants sont-ils organisés et soudés ?
- Ses points de contact : qui sont les personnes appropriées pour communiquer ou négocier ?
- Son idéologie et sa vision du monde : quelles sont ses attitudes, ses croyances et ses objectifs, s'ils sont connus ?
- Ses déclarations publiques : a-t-il fait des remarques sur les opérations ou les organisations humanitaires ?
- Ses actions passées : qu'a-t-il fait et comment l'a-t-il justifié ?
- Ses symboles ou sa mythologie : utilise-t-il des symboles ou des récits notables ?
- Ses relations avec la population locale : s'agit-il de nationaux ou d'étrangers ? Gouverne-t-il ou fournit-il des services ? Plus il est violent envers les civils, plus le danger potentiel pour les organisations humanitaires est grand.

► *Pour plus d'informations sur la manière de dialoguer avec les acteurs armés, voir les chapitres 2.1. et 4.2.*

Acteurs criminels

Les acteurs criminels peuvent considérer les organisations humanitaires comme des cibles lucratives pour l'extorsion, le vol ou l'enlèvement contre rançon, ou comme des obstacles à leurs opérations. Pour mieux comprendre ces acteurs, les organisations peuvent prendre en compte les éléments suivants :

- Structure organisationnelle et hiérarchie : qui sont les dirigeants et les membres clés ?
- Motivations et objectifs : sont-ils motivés par le gain financier, le contrôle territorial ou des activités illicites ?
- Tactiques : quelles sont les méthodes utilisées (par exemple, extorsion, enlèvement contre rançon, cybercrime) ?

- Relations : comment interagissent-ils avec les autorités locales et les communautés?
- Incidents passés : quels sont les schémas de comportement observés, en particulier à l'égard des travailleurs humanitaires et des biens?
- Impact : quels sont les effets économiques et sociaux de leurs activités sur l'économie et la société locales?
- Canaux de communication: existe-t-il des interlocuteurs potentiels pour négocier, si nécessaire?

Acteurs de l'économie de guerre

De nombreux conflits modernes ont été alimentés par des «économies de guerre», notamment le commerce illégal et quasi légal d'armes, de drogues, de diamants, de pétrole, de minéraux et d'autres matières premières. Dans les zones où l'économie est marquée par la guerre, les organisations humanitaires pourraient utilement examiner les aspects suivants:

- Importance des ressources - dans quelle mesure les ressources locales sont-elles essentielles à l'économie de guerre, et les ressources alternatives sont-elles limitées (ce qui rend les organisations humanitaires plus importantes et plus vulnérables)?
- Sensibilité géographique - la zone est-elle importante en raison de ses ressources naturelles ou de ses routes commerciales stratégiques?
- Impact sur le recrutement - les programmes humanitaires offrent-ils des moyens de subsistance alternatifs susceptibles d'influencer le recrutement par des groupes armés ou des organisations criminelles?
- Impact économique de l'aide - l'aide crée-t-elle des tensions ou des dépendances que les acteurs du conflit pourraient exploiter?
- Impact environnemental - les programmes humanitaires pourraient-ils aggraver les tensions existantes ou créer de nouveaux conflits en raison de leurs effets sur l'environnement?

Acteurs gouvernementaux

Les gouvernements peuvent avoir un impact considérable sur l'acheminement de l'aide grâce à leurs structures, leur dynamique politique, leurs cadres juridiques et leurs relations avec les populations locales et les organisations humanitaires. Il est utile d'examiner la stabilité, les conditions juridiques et les possibilités de collaboration avec le gouvernement à différents niveaux, ainsi que de comprendre:

- La structure gouvernementale: quelle est la hiérarchie et qui sont les principaux décideurs au sein des ministères ou agences concernés dans les différents lieux?
- La dynamique politique: quel est le degré de stabilité du gouvernement et quels sont les intérêts politiques susceptibles d'influencer la programmation?

- Les cadres juridiques: quelles lois et réglementations s'appliquent aux opérations humanitaires et comment sont-elles appliquées?
- La position vis-à-vis de l'aide: le gouvernement soutient-il ou s'oppose-t-il aux efforts d'aide? Existe-t-il des restrictions ou des conditions imposées?
- La corruption et la redevabilité: existe-t-il des problèmes de corruption au sein du gouvernement?
- La coordination: comment le gouvernement coordonne-t-il ses actions avec les organisations humanitaires? Existe-t-il des mécanismes de coordination formels?
- La perception du public: comment le gouvernement est-il perçu par la population locale?
- La coopération en matière de sécurité: le gouvernement assure-t-il la sécurité des opérations humanitaires? Si oui, comment?

► Voir le chapitre 2.1 pour plus d'informations sur les interactions avec les autorités.

Contexte interne

L'analyse du contexte interne porte sur l'organisation, ses activités, ses actifs et son personnel. L'évaluation du contexte interne peut aider le personnel à mieux comprendre l'organisation dans son ensemble, la manière dont ses activités programmatiques profitent à la population locale et le niveau d'acceptation dont elle bénéficie dans une zone donnée, autant d'éléments qui contribuent à mieux cerner les vulnérabilités et les points forts de l'organisation. Voici quelques éléments clés à prendre en compte:

- La mission et les objectifs du programme de l'organisation.
- Le type et la nature des interventions du programme.
- La localisation géographique des équipes de projet et des actifs.
- L'historique des opérations dans la zone, le cas échéant.
- Les modalités de mise en œuvre.
- Le calendrier des activités.
- Les capacités internes de l'organisation pour gérer les risques.

Lors de l'établissement du contexte interne, le personnel de sécurité peut collaborer avec le personnel responsable de la gestion et de la mise en œuvre des activités du programme, l'équipe opérationnelle et les employés des bureaux secondaires afin d'obtenir le plus d'informations possible.

Identification et évaluation des menaces

Après l'analyse du contexte, l'étape suivante consiste à identifier les menaces spécifiques dans l'environnement opérationnel et les vulnérabilités spécifiques de l'organisation et de son personnel.

Une menace est un événement, action ou entité susceptible de porter préjudice au personnel, aux programmes ou aux biens, ou d'entraver la réalisation des objectifs de l'aide. Les menaces pour la sécurité proviennent de diverses sources, notamment la criminalité, les conflits et la violence, tandis que les menaces pour la sûreté du personnel comprennent les accidents, les maladies et les dangers naturels.

Sources de menaces internes

Les menaces peuvent provenir tant de l'intérieur que de l'extérieur de l'organisation. Les incidents de sécurité perpétrés par des travailleurs humanitaires à l'encontre de leurs collègues peuvent prendre diverses formes, notamment le harcèlement, la discrimination, l'intimidation et la violence sexuelle. Le vol, la fraude et la violation de la confidentialité des informations peuvent compromettre l'intégrité et les ressources de l'organisation, entraînant l'insécurité du personnel. La violence physique et les abus psychologiques de la part des collègues, y compris les tactiques telles que le « gaslighting » (technique de manipulation mentale consistant à désorienter une personne que l'on malmène jusqu'à ce qu'elle ne soit plus sûre de rien) et la manipulation, constituent également des risques. Les auteurs internes peuvent être motivés à causer du tort pour plusieurs raisons, notamment :

- L'identité de la cible (par exemple son genre, son ethnicité ou son orientation sexuelle).
- La situation personnelle de l'auteur, y compris ses griefs personnels, ses antécédents familiaux, sa personnalité et ses comportements.
- Les environnements organisationnels permissifs.
- Des facteurs culturels et sociétaux externes.

► Voir le chapitre 1.2 pour plus de détails sur les menaces internes.

► Voir le chapitre 7.7 pour plus d'informations sur les risques de violence sexuelle et une analyse plus approfondie sur la manière de traiter les auteurs internes.

Sources de menaces externes

Lorsque l'on examine les sources de menaces externes, il peut être utile d'élaborer des descripteurs de menaces basés sur divers acteurs et catégories d'événements. Il peut s'agir, par exemple, de menaces en lien avec :

- La criminalité (homicide, vol, détournement de voiture, cambriolage, agression).
- La violence sexuelle (viol, agression, abus).
- La détention et l'arrestation (barrages routiers, points de contrôle).
- L'enlèvement (enlèvement contre rançon, situation d'otages, extorsion).
- Les menaces liées aux combats et vestiges de guerre (fusillades, bombardements, frappes aériennes, bombes).
- Les informations, communications et technologies (cybercrime, harcèlement en ligne, désinformation, fuites de données, surveillance hostile).
- Les troubles civils (manifestations, protestations, violence de la part de bandes).

Les menaces peuvent également provenir de facteurs environnementaux, tels que les facteurs économiques (récession, inflation, perturbation de la chaîne d'approvisionnement) ou les dangers naturels (inondations, tremblements de terre, épidémies).

► *Pour une analyse plus détaillée de certains types de menaces, voir la partie 7.*

Une fois les menaces identifiées, il est important de comprendre comment, quand et pourquoi chacune d'entre elles peut se produire, et qui/quoi elle peut toucher (en termes de personnes, de programmes, d'actifs, de biens et de réputation, par exemple).

Collecte d'informations sur les menaces

Les informations utilisées pour l'analyse des menaces peuvent provenir de diverses sources, notamment les autorités locales, les membres du personnel, les dirigeants communautaires, les chefs d'entreprise, les chauffeurs de taxi, les médias locaux et internationaux et les observateurs des droits humains. Certaines de ces sources peuvent être bien informées et disposées à partager leurs connaissances, tandis que d'autres peuvent être mal informées ou donner une image délibérément déformée de la situation. Les sociétés de sécurité privée peuvent également fournir des informations et des analyses sur les conditions de sécurité et les menaces potentielles. Cela peut être utile pour l'analyse générale, même si cela ne fournit généralement pas le niveau de détail quotidien dont les organisations peuvent avoir besoin au niveau régional.

Il existe diverses méthodes pour collecter des informations sur les menaces potentielles dans l'environnement opérationnel, notamment des entretiens directs avec les parties prenantes et l'analyse de documents, tels que l'examen des rapports organisationnels antérieurs (y compris ceux d'organisations homologues), les bases de données des ONG, les forums de coordination, les agences de l'ONU et la police locale. Les sources publiques, notamment les réseaux sociaux et les médias traditionnels, peuvent également s'avérer précieuses. L'analyse quantitative des incidents passés peut aider à identifier les tendances et les zones à haut risque. Les

visites peuvent également offrir l'occasion de recueillir des observations de première main sur la situation sur place.

La fiabilité (authenticité et crédibilité de la source) et la validité (cohérence et confirmation par d'autres sources indépendantes) des informations doivent être évaluées. L'utilisation d'une matrice pour classer la fiabilité et la validité des sources peut améliorer la qualité de l'analyse des menaces.⁵⁰

Dans n'importe quel contexte, il est possible que différents individus et groupes perçoivent les menaces différemment en fonction de leurs expériences quotidiennes et de leurs interactions avec les auteurs de menaces. Les discussions de groupe, les entretiens et les évaluations participatives peuvent aider les organisations à recueillir des informations plus nuancées.

Analyse de la vulnérabilité et de l'acceptation

Une fois l'évaluation des menaces terminée, l'étape suivante consiste à évaluer les vulnérabilités de l'organisation, c'est-à-dire le degré d'exposition du personnel, des biens et des actifs aux menaces.

La vulnérabilité d'une organisation peut être influencée par :

- L'image et le niveau d'acceptation de l'organisation.
- Le type et la nature de la programmation.
- La localisation du personnel et des biens.
- Le niveau d'exposition du personnel et des biens.
- La valeur des actifs/biens.
- L'impact des interventions du programme dans la zone.
- La capacité interne de l'organisation à gérer les risques de sécurité.
- La formation, la sensibilisation et le respect des mesures de sécurité par le personnel.

Comprendre les vulnérabilités individuelles du personnel

Les vulnérabilités personnelles, qui englobent à la fois les aspects immuables de l'identité et les facteurs gérables tels que le comportement, forment collectivement le profil de risque personnel d'un individu. Toutes les caractéristiques d'identité ou vulnérabilités ne sont pas visibles, par exemple la santé, l'orientation sexuelle ou la stabilité financière. Les vulnérabilités ne sont pertinentes que lorsqu'elles se recoupent avec une menace spécifique, et le personnel de sécurité doit s'efforcer de comprendre et de traiter les vulnérabilités dans ce contexte.

Dans le cadre d'une approche de gestion des risques de sécurité centrée sur la personne, les organisations peuvent évaluer systématiquement comment différents facteurs liés à l'identité – tels que le genre, l'orientation sexuelle et l'ethnicité – influent sur la vulnérabilité d'un individu aux menaces internes et externes. Une évaluation

⁵⁰ Pour un exemple, voir RedR UK, Insecurity Insight et EISF (2017) *Manuel de la gestion de l'information en cas d'incident de sécurité (GIIIS)* (<https://siim.insecurityinsight.org/tools-and-resources/handbook-guide-and-tools>).

des risques inclusive peut englober toute une série de facteurs influençant les vulnérabilités individuelles liées à l'interaction entre les identités intersectionnelles des membres du personnel, leurs rôles au sein de l'organisation, le contexte et les facteurs de menace internes et externes. Cela garantit que les évaluations des risques sont inclusives et devraient idéalement impliquer la contribution de divers membres du personnel afin d'obtenir un large éventail d'expériences et de points de vue.

Exemple de cas : Évaluations des risques inclusives

Une organisation divise son évaluation des risques relatifs à la sécurité en menaces indirectes (« où vous êtes ») et menaces directes (« qui nous sommes, ce que nous faisons »). Cela permet au personnel d'utiliser des données externes pour établir un niveau de sécurité de base, qui est ensuite complété par une analyse plus approfondie des risques auxquels le personnel peut être exposé dans le cadre de son travail. Dans ce cadre, un pays qui peut être considéré comme à faible risque en fonction du contexte peut s'avérer être un lieu à haut risque en interne en raison de facteurs tels que la faible acceptation par la communauté.

► *Pour en savoir plus sur l'approche centrée sur la personne, voir le chapitre 1.2.*

Comprendre la vulnérabilité organisationnelle et du programme

L'analyse du contexte interne peut aider à identifier les vulnérabilités spécifiques à l'organisation et au programme. La perception de l'organisation, de son rôle, de son mandat et de sa mission peut influencer sa vulnérabilité aux menaces. Les organisations confessionnelles, qu'elles fassent ou non du prosélytisme dans le cadre de leur mission, peuvent être exposées à des risques différents de ceux des organisations laïques dans un contexte religieux. De même, les organisations internationales associées à certains pays, ou les organisations nationales associées à certaines zones ou à certains groupes ethniques, peuvent être ciblées pour des raisons politiques. Les agences de l'ONU peuvent avoir du mal à éviter d'être identifiées comme travaillant pour l'ONU en tant qu'acteur politique, malgré leur mission humanitaire. Certaines activités du programme, telles que les services de santé reproductive ou l'aide axée sur les communautés marginalisées, peuvent comporter des risques en raison de la façon dont ces programmes peuvent être perçus par les communautés locales. Les gouvernements peuvent adopter une position négative quant au lieu où les organisations travaillent et à leurs partenaires s'ils estiment que cela va à l'encontre de leurs intérêts, en particulier s'ils considèrent que cela soutient directement ou indirectement des groupes d'opposition.

Les organisations dont les programmes couvrent le « nexus » des activités humanitaires, de développement et de consolidation de la paix seront probablement confrontées à un environnement plus complexe en matière de menaces, car leur programme va au-delà de la fourniture de services humanitaires et touche à des domaines potentiellement sensibles d'intérêt politique et sociétal.

L'analyse des programmes consiste à comprendre l'organisation, ce qu'elle vise à faire, où et quand, et surtout pourquoi.

- **Pourquoi.** Pourquoi ce programme est-il nécessaire et dans quelle mesure est-il essentiel pour les personnes qu'il sert ? Quelle est son importance pour la mission et l'identité de l'organisation ?
- **Quoi.** Quelles sont les principales activités et quelles sont les modalités opérationnelles impliquées (par exemple, déplacements, distributions, chaîne logistique, travail dans les installations locales, travail au niveau communautaire) ? Comment les activités ont-elles été perçues et accueillies par la communauté dans le passé ?
- **Qui.** Qui sont la population cible, les donateurs, les parties prenantes locales et au-delà ? Qui sont les membres du personnel du programme et quelles identités intersectionnelles devront être prises en compte ?
- **Où.** Quels sont les lieux du programme et autres zones où le personnel sera ou passera ?
- **Quand.** Quel est le calendrier du programme et coïncide-t-il avec les périodes d'insécurité accrue prévues ?

Les questions ci-dessus peuvent aider à mettre en évidence la vulnérabilité et à déterminer le niveau d'acceptation dont bénéficie l'organisation.

Il est essentiel d'évaluer le niveau d'acceptation de l'organisation au sein de la communauté et parmi les parties prenantes, car un manque d'acceptation peut accroître les risques et nuire à la réussite du programme. Cette analyse peut porter sur l'influence des parties prenantes, leur perception de l'organisation et de son personnel, ainsi que leur niveau d'engagement actuel, afin d'identifier les risques et les mesures à prendre pour maintenir ou renforcer l'acceptation si nécessaire.⁵¹

► Voir le chapitre 4.2 pour plus d'informations sur l'analyse d'acceptation.

⁵¹ Pour un exemple de modèle d'analyse d'acceptation, voir GISF (n.d.) 'Acceptance analysis template - xlsx' (en anglais, « Modèle d'analyse d'acceptation - xlsx »). 2. *Stratégie d'acceptation*. Guide interfonctionnel sur la sécurité des ONG (<https://gisf.ngo/toolbox-pwa-fr/resource/2-strategie-dacceptation/>).

4.1.3 Analyse des risques

Une fois qu’une organisation a identifié les menaces et les vulnérabilités dans un contexte particulier, l’analyse peut se concentrer sur les risques. Le risque est un sujet multidisciplinaire qui revêt différentes significations selon les situations et qui implique un large éventail de possibilités connues et inconnues. En matière de sécurité, le risque est une combinaison de deux facteurs:

- la probabilité de rencontrer une menace ; et
- les conséquences qui en résulteraient.

Les risques les plus critiques à traiter sont ceux qui sont susceptibles de se produire et/ou de causer des dommages importants, tandis que les événements hautement improbables et/ou à faible impact sont généralement moins prioritaires.

Les évaluations des risques doivent être collectives et collaboratives, réunissant des membres du personnel diversifiés, y compris le personnel chargé des programmes et des opérations, afin de garantir la prise en compte d’une diversité de points de vue, de réalités vécues et de profils d’identité.

Évaluer la probabilité

L’évaluation de la probabilité permet d’évaluer la probabilité qu’un événement indésirable se produise.

L’estimation de la probabilité d’une menace pour la sécurité s’appuie généralement sur l’analyse des tendances et sur des informations provenant de sources internes et externes. Ces informations sont utilisées pour déterminer la fréquence potentielle de l’événement. La probabilité peut être évaluée à l’aide d’une échelle à cinq degrés, comme le montre le tableau 4.

Tableau 4 Évaluation qualitative de la probabilité

Descripteur d'évaluation	Descripteur de probabilité
Certain/imminent (5)	L'événement se produit régulièrement, est certain de se produire ou est déjà en cours
Très probable (4)	L'événement/la menace a de très fortes chances de se produire
Probable (3)	L'événement s'est déjà produit auparavant et pourrait se reproduire
Moyennement probable (2)	L'événement se produit rarement
Peu probable (1)	Il est peu probable que l'événement se produise

Évaluer l'impact

L'évaluation de l'impact implique de comprendre les conséquences potentielles pour les personnes, les programmes, les processus, les biens et la réputation. En d'autres termes, il s'agit d'estimer les préjudices qui pourraient être causés par une menace. L'impact peut être classé de deux manières :

- Préjudice direct - le préjudice immédiat causé par l'événement, tel que le décès ou la blessure d'un membre du personnel, la détérioration d'un véhicule ou la perte d'actifs.
- Préjudice indirect - impacts considérables tels que les retards, le temps perdu, le coût des soins médicaux et du soutien psychosocial apporté au personnel touché, l'interruption des opérations et la fermeture de bureau.

Un seul incident peut entraîner des préjudices directs et indirects.

Comme pour la probabilité, l'évaluation de l'impact peut se faire sur une échelle à cinq points (voir le tableau 5).

Tableau 5 Évaluation de l'impact

Niveau de l'impact	Descripteur d'impact
Extrême (5)	Impact exceptionnellement grave, tel que décès, nombreuses victimes, perte d'activité, suspension du programme, fermeture de bureau
Élevé (4)	Impact majeur, tel que blessures physiques ou psychologiques graves infligées au personnel, perte d'accès humanitaire, pertes financières importantes, atteinte à la réputation
Modéré (3)	Impact modéré, tel que blessures ne mettant pas la vie en danger, perte d'actifs, restrictions imposées au personnel et aux programmes, pertes financières, atteinte à la réputation, maladie non grave
Faible (2)	Impact faible, tel que la perte ou la détérioration des actifs d'une organisation, blessures légères, perturbations mineures
Négligeable (1)	Impact insignifiant

Matrice des risques

Pour déterminer le niveau de risque associé à chaque menace identifiée, l'organisation peut alors :

- Prendre la liste des menaces identifiées lors de l'évaluation des menaces.
- Estimer l'impact probable si les menaces se concrétisaient, ainsi que la probabilité que ces menaces se concrétisent.
- Définir le niveau de risque global brut (c'est-à-dire non encore atténué).
- Représenter les menaces en fonction de leur niveau de risque (probabilité x impact) dans une matrice d'analyse des risques ou une carte d'analyse des risques.

La figure 9 présente une matrice simple à quatre niveaux utilisée dans l'évaluation des risques pour évaluer et hiérarchiser les risques en fonction de leur probabilité et de leur impact. Chaque combinaison de probabilité et de conséquence correspond à une note de risque, qui peut aider les organisations à visualiser et à hiérarchiser les risques en fonction de leur gravité. Les nuances de couleur représentent les niveaux globaux de risque, allant de faible (clair) à extrême (foncé).

Figure 9 Exemple de matrice des risques

Impact Probabilité	Négligeable (1)	Faible (2)	Modéré (3)	Élevé (4)	Très élevé (5)
Certain / imminent (5)	Moyen	Élevé	Élevé	Extrême	Extrême
Très probable (4)	Moyen	Moyen	Élevé	Extrême	Extrême
Probable (3)	Faible	Moyen	Élevé	Élevé	Extrême
Moyennement probable (2)	Faible	Faible	Moyen	Élevé	Élevé
Peu probable (1)	Faible	Faible	Faible	Moyen	Moyen

Les risques peuvent être classés selon un ordre numérique ou simplement comme « élevé », « moyen » ou « faible ». Les risques élevés nécessitent généralement une attention immédiate et des mesures d'atténuation solides. Les risques modérés peuvent nécessiter un suivi régulier et des mesures d'atténuation ciblées. Les risques faibles peuvent être gérés à l'aide de mesures de base, telles que des procédures opérationnelles standards et des examens occasionnels. Ce processus d'analyse et d'évaluation détaillé peut aider une organisation à hiérarchiser efficacement ses ressources et ses efforts, en se concentrant sur les risques les plus importants et en veillant à ce que toutes les menaces potentielles soient gérées de manière adéquate.⁵²

52 Pour des exemples de modèles, voir GISF (n.d.) 3. *Évaluations des risques*. Guide interfonctionnel sur la sécurité des ONG (<https://gisf.ngo/toolbox-pwa-fr/resource/3-evaluation-des-risques/>).

Évaluations des risques contextuels

De nombreuses organisations gèrent la sécurité sur la base d'une «évaluation des risques» ou de «niveaux de sécurité» attribués à des lieux spécifiques. Il existe généralement trois à cinq niveaux, allant d'un risque faible à un risque élevé. Il peut y avoir plusieurs niveaux différents au sein d'un même pays, voire d'une même ville. Ces niveaux influencent de nombreuses décisions administratives et opérationnelles, notamment la criticité des programmes, les mesures de sécurité, la supervision de la gestion de risque liée aux déplacements, la dotation en personnel de sécurité, le budget consacré à la sécurité et les politiques RH.

Lors de l'établissement de ces évaluations de risque contextuel, un processus d'évaluation des risques similaires peut prendre en compte l'environnement de menaces, la vulnérabilité de l'organisation et de son personnel dans ce lieu, ainsi que l'importance de ce lieu pour la réalisation des objectifs globaux du programme.

Cette approche par niveaux permet de définir des exigences de sécurité pour différents lieux, de garantir une allocation efficace des ressources et de veiller à ce que les zones les plus critiques bénéficient de l'attention nécessaire pour atténuer les menaces potentielles. Bien que cette approche soit généralement utilisée pour les lieux, elle pourrait également être appliquée à d'autres catégories pertinentes. Par exemple, il peut être utile d'identifier les fonctions les plus à risque au sein de l'organisation et de définir les exigences de sécurité pour les membres du personnel concernés (par exemple, une formation spécialisée).

► Voir le chapitre 3.1 pour plus d'informations sur les exigences de sécurité.

Atténuation des risques

L'évaluation des risques peut servir de feuille de route à l'organisation pour allouer des ressources suffisantes et élaborer des mesures d'atténuation des risques spécifiques correspondant aux risques identifiés.

Les mesures de sécurité utilisées pour atténuer les risques impliquent généralement – et sont influencées par – une combinaison d'approches qui constituent une stratégie de sécurité globale pour une organisation dans un contexte spécifique.

► Voir le chapitre 4.2 pour en savoir plus sur les différentes approches de sécurité et l'élaboration d'une stratégie de sécurité.

Les mesures d'atténuation des risques (ou de traitement) sont conçues pour réduire les risques en diminuant les vulnérabilités et en renforçant les capacités par la réduction de la probabilité et de l'impact.

- **Réduire la probabilité.** Identifier et mettre en œuvre des mesures spécifiques visant à réduire la probabilité que des incidents se produisent, telles que l'établissement de procédures opérationnelles standards, la mise en place de règles telles que des couvre-feux et des limitations de vitesse, l'utilisation de

convois et de systèmes de binômes, et la formation du personnel aux techniques permettant d'éviter les menaces.

- **Réduire l'impact.** Une fois qu'un incident s'est produit, son impact peut être réduit par des mesures de protection et de préparation telles que l'accès à des abris renforcés ou à des salles de sécurité, l'équipement des installations et des véhicules avec des trousse de premiers secours et des extincteurs, la préparation de plans de gestion des incidents critiques et de plans d'urgence, et la mise en place d'assurances et de ressources pour le bien-être personnel, telles que des services de counseling.

Les mesures d'atténuation doivent refléter l'évaluation des risques en termes de probabilité et d'impact. Si une menace a un impact élevé mais une probabilité faible, il peut être plus approprié de concentrer les efforts sur la réduction de l'impact plutôt que d'investir davantage dans la réduction de la probabilité. Cela dit, il est conseillé de traiter les deux aspects dans la mesure du possible. Une fois les mesures d'atténuation des risques identifiées, celles-ci devront être mises en œuvre et financées.

Enfin, comme pour l'analyse du contexte, l'évaluation des risques devra être un document évolutif pour rester pertinente et utile. Un aspect essentiel de ce processus consiste à suivre et à analyser les incidents de sécurité et autres informations pertinentes afin d'identifier les schémas ou les tendances susceptibles d'indiquer l'évolution des risques. L'évaluation des risques et les mesures d'atténuation sont intégrées dans les plans de sécurité et y sont généralement documentées.

► Voir le chapitre 4.3 sur les Plans et dispositions de sécurité.

4.1.4 Une fois les risques évalués et atténués

Une fois qu'un risque a été « traité » par des mesures d'atténuation, la gestion de risque continue consiste à déterminer comment gérer le risque résiduel qui subsiste, car certains risques persistent généralement même après la mise en œuvre de mesures visant à les réduire. La manière dont une organisation aborde le risque résiduel dépend généralement de son mandat et de ses objectifs, de la criticité de sa programmation et de son appétence au risque. Une organisation dispose d'au moins trois options possibles.

- **Accepter le risque résiduel.** Décider d'accepter certains niveaux de risque s'ils sont conformes à la tolérance du risque de l'organisation. Cette approche est souvent appropriée pour les activités essentielles à la mission ou pour sauver des vies, lorsque les bénéfices potentiels l'emportent sur les risques.

- **Éviter le risque résiduel.** Prendre des mesures pour éviter les risques en modifiant les plans, les processus ou les comportements afin d'éliminer complètement la menace : par exemple, délocaliser les opérations loin des zones à haut risque ou interrompre les activités non essentielles.
- **Partage du risque résiduel.** Faire appel à un tiers, tel qu'une organisation partenaire, pour partager le risque en prenant en charge des activités de programmation de manière à optimiser l'efficacité et la sécurité pour les deux parties et à respecter le devoir de diligence.

Dans les cas présentant un risque très élevé, la question centrale est de savoir s'il faut rester présent et opérationnel ou cesser toute activité et se retirer. Cela peut se décomposer comme suit :

- Est-il nécessaire et approprié que l'organisation reste sur place ? Dispose-t-elle des capacités (financières et compétences) pour gérer les risques de sécurité ?
- Si ce n'est pas le cas, ces capacités peuvent-elles être développées ou mises en place suffisamment rapidement ?
- Une fois les ressources financières et humaines en place, le personnel et la direction peuvent-ils consacrer suffisamment de temps à la gestion des risques de sécurité ?

Si la réponse à l'une des questions ci-dessus est « non », les organisations doivent réfléchir sérieusement avant de prendre une décision, au moins jusqu'à ce que la situation s'améliore ou que les capacités adéquates soient disponibles pour gérer les risques. Il existe des alternatives valables à la présence physique d'une programmation, notamment le transfert de fonds ou d'autres ressources par l'intermédiaire d'organisations mieux placées pour opérer en toute sécurité dans le contexte en question.

4.1.5 Penser en dehors de la matrice des risques

La pensée actuelle sur l'analyse des risques remet en question l'approche systématique adoptée par certaines organisations, suggérant qu'elle est devenue trop complexe, obscure et rigide, au point d'être déconnectée de l'intuition et de l'expérience. Comme toute procédure établie, elle risque également de devenir un simple exercice consistant à cocher des cases plutôt qu'un outil d'aide à la prise de décision.

Comme mentionné précédemment, l'un des avantages de travailler dans un cadre d'évaluation des risques de sécurité est qu'il permet d'assurer la cohérence organisationnelle dans la réponse aux risques et peut être utilisé pour déclencher une série d'actions sans hésitation ni longue discussion. Cependant, en tant qu'outil de gestion, il peut également donner une impression trompeuse de solidité et de prévisibilité, et il est important de comprendre les limites de cette approche :

- Le caractère incomplet des informations et les difficultés liées à l'interprétation correcte d'une réalité complexe peuvent rendre difficile la décision de passer à un autre niveau d'alerte, et dans tous les cas, déterminer le niveau de sécurité approprié n'est pas la même chose que mettre en œuvre le plan.
- Les classifications des niveaux de risque peuvent parfois être trop générales pour refléter les nuances des menaces ou les catégories de personnes exposées au risque dans un même lieu.
- Dans la réalité, les situations ne s'aggravent ou ne s'améliorent pas toujours progressivement : elles peuvent se détériorer soudainement, passant d'un niveau à un autre.
- Différentes organisations opérant au même endroit peuvent interpréter la même situation de manière différente et, par conséquent, s'attribuer des niveaux de sécurité différents et prendre des mesures de sécurité différentes en conséquence.
- Les évacuations et les relocalisations en temps de crise nécessitent généralement une collaboration interagences, qui peut être compliquée par des appréciations différentes du risque. De plus, le fait que certaines organisations procèdent à des relocalisations/évacuations tandis que d'autres ne le font pas peut modifier le risque et accroître la vulnérabilité des personnes qui restent sur place.

L'autre préoccupation est que le fait de concentrer l'attention et les ressources sur les risques les plus susceptibles d'avoir un impact important, ce qui est la conclusion logique de l'exercice, peut empêcher les gens d'envisager et de prendre en compte des risques beaucoup moins probables, mais potentiellement catastrophiques. Selon cet argument, une organisation qui n'est prête à faire face qu'à une liste des risques les plus probables peut se montrer moins flexible et moins résiliente face à des événements imprévisibles. Certaines organisations adoptent un processus appelé « horizon-scanning » (analyse prospective), qui consiste essentiellement en un brainstorming collectif sur des événements improbables qui, s'ils se produisaient, auraient un impact considérable. Cet exercice peut inciter le personnel à réfléchir de manière créative à un éventail plus large de scénarios de menaces et à élaborer des stratégies de réponse susceptibles de faire face à divers événements.⁵³

La prise de décision dans un contexte d'incertitude est une constante dans les environnements humanitaires complexes, où les informations sont rares et où la situation est dynamique et imprévisible. Une prise de décision efficace nécessite de trouver un équilibre entre une réponse rapide et une analyse approfondie, en recourant souvent à la fois à des approches analytiques et naturalistes (intuitives et fondées sur l'expérience) de la prise de décision.⁵⁴ Intégrer des exercices d'analyse prospective dans le cadre de

53 GISF et Humanitarian Outcomes (2024) *State of practice: The evolution of security risk management in the humanitarian space* (en anglais, « État des lieux : l'évolution de la gestion des risques de sécurité dans le domaine humanitaire ») (https://humanitarianoutcomes.org/security_risk_mgmt_humanitarian_space_2024).

54 Pour une analyse plus détaillée, voir Cole, A. et Olympiou, P. (2022) *Risk management & decision making under uncertainty during the Afghanistan crisis 2021* (en anglais, « Gestion de risque et prise de décision dans un contexte d'incertitude pendant la crise afghane de 2021 »). GISF (<https://gisfprod.wpengine.com/resource/risk-management-under-uncertainty-during-the-afghanistan-crisis-2021/>).

l'évaluation des menaces peut éviter les approches stéréotypées qui, dans le pire des cas, réduisent les processus d'évaluation des risques à de simples outils budgétaires.

Cependant, disposer d'une méthode systématique et structurée pour l'analyse des risques n'implique pas nécessairement un processus bureaucratique lourd ou un exercice techniquement complexe. Elle doit plutôt être suffisamment simple pour que tout le personnel puisse y participer de manière significative, et suffisamment légère pour pouvoir être réalisée (et refaite si nécessaire) en peu de temps. Il est important que les organisations adaptent le processus d'analyse des risques à leur organisation, en tenant compte de leurs besoins et de leurs capacités.

4.1.6 Une approche simplifiée

Les processus d'évaluation des risques peuvent souvent sembler complexes et intimidants. Bien que ce chapitre ait présenté des méthodologies détaillées et des bonnes pratiques en matière d'analyse des risques, il peut sembler irréaliste pour les organisations disposant d'un temps ou d'un personnel limités de mettre en œuvre systématiquement toutes les étapes décrites.

Dans de tels cas, le simple fait d'examiner et de réfléchir aux questions clés suivantes peut aider à orienter l'analyse et l'atténuation des risques. Bien sûr, l'objectif n'est pas de mettre en place un processus d'analyse des risques parfait, mais d'optimiser autant que possible la compréhension de la situation et la prise de décision fondée sur des preuves.

Questions clés de l'analyse des risques

- **Quel est le contexte externe ?**
 - Quels sont les facteurs politiques, économiques, socioculturels, technologiques, environnementaux et juridiques pertinents ?
 - Qui sont les principaux acteurs (groupes armés, acteurs criminels, éléments gouvernementaux) qui influent sur la sécurité, et comment sont-ils liés entre eux ?
 - Y a-t-il un conflit actif et, si oui, quelles en sont les causes ? Qui sont les acteurs et quelle est leur relation avec l'organisation et entre eux ?
- **Quel est le contexte organisationnel interne ?**
 - Quels sont les objectifs, la structure, les capacités, les programmes, le personnel et les sites de l'organisation, et comment ceux-ci s'articulent-ils avec le contexte externe ?

- **Quelles sont les principales menaces dans l'environnement opérationnel ?**
 - Quelles sont les menaces internes et externes qui pèsent sur l'organisation ?
 - Comment, quand et pourquoi chaque menace pourrait-elle se concrétiser, et qui/quoi toucherait-elle ?
- **Dans quelle mesure l'organisation est-elle vulnérable aux menaces identifiées ?**
 - Quelles sont les vulnérabilités du personnel et de l'organisation, compte tenu notamment des facteurs d'identité intersectionnelle, des évaluations des programmes et des niveaux d'acceptation ?
- **Quelle est la probabilité que les menaces se concrétisent ?**
 - Quelle est la probabilité que les menaces identifiées se concrétisent ?
 - Quelles sont les menaces les plus probables ?
- **Quels sont les impacts potentiels des menaces identifiées ?**
 - Quel est l'impact potentiel de chaque menace identifiée ?
 - Quelles sont les menaces qui ont les conséquences les plus importantes, et qui/quoi pourrait être le plus touché ?
- **Quelles mesures d'atténuation peuvent être mises en œuvre ?**
 - Quelles sont les menaces les plus préoccupantes et qui nécessitent une atténuation des risques (généralement celles qui sont les plus probables ou dont l'impact est le plus grave) ?
 - Quelles actions peuvent réduire la probabilité et/ou l'impact des menaces identifiées ?
- **Que fera l'organisation face aux risques résiduels ?**
 - L'organisation évitera-t-elle ou acceptera-t-elle et/ou partagera-t-elle tout risque résiduel après la mise en place des mesures d'atténuation ?
- **Quels sont les risques à faible probabilité mais à fort impact qui méritent une plus grande attention ?**
 - Quels sont les risques qui nécessitent une planification de scénario ou une analyse plus approfondie en raison de leurs conséquences potentiellement graves malgré leur faible probabilité ?

Lors de l'évaluation des risques, il est utile de déterminer qui ou quoi pourrait être touché (y compris les facteurs liés à l'identité), pourquoi et comment, ainsi que quand et où les menaces pourraient apparaître (en tenant compte à la fois des sphères physique et numérique).

Informations complémentaires

Recherche et analyse

Cole, A. et Olympiou, P. (2022) *Risk management & decision making under uncertainty during the Afghanistan crisis 2021* (en anglais, « Gestion de risque et prise de décision dans un contexte d'incertitude pendant la crise afghane de 2021 »). GISF (<https://gisfprod.wpengine.com/resource/risk-management-under-uncertainty-during-the-afghanistan-crisis-2021/>).

GISF et Humanitarian Outcomes (2024) *State of practice: the evolution of security risk management in the humanitarian space* (en anglais, « État des lieux: l'évolution de la gestion des risques de sécurité dans le domaine humanitaire ») (https://humanitarianoutcomes.org/security_risk_mgmt_humanitarian_space_2024).

Recommandations et ressources

Bickley, S. (2017) *Gestion du risque sécurité: manuel de référence à l'attention des petites ONG*. European Interagency Security Forum (<https://gisf.ngo/resource/security-risk-management-a-basic-guide-for-smaller-ngos/>).

Davis, J. et al. (2020) *Security to go: a risk management toolkit for humanitarian aid agencies* (« La sécurité en pratique: boîte à outils de gestion des risques à l'attention des agences humanitaires »), 4e édition (La 4e édition n'est pas disponible en français). GISF (<https://gisf.ngo/resource/security-to-go/>).

GISF (n.d.a) 1. *Analyse du contexte*. Guide interfonctionnel pour la sécurité des ONG (<https://gisf.ngo/toolbox-pwa-fr/resource/1-analyse-du-contexte/>).

GISF (n.d.b) 2. *Stratégie d'acceptation*. Guide interfonctionnel pour la sécurité des ONG (<https://gisf.ngo/toolbox-pwa-fr/resource/2-strategie-dacceptation/>).

GISF (n.d.c) 3. *Évaluations des risques*. Guide interfonctionnel pour la sécurité des ONG (<https://gisf.ngo/toolbox-pwa-fr/resource/3-evaluation-des-risques/>).

RedR UK, Insecurity Insight et European Interagency Security Forum (2017) *Manuel de la gestion de l'information en cas d'incident de sécurité (GIIS)* (<https://siim.insecurityinsight.org/tools-and-resources/handbook-guide-and-tools>).

4.2 Élaboration d'une stratégie de sécurité

La stratégie de sécurité d'une organisation en contexte opérationnel particulier repose sur un équilibre entre les approches adoptées et les mesures spécifiques qu'elle décide de prendre. Celles-ci s'appuient sur le processus d'évaluation des risques, ainsi que sur les principes et les valeurs de l'organisation. Ce chapitre présente les trois grandes approches de sécurité qui se recoupent et qui peuvent façonner une stratégie de sécurité : l'acceptation, la protection et la dissuasion.

4.2.1 Approches de sécurité

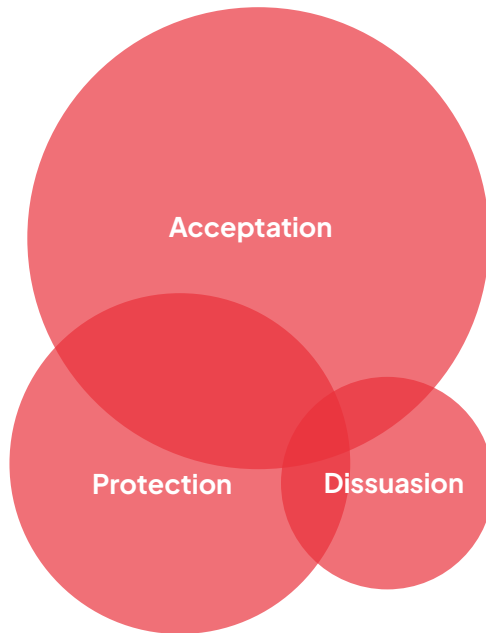
Les concepts d'acceptation, de protection et de dissuasion constituent chacun un éventail d'options et de mesures de sécurité, allant des plus « souples » aux plus « strictes ». Comme évoqué précédemment :

- Les mesures d'acceptation visent à réduire ou à éliminer les menaces en renforçant l'acceptation (la tolérance politique et sociale) de la présence d'une organisation et de son travail dans un contexte particulier.
- Les mesures de protection visent à réduire la vulnérabilité à la menace, mais n'ont pas d'incidence sur la menace elle-même⁵⁵ – on parle souvent de « durcissement des cibles ».
- Les mesures de dissuasion visent à contrer une menace par une contre-menace, telle que le recours à la force (l'exemple classique étant celui des gardes armés).

Bien que l'acceptation, la protection et la dissuasion soient parfois considérées comme des stratégies distinctes – chacune occupant un coin du « triangle de sécurité », dans la pratique, une organisation choisira généralement une combinaison d'options issues de chacune d'entre elles, en fonction de son environnement opérationnel. Dans différents contextes et à mesure que les risques évoluent, il peut être approprié de passer d'un type de mesure (ou d'une approche globale) à un autre. Plutôt qu'un triangle statique, il peut donc être plus utile d'imaginer des sphères interactives qui se chevauchent et dont l'importance peut varier en fonction du contexte, des risques et de la stratégie organisationnelle (voir la figure 10).

55 De nombreux professionnels de la sécurité, ainsi que les éditions précédentes de cette RBP, utilisaient le terme « protection ». Il convient toutefois de noter que certains professionnels de la sécurité utilisent le terme « protectrice » (comme dans « approche protectrice » et « mesures protectrices ») pour établir une distinction claire entre les mesures de gestion des risques de sécurité pour le personnel et la protection en tant que type d'intervention humanitaire axée sur les communautés à risque.

Figure 10 Exemple de combinaison de mesures dans une stratégie de sécurité



Compte tenu de leurs principes et valeurs, de nombreuses organisations humanitaires considèrent l'acceptation comme l'approche globale la plus appropriée et la plus efficace, et en font le fondement de leur stratégie de sécurité dans un lieu donné (c'est-à-dire que la plupart des mesures d'atténuation des risques sont conçues pour accroître l'acceptation, tout en évitant activement toute mesure susceptible d'avoir un impact négatif sur la perception et l'acceptation). Dans certains contextes, cela peut signifier qu'une organisation décide de ne recourir à aucune mesure de dissuasion si cela est perçu comme contraire à ses principes, à ses valeurs et à son approche par acceptation.

Les mesures d'acceptation ne sont pas efficaces contre toutes les menaces, c'est pourquoi il est souvent nécessaire de combiner plusieurs mesures. Dans les environnements où l'anarchie ou la violence sont omniprésentes ou lorsque les acteurs armés sont peu enclins à négocier, les mesures d'acceptation peuvent, à elles seules, n'avoir qu'une efficacité limitée. Cependant, ajouter d'autres types de mesures ne signifie pas nécessairement abandonner une approche axée sur l'acceptation. Au contraire, le fait d'ajouter des mesures de protection visibles, par exemple, peut nécessiter davantage de

sensibilisation et d'autres mesures d'acceptation actives. L'efficacité de toute approche dépendra également des actions menées par les autres organisations humanitaires.

Les mesures de protection et de dissuasion ne sont pas nécessairement plus efficaces dans tous les cas et peuvent engendrer leurs propres problèmes. Les mesures de protection attirent l'attention sur l'organisation en tant que cible potentielle et, contrairement à l'acceptation, ne s'adressent pas à ceux qui constituent une menace. Elles peuvent également conduire à une « mentalité de bunker », qui peut se traduire par un modèle opérationnel restrictif et une plus grande distance par rapport aux communautés cibles, tout cela dans le but de réduire les risques en isolant l'organisation, son personnel et ses actifs. Cela rend plus difficile le développement de relations avec les autres, ce qui complique à son tour l'obtention d'informations sur l'environnement et la communication efficace avec les interlocuteurs locaux.

Les mesures de dissuasion, les moins utilisées parmi les organisations humanitaires, présentent des inconvénients évidents. Si les organisations font preuve de force, par exemple en se déplaçant avec des escortes armées ou en engageant des gardes armés pour leurs bureaux, il leur est plus difficile de véhiculer une image de neutralité et de non-violence.

Une bonne stratégie de sécurité nécessite une combinaison flexible de ces mesures, ce qui peut impliquer de choisir une approche globale qui puisse guider la décision quant aux mesures à privilégier. Comme base pour toute activité de programmation, il est recommandé de cultiver l'acceptation et de bonnes relations avec la population locale et ses dirigeants, ainsi qu'avec les acteurs étatiques et non étatiques concernés. Dans les environnements plus précaires où des risques généraux ont été identifiés pour les organisations humanitaires, certaines mesures de protection sont généralement recommandées, en particulier contre la criminalité. Dans des contextes d'insécurité importante, où les risques pour l'organisation sont importants, des mesures de dissuasion peuvent s'avérer nécessaires si elles constituent le seul moyen de protéger le personnel et de continuer à fournir une aide essentielle, ce que l'on appelle parfois le « principe de dernier recours ». Si l'acceptation est l'approche principale, les mesures de protection et de dissuasion peuvent être adaptées pour maintenir l'acceptation. Les mesures d'acceptation peuvent être utilisées pour compléter les mesures d'atténuation des risques de protection et de dissuasion.

Les différentes mesures ont des implications différentes en termes de ressources. Toutes ont un coût financier. L'acceptation est peut-être la plus difficile à mesurer en termes financiers, mais elle peut nécessiter un investissement considérable en temps de la part du personnel et éventuellement de nouvelles initiatives de programme, telles que des actions de communication auprès des médias. Les équipements de protection ont un coût financier direct, tandis que les procédures de protection (par exemple, les couvre-feux ou le fait de toujours circuler avec deux voitures) peuvent alourdir le budget en limitant la capacité opérationnelle. Une approche de dissuasion peut avoir des implications en termes de ressources plus ou moins importantes, dont il peut être

difficile, voire impossible, de se défaire à long terme (par exemple, investir dans une protection armée).

4.2.2 Acceptation

L'acceptation est souvent une approche organisationnelle plus large qui vise à favoriser des relations authentiques avec les communautés touchées et les parties prenantes, tout en respectant les principes humanitaires fondamentaux. Cette approche est souvent considérée comme essentielle pour garantir la légitimité et le consentement nécessaires à la mise en œuvre efficace des programmes. Une approche par acceptation permet également aux organisations humanitaires de se distinguer d'autres acteurs, tels que les forces militaires ou les prestataires de services du secteur privé.

Dans la gestion des risques de sécurité, l'acceptation est souvent comprise comme la réduction ou l'élimination des menaces potentielles en cultivant et en entretenant des relations avec les parties prenantes concernées et en obtenant leur « consentement » pour opérer dans un lieu donné. En réalité, le « consentement » n'est peut-être pas le concept le plus approprié pour mesurer l'acceptation. Dans la pratique, l'acceptation peut être comprise de manière plus utile comme un continuum, allant de « acceptée » (la situation la plus sûre) à « ciblée » (la situation la plus dangereuse) :⁵⁶

- acceptée
- tolérée
- rejetée
- ciblée.

Défis liés à l'acceptation

Les défis et les limites liés à l'acceptation sont nombreux. Voici quelques-uns des plus importants.

- **Financement.** La perception que l'on a d'une organisation peut être liée à la provenance de ses financements. Le soupçon que ceux qui apportent l'argent contrôlent l'organisation humanitaire peut créer des problèmes importants, en particulier si le donateur en question est partie prenante au conflit ou est perçu comme ayant un agenda politique.

⁵⁶ Pour en savoir plus, voir Fast, L. et al. (2011) *The acceptance toolkit: a practical guide to understanding, assessing, and strengthening your organization's acceptance approach to NGO security management* (en anglais, « Le kit d'acceptation : un guide pratique pour comprendre, évaluer et renforcer l'approche par acceptation de votre organisation en matière de gestion de la sécurité des ONG »). Save the Children Federation (<https://acceptanceresearch.wordpress.com/acceptance-toolkit/>).

- **Action humanitaire raisonnée.** Dans certains contextes, les gouvernements nationaux et étrangers peuvent ne pas souhaiter que les organisations humanitaires négocient ou même communiquent avec des acteurs armés non étatiques, même si cela est nécessaire pour mener une action humanitaire raisonnée et accéder aux populations touchées par la crise. Les gouvernements peuvent sanctionner ces négociations, par exemple en recourant à la législation en matière de lutte antiterroriste. Les organisations qui acceptent des financements assortis de clauses sur la lutte antiterroriste devront veiller à prendre toutes les mesures raisonnables pour garantir leur respect sans compromettre la mission humanitaire.
- **Plaidoyer.** La recherche et le maintien de l'acceptation peuvent rendre difficile pour les organisations de dénoncer les violations du droit international humanitaire ou les atteintes aux droits humains, car cela peut nuire à leurs relations avec diverses parties prenantes. Les dirigeants des organisations ont tout intérêt à adopter une approche structurée pour trouver un équilibre entre les efforts de plaidoyer et les préoccupations liées à la gestion des risques de sécurité. *(Voir le chapitre 2.2 pour une analyse plus détaillée sur le plaidoyer.)*
- **Informations préjudiciables.** Les implications des informations erronées, de la désinformation, de la mauvaise information et des discours de haine pour la sécurité des travailleurs humanitaires constituent un sujet de préoccupation et d'étude croissant. *(Voir le chapitre 6.2 pour une analyse plus détaillée des défis posés par les informations préjudiciables.)*⁵⁷
- **Prolifération et fragmentation des groupes armés.** Dans de nombreux contextes, la prolifération et la fragmentation des groupes armés font qu'il est plus difficile de déterminer qui contrôle quel territoire, ainsi que qui est responsable au sein d'une organisation (c'est-à-dire les négociations avec un représentant seront-elles respectées par le reste du groupe?). Certaines organisations ont investi des ressources importantes dans le suivi des groupes armés afin de comprendre leurs structures internes et l'évolution de leurs schémas de contrôle territorial.

Éléments clés de l'acceptation active

L'acceptation ne peut être présumée ; elle doit être activement forgée et diligemment entretenue. Les mesures d'« acceptation active » comprennent la sensibilisation stratégique d'un large éventail de parties prenantes, le développement des compétences du personnel en matière de relations sociales, politiques et interpersonnelles et de communication, ainsi que la conception et la diffusion de messages clés concernant la mission, les objectifs et les programmes de l'organisation. Les éléments clés d'une approche par acceptation active comprennent :

- Travailler avec le personnel du programme pour intégrer la gestion des risques de sécurité dans la conception du programme.

⁵⁷ Pour une analyse de l'impact de la technologie sur l'acceptation, voir Al Achkar, Z. (2021) 'Digital risk: How new technologies impact acceptance and raise new challenges for NGOs' (en anglais, « Risques numériques : comment les nouvelles technologies influencent l'acceptation et posent de nouveaux défis aux ONG ») sur le site du GISF (éd.) *Achieving safe operations through acceptance: Challenges and opportunities for security risk management* (en anglais, « Assurer la sécurité des opérations grâce à l'acceptation : défis et opportunités pour la gestion des risques de sécurité ») (<https://gisf.ngo/resource/achieving-safe-operations-through-acceptance/>).

- Établir et entretenir des relations avec les principales parties prenantes, y compris les acteurs armés. Cela peut inclure la collaboration avec des acteurs nationaux, régionaux et internationaux, le cas échéant.
- Obtenir l'acceptation des populations locales (par exemple, au moyen de réunions et de rencontres).
- La gestion des communications.
- Le suivi des perceptions et de l'opinion publique.
- La gestion des perceptions du personnel et de l'organisation.

Ces éléments sont abordés plus en détail dans la section suivante.⁵⁸

Intégration du programme

Les capacités d'une organisation à répondre aux besoins des personnes de manière transparente et redevable est souvent déterminante dans la façon dont elle est perçue. Il est largement reconnu que l'acceptation est liée à une programmation efficace et adaptée qui répond aux besoins d'une communauté. La participation communautaire, la consultation et les partenariats locaux sont souvent des éléments clés d'une programmation efficace. Cependant, même si les programmes répondent aux besoins des populations touchées, ils peuvent avoir des effets négatifs sur certains acteurs ou modifier les structures du pouvoir politique, économique et social. Dans la mesure où une bonne programmation est un élément essentiel de l'acceptation, celle-ci ne peut être présumée à partir de la seule qualité de la programmation.

Le lien entre une programmation efficace et l'obtention/le maintien de l'acceptation devrait être explicitement mentionné dans les activités de planification des programmes, inclus dans les plans de programme, les évaluations des besoins et les budgets, et intégré dans les outils de suivi et d'évaluation des programmes.

Interaction avec les principales parties prenantes

Une fois que les principales parties prenantes ont été identifiées et que leurs positions, leur influence et leur disposition respectives ont été analysées, les organisations peuvent approcher celles qui exercent, de manière formelle ou informelle, une influence significative sur la capacité d'une organisation à fonctionner en toute sécurité dans un environnement donné. Celles-ci peuvent être favorables, défavorables ou neutres à l'égard de l'organisation et peuvent être identifiées dans l'analyse des acteurs. Les acteurs nationaux, régionaux et internationaux doivent être pris en compte au même titre que les parties prenantes locales, car leur acceptation est de plus en plus importante pour une action humanitaire efficace.

► Voir le chapitre 4.1 pour plus d'informations sur l'analyse des acteurs.

58 Pour une analyse plus détaillée de l'approche par acceptation active, voir Fast et al. (2011).

Il est important d'évaluer l'influence de chaque partie ; dans certaines situations, l'acceptation des acteurs clés peut suffire s'il n'est pas possible d'obtenir l'acceptation de tous. Le fait de s'appuyer sur du personnel de la zone ou de faire appel à un intermédiaire respecté (tel qu'un chef religieux ou un dirigeant communautaire) pour entrer en contact avec d'autres parties prenantes au nom de l'organisation peut favoriser l'acceptation.

Pour établir une relation avec les principales parties prenantes, il faut généralement plus que des réunions formelles rares et brèves. Les messages peuvent être transmis non seulement lors des réunions, mais aussi par le type de réunion et la manière dont elle se déroule. Les coutumes culturelles doivent être respectées et observées. Prendre le temps de rencontrer les gens et de discuter avec eux, expliquer, écouter, socialiser et faire preuve de politesse et de respect peuvent être des éléments importants pour s'assurer leur acceptation.

Les accords formels, par exemple avec le gouvernement ou avec des groupes influents, peuvent être utiles dans la mesure où ils apportent une reconnaissance officielle et un accord explicite sur des questions spécifiques. En matière de sécurité, les accords peuvent définir des responsabilités détaillées, y compris les procédures à suivre et un point de contact en cas de problèmes de sécurité. Le personnel opérationnel peut souhaiter conserver sur lui une copie de l'accord (dans la langue appropriée) afin de faciliter l'accès ou le dialogue. Il est important de garder à l'esprit que les accords écrits n'ont pas la même valeur dans tous les environnements sociaux et que d'autres pratiques culturelles peuvent être plus appropriées. Les accords formels peuvent également poser problème, par exemple s'ils ne sont valables que pour une période limitée, s'ils attirent l'attention sur des zones dans lesquelles les autorités peuvent chercher à réglementer ou à entraver les activités des organisations humanitaires de manière inappropriée, ou s'ils mobilisent plus de temps que leur valeur ne le justifie. Les accords formels peuvent également ne pas être reconnus à tous les niveaux d'un groupe/d'une entité. Ces facteurs doivent être pris en compte avant de conclure des accords formels.

Acteurs armés non étatiques

Les organisations qui travaillent dans une zone sous le contrôle de facto d'un groupe armé devront probablement signaler leur présence à ce dernier et obtenir l'assurance que leur travail est acceptable et que leur personnel ne subira aucun préjudice. Les questions à se poser lorsque l'on interagit (ou que l'on envisage d'interagir) avec ces acteurs sont les suivantes :

- Quelle est la relation entre le groupe armé et la population locale ?
- Quelle est la relation entre le groupe armé et le personnel de l'organisation ?
- Quelle est la structure de commandement et la discipline ? Quels sont les buts et objectifs du groupe armé ?

- Comment le dialogue et les négociations avec le groupe armé peuvent-ils affecter les relations avec les autres (y compris les autorités)?
- Quelles demandes ou exigences (par exemple, payer des «impôts» ou obtenir une « autorisation » quotidienne d'exercer) pourraient être formulées, et comment l'organisation devrait-elle y répondre?

Pour comprendre ces dynamiques et ces risques, il faut être capable de les analyser de manière proactive. Il sera souvent judicieux de collaborer avec d'autres organisations humanitaires afin de mettre en commun les capacités et de permettre une approche commune et des lignes rouges communes (limites non négociables) lors des interactions avec des acteurs armés non étatiques.

► Voir le chapitre 4.1 pour plus d'informations sur les groupes armés dans le cadre d'une analyse des acteurs.

Populations locales

Si le niveau d'acceptation est élevé, les membres de la communauté locale peuvent faire des suggestions sur la manière de réduire les risques et, dans certains cas, fournir des informations et des avertissements essentiels à l'organisation. Leur influence ne doit cependant pas être surestimée et, dans certaines circonstances, les communautés peuvent ne pas être en mesure de réduire de manière significative les risques de sécurité. Elles peuvent être impuissantes à influencer d'autres acteurs, négliger ou mal évaluer de nouvelles menaces, ou tirer davantage profit du soutien apporté à un autre acteur.

Il existe une différence entre la simple tolérance de la présence et du programme d'une organisation et sa véritable acceptation. Les gens peuvent accepter la présence d'une organisation uniquement parce qu'ils en ont désespérément besoin, ou utiliser l'aide comme une source de soutien sans pour autant se sentir activement responsables du bien-être de l'organisation. Écouter et répondre aux attentes des gens, les traiter avec respect, agir de manière transparente et être redevable peuvent approfondir les relations et encourager un plus grand niveau d'acceptation. Ces relations peuvent même prendre le pas sur la dimension matérielle. Une organisation humanitaire peut se trouver dans l'incapacité de fournir une aide suffisante, voire parfois aucune aide, et pourtant continuer d'être acceptée en raison de la qualité de ses relations.

La gestion des communications

Pour toutes les parties prenantes, les communications doivent être claires et cohérentes. Une organisation et son personnel doivent savoir et être capables d'expliquer, dans un langage concis et facile à comprendre, qui ils sont, pourquoi ils sont là, ce qu'ils veulent faire et comment ils interagissent avec les autres. Une simple fiche de questions-réponses à l'intention du personnel peut s'avérer utile.

Dans le cas des organisations internationales et fédérées, la nécessité de cohérence s'étend à l'harmonisation des messages à l'échelle mondiale. Si certaines communications peuvent être légèrement adaptées en fonction des différents publics, le message général doit rester le même, qu'il provienne du siège social ou d'un site de projet.

Les déclarations publiques doivent refléter les valeurs, les principes et le mandat d'une organisation et être contextualisées pour être comprises localement, tout en tenant compte de leur impact sur les perceptions locales.

Les déclarations publiques critiques à l'égard des autorités locales doivent être mûrement réfléchies. Les facteurs clés à prendre en compte sont notamment la nécessité de révéler l'information au public, le moment où informer la personne concernée, la formulation et la justification des allégations, ainsi que la méthode de diffusion.

► *Pour une analyse plus détaillée, voir le chapitre 2.2 sur le plaidoyer et la sécurité.*

La gestion des perceptions du personnel

La façon dont le personnel est perçu peut influencer la perception de l'organisation dans son ensemble. Les caractéristiques liées à l'identité jouent un rôle à cet égard et peuvent constituer à la fois des atouts et des vulnérabilités, selon la perception locale de ces caractéristiques liées à l'identité.⁵⁹

► *Voir le chapitre 1.2 pour une analyse plus détaillée des facteurs et des perceptions liés à l'identité.*

L'aspect physique et le comportement sont également importants. L'aspect physique peut revêtir une importance sociale et politique considérable, et un comportement inapproprié peut susciter du ressentiment et aggraver les soupçons et les tensions existants.

Le respect des normes sociales et culturelles (par exemple, les coutumes en matière d'habillement, d'alcool et de relations interpersonnelles) peut améliorer la perception du personnel et de l'organisation. Les personnes qui découvrent un nouveau contexte ne peuvent pas connaître ou respecter toutes les coutumes, mais les erreurs peuvent être plus facilement pardonnées si elles s'accompagnent d'une attitude polie, posée et respectueuse, ou d'une position claire expliquant pourquoi les coutumes ne sont pas respectées.

59 Pour une analyse sur les avantages du recrutement d'un personnel diversifié et inclusif en termes d'acceptation, voir Williams, C., Kinch, P. et Herman, L. (2021) 'Promoting a blended risk management approach: the place of programming and diversity within a SRM strategy' (en anglais, «Promouvoir une approche mixte de gestion de risque : la place de la programmation et de la diversité dans une stratégie GRS») sur le site du GISF (éd.) *Achieving safe operations through acceptance: challenges and opportunities for security risk management* (en anglais, «Assurer la sécurité des opérations grâce à l'acceptation : défis et opportunités pour la gestion des risques de sécurité») (<https://gisf.ngo/resource/achieving-safe-operations-through-acceptance/>).

Les normes religieuses doivent également être prises en compte et respectées dans la mesure du possible ; les organisations confessionnelles peuvent être amenées à faire preuve d'une prudence particulière quant à leur image et leurs activités.

La gestion des perceptions de l'organisation

Il est important de tenir compte de la manière dont l'organisation et ses activités sont perçues. Les programmes correspondent-ils aux attentes et aux besoins de la communauté locale ? Certaines programmations peuvent ne pas être considérées comme prioritaires ou être perçues négativement par certains segments de la communauté. Comment les parties prenantes qui ne bénéficient pas du programme perçoivent-elles l'organisation et son personnel ? Ces parties prenantes sont-elles en mesure d'avoir un impact négatif sur l'acceptation du programme par les autres, d'entraver les programmes ou de nuire au personnel ?

Pour comprendre ces questions, il faut écouter les gens et s'adapter en conséquence. Même si un programme est largement accepté au sein d'une communauté, il peut encore irriter d'autres parties prenantes. Cela vaut pour pratiquement tous les secteurs : un programme d'aide alimentaire peut irriter les commerçants locaux en réduisant leurs profits ; la fourniture de services de santé gratuits peut détourner les patients des cliniques payantes, ce qui frustre les responsables locaux de la santé ; et rapporter les menaces de protection pesant sur la population peut irriter les responsables des violences.

La stratégie de sortie est un autre élément à prendre en compte. Les organisations peuvent mener à bien d'excellents programmes, mais constater que des stratégies de sortie mal exécutées compromettent la bonne volonté qui s'était développée au cours de la période du programme. Cela signifie qu'elles pourraient avoir du mal à se faire accepter à l'avenir.

Capacités et compétences pour l'acceptation

L'acceptation a des implications pratiques en termes de ressources humaines, de finances et d'administration. Une approche par acceptation active nécessite du personnel possédant certaines compétences clés. Celles-ci peuvent inclure :

- Les capacités à cartographier les acteurs clés et à établir un vaste réseau avec les parties prenantes.
- Une compréhension approfondie de la mission et des valeurs de l'organisation.
- De solides compétences en matière de négociation et d'établissement de relations.
- La maîtrise de la langue locale et d'excellentes compétences en communication.
- Les capacités à analyser l'évolution de la situation politique et des conditions de sécurité.

Pour appliquer efficacement une approche par acceptation, il faut que les cadres supérieurs fassent preuve de leadership. Ceux-ci devront non seulement posséder les compétences requises, mais aussi disposer de suffisamment de temps par rapport à leurs autres responsabilités.

L'acceptation a un coût. Elle entraîne des coûts opérationnels, notamment :

- Le temps consacré par le personnel, y compris l'embauche de personnel de sécurité supplémentaire, de la sensibilisation ou des relations avec les médias.
- La formation du personnel à la communication de la mission et des valeurs de l'organisation, ainsi qu'à la communication interculturelle et aux compétences diplomatiques et de négociation.
- Des déplacements supplémentaires (véhicules, carburant, temps de travail du personnel) peuvent être nécessaires pour rencontrer les parties prenantes.
- La traduction des documents ou des messages de l'organisation dans des formats et des langues adaptés au contexte local.
- Le paiement de l'utilisation de la radio, de la télévision et d'autres médias, si nécessaire.
- Le temps supplémentaire nécessaire pendant la phase de conception d'un programme.
- Les supports de communication, tels que les dépliants.

Ces coûts doivent être identifiés dans la conception du programme et intégrés dans le processus budgétaire.

► *Voir le chapitre 3.3 pour plus d'informations sur le financement de la sécurité.*

La mise en œuvre d'une approche par acceptation peut également nécessiter des ajustements des normes administratives ou juridiques au sein de l'organisation, comme dans les exemples suivants.

- Bien que les prestataires soient généralement choisis en fonction du prix et de la qualité, une approche par acceptation peut nécessiter la répartition des contrats entre différents secteurs de la population locale afin que les bénéfices soient perçus comme équitablement répartis. De même, il peut être judicieux d'acheter localement, même si un prestataire non local offre un meilleur rapport qualité-prix.
- L'organisation peut choisir d'adapter ses procédures de recrutement afin d'obtenir un équilibre de profils diversifiés (en tenant compte de l'ethnicité et du fait que les personnes soient issues de la zone, par exemple).

Suivi des perceptions et mesure de l'acceptation

Il n'existe pas de moyen simple de savoir comment une organisation est perçue et si (et pourquoi) elle est acceptée. Cela peut être un signe positif d'acceptation si les parties prenantes concernées :

- S'engagent publiquement à assumer la responsabilité de la sécurité du personnel.
- Partagent avec l'organisation des informations précises relatives à la sécurité (par exemple, avertir que quelqu'un a posé des questions sur l'organisation ou qu'une certaine menace est probable).
- Coopèrent activement avec l'organisation ou soutiennent ses activités.
- Autorisent l'accès (par exemple, les groupes armés laissent passer le personnel de l'organisation aux points de contrôle pour atteindre les zones couvertes par le programme).
- Aident à obtenir la libération d'un membre du personnel enlevé ou à récupérer des biens volés.
- Reconnaissent que l'organisation a eu un impact positif sur la vie des gens.
- Présentent leurs excuses si des membres d'un groupe causent du tort à l'organisation.

L'acceptation peut être le résultat des relations solides qu'entretient un membre du personnel dans un lieu ou un contexte particulier. Les organisations doivent en être conscientes et mesurer les implications potentielles si ce membre du personnel quitte l'organisation ou si la perception que l'on a de lui change.

L'acceptation peut également diminuer avec le temps, à mesure que les besoins et les attentes des personnes évoluent. Une fois qu'une situation s'est stabilisée, de nouvelles aspirations peuvent apparaître. Les organisations doivent s'efforcer de suivre en permanence les attitudes des populations locales et des principales parties prenantes afin d'évaluer leur niveau d'acceptation et tout changement susceptible d'entraver l'accès et la sécurité.

Cependant, un manque d'acceptation peut ne pas être lié à l'organisation elle-même et ne peut pas nécessairement être amélioré par ses efforts ; il peut s'agir, par exemple, d'un rejet du concept d'action humanitaire dans son ensemble.⁶⁰

60 Pour une analyse plus détaillée des limites de l'acceptation, voir Daudin, P. (2021) 'Acceptance under stress: old recipes for new problems' (en anglais, « L'acceptation sous pression : vieilles recettes pour de nouveaux problèmes ») sur le site du GISF (éd.) *Achieving safe operations through acceptance: challenges and opportunities for security risk management* (en anglais, « Assurer la sécurité des opérations grâce à l'acceptation : défis et opportunités pour la gestion des risques de sécurité ») (<https://gisf.ngo/resource/achieving-safe-operations-through-acceptance/>).

Comment suivre et mesurer l'acceptation – quelques idées

- Une bonne compréhension du contexte et des parties prenantes concernées est un élément fondamental pour suivre l'acceptation.
- Intégrer l'analyse de l'acceptation dans les méthodes de travail existantes. Cette Revue des bonnes pratiques (RBP) la présente comme une étape du processus d'analyse de la sécurité. Les évaluations de l'acceptation pourraient également être intégrées dans les audits de sécurité ou les forums communautaires.
- Les niveaux d'acceptation peuvent être mesurés à l'aide de critères/indicateurs objectifs, tels que la fréquence des réunions avec les principales parties prenantes et le niveau et la nature des interactions avec les principaux acteurs. Les données sur les incidents peuvent être utiles mais ne doivent pas être le seul indicateur.ⁱ
- Il peut être utile de répartir les parties prenantes concernées et de déterminer le niveau d'acceptation de chacune d'entre elles, ainsi que de définir les informations utiles et les principales mesures de suivi.ⁱⁱ Il peut également être utile de répartir les niveaux d'acceptation des différents acteurs sur le terrain : le secteur humanitaire dans son ensemble, l'organisation et les programmes et équipes spécifiques.ⁱⁱⁱ
- Les moyens de recueillir des informations pour étayer cette analyse comprennent :
 - la surveillance des publications sur les réseaux sociaux et dans les médias grand public ;
 - la mise en place de groupes de discussion et de consultations ;
 - la réalisation d'enquêtes périodiques sur la perception ;
 - la mise en place de mécanismes de rétroaction ;
 - la documentation de la nature des conversations informelles.
- Une fois les niveaux d'acceptation déterminés, ceux-ci peuvent être intégrés dans un plan d'action dédié ou incorporés dans des mesures d'atténuation des risques et d'autres activités. L'analyse des différents facteurs susceptibles d'influencer les perceptions et la détermination du niveau de maîtrise du risque dont dispose l'organisation sur ceux-ci peuvent orienter les actions à mener (par exemple, le comportement du personnel par rapport aux motivations politiques des groupes armés).

ⁱ Pour d'autres exemples d'indicateurs, voir Fast et al. (2011).

ⁱⁱ Voir, par exemple, GISF (n.d.) 2. *Stratégie d'acceptation*. Guide interfonctionnel pour la sécurité des ONG (<https://gisf.ngo/toolbox-pwa-fr/resource/2-strategie-dacceptation/>).

ⁱⁱⁱ Voir, par exemple, Billaudel, R. (2021) 'Measuring and improving acceptance: ACF's experience and perspectives' (en anglais, « Mesurer et améliorer l'acceptation : l'expérience et les perspectives d'ACF ») sur le site du GISF (éd.) *Achieving safe operations through acceptance: challenges and opportunities for security risk management* (en anglais, « Assurer la sécurité des opérations grâce à l'acceptation : défis et opportunités pour la gestion des risques de sécurité ») (<https://gisf.ngo/resource/achieving-safe-operations-through-acceptance/>).

Le suivi et l'analyse des niveaux d'acceptation sont des exercices largement subjectifs. Cette subjectivité peut être gérée en encourageant plusieurs personnes à participer au processus d'évaluation et en leur demandant de partager des exemples concrets pour expliquer leurs impressions, en utilisant plusieurs sources d'information et en recourant à des indicateurs objectifs et standardisés pour toutes les équipes et tous les sites.

4.2.3 Protection

Les mesures de protection visent à réduire la vulnérabilité. Cela peut être réalisé soit en durcissant les cibles, soit en augmentant ou en réduisant sa visibilité.

Durcissement des cibles

Les actifs physiques et les procédures peuvent réduire la probabilité qu'une menace s'approche de la cible ou réduire l'impact potentiel des dommages causés à la cible. Dans la pratique, cela peut se traduire par :

- Des équipements de sécurité du site, tels que l'installation de systèmes d'éclairage et d'alarme, la construction de murs d'enceinte ou l'installation de portails métalliques et de barres métalliques aux fenêtres (*voir le chapitre 7.2 pour plus de détails*).
- La protection des biens, comme des coffres-forts pour l'argent liquide et les équipements de valeur, et des alarmes pour les véhicules.
- Des procédures de protection telles que le contrôle de l'accès des visiteurs, l'accès des véhicules et les dispositions en matière de stationnement, ainsi que l'embauche de gardes pour patrouiller les lieux et avertir en cas d'intrusion.
- L'utilisation de véhicules blindés, d'équipements de protection individuelle (EPI) et de films anti-explosion sur les fenêtres.
- La formation du personnel à la sécurité numérique (*voir le chapitre 6.2 pour plus de détails*).
- Conduire en convoi ou organiser le logement du personnel de manière à ce que les résidences soient regroupées à proximité les unes des autres.

La force du nombre peut être efficace, mais elle ne permet pas nécessairement d'arrêter un agresseur déterminé et peut être contre-productive si l'objectif est de faire un plus grand nombre de victimes, ou si une autre organisation est visée et que d'autres personnes deviennent des victimes collatérales. De même, si les équipements de communication sont généralement nécessaires, les équipements visibles et coûteux peuvent attirer une attention indésirable. La lumière et le son (par exemple, des projecteurs sensibles au mouvement à l'extérieur d'un bâtiment) peuvent donner un avertissement préalable en cas d'attaque, permettant au personnel de prendre des mesures d'évitement (se réfugier dans une pièce sécurisée, s'échapper) ou d'appeler à l'aide. Cependant, là encore, ces dispositifs ne permettent pas toujours d'empêcher un incident.

Programmation discrète/à faible visibilité

La programmation à faible visibilité est devenue de plus en plus courante parmi les organisations humanitaires, en particulier lorsque l'acceptation n'est pas considérée comme une approche viable. Elle consiste à supprimer toute référence à l'organisation sur les bâtiments administratifs, le personnel, les véhicules et les résidences. Elle peut également impliquer l'utilisation de voitures privées ou de taxis. Dans les environnements à très haut risque, tout ce qui pourrait relier le personnel à une organisation (documents d'identité de l'organisation, téléphones portables, ordinateurs) peut être «expurgé». Le personnel susceptible de se démarquer de la population locale peut être déplacé vers un autre lieu. Dans les situations extrêmes où la discrétion est de mise, les bénéficiaires de l'aide peuvent ne pas être informés de la source de l'aide.

Une autre tactique de l'approche à faible visibilité consiste à utiliser des logos amovibles pour les véhicules dans les zones où la visibilité est déconseillée. Savoir quand afficher un logo et quand le retirer nécessite une évaluation des risques très précise, localisée et dynamique. Il est toutefois important de garder à l'esprit que les autocollants magnétiques amovibles peuvent être facilement volés et utilisés par d'autres personnes pour usurper l'identité de l'organisation.

Une approche discrète et à faible visibilité peut compliquer la programmation et éloigner l'organisation des sources d'information qui pourraient autrement renforcer sa sécurité. Elle peut également susciter des soupçons et des perceptions erronées sur les activités de l'organisation, ce qui nuit à son acceptation. Il s'agit d'une approche difficile à maintenir si l'organisation cherche à obtenir une plus grande reconnaissance de son travail auprès du public ou des donateurs. Les organisations ne considèrent généralement pas l'approche discrète comme un mode de fonctionnement permanent; elle est plutôt considérée comme exceptionnelle et limitée dans le temps. Elle peut également être adoptée au début d'un programme, puis progressivement modérée à mesure que les opérations se développent.

4.2.4 Dissuasion

La dissuasion consiste à faire peser une contre-menace: il s'agit essentiellement de décourager les attaquants potentiels en leur faisant craindre une riposte ou d'autres conséquences graves. La protection armée est la forme de dissuasion la plus forte utilisée par les organisations humanitaires. Il existe toutefois d'autres moyens de dissuasion potentiels, que cette section aborde brièvement avant de passer à un examen approfondi de la protection armée dans les opérations humanitaires.

Formes de dissuasion

Instruments juridique et diplomatique

Les travailleurs humanitaires bénéficient de protections juridiques en vertu du droit national et international. Malheureusement, les mesures juridiques de dissuasion ne sont pas toujours efficaces. Certaines organisations humanitaires peuvent tirer parti du soutien des autorités du pays donateur étranger, notamment pour négocier l'accès ou résoudre des problèmes administratifs avec les autorités nationales, mais leur influence sera limitée, et une interaction étroite avec les autorités du pays donateur peut nuire à leur apparence d'indépendance et de neutralité.

Suspension des opérations ou retrait

Face à certaines menaces ou à la suite d'incidents de sécurité, certaines organisations ont temporairement suspendu leurs programmes d'aide ou menacé de le faire. La poursuite ou la reprise du programme est alors subordonnée à la résolution ou à l'amélioration de la situation. Des données empiriques suggèrent que cette tactique ne fonctionne pas toujours très bien et que les organisations reprennent souvent leurs programmes malgré l'absence d'amélioration notable, ce qui peut nuire à leur crédibilité et compromettre l'efficacité de menaces similaires à l'avenir.

Une suspension ou la menace d'une suspension pourrait être efficace dans les circonstances suivantes :

- Si elle n'est pas perçue comme une sanction à l'encontre de personnes qui ne sont pas liées aux causes de l'insécurité et qui ne sont pas en mesure d'améliorer la sécurité.
- Si une partie influente de la population ou les dirigeants/autorités locaux peuvent être mobilisés au nom de l'organisation.
- Lorsque les organisations sont prêtes à maintenir la suspension jusqu'à ce que la situation soit résolue de manière satisfaisante et qu'elles ne reviendront pas trop rapidement sur leur décision en raison de pressions internes ou externes.
- Lorsque d'autres organisations ne compromettent pas l'action en intervenant pour combler le vide, un front commun doit idéalement être établi avant que les opérations ne soient suspendues.

À moins que l'incident ne soit très grave, une suspension sélective (par exemple, dans un lieu donné ou pour une période donnée) ou la réintroduction progressive des services peut offrir une plus grande marge de manœuvre. Une suspension totale tend à créer une situation difficile de « tout ou rien ».

- Voir le chapitre 4.3 pour une analyse pratique sur les implications des suspensions et des retraits en matière de sécurité.

Association informelle

Une autre option de dissuasion consiste à s'associer de manière informelle avec des acteurs locaux influents. Dans ce scénario, une attaque contre l'organisation pourrait être implicitement perçue comme un affront à ces acteurs. Cette option doit être abordée avec beaucoup de prudence, car elle pourrait compromettre les principes humanitaires de l'organisation et son acceptation par les autres parties prenantes, et pourrait même conduire l'organisation à devenir l'otage de la protection du décideur en question.

Protection armée

Les organisations humanitaires n'ont généralement pas recours à une protection armée. Cependant, dans certaines circonstances exceptionnelles, celle-ci peut s'avérer nécessaire pour permettre l'action humanitaire, par exemple pour les convois humanitaires entrant dans des environnements de combat importants ou lorsque les autorités l'exigent comme condition d'accès. Cela dit, si la protection armée peut apporter une certaine sécurité et une protection aux travailleurs humanitaires sur le moment (même si elle peut aussi avoir l'effet inverse et attirer les tirs), elle peut également compliquer les efforts visant à maintenir l'accès humanitaire sur le long terme. En d'autres termes, cette pratique compromet l'action humanitaire fondée sur des principes. Les directives du Comité permanent interorganisations (IASC) avancent plusieurs raisons pour éviter le recours à des escortes armées pour les convois humanitaires en raison de leurs implications contre-productives à long terme.⁶¹

La relation entre protection armée et action humanitaire est délicate. Bien que pratiquement toutes les organisations humanitaires aient, à un moment ou à un autre, eu recours à une forme ou une autre de protection armée, celle-ci est souvent considérée comme un tabou, et les discussions à ce sujet sont très sensibles. La coopération avec un acteur armé – y compris une force mandatée par l'ONU – peut amener les acteurs locaux, nationaux et internationaux, ainsi que la population, à associer les organisations humanitaires et les bénéficiaires de l'aide aux objectifs politiques et/ou militaires de cet acteur armé. Cela pourrait potentiellement compromettre la neutralité, l'impartialité et l'indépendance réelles et perçues de l'organisation humanitaire et de la communauté humanitaire au sens large, ainsi que son acceptation. L'impact d'une protection armée sur l'acceptation n'est pas toujours évident et peut varier en fonction du contexte et d'autres facteurs d'influence.⁶²

61 Comité permanent interorganisations (IASC) (2013) *IASC non-binding guidelines on the use of armed escorts for humanitarian convoys* (en anglais, «Directives non contraignantes du IASC relatives à l'utilisation d'escortes armées pour les convois humanitaires») (<https://reliefweb.int/report/world/iasc-non-binding-guidelines-use-armed-escorts-humanitarian-convoys>).

62 Pour une analyse sur ce thème, voir Jourde, J. (2021) 'Private security contracting and acceptance: a dangerous match?' (en anglais, «La passation de contrats privés en matière de sécurité et acceptation: une combinaison dangereuse?») sur le site du GISF (éd.) *Achieving safe operations through acceptance: challenges and opportunities for security risk management* (en anglais, «Assurer la sécurité des opérations grâce à l'acceptation: défis et opportunités pour la gestion des risques de sécurité») (<https://gisf.ngo/resource/achieving-safe-operations-through-acceptance/>).

Bien que cette section fournisse un cadre plus systématique pour l'examen de la question, elle ne vise pas à plaider en faveur du recours à la protection armée, mais plutôt à en explorer les avantages, les risques et les défis potentiels. Avant de décider de recourir à une protection armée, il est conseillé d'en examiner les avantages et les inconvénients dans la situation spécifique et d'explorer toutes les alternatives possibles.

Les questions suivantes peuvent être prises en compte pour décider s'il convient de recourir à une protection armée :

- Dans quelles circonstances l'organisation autorise-t-elle, en principe, le recours à une protection armée ?
- Les avantages liés au recours à une protection armée dans ce contexte l'emportent-ils sur les risques ?
- Existe-t-il de sérieuses inquiétudes quant à la manière de gérer la protection armée, et ces inquiétudes peuvent-elles être surmontées ?
- Comment le recours à une protection armée affectera-t-il la perception de l'organisation en particulier, et des organisations humanitaires en général, et quel sera son impact sur le niveau d'acceptation parmi les principales parties prenantes ?
- Quelles sont la culture et les pratiques locales en matière de recours à la protection armée ? (Cela peut influencer la manière dont son recours est perçu et accepté.)

À chaque étape du raisonnement, il est possible d'arriver à la conclusion qu'une protection armée n'est peut-être pas appropriée. Gardez également à l'esprit que la nécessité d'envisager une protection armée peut indiquer que le seuil de risque acceptable a déjà été franchi et que la véritable décision à prendre peut être de se retirer ou de ne pas commencer la programmation. Si ce seuil n'a pas encore été atteint, ou si une protection armée pourrait réduire le risque à un niveau plus acceptable, alors trois grands domaines entrent en jeu dans la réflexion sur la décision : les principes et l'éthique, le contexte et la gestion.

Questions de principes et d'éthique

Certains affirment que la protection armée va à l'encontre des principes fondamentaux de l'action humanitaire. Cette position se fonde généralement sur des considérations éthiques ou opérationnelles à long terme. L'argument éthique soutient que l'action humanitaire n'est jamais compatible avec le recours à la force. D'un point de vue idéologique, une organisation peut refuser la protection armée parce que son utilisation, par principe, contribue à la poursuite de la production et de la distribution d'armes.

La considération opérationnelle à long terme est que, si la protection armée peut être justifiée dans un contexte donné, elle peut également fragiliser l'image globale

de l'action humanitaire dans le monde et peut donc conduire à une augmentation de l'insécurité ailleurs ou plus tard. Selon ce raisonnement, le recours trop rapide ou trop fréquent à la protection armée sape les efforts mondiaux visant à renforcer le respect du droit international humanitaire et l'action humanitaire indépendante.

Il y a également des considérations pratiques. Les escortes armées rendent le travail humanitaire beaucoup moins flexible en termes de déplacements, car les autorisations et les escortes doivent souvent être organisées à l'avance. Rendre les déplacements plus prévisibles peut accroître la vulnérabilité d'une organisation aux attaques, en particulier si les escortes ne sont pas entièrement fiables.

Les arguments en faveur du recours à une protection armée soutiennent qu'elle peut être acceptable en dernier ressort, lorsque la survie des populations serait à risque si l'aide humanitaire et autres formes d'assistance étaient réduites.⁶³ Dans certains contextes, le recours à une protection armée pour faciliter la fourniture de l'aide peut relever de l'exercice par l'État de ses obligations en vertu du droit national et international ou de la politique gouvernementale.

Une autre considération importante concerne les bénéficiaires de la protection armée:

- S'agit-il uniquement de l'organisation humanitaire et de son personnel, ou cette protection peut-elle apporter des avantages publics plus larges et renforcer la sécurité publique?
- Le recours aux armes et à des gardes armés – peut-être recrutés localement – aura-t-il un effet pacificateur sur la situation locale ou augmentera-t-il les tensions?
- Contribue-t-il à la «privatisation» de la sécurité, selon laquelle seuls ceux qui en ont les moyens peuvent bénéficier de la sécurité?
- Cela met-il indirectement d'autres personnes en danger en les rendant plus vulnérables en comparaison? Il est important d'examiner l'effet qu'elle a, le cas échéant, sur l'environnement de sécurité au sens large.

Même si le recours à une protection armée est jugé nécessaire et légitime, il peut ne pas être éthique ou pratique de payer pour ce service auprès de prestataires privés, de groupes ou d'individus. La protection assurée par les forces de police ou militaires mandatées par l'État ou la communauté internationale peut être fournie gratuitement dans certains contextes, mais ce n'est pas toujours le cas. À la suite d'expériences de racket de protection par les milices somaliennes dans les années 1990, certains travailleurs humanitaires ont fait valoir que les organisations humanitaires ne devraient jamais payer pour une protection armée. En réalité, la

63 ONU et Comité permanent interorganisations (IASC) (2008) *Civil-military guidelines & reference for complex emergencies* (en anglais, «Directives et références civiles et militaires pour les situations d'urgence complexes»). Bureau de la coordination des affaires humanitaires de l'ONU (OCHA) (<https://digitallibrary.un.org/record/697614?ln=en&v=pdf>).

plupart l'ont fait lorsqu'elles ont jugé que les circonstances l'exigeaient. Dans certains contextes, il s'agit parfois d'une obligation légale.⁶⁴

La dépendance à l'égard du soutien d'un acteur armé peut également rendre extrêmement difficile, voire impossible, toute intervention future sans ce soutien, ce qui compromet la durabilité des opérations humanitaires. Le prestataire de protection armée peut développer un intérêt financier à maintenir le service. En outre, la cessation soudaine de la protection armée peut faire d'une organisation humanitaire une cible facile.

La décision d'une organisation de recourir à une protection armée a des implications pour les autres, car elle peut influencer l'image et la perception de toutes les organisations humanitaires, et donc potentiellement affecter l'acceptation et les relations plus largement. Il s'agit d'un sujet qui mérite une réflexion et une discussion interagences structurées. Bien que généralement rares parmi les ONG, les gardes armés et/ou les escortes armées sont couramment utilisés par les agences de l'ONU opérant dans des contextes jugés à haut risque, tels que l'Afghanistan, l'Irak et le Yémen. Dans de nombreux contextes, cela a conduit à des divergences entre les positions en matière de sécurité de l'ONU et celles des acteurs humanitaires des ONG. Lors des affrontements dans la région de Gambella en Éthiopie en 2022, l'UNDSS a recommandé le recours à des escortes armées pour les livraisons humanitaires. Certaines ONG internationales ont par la suite été alarmées de découvrir que leurs équipes locales à Gambella avaient suivi cette recommandation.

Questions de contexte

Au-delà des questions de principe, d'éthique et des risques pour l'acceptation d'une organisation, une série de questions supplémentaires, spécifiques au contexte, peuvent être posées lorsqu'il s'agit de décider du recours à une protection armée.

► Quelles sont les menaces et qui sont les cibles?

Une analyse plus approfondie peut permettre de mieux comprendre l'origine de la menace, la cible et les motivations des auteurs potentiels. Il est important de faire la distinction entre les menaces liées à la sécurité du site et à la sécurité des déplacements, et les menaces qui visent spécifiquement l'organisation humanitaire (son personnel et ses biens) et, plus généralement, les populations touchées. Même lorsque la protection armée semble justifiée, elle peut ne pas constituer un moyen de dissuasion raisonnable ou peut augmenter le risque. Par exemple, si des cambrioleurs soupçonnent qu'un résident possède une arme à feu, ils peuvent devenir violents s'ils sont surpris en flagrant délit. Si des bandits de grand chemin aperçoivent un convoi armé, ils peuvent tirer avant de le dévaliser. L'identité de la cible est également un élément important à prendre en compte. Si la protection armée est assurée par les forces gouvernementales ou une faction particulière, l'organisation peut devenir une cible légitime aux yeux de l'opposition armée. Il existe également un

64 Stoddard, A., Harmer, A. et DiDomenico, V. (2008) *The use of private security providers and services in humanitarian operations* (en anglais, « Le recours à des entreprises de sécurité privée dans les opérations humanitaires »). Rapport 27 du HPG. Londres: ODI (<https://odi.org/en/publications/private-security-providers-and-services-in-humanitarian-operations-2/>).

risque d'accidents dus à des « tirs amis » ou à une mauvaise manipulation ou un dysfonctionnement des armes.

Maintenir la distinction entre l'organisation et sa protection armée

Les organisations humanitaires peuvent envisager les mesures suivantes pour se distinguer ou se distancier de la protection armée :

- Veiller à ce que les acteurs armés qui protègent les convois voyagent dans des véhicules séparés.
- Interdire les armes à l'intérieur des locaux ou des véhicules de l'organisation.
- Éviter de porter des vêtements (y compris des couleurs) qui ressemblent à ceux des forces armées.
- S'abstenir d'utiliser des moyens militaires (camions, hélicoptères, etc.) ; repeindre et refaire le marquage si cela est inévitable.
- Exclure les gardes armés des enceintes, sauf en cas d'absolue nécessité.
- N'utiliser des gardes du corps armés que pour des menaces ciblées telles que les enlèvements contre rançon ou les assassinats, en exerçant une « protection rapprochée » lorsque cela est nécessaire.

La question de savoir si ces mesures contribuent réellement à maintenir une distinction perceptible et permettent à l'organisation de conserver une partie de son image civile et non combattante dépend souvent du contexte local spécifique.

► *Qui est protégé ?*

Dans les environnements dangereux, les organisations ont tendance à réfléchir à des mesures qui renforceront leur propre sécurité. Il peut être utile d'examiner si et comment la sécurité pourrait être améliorée dans la zone de manière plus générale. Par exemple, les gardes armés dans un camp de réfugiés pourraient être déployés de manière à protéger non seulement le personnel de l'organisation, mais aussi les femmes réfugiées exposées à des risques d'agression sexuelle lorsqu'elles vont chercher de l'eau et du bois de chauffage. Un système pourrait être mis en place afin que les gardes armés de plusieurs organisations individuelles patrouillent dans le quartier et renforcent ainsi la sécurité de tous. Lorsqu'une opération de maintien de la paix de l'ONU est en cours et a pour mandat de protéger les civils, des troupes peuvent être déployées dans des zones dangereuses tant pour les travailleurs humanitaires que pour la communauté locale.

► *Qui assure la protection ?*

Il est également important de déterminer qui assure la protection armée. Les sources potentielles comprennent les acteurs militaires nationaux, la police nationale, un groupe de résistance armé, les forces de maintien de la paix ou la police de l'ONU, les milices locales, les sociétés de sécurité privée et les gardes armés directement rémunérés par l'organisation. Dans certaines circonstances, une organisation qui n'est pas opposée en principe à l'usage de la force peut estimer qu'aucun des prestataires potentiels n'est acceptable et efficace, ce qui lui laisse le choix entre opérer sans protection armée ou se retirer.

Exemples de questions à se poser lors du choix d'un prestataire de services de protection armée

- Quelle est la position politique du prestataire dans un conflit donné ? L'organisation peut-elle être perçue comme prenant parti si elle s'associe à un acteur particulier ?
- Quelle est l'image publique et la réputation du prestataire ?
- Quelle importance le prestataire accorde-t-il à l'extension de la protection à une organisation humanitaire par rapport à ses autres objectifs ? Le prestataire peut avoir d'autres objectifs (par exemple engager l'ennemi ou capturer un criminel) qui, dans les moments critiques, peuvent prendre le pas sur la sécurité de l'organisation, voire la compromettre.
- Quel est le niveau de professionnalisme du prestataire ? Les gardes sont-ils bien formés, rémunérés de manière raisonnable, équipés de matériel en bon état de fonctionnement, bien encadrés, supervisés et disciplinés ?
- Quel niveau de maîtrise du risque l'organisation a-t-elle besoin ou souhaite-t-elle exercer ? Le fait d'exercer une autorité plus directe sur les prestataires de services de protection armée permet une meilleure maîtrise du risque, mais rend également l'organisation directement responsable de leur comportement et de leurs actions.
- Quelles sont les « règles d'engagement » du prestataire en matière d'usage de la force et qui en a la responsabilité en cas d'usage de la force et de blessures ?

► Voir le chapitre 2.1 pour une analyse plus approfondie sur les entreprises de sécurité privée, y compris des questions plus détaillées sur le code de conduite.

Questions de gestion

Une question clé en matière de gestion concerne les règles d'engagement (c'est-à-dire quand la force peut être utilisée et dans quelle mesure). La règle de base est généralement que la force ne peut être utilisée que pour protéger des vies clairement menacées, et tant que la menace persiste. En d'autres termes, la force létale ne peut être utilisée qu'à des fins de défense et non, par exemple, pour tirer sur un cambrioleur, même armé, qui s'enfuit et ne constitue plus une menace immédiate. Ce qui constitue une menace immédiate pour la vie et le bien-être doit être défini de manière concrète, en imaginant différents scénarios.

Les règles d'engagement doivent également être précisées pour la protection des biens. Alors que la préférence instinctive d'une organisation peut être de ne recourir à aucune force lorsque seuls des biens sont menacés, est-il acceptable de ne rien faire alors qu'un entrepôt est vidé ou que toute la nourriture d'un convoi est volée par des acteurs armés, en particulier si des personnes ont réellement besoin de ces fournitures et en dépendent ? Les organisations doivent s'efforcer de préciser clairement à quel moment et dans quel scénario l'engagement est acceptable.

Exemple de cas : Règles d'engagement dans la pratique

Une organisation internationale a fait appel à des gardes non armés d'une entreprise de sécurité privée en République démocratique du Congo et au Soudan du Sud. Cette entreprise dispose également d'une unité de réponse armée composée soit de ses propres gardes armés, soit d'un policier armé intégré. Bien que l'organisation utilise principalement des gardes non armés, les discussions avec l'entreprise de sécurité privée ont également porté sur des questions clés, notamment les règles d'engagement en cas de mobilisation de cette unité de réponse armée.

Un autre aspect important de la gestion consiste à convenir de procédures et d'approches pour un certain nombre de scénarios possibles, notamment ce qu'il faut faire lorsqu'un visiteur refuse d'être fouillé ou insiste pour faire venir ses propres gardes armés, et jusqu'où aller dans la poursuite de voleurs ou d'agresseurs en fuite.

Dans les cas où une protection armée est demandée, il peut être nécessaire de parvenir à un accord sur :

- Qui fournit les armes (il s'agit généralement du fournisseur de personnel).
- Quel type d'armes les gardes utiliseront (par exemple, pistolets, fusils à un coup ou mitrailleuses).
- Qui est chargé de fournir les munitions et de vérifier que les armes sont bien entretenues et correctement enregistrées.
- Qui est responsable de fournir l'équipement supplémentaire, tel que les vêtements et les lampes torches pour les gardes.
- Quels véhicules, le cas échéant, les gardes armés peuvent-ils utiliser ? Les gardes armés ne disposent pas toujours de véhicules et il peut être nécessaire de décider s'ils peuvent utiliser ceux de l'organisation et à quel moment.

Le commandement et la maîtrise du risque fonctionnent dans les deux sens : si une organisation se place sous la protection d'un acteur armé, on peut s'attendre à ce qu'elle se conforme aux règles de cet acteur armé. Par exemple, quitter soudainement un convoi, rouler à vive allure ou prendre la fuite peut ne pas être accepté par le prestataire de services de sécurité.

Au sein d'une force multinationale de maintien de la paix, les différentes armées nationales ont tendance à avoir des traditions et des cultures différentes, notamment en matière de commandement et de maîtrise du risque, de règles d'engagement et de ce qui est considéré comme un usage approprié ou excessif de la force. Des consultations approfondies avec les commandants à différents niveaux peuvent être nécessaires pour garantir une compréhension commune. Les commandants peuvent avoir des points de vue différents, et il peut être utile de conclure un accord écrit détaillé avec un commandant supérieur afin de gérer les relations entre les différents niveaux. Il est conseillé de suivre les changements afin de s'assurer que les remplaçants sont bien informés.

► *Pour en savoir plus sur la coordination civilo-militaire, voir le chapitre 2.1.*

Synthèse des questions de gestion clés

Les questions de gestion clés à prendre en compte sont les suivantes :

- Les politiques, procédures et compétences de gestion nécessaires pour gérer cette relation sont-elles disponibles au sein de l'organisation et sur le site en question ?
- Quelles sont les clauses contractuelles nécessaires ?
- Qui exerce le commandement et la maîtrise du risque, et qui a l'autorité et la responsabilité de quoi ?
- Qui, au sein de l'organisation humanitaire, prend la décision/approuve le recours à une protection armée ?

- Les gardes armés seront-ils toujours présents ou seulement à certains moments ou à certains endroits?
- Comment les appels d'offres sont-ils rédigés et les offres des entreprises de sécurité privée évaluées?
- Quelles vérifications peuvent être effectuées concernant le professionnalisme et l'intégrité d'un prestataire de services potentiel?
- À qui les gardes doivent-ils rendre des comptes, qui détient l'autorité de commandement et qui est responsable de la discipline?
- Lorsque des forces de sécurité externes assurent une protection armée, quelle est l'autorité de leur commandant par rapport à celle de l'organisation?
- Qui détermine les règles régissant le recours à la force létale et qui s'assure que les gardes les ont bien comprises?

Politique

Les organisations ont tout intérêt à se doter d'une politique sur le recours à la protection armée à l'échelle de l'organisation. Les points importants à prendre en compte sont les suivants:

- Clarification de la position de l'organisation concernant le recours à la protection armée en principe.
- Les conditions qui pourraient justifier le recours à la protection armée, par exemple lors de l'évacuation ou de la réinstallation du personnel en période d'insécurité extrême (cela peut inclure des références à la criticité des programmes et aux conséquences du recours à la protection armée).
- Quelles alternatives ont été envisagées pour faire face aux risques, et si la protection armée est vraiment le dernier recours.
- Les principaux éléments et risques à prendre en considération (juridiques, réputationnels et physiques), tant pour l'organisation concernée que pour les autres, lors du choix des prestataires potentiels, et la manière dont ils doivent être évalués.
- Les conditions qui doivent être convenues entre l'organisation et le prestataire.
- La procédure organisationnelle pour la prise de décision et le bilan périodique.

- L'obligation d'accompagner le recours à la protection armée d'efforts de communication accrus pour expliquer sa raison d'être, c'est-à-dire la manière dont elle peut soutenir d'autres approches en matière de sécurité, en particulier l'acceptation.

Politique possible

Selon la politique d'une organisation, une protection armée peut être envisagée quand :

- un grand nombre de vies sont à risque ;
- la menace est liée à un banditisme généralisé et non à des raisons politiques ;
- le prestataire répond aux normes applicables ;
- la dissuasion peut être efficace ; et
- le recours à la protection armée est autorisé au niveau organisationnel approprié.

Une politique de protection armée n'est pas la même chose qu'une politique relative aux sociétés de sécurité privée, même si ces dernières sont souvent les prestataires de services de la protection armée. Une organisation peut faire appel à des sociétés de sécurité privée à d'autres fins (par exemple, pour des évaluations des risques ou des audits de sécurité) et d'autres types d'acteurs peuvent également fournir une protection armée. Le recours à l'un ou l'autre doit être guidé par une politique établie.

► Pour en savoir plus sur les entreprises de sécurité privée, voir le chapitre 2.1.

Informations complémentaires

Recherche et analyse

Al Achkar, Z. (2021) 'Digital risk: How new technologies impact acceptance and raise new challenges for NGOs' (en anglais, «Risques numériques: comment les nouvelles technologies influencent l'acceptation et posent de nouveaux défis aux ONG») sur le site du GISF (éd.) *Achieving safe operations through acceptance: challenges and opportunities for security risk management* (en anglais, « Assurer la sécurité des opérations grâce à l'acceptation: défis et opportunités pour la gestion des risques de sécurité») (<https://gisf.ngo/resource/achieving-safe-operations-through-acceptance/>).

Bamber-Zyrd, M. (2023) 'ICRC engagement with armed groups in 2023' *Humanitarian Law & Policy* (en anglais, « L'engagement du CICR auprès des groupes armés en 2023 », *Droit humanitaire et politique*), CICR (<https://blogs.icrc.org/law-and-policy/2023/10/10/icrc-engagement-with-armed-groups-in-2023/>).

Daudin, P. (2021) 'Acceptance under stress: old recipes for new problems' (en anglais, « L'acceptation sous pression : vieilles recettes pour de nouveaux problèmes ») sur le site du GISF (éd.) *Achieving safe operations through acceptance: challenges and opportunities for security risk management* (en anglais, « Assurer la sécurité des opérations grâce à l'acceptation : défis et opportunités pour la gestion des risques de sécurité ») (<https://gisf.ngo/resource/achieving-safe-operations-through-acceptance/>).

GISF (2021) *Achieving safe operations through acceptance* (en anglais, *Assurer la sécurité des opérations grâce à l'acceptation*) (<https://gisf.ngo/resource/achieving-safe-operations-through-acceptance/>).

Stoddard, A., Harmer, A. et DiDomenico, V. (2008) *The use of private security providers and services in humanitarian operations* (en anglais, « Le recours à des entreprises de sécurité privée dans les opérations humanitaires »). Rapport 27 du HPG. Londres: ODI (<https://odi.org/en/publications/private-security-providers-and-services-in-humanitarian-operations-2/>).

Williams, C., Kinch, P. et Herman, L. (2021) 'Promoting a blended risk management approach: the place of programming and diversity within a SRM strategy' (en anglais, « Promouvoir une approche mixte de gestion de risque : la place de la programmation et de la diversité dans une stratégie GRS ») sur le site du GISF (éd.) *Achieving safe operations through acceptance: challenges and opportunities for security risk management* (en anglais, « Assurer la sécurité des opérations grâce à l'acceptation : défis et opportunités pour la gestion des risques de sécurité ») (<https://gisf.ngo/resource/achieving-safe-operations-through-acceptance/>).

Recommandations et ressources

Fast, L. et al. (2011) *The acceptance toolkit: a practical guide to understanding, assessing, and strengthening your organization's acceptance approach to NGO security management* (en anglais, « Le kit d'acceptation : un guide pratique pour comprendre, évaluer et renforcer l'approche par acceptation de votre organisation en matière de gestion de la sécurité des ONG »). Save the Children Federation (<https://acceptanceresearch.wordpress.com/acceptance-toolkit/>).

GISF (n.d.) 'Acceptance analysis template - xlsx' (en anglais, « Modèle d'analyse d'acceptation - xlsx »). 2. *Stratégie d'acceptation*. Guide interfonctionnel sur la sécurité des ONG (<https://gisf.ngo/toolbox-pwa-fr/resource/2-strategie-dacceptation/>).

ONU et Comité permanent interorganisations (IASC) (2008) *Civil-military guidelines & reference for complex emergencies* (en anglais, « Directives et références civiles et militaires pour les situations d'urgence complexes »). Bureau de la coordination des affaires humanitaires de l'ONU (OCHA) (<https://digitallibrary.un.org/record/697614?ln=en&v=pdf>).

4.3 Plans et dispositions de sécurité

Une fois qu'une organisation a identifié et évalué les risques, elle peut élaborer des plans pour les gérer. Un plan de sécurité consiste à documenter ces risques ainsi que les mesures d'atténuation correspondantes. Ce chapitre recense les bonnes pratiques en matière d'élaboration de plans de sécurité, en mettant l'accent sur deux éléments majeurs : les procédures opérationnelles standards (comment l'organisation atténuera les menaces identifiées dans l'évaluation des risques) et les dispositifs d'urgence (comment l'organisation réagira aux événements et situations perturbateurs et potentiellement à haut risque).

4.3.1 Plans de sécurité

Le plan de sécurité sert de base à la gestion des risques de sécurité au niveau de la mise en œuvre du programme. En fonction du contexte et des risques, un plan de sécurité peut s'appliquer à l'ensemble d'un pays, à une zone géographique spécifique ou même, parfois, à un projet individuel.

Il est préférable que le processus de planification soit inclusif – en impliquant un groupe diversifié de collaborateurs ayant des rôles, des parcours et des profils personnels différents – plutôt qu'individuel, car cela permet de tirer parti des connaissances et de l'expérience collectives et favorise une large appropriation du produit final. Une bonne pratique en matière de planification consiste également à effectuer des révisions périodiques afin d'adapter le plan à l'évolution de l'environnement.

Éléments d'un plan de sécurité

Les plans de sécurité varient d'une organisation à l'autre, reflétant les besoins et les politiques spécifiques de chaque organisation ainsi que le contexte. Les principaux éléments d'un plan de sécurité peuvent être les suivants (adapté de l'European Interagency Security Forum (aujourd'hui GISF) *Gestion du risque sécurité: manuel de référence à l'attention des petites ONG*):⁶⁵

- 1. Résumé des informations essentielles.** Un résumé d'une page contenant les informations essentielles pour une consultation rapide, notamment les numéros d'urgence et les procédures ou règles importantes, telles que les horaires de couvre-feu ou d'appel.
- 2. Aperçu.** L'objectif et la portée du plan, la partie responsable, une déclaration de la mission et de la politique de sécurité de l'organisation (y compris l'appétence au risque et le seuil), ainsi que les dates de création, de dernière révision et de prochaine révision du plan.

⁶⁵ Bickley, S. (2017) *Gestion du risque sécurité: manuel de référence à l'attention des petites ONG*. European Interagency Security Forum (EISF) (<https://gisf.ngo/resource/security-risk-management-a-basic-guide-for-smaller-ngos/>).

3. **Contexte actuel et évaluation des risques.** Un résumé de l'environnement opérationnel dans un laps de temps défini, y compris, le cas échéant, la dynamique des conflits, ainsi que les menaces, les risques et les niveaux de risque identifiés.
4. **Niveaux de sécurité.** Phases basées sur les indicateurs de risque et les actions requises.
5. **Rôles et responsabilités.** Les noms des personnes et les postes responsables de la gestion des risques de sécurité.
6. **Procédures opérationnelles standards.** Des procédures de sécurité claires et concises pour la prévention et la réponse, basées sur les risques évalués et couvrant des domaines clés tels que la gestion des espèces, les communications, la sécurité du site, la santé et la sûreté, la sécurité de l'information, la conduite personnelle, la sécurité des déplacements et la sécurité des véhicules.
7. **Mesures de santé et de sûreté.** Des procédures opérationnelles standards spécifiques et autres mesures visant à protéger le personnel contre les menaces en matière de santé, les accidents et le stress.
8. **Ressources humaines.** Résumés des politiques de recrutement, de vérification des antécédents, de contrats, de confidentialité, d'intégration et d'évaluation des risques liés aux fonctions.
9. **Briefings sur la sécurité.** Une liste des sujets abordés et des informations fournies aux nouveaux employés/visiteurs, ainsi que des exigences/attentes en matière de formation.
10. **Signalement des incidents.** Définitions, procédures, responsabilités, structure et format du signalement.
11. **Gestion de crise et plans d'urgence.** Structure de gestion de crise, plans, équipes et règles d'activation en cas de crise et d'incidents critiques, ainsi que plans d'urgence pour la relocalisation, l'hibernation, l'évacuation, les catastrophes et les urgences médicales, par exemple.
12. **Annexes.** Documents d'appui et modèles, notamment des cartes de l'environnement opérationnel, des listes de contacts, des listes de contrôle et des formulaires.

Les plans de sécurité doivent tenir compte d'un certain nombre d'éléments :

- Le fait de partager les plans dans des formats accessibles appropriés et de les expliquer clairement au personnel contribuera à garantir leur mise en œuvre réussie.
- Les membres du personnel qui comprennent la raison d'être des procédures sont plus enclins à les respecter. L'élaboration collective du plan avec un large éventail de membres du personnel augmente les chances d'adhésion.
- Il est recommandé de revoir les plans à mesure que les conditions changent et que des événements se produisent, quelle que soit la date prévue pour la prochaine révision.
- La mise en œuvre de certains aspects du plan peut nécessiter des connaissances ou des compétences spécialisées.
- Une gestion des risques de sécurité efficace dépend de la pratique, à travers des simulations et des formations.

Révision et mise à jour des plans de sécurité

Même dans un environnement stable et sûr, les plans de sécurité doivent être revus chaque année. Dans les environnements à haut risque, il est recommandé de procéder à des révisions plus fréquentes afin de s'assurer que le plan reflète les risques actuels et que les informations sont à jour. Exemples de déclencheurs de révision :

- Lorsque des changements significatifs surviennent dans le contexte externe, notamment à la suite d'actions menées par des acteurs majeurs dans la région.
- Lorsque des changements significatifs surviennent au sein de l'organisation, par exemple au niveau de l'approche opérationnelle, du personnel ou des relations avec les acteurs clés.
- Lorsque l'organisation, ou une autre organisation opérant dans la même zone opérationnelle ou à proximité, est victime d'un incident de sécurité.

Les sections suivantes abordent deux des principaux éléments d'un plan de sécurité : les procédures opérationnelles standards et les plans d'urgence. D'autres sections d'un plan de sécurité, telles que l'évaluation des risques et la gestion de crise, sont traitées plus en détail dans d'autres chapitres du présent recueil de bonnes pratiques.

- *Pour en savoir plus sur l'évaluation des risques, voir le chapitre 4.1.*
- *Pour en savoir plus sur la réponse aux incidents et la gestion de crise, voir le chapitre 4.4.*

4.3.2 Procédures opérationnelles standards

Les procédures opérationnelles standards fournissent des instructions détaillées sur la manière d'exécuter les tâches ou les processus spécifiques nécessaires à la mise en œuvre du plan de sécurité. Il s'agit essentiellement des instructions opérationnelles permettant d'atténuer chacun des risques évalués.

Les bonnes pratiques recommandent de disposer de procédures opérationnelles standards distinctes, rédigées de préférence dans un langage clair et simple, couvrant tous les domaines des opérations quotidiennes où des risques ont été identifiés. Les procédures opérationnelles standards peuvent couvrir un large éventail d'activités, des routines quotidiennes aux procédures de réponse d'urgence, et être adaptées pour répondre aux risques et défis spécifiques présents dans l'environnement opérationnel. Par exemple, dans les zones où les déplacements routiers comportent des risques de sécurité, une organisation mettra généralement en place des procédures opérationnelles standards concernant l'évaluation de la sécurité des itinéraires prévus, les autorisations de déplacement, les contrôles de sûreté des véhicules, les vérifications à intervalles réguliers, les limitations de vitesse et le comportement aux points de contrôle.

Les procédures opérationnelles standards doivent idéalement être rédigées dans un langage clair et concis, en évitant le jargon technique, les acronymes et les abréviations. Les éléments clés d'une procédure opérationnelle standard sont les suivants :

- **Titre/en-tête** - indiquant clairement le nom de la procédure et comprenant le numéro et la version du document.
- **Objectif** - une brève explication de l'intention et des objectifs de la procédure opérationnelle standard.
- **Champ d'application** - définition de ce que couvre la procédure opérationnelle standard et à qui elle s'applique.
- **Responsabilités** - description des rôles et responsabilités des personnes impliquées dans la mise en œuvre de la procédure.
- **Définitions** - clarification des termes ou références qui peuvent être peu connus.
- **Procédure** - instructions étape par étape pour le personnel chargé d'effectuer la tâche ou le processus (partie principale de la procédure opérationnelle standard).
- **Contrôle qualité** - précisant les contrôles de qualité ou les inspections requis.
- **Signature(s) d'approbation/de l'auteur.**
- **Historique des révisions** - enregistrement des modifications apportées à la procédure opérationnelle standard au fil du temps.
- **Annexes** - tout document, formulaire ou liste de contrôle supplémentaire.

Disposer de procédures opérationnelles standards bien développées permettra d'assurer la cohérence et de réduire les erreurs humaines. Lorsqu'une organisation définit quelque chose comme une procédure opérationnelle standard, il s'agit plutôt d'une exigence que d'une recommandation ou d'un conseil. Ces termes étant parfois confondus ou utilisés de manière interchangeable, il est utile que l'organisation précise clairement à son personnel le niveau de conformité attendu. Cependant, le terme « standard » signifie « dans la plupart des cas la plupart du temps », et non pas qu'il doit nécessairement prévaloir sur le jugement professionnel ou la réflexion critique dans des circonstances exceptionnelles. Idéalement, le personnel évaluera la situation et sera en mesure de s'écarter des procédures opérationnelles standards lorsque cela est nécessaire pour des raisons de sécurité ou pour atteindre des objectifs critiques, en documentant et en justifiant tout écart de ce type.

► *Pour obtenir des informations utiles pouvant guider l'élaboration de procédures opérationnelles standards spécifiques, voir la partie 7, qui traite des activités organisationnelles spécifiques et des risques associés, ainsi que des types particuliers de menaces.*

4.3.3 Plans d'urgence et de continuité

Plans d'urgence

Les plans d'urgence aident une organisation à gérer les événements et situations à haut risque anticipés là où les opérations normales sont perturbées ou deviennent intenables.

Les questions clés pour guider l'élaboration des plans d'urgence sont les suivantes :

- Que pourrait-il se passer ?
- Qui pourrait être touché ?
- Que faut-il pour répondre ?
- Qui doit être informé ?
- Qui prend quelles décisions ?
- Que peut-on faire pour être mieux préparé ?

Les plans d'urgence et les plans de gestion de crise sont des concepts liés mais distincts de la préparation organisationnelle. Les crises exigent une réponse organisationnelle qui dépasse les structures de gestion normales. Toutes les situations d'urgence ne constituent pas nécessairement des crises ; par exemple, certaines perturbations, comme l'hibernation, peuvent être gérées dans le cadre opérationnel normal sans nécessiter de gestion de crise. Le plan d'urgence consiste à se préparer à d'éventuelles perturbations, et la gestion efficace de ces perturbations peut nécessiter une gestion de crise.

► Pour plus d'informations sur la gestion de crise, voir le chapitre 4.4.

Dans la gestion des risques de sécurité, les plans d'urgence se concentrent généralement sur les situations où l'insécurité a augmenté soudainement ou de manière spectaculaire, nécessitant de prendre des décisions quant à la poursuite ou non de la programmation et à la manière de la mener à bien. Dans ce cas, une organisation peut être confrontée aux options d'hibernation, de relocalisation ou d'évacuation (dans le cas des organisations internationales) et peut les aborder comme des phases progressives et croissantes à mesure que les conditions de sécurité se détériorent. Le plan d'urgence peut comprendre des déclencheurs spécifiques pour chaque phase, ou être un processus au cas par cas. Les bonnes pratiques recommandent de définir des critères objectifs pour orienter la décision, afin de contourner la tendance naturelle à retarder les décisions difficiles.

L'hibernation est souvent la première mesure prise lorsque les circonstances indiquent une insécurité accrue. Si la situation s'aggrave, il peut être conseillé de déplacer le personnel dans un endroit plus sûr. Dans des circonstances extrêmes, les organisations internationales peuvent décider de retirer tout ou partie de leur personnel (généralement des ressortissants étrangers) du pays, tout en apportant leur soutien aux membres du personnel qui ne sont pas évacués. Les organisations nationales ne sont généralement pas en mesure d'évacuer leur personnel et doivent alors recourir au travail à distance, à la réinstallation dans des zones plus sûres ou à la suspension de leurs activités jusqu'à ce que la situation redevienne sûre. Une évaluation des risques doit être effectuée avant de retourner sur les lieux et de reprendre les activités.

Hibernation

L'hibernation consiste à interrompre les déplacements du personnel et les programmes dans un lieu donné en demandant au personnel de rester chez lui ou de se réfugier dans un bureau ou un autre bâtiment de l'organisation. Cela peut être dû au fait qu'il est impossible de quitter la zone ou que c'est trop dangereux, ou parce que la situation devrait s'améliorer dans un avenir proche. L'hibernation peut être une bonne solution lorsqu'il est plus sûr de rester sur place que de se déplacer, ou lors de périodes temporaires de risque accru, comme à l'approche d'élections. La connexion Internet a permis à certains employés de travailler à domicile, élargissant ainsi la définition traditionnelle de l'hibernation. La pandémie de Covid-19 a démontré la viabilité du travail à distance pendant de longues périodes pour les employés dont les fonctions ne nécessitent pas une présence physique. En Afghanistan, après le retour au pouvoir des talibans en 2021 et l'interdiction faite aux femmes afghanes de travailler pour des organisations humanitaires, des accords tacites de «travail à domicile» ont permis à certaines organisations de maintenir l'emploi de nombreux membres de leur personnel pendant qu'elles tentaient de négocier des dérogations ou de s'opposer à l'interdiction.

Il est avantageux pour les organisations d'identifier un lieu de retraite ou d'hibernation (et, si possible, plusieurs) et de les équiper des éléments suivants en vue d'éventuels séjours prolongés:

- nourriture, eau, trousse de premiers secours et médicaments essentiels ;
- installations pour dormir, se laver, aller aux toilettes et assurer la circulation de l'air ;
- éclairage, sources d'énergie et chargeurs ;
- combustible et équipement pour cuisiner ;
- équipements de communication ;
- livres, jeux, vidéos ou autres articles de divertissement ; et
- équipement d'exercice et espace d'entraînement et de loisirs.

En cas de risque de bombardements ou d'attaques à l'artillerie, les organisations peuvent être amenées à aménager des abris sécurisés ou des bunkers, ou à identifier les abris situés à proximité.

► *Pour plus de détails sur les abris sécurisés et les abris, voir le chapitre 7.10 - Menaces liées aux combats et aux vestiges de guerre et le Chapitre 7.2 - Sécurité du site.*

Évacuation et relocalisation

L'évacuation ou la relocalisation désigne le retrait physique du personnel (et, lorsque cela est possible et prévu, de leurs familles) et des biens d'un environnement dangereux. L'évacuation désigne généralement le déplacement au-delà d'une

frontière internationale, tandis que la relocalisation désigne le déplacement à l'intérieur d'un pays. Cela peut être précipité par un conflit ou des événements extrêmement dangereux, mais cela peut également être imposé, dans le cas d'une expulsion par le gouvernement. Dans certaines circonstances, il peut être prudent de prévoir un retrait temporaire et préventif, par exemple en retirant le personnel de certains endroits à l'approche d'événements politiques potentiellement explosifs.

Il est important d'être conscient de quatre hypothèses courantes mais souvent trompeuses concernant l'évacuation et la relocalisation :

- **La détérioration sera progressive** - gardez à l'esprit que les événements peuvent prendre le pas sur les plans. La planification progressive des niveaux de sécurité, bien qu'utile, peut donner l'impression d'une progression linéaire, alors que ce n'est pas toujours le cas.
- **L'évacuation et la relocalisation se dérouleront exactement comme prévu** - le personnel ne se réfère souvent pas au plan en cas de crise soudaine et aiguë, des éléments importants peuvent avoir été négligés et non prévus, certains membres du personnel peuvent refuser de partir et des facteurs externes peuvent prendre le pas sur les plans initiaux et forcer les résultats.
- **Le départ sera possible** - dans de nombreuses situations, les voies d'évacuation peuvent être bloquées, les capacités logistiques pour l'évacuation peuvent être insuffisantes, ou il peut tout simplement être trop dangereux de partir et le personnel devra rester sur place et faire face à la crise.
- **Le retour sera possible** - le personnel évacué et relocalisé peut ne pas être en mesure de revenir rapidement et l'organisation peut se retrouver retirée du contexte ou à gérer des programmes à distance pendant des semaines, des mois, voire des années.

La décision de se retirer

La relocalisation - et en particulier l'évacuation - est une décision difficile à prendre, tant d'un point de vue moral qu'opérationnel. Dans presque tous les cas, partir aura des conséquences négatives pour la population servie, tandis que rester peut offrir une certaine protection à une population en danger, ou au moins une présence témoin.

La décision peut également être influencée par la pression des donateurs ou la crainte d'une perte de financement à l'avenir, par des désaccords au sein du personnel quant à la gravité du risque, par des liens familiaux dans la zone et par la crainte de perdre l'acceptation et la confiance de la communauté locale.

Le plan d'urgence devra indiquer clairement qui est habilité à prendre les décisions relatives à l'hibernation, à la relocalisation et à l'évacuation, et ce qu'il faut faire en cas de divergences d'opinions.

Considérations interorganisations

En cas de crise grave, les relocalisations (et surtout les évacuations) nécessitent généralement une collaboration interorganisations. Cela peut être compliqué par des appréciations différentes du risque. Le fait que certaines organisations partent tandis que d'autres restent peut accroître la vulnérabilité de celles qui restent sur place. Il se peut qu'il n'y ait plus de masse critique d'organisations présentes, ce qui peut encourager le pillage, le vol et les attaques. En outre, il n'est ni plausible ni pratique pour une organisation de compter sur une entité externe telle que l'ONU ou un gouvernement étranger pour l'aider à l'évacuation ou à la relocalisation. Il est conseillé aux organisations de se préparer à gérer ce type de situation de manière indépendante.

Planifier et gérer le retrait du personnel

La politique organisationnelle de relocalisation et d'évacuation doit être documentée et communiquée clairement au personnel et aux partenaires au préalable, dans le cadre du devoir de diligence. Si les attentes du personnel diffèrent de la politique, les conséquences pour les membres du personnel et le moral général pourraient être désastreuses. Dans la mesure du possible, les droits et responsabilités des employeurs et des employés en cas d'évacuation et de relocalisation doivent être définis dans les contrats de travail ou dans la politique de sécurité, y compris les dispositions que l'organisation prendra pour les membres de la famille résidant dans le pays. Les directives peuvent stipuler, par exemple, qu'en cas de risque de sécurité accru, le personnel qui ne participe pas à des activités essentielles au programme sera relocalisé ou évacué de la zone.

Pour les membres du personnel qui sont des ressortissants du pays, il convient de préciser clairement quels sont leurs droits et ceux des personnes à leur charge en matière de relocalisation (à l'intérieur du pays) et d'évacuation (à l'étranger). Si ces questions sont abordées lors du processus de planification d'urgence, ces membres du personnel peuvent évaluer leurs options à l'avance afin d'optimiser leur propre sécurité et celle des personnes à leur charge. Il est peu probable que les organisations internationales soient en mesure d'évacuer un grand nombre de membres du personnel nationaux au-delà des frontières internationales, mais pour les membres du personnel qui sont exposés à des risques particulièrement élevés, l'organisation a sans doute la responsabilité éthique de les aider, par exemple en recourant à des instruments juridiques internationaux et à des procédures nationales d'asile. Le soutien au personnel qui reste peut prendre la forme d'une avance sur salaire de quelques mois, de téléphones portables, de cartes téléphoniques prépayées, d'un accès aux bâtiments de l'organisation pour eux-mêmes et leur famille, ou encore de lettres d'emploi ou de référence.

Dans certaines circonstances, il peut être approprié que seule une partie de l'équipe se retire. La relocalisation préventive de certains membres du personnel en période de tension croissante, ou dans le cadre de la procédure associée à une phase de sécurité spécifique, peut réduire la vulnérabilité globale en diminuant le nombre de personnes exposées au risque et en facilitant la gestion d'une éventuelle relocalisation ou évacuation d'urgence à l'avenir.

Le personnel susceptible d'être relocalisé dans ces scénarios peut inclure toute personne dont le rôle n'est pas essentiel à la poursuite du programme. Les organisations peuvent également envisager de retirer les membres du personnel exposés à un risque particulièrement élevé, qu'ils occupent ou non des postes essentiels au programme. Par exemple, certaines nationalités ou certains groupes ethniques ou religieux peuvent constituer une cible potentielle.

Un membre du personnel peut avoir des difficultés psychologiques à faire face à l'insécurité croissante ou se percevoir comme étant exposé à un risque élevé. Étant donné qu'un niveau de stress ingérable peut nuire à la prise de décision, il est conseillé de retirer la personne concernée, même si elle occupe un poste opérationnel clé.

Lorsque les organisations internationales évacuent leur personnel étranger et suspendent leur programmation, les organisations locales peuvent être confrontées à des défis, des risques et des responsabilités accrus. Voici quelques éléments à prendre en compte.

- **Risques de sécurité accrus.** Les suspensions, évacuations ou relocalisations décidées par les organisations internationales peuvent modifier la dynamique locale et exposer les organisations locales à des menaces plus importantes. Il est donc conseillé à ces organisations de réévaluer leurs risques et leurs stratégies d'atténuation dans ces moments-là.
- **Continuité opérationnelle.** Les organisations locales peuvent être amenées à s'adapter rapidement pour combler les lacunes laissées par le départ de leurs homologues internationales. Cela peut impliquer d'assumer des responsabilités supplémentaires dans le cadre du programme ou des rôles de direction pour maintenir les services essentiels.
- **Contraintes de ressources.** L'évacuation des ressortissants étrangers peut souvent coïncider avec une réduction du financement et du soutien matériel. Les organisations locales peuvent être amenées à communiquer de manière proactive avec les donateurs au sujet de leurs besoins financiers continus et à explorer d'autres sources de financement.
- **Opportunités de partenariat.** À l'inverse, comme les organisations internationales peuvent se trouver dans l'incapacité de poursuivre leurs programmes en raison d'un manque de personnel, elles peuvent se tourner vers des organisations locales pour poursuivre leurs projets. Ces organisations devront évaluer ces nouvelles opportunités par rapport aux risques potentiels, tels que des menaces de sécurité accrues ou différentes, des exigences de conformité supplémentaires, ainsi que la pression supplémentaire exercée sur les capacités du personnel dans des environnements déjà soumis à des menaces accrues.
- **Bien-être et soutien du personnel.** Le personnel peut ressentir une peur, un stress et une anxiété accrus à la suite de l'évacuation et de la relocalisation d'autres organisations. Les organisations peuvent contribuer au bien-être de leurs employés en leur offrant un soutien psychosocial, une communication claire et, si possible, des conditions de travail flexibles.

Se préparer à être expulsé par le gouvernement – un cas particulier

Dans le cas d'une expulsion par le gouvernement, la plupart des préparatifs seront similaires à ceux d'une évacuation en réponse à une situation d'insécurité. Cependant, les organisations peuvent également envisager les points suivants :

- L'organisation va-t-elle faire appel de la décision et, si oui, par quels moyens (voie judiciaire, discussions directes avec les autorités, plaidoyer ou lobbying dans le cadre d'un consortium, campagnes médiatiques, discussions avec les donateurs ou les ambassades) ?
- Quelles mesures ont été prises pour protéger les informations potentiellement sensibles, confidentielles ou personnelles contre toute divulgation involontaire ?
- L'expulsion va-t-elle exposer le personnel restant dans le pays à un risque particulier ?
- Des mesures peuvent-elles être prises pour empêcher que le personnel (en particulier celui qui reste) ne soit harcelé ou menacé par les autorités gouvernementales ?
- Le personnel restant percevra-t-il un salaire ou une indemnité de licenciement, et pendant combien de temps ? (Cela peut être exigé par le gouvernement.)
- Le risque que les biens soient définitivement saisis peut-il être minimisé ?
- Quel rôle les donateurs gouvernementaux ou d'autres acteurs (tels que l'ONU) pourraient-ils jouer pour faire annuler la décision ou demander aux autorités nationales un traitement plus clément ?
- Quelle sera la réaction des médias (au niveau local et international) et comment sera-t-elle reçue ?

Planifier et effectuer une évacuation ou une relocalisation

Les organisations ont tout intérêt à revoir régulièrement les plans d'évacuation et de relocalisation avec le personnel, surtout s'il devient de plus en plus probable qu'un retrait sera nécessaire. Cela peut se faire au moyen d'exercices de simulation ou d'une réunion d'équipe pour examiner les politiques, les procédures et les plans.

Logistique et planification de l'itinéraire

Lorsqu'elles planifient un itinéraire d'évacuation ou de relocalisation, les organisations peuvent tenir compte des éléments suivants :

- Quels itinéraires et moyens de transport sont les plus envisageables dans différents scénarios ? Il est recommandé de planifier à l'avance des itinéraires détaillés, y compris des itinéraires alternatifs.

- Qu'est-ce qui est le plus susceptible de réduire les risques: se déplacer de manière visible avec des logos et d'autres marques identifiables, ou de manière discrète en supprimant tous ces éléments?
- Quels sont les moyens de transport disponibles et pour combien de personnes? Quels types de biens ou d'effets personnels peuvent être emportés?
- Quel est le mode de transport le plus approprié et convient-il à l'ensemble du personnel? Par exemple, les membres du personnel à mobilité réduite peuvent ne pas être en mesure de parcourir de longues distances à pied.
- Existe-t-il des logements ou des campings sûrs le long du trajet si les itinéraires deviennent dangereux?
- Les communications fonctionneront-elles à tous les points de l'itinéraire, et à quels points le personnel doit-il prendre contact avec ses collègues?
- Qui assurera le transport? Si ce n'est pas l'organisation elle-même, il est important de comprendre la capacité, les exigences procédurales et les limites de la responsabilité et de l'obligation de l'entité chargée du transport.
- La relocalisation ou l'évacuation se fera-t-elle en collaboration avec d'autres organisations? Bien qu'il puisse être plus sûr de voyager en convoi avec d'autres organisations, cela peut également signifier moins de maîtrise du risque sur la manière dont le départ est effectué. Il peut être utile pour les organisations de discuter au préalable de la manière dont ces questions seront traitées.

Préparations

Les plans doivent viser à identifier les sites qui serviront de points de rassemblement, où le personnel devra se réunir avant le départ. Les points de rassemblement doivent être accessibles, sécurisés, suffisamment grands pour accueillir un grand nombre de personnes et plusieurs véhicules, et disposer de moyens de communication fiables et de stocks d'urgence.

Des informations précises et régulièrement mises à jour sur le nombre d'employés (et de personnes à leur charge) pouvant bénéficier d'une évacuation internationale doivent être disponibles. D'une manière générale, il est utile de disposer d'informations clés sur tous les membres du personnel susceptibles de partir, y compris sur leurs besoins particuliers, tels que des besoins médicaux, ou si certains d'entre eux voyagent avec de jeunes enfants. Les personnes qui partent devront se munir des documents personnels nécessaires pour faciliter leur voyage. Le stockage électronique des documents essentiels de l'organisation (en particulier dans le cloud) peut contribuer à prévenir leur perte et à faciliter leur accès par le personnel situé en dehors de la zone de relocalisation/évacuation.

- *Pour en savoir plus sur la protection des informations sensibles, voir le chapitre 6.1.*

Fermeture de bureau

Lorsqu'elles élaborent des plans d'urgence en cas de fermeture de bureau pour cause d'urgence, les organisations peuvent souhaiter prendre en compte à la fois la gestion des biens et le respect de la législation. Il est conseillé d'identifier les biens susceptibles d'être sécurisés ou transférés, en veillant à ce que les cessions soient conformes aux exigences des donateurs, de l'organisation et des autorités locales. Il convient également d'anticiper les obligations juridiques envers les propriétaires, les fournisseurs et les autorités afin d'éviter tout retard ou litige. Les risques de sécurité associés aux transferts de biens aux partenaires ou aux communautés locales doivent être évalués. Les plans d'urgence peuvent également inclure la sécurisation des biens clés tels que les véhicules et les équipements de communication, qui peuvent être déplacés ou mis hors service pour éviter toute utilisation abusive. Le personnel peut souhaiter détruire les informations sensibles avant son départ.⁶⁶

Destination

Lorsqu'elles choisissent une destination pour leurs nouveaux employés qui ne résident pas dans cette zone, les organisations doivent s'assurer que le lieu offre un niveau de sûreté et de confort adéquat et un accès aux services essentiels. Le logement choisi, tel qu'un hôtel, doit être sûr et capable de répondre à tous les besoins médicaux, alimentaires ou de communication.

Après l'évacuation ou la relocalisation

Un certain nombre de mesures immédiates et pratiques peuvent être prises après une relocalisation ou une évacuation :

- À la première occasion, contacter les dirigeants de l'organisation pour faire le point sur la situation.
- Si l'évacuation a été internationale, contacter les autorités du pays d'arrivée (si cela n'a pas déjà été fait), ainsi que les ambassades concernées et les autorités locales si le séjour risque d'être prolongé.
- Établir ou rétablir le contact et la communication avec le personnel resté sur place (voir ci-dessous).
- Préparer un rapport pour le siège et les donateurs, avec des mises à jour détaillées sur le personnel, les biens, les stocks et les finances, ainsi que les dettes en cours au moment de l'évacuation ou de la relocalisation.
- Interroger le personnel évacué ou relocalisé et lui apporter un soutien psychosocial, car ce changement peut susciter divers sentiments difficiles, notamment un épuisement émotionnel et un sentiment d'échec, de colère ou de culpabilité envers ceux qui sont restés sur place.

66 Pour des recommandations plus détaillées, voir Safer Edge (2014) *Office closure (en anglais, « Fermeture de bureau »)*. European Interagency Security Forum (<https://gisf.ngo/resource/office-closure/>).

Considérations relatives au bien-être du personnel à la suite d'une relocalisation ou d'une évacuation

Préparations avant l'arrivée

- Kit de bienvenue (comportant de l'eau en bouteille, de la nourriture, des articles de toilette, un bloc d'alimentation et des câbles de recharge, une carte SIM locale avec forfait data et une trousse de premiers secours).
- Identifier l'hôpital ou l'établissement médical le plus proche de la destination au cas où le personnel aurait besoin de soins médicaux à l'arrivée.

À l'arrivée

- Fournir un kit de bienvenue au personnel.
- Aider le personnel à contacter ses proches.
- Identifier tout besoin médical urgent/immédiat, tel que des blessures ou des médicaments à renouveler.
- Fournir au personnel un briefing sur la sécurité du lieu.
- Aider le personnel à se procurer de la monnaie locale.
- Fournir au personnel les coordonnées du personnel de soutien concerné et sa disponibilité.
- Le jour de l'arrivée, il est recommandé que l'équipe de soutien reste dans un endroit public/visible (par exemple, le hall d'un hôtel ou un café) facilement accessible afin que le personnel puisse s'y rendre pour obtenir de l'aide.
- Le personnel sera probablement épuisé par le voyage et voudra se reposer dans sa chambre. Demander aux personnes de signaler leur présence afin que l'équipe de soutien sache qu'elles vont bien. Par exemple, les inviter à dîner et leur demander d'envoyer un SMS si elles ne souhaitent pas s'y rendre, ou leur demander d'envoyer un SMS à une heure précise pour donner rapidement de leurs nouvelles.

Pendant leur séjour

- Veiller à ce qu'un membre de l'équipe de soutien établisse au moins un contact par jour avec le personnel concerné. Il peut s'agir d'un message ou d'un appel bref, ou d'une rencontre informelle.
- Aider les membres du personnel à rentrer chez eux, le cas échéant.
- S'assurer que le personnel sait s'il a droit à des repas et à des frais accessoires (indemnités journalières) pendant la relocalisation/l'évacuation.

- Aider le personnel à trouver des prestataires médicaux locaux ou des pharmacies pour le renouvellement des ordonnances.
- Les mettre en relation avec leur assurance maladie et leur prestataire d'aide médicale ou leur soutien psychologique, selon les besoins.

► Voir le chapitre 5.4 pour plus d'informations sur le bien-être du personnel.

Plans et approches de continuité

Certaines organisations peuvent ne pas être en mesure de relocaliser, comme c'est le cas, par exemple, des organisations locales qui n'opèrent que dans un seul endroit. L'hibernation peut prendre la forme d'une fermeture des bureaux et d'un licenciement du personnel, d'une «réintégration» dans la communauté et d'une attente de conditions plus favorables pour redémarrer les programmes. Plusieurs organisations locales dans certaines régions d'Afghanistan ont utilisé cette stratégie pendant des années entre 2001 et 2021, interrompant et reprenant leurs activités à plusieurs reprises en fonction de l'évolution de la situation politique et des conditions de sécurité.

Gestion de programmes à distance

Lorsque les relocalisations ou les évacuations durent beaucoup plus longtemps que prévu initialement, les plans de continuité peuvent évoluer vers une programmation à distance prolongée par l'intermédiaire de partenaires ou d'une «gestion à distance» des programmes. Le passage à la gestion de programmes à distance peut inclure un ou plusieurs des éléments suivants:

- Retirer du lieu de programmation certaines catégories de personnel (par exemple, les non-résidents de la zone en question), en particulier celles qui sont considérées comme présentant un risque particulièrement élevé.
- Modifier les structures de gestion afin de confier davantage de responsabilités au personnel qui reste sur place.
- Mettre en place des modalités opérationnelles nouvelles ou modifiées avec les partenaires, y compris les organisations et les autorités locales.
- Faire appel à des contrôleurs tiers pour s'assurer que les objectifs du programme sont atteints en l'absence d'une gestion directe.

Lorsqu'elle est utilisée en dernier recours et à titre exceptionnel, la gestion de programmes à distance présente généralement de sérieux défis. Ceux-ci peuvent inclure:

- Des problèmes éthiques liés au transfert du risque, en particulier si les membres du personnel ou les partenaires qui prennent en charge les responsabilités du programme sont invités – et fortement incités – à accepter des niveaux de risque plus élevés.
- Des difficultés à évaluer l'évolution des risques de sécurité et l'environnement en général, car le personnel et les partenaires sur place peuvent être moins sensibles aux changements subtils.
- Des difficultés de communication et de logistique.
- Les implications en matière de sécurité liées à l'acheminement d'argent ou de fournitures au personnel et aux partenaires.
- Une dépendance excessive à l'égard d'un petit nombre d'employés dans des environnements très stressants, conduisant à l'épuisement professionnel.
- La difficulté à assurer une surveillance adéquate du programme et des finances.
- Des difficultés à répondre aux exigences des donateurs en matière de suivi et de signalement.

Les enseignements pratiques tirés de la Covid-19 ont atténué certaines de ces difficultés, notamment en termes de communications à distance continues, de suivi à distance et de capacités de formation à distance, mais en aucun cas toutes.⁶⁷

Gestion des risques de sécurité lors de la programmation à distance

La programmation à distance soulève un nouvel ensemble de considérations financières, contractuelles et de sécurité, entraînant une nouvelle analyse des avantages et des risques. Poursuivre les programmes sous gestion à distance peut être plus risqué que de les interrompre complètement, et la fermeture d'un programme géré à distance peut présenter des risques si elle suscite l'hostilité du personnel concerné.

S'il est possible de continuer à fonctionner selon une approche de programmation à distance, des changements seront probablement nécessaires dans la structure, le style et l'approche de gestion. Les procédures de gestion pourraient devenir plus complexes et plus lourdes, avec des vérifications ou des rapports fréquents sur les questions financières, programmatiques ou relatives au personnel. De nouvelles méthodes de suivi des programmes pourraient devoir être mises au point, comme la prise de photos des résultats des projets (par exemple, les sources d'eau ou les écoles construites), accompagnées des coordonnées GPS.

Les conditions de sécurité peuvent évoluer rapidement, d'où l'importance de trouver des moyens de suivre l'évolution de la situation et de réévaluer les dispositions prises si les risques pour le personnel restant deviennent trop élevés. Outre le personnel restant, les informations utiles à l'évaluation des risques peuvent être recueillies auprès de contacts locaux (par exemple, les commerçants et les autorités locales) et par le partage d'informations et d'analyses avec d'autres organisations opérant dans la zone.

67 GISF (2020) *Keeping up with COVID-19: Essential guidance for NGO security risk managers* (en anglais, « Se tenir informé sur la COVID-19 : conseils essentiels pour les responsables de la gestion des risques de sécurité dans les ONG ») (www.gisf.ngo/resource/keeping-up-with-covid-19-essential-guidance-for-ngo-security-risk-managers/).

Des ressources et des formations supplémentaires pourraient être nécessaires pour soutenir le personnel restant ou les partenaires qui ont pris en charge des responsabilités supplémentaires, ainsi qu'un soutien financier et matériel, sous forme de véhicules et d'équipements de communication, par exemple.

► Pour en savoir plus sur les accords de partenariat, voir le chapitre 3.5.

D'autres pratiques contribuant à la réussite de la gestion de programmes à distance comprennent:⁶⁸

- Établir des procédures et des instructions claires pour le personnel et les partenaires en ce qui concerne les communications et les rapports sur les activités et les progrès.
- Intégrer le scénario de gestion à distance dans les exercices de planification d'urgence, en réfléchissant à l'avance aux partenaires potentiels, aux structures de gestion et de suivi, ainsi qu'aux stratégies de sortie et de transition.
- Faire sortir le personnel local ou les représentants des partenaires de la zone pour des réunions et des discussions régulières sur la gestion.
- Effectuer des contrôles ponctuels et des visites imprévues, dans la mesure du possible.
- Faire appel à des contrôleurs tiers ou recouper et vérifier les informations de contrôle avec d'autres organisations et des contacts locaux.
- Mettre en place et entretenir un réseau local de fournisseurs d'informations, d'intermédiaires et de facilitateurs au sein de la communauté locale.

Retour

Une évaluation des risques peut permettre de déterminer s'il est suffisamment sûr de revenir ou de renforcer la présence du personnel, et qui, au sein de l'organisation, devrait assumer la responsabilité de cette décision. En l'absence d'un changement assez radical sur le terrain (par exemple, un transfert de la maîtrise du risque territorial d'un acteur à un autre), le retour peut également être progressif et échelonné. Il peut d'abord s'agir de quelques missions exploratoires de courte durée visant à réévaluer la situation, puis éventuellement d'une présence plus permanente de certains membres clés du personnel dans une base opérationnelle, suivie du retour progressif d'un plus grand nombre d'employés et de personnel associé dans d'autres bases opérationnelles.

68 Stoddard, A., Harmer, A. et Renouf, J.S. (2010) *Once removed: lessons and challenges in remote management of humanitarian operations for insecure areas* (en anglais, « Une fois retiré: enseignements et défis de la gestion à distance des opérations humanitaires dans les zones instables »). Humanitarian Outcomes (<https://humanitarianoutcomes.org/publications/once-removed-lessons-and-challenges-remote-management-humanitarian-operations-insecure>).

Exemple de cas : Considérations relatives au retour

Après l'intensification de la guerre civile au Soudan du Sud en 2016, de nombreuses organisations humanitaires ont réduit leurs opérations et évacué le personnel étranger du pays. Lors de la reprise de ses activités, une organisation internationale a été confrontée à des défis importants dans la mise en œuvre de programmes dans les zones rurales en raison de l'insécurité, des difficultés d'accès et des problèmes de communication. Après plusieurs mois, le directeur de la sécurité a organisé une réunion rassemblant des représentants de divers départements du pays, notamment les programmes, les finances, les ressources humaines, les subventions, les réponses d'urgence et l'éducation.

Des collègues du siège, du bureau régional et du personnel national ont participé aux réunions de planification. Au cours de cette session d'une semaine, l'équipe a identifié les risques et élaboré des stratégies d'atténuation, créé des programmes de bien-être pour le personnel national et déterminé les ressources nécessaires en matière de sécurité. Le personnel national a mené des discussions sur les risques et le bien-être, qui ont débouché sur des changements significatifs, tels que l'octroi à tous les membres du personnel national d'un congé payé tous les deux mois pour se reposer et se ressourcer (R&R).

Grâce à ce plan d'urgence interfonctionnel mis en place par le personnel de sécurité, les programmes ont pu reprendre, les donateurs ont augmenté leur financement et les objectifs programmatiques de l'organisation ont été atteints.

Les informations essentielles pour évaluer la situation de la sécurité lors d'une mission exploratoire comprennent:

- La situation réelle sur le terrain (sécurité, militaire, politique), ainsi que les profils personnels du personnel de retour et les éventuels risques associés.
- Les changements probables au cours des 3 à 6 prochains mois et leurs implications en matière de sécurité.
- L'état des infrastructures locales (aéroports et routes), des communications et des services (par exemple, les banques).
- La localisation et le statut du personnel resté sur place.

- Le statut des biens, des actifs et des stocks laissés sur place.
- La disponibilité des provisions essentielles, en particulier la nourriture, l'eau et le carburant.
- L'image ou la réputation de l'organisation au niveau local et la manière dont les perceptions peuvent être gérées.
- Le niveau de ciblage direct des organisations humanitaires et, dans le cas des organisations internationales ou de celles ayant des liens avec l'étranger, des éléments étrangers.
- La capacité organisationnelle à gérer la sécurité dans le contexte actuel.
- Une analyse des risques et avantages globaux.

Informations complémentaires

Recommandations et ressources

Bickley, S. (2017) *Gestion du risque sécurité: manuel de référence à l'attention des petites ONG*. European Interagency Security Forum (<https://gisf.ngo/resource/security-risk-management-a-basic-guide-for-smaller-ngos/>)

Davis, J. et al. (2020) *Security to go: a risk management toolkit for humanitarian aid agencies* (« La sécurité en pratique: boîte à outils de gestion des risques à l'attention des agences humanitaires »), 4e édition (La 4e édition n'est pas disponible en français). GISF (<https://gisf.ngo/resource/security-to-go/>).

GISF (2020) *Keeping up with COVID-19: Essential guidance for NGO security risk managers* (en anglais, « Se tenir informé sur la COVID-19: conseils essentiels pour les responsables de la gestion des risques de sécurité dans les ONG ») (www.gisf.ngo/resource/keeping-up-with-covid-19-essential-guidance-for-ngo-security-risk-managers/).

GISF (n.d.a) 1. *Plans de sécurité*. Guide interfonctionnel sur la sécurité des ONG (<https://gisf.ngo/toolbox-pwa-fr/resource/1-plans-de-securite/>).

GISF (n.d.b) 5. *Plans d'urgence*. Guide interfonctionnel pour la sécurité des ONG (<https://gisf.ngo/toolbox-pwa-fr/resource/5-plans-durgence/>).

Safer Edge (2014) *Office closure* (en anglais, « Fermeture de bureau »). European Interagency Security Forum (<https://gisf.ngo/resource/office-closure/>).

Recherche et analyse

Donini, A. et Maxwell, D. (2013) 'From face-to-face to face-to-screen: remote management effectiveness and accountability of humanitarian action in insecure environments' (en anglais, « Du face à face au face à l'écran: efficacité de la gestion à distance et redevabilité de l'action humanitaire dans les environnements instables ») *International Review of the Red Cross* 95(890) (<https://doi.org/10.1017/S1816383114000265>).

Stoddard, A., Harmer, A. et Renouf, J.S. (2010) *Once removed: lessons and challenges in remote management of humanitarian operations for insecure areas* (en anglais, « Une fois retiré: enseignements et défis de la gestion à distance des opérations humanitaires dans les zones instables »). Humanitarian Outcomes (<https://humanitarianoutcomes.org/publications/once-removed-lessons-and-challenges-remote-management-humanitarian-operations-insecure>).

4.4 Réponse aux incidents et gestion de crise

Lorsqu'un incident de sécurité ou une crise survient, une réponse efficace implique de prendre des mesures pour gérer et atténuer les impacts, ainsi que de gérer les informations liées à l'incident et d'en tirer des enseignements. Ce chapitre commence par présenter les éléments d'information avant de décrire les éléments clés de la réponse et du suivi post-incident. Il présente un certain nombre de structures et d'approches de gestion de crise et d'incident qui sont généralement considérées comme des bonnes pratiques. Cependant, chaque événement et chaque organisation sont différents, et il est important de s'adapter aux circonstances individuelles, y compris aux structures organisationnelles.

4.4.1 Analyse et signalement des incidents

La gestion de l'information en cas d'incident de sécurité est le processus de collecte et d'utilisation des informations relatives aux incidents de sûreté et sécurité afin d'éclairer la prise de décision, les politiques et les procédures au sein d'une organisation. Il s'agit d'un élément essentiel de l'apprentissage au sein d'une organisation qui garantit que les expériences liées à la sécurité sont enregistrées et analysées afin d'améliorer les processus organisationnels. Cela en fait un élément important pour permettre à une organisation de remplir son devoir de diligence. Le signalement des incidents soutient la sécurité du personnel et des opérations de quatre manières principales :⁶⁹

- **Signalement des incidents et réponse immédiate.** Alerter les équipes concernées afin qu'elles soient informées et puissent, si nécessaire, venir en aide à toute personne touchée par un incident. Les autres acteurs humanitaires opérant dans la zone peuvent également être alertés afin de renforcer la sécurité de l'ensemble de la communauté.
- **Analyse d'incident et enseignements tirés.** Analyser l'incident et mettre en œuvre les enseignements tirés afin d'éviter que des incidents similaires ne se reproduisent à l'avenir et d'y répondre plus efficacement s'ils se reproduisent.
- **Analyse du contexte.** Le suivi des incidents et l'analyse des tendances et des modèles permettent d'éclairer les analyses contextuelles et les évaluations des risques relatifs à la sécurité. L'analyse des données agrégées sur les incidents provenant de l'intérieur et de l'extérieur de l'organisation facilite la prise de décision et indique si les procédures doivent être adaptées.
- **Prise de décision stratégique et politiques éclairées.** Permettre le partage d'informations sur les incidents de sécurité au sein d'une organisation afin d'éclairer les actions et les décisions visant à améliorer les méthodes de travail.

69 Ces points sont tirés et adaptés du *Manuel de la gestion de l'information en cas d'incident de sécurité (GIIS)*, disponible à l'adresse suivante : <https://siim.insecurityinsight.org/tools-and-resources/handbook-guide-and-tools>.

Une gestion de l'information en cas d'incident de sécurité rigoureuse peut également aider les organisations à satisfaire aux exigences légales ou réglementaires en matière de signalement à la suite d'un incident.

Signalement des incidents et partenaires

Certaines organisations peuvent avoir conclu des accords de partenariat qui prévoient la collecte de comptes rendus d'incident auprès de leurs organisations partenaires (bien que cela reste rare). Les partenaires peuvent utiliser ces informations pour s'entraider afin de tirer les enseignements des incidents et répondre collectivement aux besoins identifiés en matière de gestion des risques de sécurité. Le partage d'informations sur les incidents entre partenaires devrait idéalement se faire sur la base d'un soutien mutuel afin d'améliorer de manière collaborative la sécurité du personnel, plutôt que dans le cadre d'une obligation de conformité, même si cela peut être une exigence pour des raisons légales ou réglementaires.

- Voir le chapitre 3.5 pour d'autres bonnes pratiques en matière de collaboration avec les partenaires.

Signalement des incidents et réponse immédiate

Les organisations ont tout intérêt à mettre en place des procédures bien établies de signalement des incidents et à veiller à ce que leur personnel soit formé à la manière de signaler un incident et de demander de l'aide. Les incidents graves doivent être signalés immédiatement par les moyens les plus efficaces, par exemple par téléphone ou par radio, et le signalement ne doit contenir que les informations essentielles (voir l'encadré ci-dessous). Les incidents en cours nécessitent des mises à jour régulières.

Le signalement initial peut être suivi d'un débriefing une fois que le personnel est sorti de la situation immédiate et a reçu l'aide médicale et psychosociale dont il a besoin (ceci est différent d'un débriefing psychologique, qui est abordé plus en détail au chapitre 5.4). Il peut être utile de laisser un peu de temps aux personnes impliquées dans un incident pour en parler avant de rassembler leurs idées pour rédiger un compte rendu d'incident plus formel. En cas d'incident grave susceptible d'affecter d'autres personnes vivant ou travaillant dans la zone, l'organisation peut souhaiter alerter les personnes travaillant pour d'autres organisations – et, le cas échéant, les autorités locales et la population – afin qu'elles puissent prendre des précautions.

Cela doit être fait de manière à garantir la confidentialité des personnes concernées et sans exposer le personnel à un risque accru.

Informations clés à fournir lors du signalement initial d'un incident (les 6W ou questions fondamentales)

- Qui est impliqué ? Qui sont les victimes (s'il y en a) ? S'agit-il de membres du personnel de l'organisation, de membres du personnel des partenaires ou de consultants ? Quels sont leur genre et leur ethnicité ?
- Que s'est-il passé ?
- Où (de manière aussi précise que possible) l'incident s'est-il produit ?
- Quand l'incident s'est-il produit ?
- Qu'a-t-on fait jusqu'à présent concernant cet incident ? Quelles actions de réponse d'urgence ont été entreprises ?
- Quelle est l'aide nécessaire ? Une réponse immédiate supplémentaire est-elle nécessaire ? La situation perdure-t-elle ?

Il est important d'alerter les collègues et les associés dès que possible après qu'un incident s'est produit, lorsque cela peut être fait en toute sécurité, même si toutes les informations n'ont pas encore été obtenues. Un compte rendu d'incident plus complet est généralement rédigé après l'incident et la réponse immédiate, bien que pour les situations prolongées (par exemple, un enlèvement contre rançon), un compte rendu puisse être rédigé avant la fin de l'incident.

► Voir le chapitre 7.9 pour plus d'informations sur les scénarios d'enlèvement contre rançon et d'enlèvement.

Il est recommandé aux organisations de disposer d'un formulaire standard de compte rendu d'incident qui soit familier et facilement accessible hors ligne et en ligne. Certaines organisations ont investi dans des logiciels qui permettent d'effectuer des signalements via un portail ou une application sur des appareils mobiles. Quel que soit le format utilisé, l'important est que toutes les informations clés soient fournies et qu'elles soient accessibles à l'ensemble du personnel concerné. L'élaboration de modèles simples et faciles à utiliser peut encourager le signalement.

Le compte rendu d'incident peut se concentrer sur certaines questions fondamentales : Que s'est-il passé ? Qui a fait quoi ? À qui ? Quand ? Où ? (Certaines de ces informations peuvent ne pas être incluses car elles sont confidentielles) Il est important que le personnel responsable vérifie toutes ces informations dans la

mesure du possible. Il peut être pertinent ou non d'ajouter des informations sur le « pourquoi » et le « pourquoi cette organisation ou ce membre du personnel ». Parfois, cela est évident parce que les auteurs l'ont dit, mais dans d'autres cas, il peut s'agir de simples spéculations. Il est important de comprendre si l'organisation et le(s) membre(s) du personnel ont été spécifiquement ciblés et, si tel est le cas, pourquoi, sur la base des informations disponibles. Le compte rendu peut indiquer le degré de confiance dans les réponses à ces questions et être transparent quant à la part de spéculation.

Le sous-signalement est l'un des aspects les plus difficiles de la gestion de l'information en cas d'incident de sécurité. Il s'explique souvent par une compréhension insuffisante ou une méconnaissance du processus de signalement des incidents, notamment de la manière dont les informations seront utilisées et par qui. Pour y remédier, il convient de mettre en place un processus de signalement simple, des modèles faciles à utiliser et de former le personnel à la manière et aux raisons de signaler les incidents.⁷⁰ Un autre défi important peut être le manque d'accès aux mécanismes de signalement. Cela peut être dû à des barrières linguistiques (par exemple, lorsque le signalement doit être rédigé en anglais) ou à d'autres facteurs, notamment la culture organisationnelle (par exemple, s'il existe une culture du blâme ou de la honte, ou si le signalement est considéré comme une charge bureaucratique plutôt que comme une occasion d'apprendre et de s'améliorer). Parmi les autres défis courants liés au compte rendu d'incident, on peut citer :

- Le manque de temps et de ressources pour signaler ou gérer les informations relatives aux incidents ; dans les endroits où les incidents sont fréquents, il peut être difficile pour les points focaux de traiter efficacement un grand nombre de comptes rendus d'incident.
- L'incohérence des formats ou des procédures de signalement entre les différents départements ou bureaux.
- Les préjugés et la subjectivité, les signalements pouvant être influencés par des préjugés, des perceptions ou des interprétations personnels. Par exemple, le personnel peut être insensible à certains types d'incidents et ne pas les considérer comme pertinents à signaler.
- Le fait de ne pas connaître l'identité des auteurs ou leurs motivations avant longtemps, voire jamais dans certains cas. Il est important d'indiquer le degré de fiabilité des déclarations et de modifier les registres internes de l'organisation si de nouveaux détails apparaissent.
- Une réticence naturelle à reconnaître que les actes ou omissions de l'organisation ou de certains de ses membres du personnel ont contribué à la survenue d'un incident. Le personnel peut craindre des mesures disciplinaires ou d'autres représailles pour ne pas avoir respecté les exigences de l'organisation.

⁷⁰ Insecurity Insight et DisasterReady ont collaboré à l'élaboration d'un guide mobile destiné au personnel sur la gestion et le signalement des incidents. Voir : <https://siim.insecurityinsight.org/tools-and-resources/siim-app-and-short-guides>.

- Les difficultés de classification, par exemple pour distinguer entre vol, cambriolage et braquage à main armée, ou entre enlèvement et enlèvement contre rançon. La définition de ces différentes catégories doit être claire pour toutes les personnes qui font un signalement. Il peut être utile de disposer de systèmes de classification organisationnels, et des recommandations externes sont disponibles.⁷¹

Il est important de ne pas laisser ces défis, ni la confusion ou les désaccords concernant les classifications et les terminologies, entraver la mise en place d'un système de signalement des incidents. Si les membres du personnel ne sont pas en mesure d'appliquer les classifications de manière cohérente, s'il existe des barrières linguistiques ou si le personnel trouve le processus intimidant et rebutant, le personnel de sécurité doit s'efforcer de veiller à ce que les informations soient consignées. Certaines organisations et plateformes de sécurité centralisent la classification des incidents, afin que le personnel puisse simplement transmettre les informations dont il dispose le plus rapidement possible. Les points focaux pour les questions de sécurité assurent ensuite le suivi, répondent aux questions si nécessaire et procèdent à la classification et à l'enregistrement officiel de manière centralisée.

Qu'est-ce qui constitue un « incident à signaler » ?

Des recommandations managériales sont nécessaires pour s'assurer que les personnes comprennent ce qu'elles sont tenues de signaler et comment elles doivent le faire, ainsi que la manière dont les informations peuvent être utilisées. Même en cas de doute, le personnel doit être encouragé à signaler tout incident.

Un incident de sécurité est tout événement causant un préjudice au personnel ou aux personnes associées, ou entraînant la perte ou l'endommagement des biens. Un « quasi-incident » ou « incident évité de justesse » est un événement qui a failli causer un tel préjudice, dommage ou perte. Il est recommandé d'inclure les incidents susceptibles de causer un préjudice (c'est-à-dire une menace). Une action menaçante peut être écrite, verbale ou physique, si elle traduit de manière crédible l'intention d'un acteur de causer un préjudice. Il est important d'inclure même les incidents mineurs et les quasi-incidents.

La plupart des organisations enregistrent à la fois les incidents de sûreté et sécurité, tels que les accidents de la route, ainsi que les attaques délibérées contre le personnel.

⁷¹ Voir par exemple, la Classification des incidents par Insecurity Insight: <https://siim.insecurityinsight.org/tools-and-resources/classification-of-incidents>.

Les signalements peuvent également inclure les incidents ou quasi-incidents affectant d'autres entités impliquées dans le programme, y compris les organisations partenaires et les sous-traitants. Il peut également être utile d'inclure, dans les exigences de signalement, tout incident dans lequel un membre du personnel a causé un préjudice à un tiers, ou une perte ou un dommage aux biens ou aux actifs d'un tiers. D'autres types d'incidents peuvent être inclus s'ils indiquent des tendances dans l'environnement opérationnel, tels que des cas de troubles communautaires ou de violence à proximité des sites du projet.

Dans certaines circonstances, telles que le harcèlement et la violence sexuelle, et lorsque l'incident est perpétré par un employé (c'est-à-dire les incidents de sauvegarde), certaines organisations peuvent disposer de mécanismes de signalement distincts. Cela peut s'expliquer par le fait que ces incidents ne relèvent généralement pas des responsabilités de la fonction de sécurité et aussi parce qu'il est primordial de garantir la confidentialité et la sûreté de la personne qui effectue le signalement. Si la confidentialité peut être garantie, les organisations ont également intérêt à établir un compte rendu d'incident de sécurité. L'enregistrement des incidents dans un système centralisé permet de dégager des tendances et de mettre en place des mesures d'atténuation appropriées.

Analyse d'incident et enseignements tirés

Le suivi auprès du personnel concerné peut avoir lieu à différents moments, en fonction de la gravité de l'incident et de la manière dont il a été signalé. Il est recommandé aux membres du personnel responsables, tels que les points focaux pour les questions de sécurité, de rechercher toute information supplémentaire non mentionnée dans le compte rendu d'incident et d'organiser un débriefing factuel avec les personnes concernées afin d'en tirer des enseignements. Ceux-ci se concentrent sur les faits de l'incident plutôt que sur les réponses émotionnelles à l'événement. Lors de la planification de ces réunions, il convient de tenir compte des questions de confidentialité, de la nécessité de faire appel à des professionnels qualifiés pour mener le débriefing (et non nécessairement au personnel de sécurité), ainsi que des besoins individuels des membres du personnel concernés (tels que la langue) et de la manière dont ceux-ci peuvent être conciliés. Si l'incident est dû au non-respect des procédures par le personnel, l'organisation devra trouver un équilibre entre la nécessité d'appliquer des mesures disciplinaires et celle d'encourager le personnel à signaler les incidents.

Une fois les informations sur l'incident recueillies, le personnel concerné peut analyser plus en détail ce qui s'est passé et pourquoi. Les questions clés à prendre en compte lors de l'analyse d'incident sont les suivantes :

- Quels ont été la cause et l'impact de l'incident ? Il convient d'examiner les caractéristiques d'identité et les perceptions de l'organisation et des personnes concernées, et de déterminer si elles ont joué un rôle dans la survenue de l'incident. Par exemple, une attaque a-t-elle été délibérément menée contre un membre du personnel en particulier en raison de son ethnicité ?
- Des incidents similaires se sont-ils déjà produits par le passé (y compris dans d'autres organisations travaillant dans la même zone) ?
- Les procédures organisationnelles ont-elles été respectées ?
- La réponse aux incidents a-t-elle été bien gérée, notamment le processus de signalement ? Qu'aurait-on pu faire différemment ?

Un signalement des incidents transparent et cohérent contribue à maintenir la confiance du personnel, des parties prenantes et du public. Il démontre que l'organisation prend la sûreté et sécurité au sérieux et qu'elle s'efforce de répondre de manière proactive aux préoccupations. Communiquer avec le personnel et les autres parties concernées sur les enseignements tirés, les décisions prises et les mesures mises en œuvre peut améliorer la compréhension et la confiance des membres du personnel à l'égard de la gestion de l'information en cas d'incident et encourager le signalement.

Analyse du contexte

Le signalement des incidents peut grandement aider le personnel de sécurité à comprendre le contexte opérationnel et à prévoir le type d'incidents ou de menaces susceptibles de se produire à l'avenir. Une vue d'ensemble fiable des incidents à signaler dans le monde entier, élaborée à partir d'une base de données, permet une meilleure analyse de la sécurité aux niveaux national, régional et mondial, ainsi qu'en relation avec des programmes spécifiques et des profils organisationnels ou personnels.

De nombreuses organisations humanitaires disposent de systèmes internes de signalement des incidents, allant de simples tableurs Excel à des portails ou des applications affichant des données visualisées dans des tableaux de bord.

► Voir le chapitre 3.4 pour plus d'informations sur les tableaux de bord.

Disposer d'un système de gestion et d'enregistrement des données relatives aux incidents permet de normaliser les types d'incidents signalés, le type d'informations collectées et la manière dont les incidents sont classés, ce qui facilite l'analyse des tendances et des schémas. Ces détails peuvent révéler la concentration géographique des incidents, donner des informations sur les types d'incidents et montrer si le nombre total d'incidents est en augmentation ou en diminution. Ce type d'informations peut à son tour aider à décider où allouer les ressources de sécurité (humaines et financières) et où il est nécessaire d'investir davantage, par exemple dans la formation, la technologie ou la modernisation des infrastructures. L'analyse

des informations relatives aux incidents peut contribuer à garantir que les ressources sont affectées là où elles sont le plus nécessaires afin d'améliorer la sûreté, la sécurité et la résilience opérationnelle.

L'analyse des incidents individuels et des données agrégées sur les incidents est également essentielle à l'apprentissage et au développement organisationnels. Cette analyse aide les organisations à identifier les tendances, les causes profondes et les problèmes systémiques qui doivent être traités, et permet d'apporter des améliorations ciblées aux protocoles de sécurité, aux programmes de formation et aux procédures opérationnelles. Ces informations peuvent également être utilisées pour déterminer et structurer l'orientation et la formation du personnel, des visiteurs et des voyageurs, ainsi que les protocoles connexes.

Les organisations voudront contrôler qui a accès aux bases de données sur les incidents afin de protéger la vie privée des personnes concernées. Cependant, il est important que les informations soient partagées, et les organisations devraient permettre aux utilisateurs de consulter les tendances et les schémas ventilés sans révéler d'informations sensibles sur des incidents spécifiques. Cela peut se faire en imposant des restrictions d'accès aux bases de données ou en élaborant des comptes rendus à partir de données pouvant être partagées plus largement.

La comparaison des données relatives aux incidents avec celles de pairs situés dans les mêmes lieux peut permettre une analyse plus objective des schémas d'incidents et aider à déterminer les tendances si les données sont analysées dans le temps. Les données externes sur les incidents sont accessibles via des forums interagences sur la sécurité et des bases de données publiques (voir « Informations complémentaires » ci-dessous pour des exemples). Certaines organisations peuvent également avoir conclu entre elles des accords de partage de données sur les incidents, par exemple entre organisations partenaires. Toutes les données externes doivent être analysées en tenant compte de la validité et de la fiabilité des données sur les incidents qui ont été partagées. Les organisations doivent s'efforcer de partager les données sur la gestion des risques de sécurité de manière à garantir la confidentialité et à favoriser la collaboration.⁷²

Prise de décision stratégique et politiques éclairées

Les données sur les incidents de sécurité peuvent éclairer la prise de décision dans l'ensemble d'une organisation, tant au sein des fonctions de sécurité qu'en dehors de celles-ci, et les organisations devraient disposer de procédures pour le partage et l'utilisation des données sur les incidents en interne.

Les informations issues de l'analyse d'incident peuvent éclairer la planification des programmes, les propositions de financement, les descriptions de poste et les politiques RH, ainsi que les évaluations des risques et l'analyse du contexte. Les

72 Insecurity Insight et GISF ont élaboré des recommandations et des outils sur la manière de partager les informations relatives aux incidents de sécurité entre les organisations, accessibles ici : <https://gisf.ngo/long-read/ngo-security-collaboration-guide/> and <https://siim.insecurityinsight.org/tools-and-resources/siim-in-ngo-security-collaboration>.

cadres supérieurs peuvent utiliser les données sur les incidents pour décider des activités et des ressources à financer, des mesures de gestion des risques de sécurité à mettre en œuvre, ainsi que où et comment opérer dans des endroits donnés. Une telle analyse peut également aider à orienter les décisions stratégiques concernant les contextes dans lesquels travailler, les approches de sécurité à privilégier et la manière de communiquer avec les différentes parties prenantes (notamment les donateurs, les groupes locaux et les autorités). Les données sur les incidents peuvent également servir à soutenir les actions de plaidoyer contre la violence à l'égard des travailleurs humanitaires et les restrictions d'accès humanitaire.

► Voir le chapitre 2.2 pour plus d'informations sur le plaidoyer.

4.4.2 Réponse aux incidents et gestion de crise

Si tous les incidents nécessitent une réponse, c'est leur gravité qui détermine le type de réponse requis. Un incident non critique peut être traité à l'aide des procédures et des capacités organisationnelles existantes sur le lieu où l'incident s'est produit. Pour ce type d'incident, le point focal pour les questions de sécurité et les autres membres du personnel concernés peuvent appliquer les procédures opérationnelles standards et les plans de l'organisation afin de s'assurer que le personnel touché est pris en charge et que l'impact plus large de l'incident est géré. Ce qui est considéré comme un incident non critique varie selon les organisations. Il peut s'agir, par exemple, de harcèlement non verbal de faible intensité, de dommages matériels causés à des équipements, de détentions de courte durée ou d'accidents de la route mineurs n'entraînant aucune blessure grave. Les incidents non critiques sont généralement traités par l'autorité décisionnelle, avec des mesures supplémentaires pouvant inclure des discussions avec des parties prenantes externes, le partage d'informations avec le personnel et le respect des exigences légales ou des exigences en matière d'assurance (par exemple, lors du signalement d'un vol). Les intervenants doivent toujours tenir compte des circonstances personnelles (par exemple, l'ethnicité, le statut personnel ou le genre) qui peuvent nécessiter une approche personnalisée.

Les incidents critiques sont des événements qui menacent gravement la vie ou la santé du personnel. Un incident critique est généralement trop grave pour être géré par les structures de direction habituelles, nécessite un soutien supplémentaire (financier, humain, administratif et technique) et implique souvent le personnel de plusieurs bureaux, y compris le siège social. La plupart des incidents critiques nécessitent une réponse de crise, ce qui signifie que la structure de gestion de crise d'une organisation doit être activée.

Une crise est un événement extrêmement perturbateur qui interrompt gravement le fonctionnement normal, entraîne ou menace d'entraîner des conséquences graves et nécessite des mesures extraordinaires et une action immédiate de la part de l'autorité décisionnelle. Les crises peuvent prendre diverses formes et menacer la

réputation, les programmes, les actifs, les finances et la sécurité du personnel d'une organisation. Une crise peut être déclenchée par un incident critique, mais toutes les crises ne sont pas liées à un incident critique.

Ce qui est considéré comme une crise ou un incident critique varie selon les organisations, mais les exemples courants comprennent une situation d'otages ou un enlèvement contre rançon, le décès d'un membre du personnel, une attaque grave affectant directement ou indirectement l'organisation (par exemple, une attaque ciblée contre le personnel ou un attentat à la bombe près des installations de l'organisation, un coup d'État ou un danger naturel, tel qu'un tremblement de terre).

La réponse de la direction d'une organisation à un incident critique ou à une crise peut être décomposée en plusieurs étapes.⁷³

- Planification et préparation
 - Élaboration d'une structure et d'un plan de gestion de crise.
 - Formation à la gestion de crise et sensibilisation.
- Gestion de crise et des incidents
 - La réponse initiale, comme la fourniture d'un soutien médical et l'information des principales parties prenantes.
 - La gestion de la situation, telle que l'élaboration et la mise en œuvre d'une stratégie visant à soutenir les personnes touchées, ainsi que la gestion des communications, des parties prenantes et des informations.
 - La résolution de la situation, telle que la libération réussie du personnel kidnappé.
- Actions post-incident
 - Un examen de l'événement, de la réponse de l'organisation et des politiques et procédures de gestion des risques de sécurité, ainsi que du soutien à plus long terme pour les personnes touchées.

Ces étapes peuvent varier dans la pratique en fonction du type d'incident et de sa durée.

Planification et préparation à la gestion de crise

Une gestion de crise efficace implique la mise en place d'une structure adéquate, de plans complets, de formations et d'exercices. Pour prendre des décisions et mener les actions appropriées en réponse à un incident critique ou à une crise, les organisations peuvent être amenées à activer leur plan de gestion de crise et à mobiliser ou constituer la structure de gestion de crise (un cadre au sein d'une organisation permettant de faire face à une crise ou à un incident critique).

Un plan de gestion de crise peut comprendre:

⁷³ Désormais décrite comme « gestion de crise », cette expression englobe à la fois les incidents critiques et les crises. Certaines organisations peuvent utiliser le terme « gestion des incidents critiques » pour désigner les efforts de réponse aux incidents critiques.

- Les définitions des types d'incidents critiques et de crises.
- Quand activer et mettre fin à la structure de gestion de crise, y compris qui en décide en dernier ressort.
- La délimitation des rôles et des responsabilités des acteurs clés, y compris la composition de l'équipe de gestion de crise (EGC) et de l'équipe de gestion de l'incident.⁷⁴
- Protocoles et modèles pertinents, tels que les protocoles d'évacuation médicale et les modèles de compte rendu d'incident.

Ces plans peuvent être testés régulièrement et intégrés dans des exercices de formation et de simulation. Ils doivent être revus et (éventuellement) mis à jour après une crise ou une réponse aux incidents critiques.

La structure de gestion de crise varie selon l'organisation et la situation, mais peut comprendre les éléments suivants :

- Une **autorité décisionnelle** - une personne ou un groupe disposant de l'autorité décisionnelle ultime en cas de crise ou d'incident critique – qui ne participe généralement pas à la gestion quotidienne de la crise, mais qui est régulièrement informée et qui, à son tour, tient les autres cadres supérieurs et les membres du conseil d'administration informés des actions de l'équipe de réponse. L'autorité décisionnelle est généralement chargée d'évaluer la gravité et l'impact d'un événement ou d'une situation par rapport à des critères ou des seuils prédéterminés qui définissent ce qui constitue un incident critique ou une crise nécessitant une réponse de gestion de crise.
- Une **équipe de gestion de crise** au siège social ou au bureau régional, et éventuellement une autre au niveau du bureau de pays (pour les organisations internationales). Cette équipe est responsable de tous les aspects de la réponse à la crise. Les équipes de gestion de crise virtuelles, composées de membres provenant de différents endroits, sont devenues plus courantes à mesure que la technologie est devenue plus fiable.
- Une **équipe de gestion de l'incident** au niveau local où l'incident se produit, chargée de mettre en œuvre la stratégie de gestion de l'incident sous la direction de l'équipe de gestion de crise.
- Des **équipes de soutien à la réponse à la crise**, telles que le personnel chargé de la sécurité, de la santé, des technologies de l'information et des communications, qui peuvent apporter un soutien supplémentaire sans être membres officiels de l'équipe de gestion de l'incident ou de crise.

74 Désormais, toute référence aux équipes de gestion de crise inclut toute équipe de gestion de crise et toute équipe de gestion de l'incident activées dans différents lieux.

- Les fonctions de **liaison avec les familles** et de **communication de crise** sont liées aux équipes de gestion de l'incident ou de crise, mais souvent distinctes de celles-ci. Les organisations peuvent veiller à ce qu'elles fassent partie intégrante de leurs plans de préparation (voir les sections suivantes).

L'équipe de gestion de crise peut établir une hiérarchie des responsabilités et établir une distinction claire entre les rôles joués dans les différents bureaux (par exemple, bureau de projet, bureau régional ou siège social). Un organigramme clair peut être élaboré et tenu à jour, avec des responsabilités définies et une liste de contacts. Toutes les personnes impliquées doivent savoir où elles se situent. Pour certains incidents, une équipe de gestion de l'incident peut intervenir uniquement au niveau local, mais il est nécessaire de bien comprendre quand il convient d'impliquer le siège social (y compris les équipes régionales de réponse à la crise, le cas échéant). Les incidents graves ou prolongés (assassinat, attentat à la bombe, enlèvement contre rançon ou mise en hibernation forcée, par exemple) ou les changements majeurs (tels qu'une relocalisation ou une évacuation) nécessiteront généralement une équipe de gestion de crise dédiée, soutenue par une équipe de gestion de l'incident. La répartition exacte des responsabilités entre ces équipes dépendra du contexte et de la situation. Par exemple, la désignation d'agents de liaison familiale formés pour soutenir le personnel touché et leurs familles peut se faire tant au niveau de l'équipe de gestion de crise qu'à celui de l'équipe de gestion de l'incident, selon la situation.

Dans l'idéal, les équipes de gestion de crise devraient être petites afin de garantir souplesse et rapidité dans la prise de décision. Elles peuvent comprendre des représentants d'un certain nombre de fonctions essentielles (voir l'encadré ci-dessous). Un gestionnaire de crise peut être nommé et habilité à mobiliser le personnel, l'équipement, les moyens financiers et les autres ressources nécessaires pour garantir une réponse efficace et rapide. La gestion de l'information doit être soigneusement étudiée au sein de l'équipe de gestion de crise et des fonctions de soutien, d'autant plus que les personnes chargées de communiquer avec les parties prenantes externes (telles que le personnel chargé de la liaison familiale et de la communication) peuvent se trouver dans une position délicate si elles ont accès à toutes les informations.

La gestion de crise est un défi qui requiert toute une gamme de compétences et d'expertises – juridiques, médicales, psychologiques et de négociation avec des preneurs d'otages, par exemple – dont certaines peuvent devoir être recherchées à l'extérieur de l'organisation. Tout besoin de soutien externe devrait idéalement être identifié et ce soutien obtenu dès que possible, puis utilisé aussi longtemps que nécessaire (ce qui peut aller d'une consultation initiale à une intervention plus régulière pendant la période de réponse). Certaines organisations font appel à d'anciens membres du personnel qui connaissent l'organisation et dont les compétences et l'expérience sont reconnues et fiables. Les membres du personnel actuels qui ne font pas partie des équipes de gestion de l'incident ou de crise, mais qui possèdent les connaissances, les contacts et les compétences nécessaires, peuvent également être impliqués.

Fonctions de l'équipe de gestion de crise

La composition des équipes de gestion de l'incident et de crise varie en fonction de l'organisation et de l'événement auquel elles doivent faire face. Voici quelques fonctions que les organisations pourraient envisager :

- Chef d'équipe/gestionnaire de crise
- Ressources humaines
 - Soutien administratif (par exemple, dossiers du personnel et liaison avec les assurances)
 - Soutien aux familles (coordination des contacts et du soutien aux familles, gestion des agents de liaison familiale)
 - Soutien au personnel (prise en charge psychosociale du personnel concerné, notamment les intervenants)
- Médias et communication (généralement assurés par une équipe distincte chargée de la communication de crise)
- Assistant chargé des tâches administratives, notamment la prise de notes et l'organisation des réunions
- En fonction de la nature de l'incident ou de l'événement, le point focal pour les questions de sécurité, le directeur de pays, le chef des opérations sur place, des experts du contexte, des experts médicaux, juridiques, logistiques et informatiques.

Les personnes intervenant en cas d'incident critique ou de crise ne sont pas nécessairement toutes basées au même endroit. La gestion de crise peut impliquer une collaboration et une coordination à distance et virtuelles entre les membres de l'équipe.

La gestion de crise peut être un travail à plein temps au début. Le personnel impliqué doit être libéré de ses autres tâches et protégé de toute intrusion inutile afin de pouvoir se concentrer sur la tâche à accomplir. Il est utile que ce personnel dispose de son propre espace de travail et de ses propres installations, y compris une salle de crise temporaire. Il doit s'efforcer de suivre la situation au quotidien et de décider et revoir régulièrement la politique à l'égard des différentes parties prenantes. Les membres de l'équipe peuvent avoir besoin de repos et de détente réguliers, ainsi que de soutien pendant et après la crise.

Fichier de données personnelles

Le personnel des ressources humaines peut contribuer à la gestion de crise en s'assurant de disposer des informations et des documents appropriés pour tous les employés en cas de crise ou d'incident critique. Certaines organisations tiennent à jour un dossier contenant des informations personnelles clés telles que :

- Preuve de vie
- Personne(s) à contacter en cas d'urgence (qui peut être différente selon les circonstances)
- Informations médicales
- Informations relatives à l'activité sur les réseaux sociaux
- Informations supplémentaires pouvant être utiles pour contacter la famille ou apporter un soutien d'urgence au membre du personnel.

Ce dossier devra être traité avec la plus grande confidentialité, mais devra être rapidement accessible en cas d'urgence.

Si la crise se prolonge, les membres des équipes de gestion de l'incident et de crise pourront être remplacés. Les congés, les déplacements et autres engagements professionnels peuvent également avoir une incidence sur la durée pendant laquelle les personnes peuvent remplir leurs fonctions de gestion de crise. Une transition en douceur peut être préparée en veillant à ce que le dossier de transfert soit tenu à jour avec les rapports et les analyses, et en planifiant le transfert de manière à ce que les membres de l'équipe se passent le relais. Les bonnes pratiques recommandent de disposer d'un ou deux remplaçants pour chaque poste, tous formés et prêts à prendre la relève en cas de besoin.

La formation à la gestion de crise est l'un des éléments les plus importants de la préparation à une crise ou à un incident critique. Tous les membres du personnel identifiés pour jouer un rôle dans la gestion de crise ou d'incident doivent être formés et être capables de travailler ensemble. Des fonds sont nécessaires pour financer la formation à la préparation, y compris les exercices de simulation.

Formation à la gestion de crise

La formation et les exercices de gestion de crise peuvent prendre différentes formes, allant des exercices sur table aux simulations à grande échelle. Les premiers exercices basés sur l'analyse permettent d'identifier les principaux intervenants, les capacités et les lacunes. Des exercices de simulation plus avancés permettent de tester les plans de crise dans des scénarios réalistes. Des formations et des exercices réguliers en matière de réponse aux crises et de communication améliorent la prise de décision, la sensibilisation et la confiance dans les capacités d'une organisation à gérer efficacement les crises et les incidents critiques.

Réponse initiale et stratégie

La première étape pour faire face à un incident critique ou à une crise consiste à déterminer si une action immédiate est nécessaire pour préserver la vie ou assurer la sûreté. Il faut établir des informations vérifiables décrivant les détails de l'événement. Cela peut faire partie du signalement initial. Les informations supplémentaires ou les changements doivent être communiqués dès qu'ils se produisent.

Dans l'idéal, un registre devrait être créé immédiatement après le signalement d'un incident et régulièrement mis à jour afin de consigner la chronologie des événements, d'enregistrer les appels téléphoniques, de consigner les notes des réunions et de s'assurer que tous les documents sont enregistrés et classés.

À la réception d'un compte rendu d'incident, la première décision à prendre consiste à déterminer si une situation particulière peut être qualifiée de crise ou d'incident critique, et s'il convient d'activer la structure de gestion de crise de l'organisation. Comme il est souvent plus facile de suspendre une réponse de gestion de crise que de se démener pour rattraper le retard, les organisations peuvent envisager d'agir avec une « réaction prudente ». Si la fonction de gestion de crise est activée, l'équipe peut être amenée à décider :

- Si les activités du programme doivent être suspendues ou si le personnel doit être transféré vers un lieu plus sûr.
- Si du personnel de soutien supplémentaire doit être déployé pour apporter son aide.
- Quelles informations doivent être diffusées en interne et en externe, et quelles sont les éventuelles restrictions ou questions de confidentialité.
- L'objectif final (par exemple, évacuation des blessés, rapatriement des corps, libération des membres du personnel enlevés).

L'importance de tenir un registre

Un élément important de la gestion de crise et d'incident consiste à ouvrir et à tenir à jour un registre afin de consigner les décisions prises, les raisons qui les ont motivées, les personnes qui les ont prises, le moment où elles ont été prises et les actions qui en ont résulté. Cela présente plusieurs avantages, notamment :

- Il fournit un compte rendu complet qui facilite la passation de pouvoir aux nouveaux membres de l'équipe de gestion de crise dans le cadre d'une réponse prolongée.
- Il peut aider à orienter les actions à entreprendre post-incident/post-crise.
- Il fournit la preuve documentaire que l'organisation a fait de son mieux pour remplir son devoir de diligence envers le personnel concerné.
- Les archives peuvent démontrer que l'organisation a utilisé une approche réfléchie et systématique pour décider des actions à entreprendre, même si celles-ci n'ont pas donné les résultats escomptés.

Il est conseillé de gérer avec soin les informations contenues dans le registre et de les conserver en toute sécurité, en préservant et en respectant leur confidentialité.

L'un des rôles clés de l'équipe de gestion de crise consiste à élaborer une stratégie de gestion de crise ou d'incident qui définit l'approche de l'organisation face à l'événement, notamment :

- La gestion des parties prenantes, y compris le soutien aux familles et la liaison avec les autorités, les médias, les communautés et d'autres organisations.
- Communications.
- Les négociations et la communication avec les auteurs, le cas échéant.
- La gestion de l'information, y compris la collecte et l'analyse d'informations, le maintien de la sécurité de l'information, l'archivage et la documentation.
- Ressources (matérielles et humaines).

La stratégie doit être élaborée en consultation avec des experts compétents, tels que des conseillers juridiques, afin de garantir qu'elle tient compte des cadres juridiques et des juridictions applicables. Chaque incident doit faire l'objet d'une stratégie spécifique, qui doit être révisée régulièrement.

Dans l'ensemble, l'équipe de gestion de crise doit généralement prendre en compte les questions médicales et de sécurité, le soutien logistique et la capacité de réaction rapide, ainsi que les questions liées à la réputation, aux aspects juridiques, à la communication et aux médias. L'équipe de gestion de crise peut être amenée à assurer la liaison avec les assureurs et à garantir une couverture, des décaissements et un soutien adéquats. Il peut y avoir des blessés qui nécessitent des soins immédiats ou de longue durée. En cas de décès, les membres de la famille doivent être informés et des mesures doivent être prises pour couvrir les frais funéraires, d'inhumation et autres. La sécurité peut encore être un sujet de préoccupation si des personnes qui n'ont pas été touchées par l'incident proprement dit sont toujours à risque et un soutien logistique peut être nécessaire pour organiser les évacuations médicales, le rapatriement ou le retour des corps à leurs familles. En fonction de la situation, du personnel spécialisé peut être envoyé sur place, par exemple pour fournir des moyens de recherche et de sauvetage, une aide médicale ou médico-légale et un soutien psychologique et psychothérapeutique. D'autres bureaux, au niveau régional et/ou au siège, peuvent également avoir besoin de cette expertise.

L'équipe de gestion de l'incident joue un rôle clé dans la mise en œuvre des directives de l'équipe de gestion de crise, qui peut inclure les responsabilités suivantes :

- Gestion de la crise au niveau local.
- Communication avec les parties prenantes locales, notamment la famille, les autorités locales (y compris la police), les ambassades et autres représentants du gouvernement, l'ONU et les ONG, ainsi que les médias locaux.
- Soutien aux familles, si elles sont présentes sur place, et soutien moral et matériel aux personnes touchées, si possible.
- Partage d'informations et évaluation des risques pour l'équipe de gestion de crise au siège.

Gestion de la communication et des médias

La gestion de la communication est un élément essentiel de la gestion de crise ou d'incident critique. Compte tenu des risques liés à la fuite d'informations, la confidentialité et l'adoption d'une approche « besoin de savoir » sont considérées comme de bonnes pratiques. Le guide du GISF intitulé *Gérer le message* fournit des recommandations détaillées et des outils sur la manière de gérer la communication avec les parties prenantes internes et externes lors d'une crise ou d'un incident critique.⁷⁵

75 Davidson, S. (2013) *Gérer le message : gestion de la communication et des médias en cas de crise de sécurité*. European Interagency Security Forum (www.gisf.ngo/resource/managing-the-message/).

Coordination en cas de crise ou d'incident critique

Certains événements peuvent nécessiter une coordination entre plusieurs organisations, comme l'attaque d'un convoi ou l'enlèvement contre rançon d'un groupe. Dans ces circonstances, l'équipe de gestion de crise de l'organisation assurerait la liaison avec les principales parties prenantes et pourrait partager des informations, des conseils, une expertise contextuelle et des ressources avec d'autres organisations.

Lorsque plusieurs organisations décident de déplacer ou d'évacuer leur personnel en cas de crise majeure, comme un conflit civil, elles peuvent compter en grande partie sur les mêmes ressources ou sur l'aide de l'ONU. Dans ces circonstances, la coordination est essentielle, mais elle peut s'avérer difficile dans la pratique, car les ressources peuvent être dépassées et l'accès limité. Il est essentiel que toutes les organisations sachent clairement de quel soutien elles ont besoin lors de ce type d'événements et s'assurent que ce soutien est en place avant qu'un événement ne se produise.

Il est toujours bon d'établir des relations avec les parties prenantes externes avant qu'un événement ne se produise et que tous les acteurs sachent clairement quel soutien ils peuvent attendre les uns des autres et quels sont les mécanismes de coordination. Un bon point de départ consiste pour les organisations à établir des contacts avec les acteurs concernés, y compris d'autres organisations humanitaires et l'ONU lorsqu'elles arrivent dans une nouvelle région, et à leur demander comment se déroulerait la coordination en cas de crise majeure.

► *Voir le chapitre 2.1 pour plus de détails sur les mécanismes de coordination entre les organisations.*

Les plans de gestion de crise médiatique et de communication constituent un élément important de la préparation à la gestion de crise et doivent être mis en place avant qu'un incident critique ou une crise ne survienne. Si les communications avec les parties prenantes internes et externes doivent être dirigées par l'équipe de gestion de crise avec le soutien d'une équipe de communication de crise, cette dernière est principalement chargée de traiter avec les médias, d'élaborer et de mettre en œuvre la stratégie de communication et de relations avec les médias, de préparer et de rédiger les communications destinées aux publics externes et internes, de surveiller les médias (y compris les réseaux sociaux) et de désigner un porte-parole.

L'équipe de communication de crise peut être composée d'un chef d'équipe, d'un porte-parole, d'un chargé du suivi des médias et de personnel de soutien. Comme pour l'équipe de gestion de crise, il est recommandé que cette équipe soit correctement formée et s'entraîne régulièrement à mettre en œuvre le plan de communication de crise et le plan média de l'organisation.

L'équipe de communication de crise assume la responsabilité des activités liées à la communication, souvent sous la direction, en collaboration ou avec l'approbation finale de l'équipe de gestion de crise, telles que la rédaction de messages clés pour différents groupes (internes et externes) et la définition d'une stratégie médiatique.

Communications au niveau du projet et du pays

En cas de crise, il peut être nécessaire d'informer rapidement un grand nombre de personnes et d'organisations. Plutôt que de confier cette tâche à une seule personne, les organisations peuvent mettre en place un réseau ou une chaîne de communication dans laquelle chaque « nœud » est chargé de transmettre les informations à trois ou quatre autres nœuds. Pour ce faire, le plus simple est d'utiliser l'organigramme du personnel. Celui-ci peut être mis à jour régulièrement à intervalles prédéfinis afin que les noms et coordonnées soient exacts et immédiatement modifiés en cas de changement de personnel. Il est également possible de préciser à l'avance si les communications se feront par téléphone, SMS ou radio. Un système de gardes, s'il existe, peut être intégré à ce dispositif. En cas d'urgence, les réseaux de communication nationaux sont susceptibles de tomber en panne ou d'être saturés : dans la mesure du possible, l'organisation doit prévoir des moyens de communication alternatifs indépendants de l'infrastructure nationale.

Si l'incident remet en cause la poursuite des activités du programme, voire la présence continue de l'organisation sur le site, il peut être nécessaire de communiquer avec les communautés touchées, les principales parties prenantes (par exemple les autorités), le grand public et les principaux donateurs.

Communication entre les équipes organisationnelles et les bureaux

Une communication fiable, dédiée, dotée de ressources suffisantes, disponible 24 heures sur 24 et sécurisée est souvent nécessaire entre le site touché et les différentes équipes de gestion de crise. Il est conseillé d'anticiper une perte temporaire des communications et de s'y préparer en conséquence. Une aide à la traduction peut être nécessaire s'il existe des différences linguistiques entre les parties prenantes et les équipes. Il est important de contrôler les rumeurs au sein de l'organisation, car les spéculations risquent d'être nombreuses et exprimées de multiples façons, par exemple sur les réseaux sociaux, les applications de messagerie et les e-mails. Une communication interne efficace avec les autres membres du personnel de l'organisation doit être proactive et bien gérée. Il est conseillé aux organisations d'anticiper les questions et de maintenir le moral et la confiance du

personnel dans l'organisation, tout en essayant de tenir les employés non essentiels à l'écart des efforts de gestion de crise.

La communication peut impliquer :

- Des séances d'information régulières ou ponctuelles pour l'ensemble du personnel, animées par le responsable de l'équipe de gestion de crise.
- Une fiche d'information accessible à l'ensemble du personnel (en plusieurs langues si nécessaire) et publiée sur l'intranet ou via un autre moyen de communication.
- Offrir au personnel la possibilité de se sentir impliqué et de manifester son soutien aux collègues concernés, par exemple en signant des messages de soutien. Une fois les incidents résolus, les membres du personnel concernés semblent apprécier ces efforts.

En cas d'incident grave ou de crise, les membres du conseil d'administration de l'organisation peuvent avoir besoin d'être tenus informés et consultés sur les décisions critiques.

Communication avec les médias

Les incidents graves touchant un membre du personnel (décès ou blessure, par exemple) nécessitent généralement d'informer immédiatement la famille, puis de publier une déclaration ou un communiqué de presse rédigé par la direction. Parfois, cette notification est effectuée par d'autres entités, telles que l'ambassade ou les autorités locales. Dans ce cas, l'organisation doit essayer de contacter la famille dès que possible. Une conférence de presse peut également être organisée ou un communiqué de presse publié.

Les organisations doivent disposer d'un plan média préparé à l'avance qui puisse informer la stratégie médiatique adoptée pour une crise ou un incident critique particulier. Les organisations peuvent désigner à l'avance les personnes qui s'adresseront aux médias (il peut s'agir d'un porte-parole désigné) et leur proposer une formation. Le porte-parole travaille en étroite collaboration avec l'équipe de gestion de crise, même s'il n'en fait généralement pas officiellement partie. Il est toutefois recommandé que ces personnes participent à la formation dispensée à l'équipe de gestion de crise.

Il peut être nécessaire de communiquer avec les médias locaux, nationaux et internationaux, et d'être prêt à répondre lorsqu'ils contactent l'organisation. Il est important que les organisations soient au courant des discussions qui ont lieu sur les réseaux sociaux au sujet des incidents et du personnel concerné. Les influenceurs des réseaux sociaux peuvent publier du contenu sur des cas très médiatisés, et l'équipe chargée des relations avec les médias de l'organisation peut être amenée à surveiller ces plateformes et à se tenir prête à réagir si nécessaire. Les organisations qui ne

comptent pas de professionnels des médias parmi leur personnel peuvent solliciter des conseils professionnels à l'extérieur.

Dans certaines circonstances, il peut être approprié de publier une déclaration sur le site Web, l'intranet et les plateformes de médias sociaux pertinentes de l'organisation. Compte tenu de la prolifération des informations, il convient de noter que toute déclaration rendue publique peut avoir une portée mondiale. Les communications partagées avec le personnel peuvent être divulguées aux médias. En règle générale, l'identité des membres du personnel concernés doit toujours rester confidentielle. Au sein de l'organisation, il convient de préciser quelles informations doivent rester confidentielles, qui fait partie du cercle d'information et comment la confidentialité sera protégée.

Considérations relatives aux médias sociaux

Les communications diffusées sur les plateformes de médias sociaux peuvent susciter des sentiments très négatifs à la suite d'un incident. Par exemple, après l'attaque meurtrière contre deux employés d'une ONG internationale au Burkina Faso en 2023, une analyse des réactions sur les réseaux sociaux a révélé une incompréhension et une négativité généralisées à l'égard de l'organisation et du travail humanitaire en général. Plusieurs commentateurs ont accusé l'organisation de collaborer avec des groupes armés et de servir de mandataire aux gouvernements occidentaux. L'intention publiquement exprimée par l'organisation (le jour de l'incident) d'engager le dialogue avec toutes les parties au conflit a suscité de vives réactions sur les réseaux sociaux, de nombreux commentaires interprétant cette initiative comme une tentative de légitimer les groupes armés islamistes.

Le suivi des réseaux sociaux pour évaluer le sentiment local à l'égard des organisations humanitaires est un aspect de plus en plus important pour mesurer les perceptions locales, l'acceptation du travail humanitaire en contextes opérationnels et la gestion des risques de sécurité. Ce type de suivi est encore plus important en cas de crise ou d'incident critique. Certaines organisations investissent directement dans ce travail de suivi, tandis que d'autres s'appuient sur des sources publiques (par exemple, les rapports de suivi des réseaux sociaux de Insecurity Insight: <https://insecurityinsight.org/projects/aid-in-danger/social-media-monitoring>).

Source : Insecurity Insight (2023) 'MSF ambush in Burkina Faso' (en anglais, « Embuscade contre MSF au Burkina Faso ») (<https://insecurityinsight.org/wp-content/uploads/2023/03/MSF-attack-Burkina-Faso-Social-Media-Monitoring-March-2023.pdf>).

L'objectif principal de toutes les activités médiatiques devrait être de protéger le personnel concerné ; dans certains cas d'incident critique, cela peut signifier faire profil bas, mais dans d'autres, cela peut signifier accroître la visibilité médiatique de manière soigneusement contrôlée. Dans certains cas d'incident critique, tels que les enlèvements, l'objectif principal de l'auteur peut être d'attirer l'attention des médias. Dans certains contextes, les médias ne sont pas autorisés à publier des détails sur les cas de violence sexuelle, et même lorsque cela n'est pas interdit, si l'identité des personnes survivantes est divulguée, celles-ci risquent d'être stigmatisées ou de subir une victimisation supplémentaire.

Communications avec les voisins et d'autres organisations

Si le bureau de l'organisation a été attaqué, par exemple, il est conseillé de parler aux voisins, dont le sentiment d'insécurité a probablement été exacerbé. Il peut également être nécessaire d'alerter d'autres organisations humanitaires sur un incident de sécurité majeur, afin qu'elles puissent prendre des mesures de précaution.

Liaison familiale et soutien aux familles

La liaison familiale et le soutien aux familles des membres du personnel concernés sont des éléments essentiels de la gestion d'un incident. Il s'agit essentiellement de veiller à ce que la famille ait l'assurance que la situation dans laquelle se trouve leur proche est bien gérée par l'organisation. Il s'agit non seulement d'un aspect important du devoir de diligence, mais le non-respect de cette obligation pourrait également compromettre les efforts de gestion de crise de l'organisation. Les membres de la famille qui n'ont pas confiance dans la réponse apportée par l'organisation peuvent, par exemple, s'adresser aux médias ou se rendre dans la zone de crise avec leurs propres plans. Bien que ces actions ne soient pas problématiques en soi (il peut parfois être souhaitable que les membres de la famille fassent des déclarations ou que l'organisation facilite leur présence sur place), des actions non coordonnées peuvent interférer avec le plan de gestion de crise de l'organisation. En 2017, l'European Interagency Security Forum (désormais GISF) a élaboré *La Famille avant tout*, un guide détaillé sur la liaison avec les familles et le soutien à leur apporter lors d'incidents critiques et de crises.⁷⁶ La section suivante traite de quelques considérations fondamentales.

Dans un premier temps, une organisation doit communiquer avec les familles des membres du personnel et les autres personnes touchées par un incident. Tout doit être mis en œuvre pour que la famille des membres du personnel concernés soient les premiers informés d'un incident. Il est recommandé de ne publier aucun message ni aucune déclaration avant que les membres de la famille aient été informés directement par le personnel de l'organisation.

L'équipe de communication de crise peut travailler avec le personnel de liaison familiale afin de soutenir les membres de la famille qui pourraient souffrir de l'intrusion des médias, ce qui peut inclure la fermeture des comptes de réseaux

⁷⁶ Davidson, S. (2013) *La famille avant tout: soutien et liaison en situation de crise*. European Interagency Security Forum (www.gisf.ngo/resource/family-first/).

sociaux du personnel concerné et des membres de sa famille. Cette mesure peut également empêcher des groupes hostiles, y compris les auteurs des faits, d'accéder à des informations personnelles et de les utiliser à des fins malveillantes. Pour cela, les organisations devraient idéalement disposer de plans et, dans la mesure du possible, établir des voies de communication avec les réseaux sociaux et d'autres plateformes afin de fermer les comptes ou de supprimer les articles susceptibles de compromettre la sûreté et la vie privée du personnel concerné ou des membres de sa famille.

Le soutien aux familles peut également nécessiter une implication plus active en fonction de la nature et de la durée de l'incident. Il est également important que les organisations soient conscientes que les familles peuvent prendre elles-mêmes des initiatives, en particulier si l'incident dure longtemps. Il est important qu'elles se sentent habilitées à le faire, mais que leurs plans et leurs actions soient coordonnés autant que possible avec le plan de gestion de crise de l'organisation. Pour soutenir les membres de la famille du personnel touchés, les organisations doivent prendre en compte les éléments suivants :

- Identifier la personne à contacter en cas d'urgence et prendre note de toute circonstance personnelle susceptible d'influencer les interactions avec la famille.
- Choisir la personne chargée d'annoncer la nouvelle et le point focal pour la liaison familiale. En général, la première personne à entrer en contact avec les membres de la famille sera un membre senior de l'organisation, et le point focal pour la liaison familiale pourra ensuite apporter son soutien.
- Annoncer la nouvelle sans délai, avec franchise et compassion.
- Présenter la personne désignée comme point focal pour les membres de la famille, expliquer son rôle et comment la contacter.
- Évaluer et répondre aux besoins immédiats de la famille.
- Garantir la confidentialité et établir une relation de confiance réciproque entre la famille et l'organisation.
- Mettre en place un calendrier de contacts réguliers avec la famille.
- Gérer le flux d'informations entre l'organisation, les équipes de gestion de crise et la famille.
- Faire appel à des services et à des conseillers externes pour soutenir la famille.
- Conserver des traces écrites des communications et des décisions prises.
- Élaborer une stratégie de sortie, par exemple, après la résolution de l'incident ou si l'incident n'est jamais résolu.

Un membre du personnel formé et doté de bonnes compétences interpersonnelles peut être désigné comme point focal pour la famille. La personne choisie doit être capable de communiquer avec la famille dans sa langue et être acceptée et

considérée comme digne de confiance par celle-ci. Certaines organisations ont un poste de liaison avec les familles (parfois appelé «agent de liaison familiale») spécialement prévu pour ce type de situation, tandis que dans d'autres cas, il peut s'agir d'une personne déjà connue de la famille, comme le supérieur hiérarchique du membre du personnel concerné, qui est lui-même soutenu par un agent de liaison familiale formé à cet effet. Lorsque les organisations ne disposent pas d'un poste spécifique à cet effet, il est recommandé de former au moins un ou deux membres du personnel à la liaison familiale afin qu'ils puissent assumer ce rôle en cas d'incident. L'une des fonctions de ce poste consiste à agir en tant que point de contact désigné pour la famille (lorsque plusieurs personnes ont été enlevées, il peut être nécessaire de désigner plusieurs personnes pour agir en tant qu'interlocuteurs avec les familles touchées). Dans l'idéal, la même personne devrait jouer ce rôle tout au long de l'incident, même si, dans la pratique, cela peut s'avérer difficile dans le cas d'incidents de longue durée. Il s'agit d'une responsabilité exigeante qui nécessite souvent le soutien de l'organisation.

La personne chargée de la liaison familiale ne fait généralement pas partie officiellement de l'équipe de gestion de crise, mais elle doit connaître la structure et les méthodes de travail de l'équipe et rester en contact régulier avec elle. Cependant, elle ne doit pas être impliquée dans la gestion opérationnelle quotidienne de l'incident ou de la crise, ce qui lui permet de se concentrer pleinement sur le soutien aux familles. Les tâches d'un point focal pour la liaison familiale peuvent comprendre:

- Agir en tant que seul canal de communication entre l'organisation et la famille.
- Établir et maintenir un contact régulier avec la famille, y compris être joignable à tout moment en cas d'enlèvement ou d'enlèvement contre rançon.
- Guider la famille sur la conduite à tenir si elle est approchée par les médias ou les auteurs (par exemple, les auteurs d'un enlèvement).
- Partager les informations, les recommandations et le soutien d'autres équipes, telles que l'équipe de communication de crise.
- Organiser le paiement des salaires et d'autres formes d'aide à la famille.
- Assurer la liaison avec d'autres personnes, le cas échéant.

Les circonstances personnelles peuvent nécessiter davantage de tact et de sensibilité dans la liaison avec les membres de la famille. Les cellules familiales peuvent prendre diverses formes et structures. Dans certaines situations, une famille peut être divisée ou séparée. De plus, il arrive que le partenaire sentimental d'un membre du personnel ne soit pas connu ou reconnu par ses proches. Les relations et les dynamiques familiales peuvent être complexes et non traditionnelles, s'écartant des normes conventionnelles. Il est impératif que le personnel chargé de la liaison familiale tienne compte des souhaits et des besoins du personnel touché. Certains membres du personnel, par exemple, peuvent ne pas souhaiter que leur famille soit informée de certains incidents, tels que des violences sexuelles. D'autres peuvent souhaiter

que certaines informations personnelles, telles que leur orientation sexuelle ou leurs antécédents médicaux, ne soient pas divulguées à leur famille. Les organisations doivent disposer d'informations sur les personnes à contacter en cas d'urgence dans les dossiers du personnel, qui peuvent faire état de circonstances particulières susceptibles d'être intégrées dans le travail de liaison familiale, y compris différentes personnes à contacter en cas d'urgence pour différents types de situations.

Relations avec les autorités

Les organisations peuvent être amenées à coordonner leurs actions avec les autorités, notamment le gouvernement du pays où l'incident ou la crise se produit et, s'il est différent, le gouvernement du pays d'origine des membres du personnel touchés. Il n'est pas rare non plus que les travailleurs humanitaires soient ressortissants de différents pays, ce qui signifie qu'il peut y avoir plusieurs « pays d'origine » à prendre en considération. Divers ministères et institutions gouvernementales peuvent également être impliqués.

Il peut être nécessaire de conclure des accords et de collaborer avec les autorités afin d'accélérer le traitement des demandes de visa pour le personnel de soutien en cas de crise ou pour d'autres personnels d'urgence. Les gouvernements peuvent mobiliser leurs propres experts en fonction du type d'incident et de la nationalité des personnes touchées. Cela peut créer une situation difficile en termes de responsabilité et de devoir de diligence. Si une autre entité prend les devants, les organisations peuvent défendre ce qu'elles considèrent comme étant dans le meilleur intérêt des personnes touchées, en espérant que cela corresponde aux souhaits de la famille. Il est possible d'anticiper cela en demandant aux responsables gouvernementaux concernés les mesures qu'ils prévoient de prendre en cas d'incident particulier.

Considérations administratives, juridiques et financières

Certaines situations peuvent nécessiter des conseils juridiques. Ces conseils peuvent porter sur les clauses contractuelles, les avantages sociaux, les questions d'assurance, les droits prévus par le droit du travail applicable, la représentation juridique auprès d'un gouvernement hôte ou d'origine, ou encore le traitement des contestations judiciaires et des demandes de dommages-intérêts.

La gestion d'un incident critique ou d'une crise, en particulier lorsqu'elle se prolonge, nécessite également un soutien administratif et des ressources humaines spécialisées. Il peut y avoir d'autres dépenses urgentes liées aux déplacements, à l'équipement ou aux services externes. Le personnel touché peut être temporairement incapable de travailler en raison d'une blessure physique ou d'un stress psychologique, et il peut être nécessaire de faire appel à des remplaçants temporaires et de fournir un soutien au bien-être. Les organisations peuvent avoir besoin de liquidités supplémentaires en raison de dépenses imprévues et non budgétisées, notamment dans le cadre de la mise en œuvre de la stratégie de réponse à la crise. Certaines de ces dépenses peuvent être couvertes par l'assurance de l'organisation.

► Pour en savoir plus sur l'assurance et le bien-être du personnel, voir le chapitre 5.4.

Gestion post-incident

Désactivation de la réponse de gestion de crise

Il arrive un moment où la structure de gestion de crise est dissoute, souvent lorsqu'un incident est considéré comme « résolu », par exemple lorsque les personnes touchées par un événement ne sont plus en danger et ont reçu le soutien nécessaire. Il se peut toutefois qu'il n'y ait pas de résolution claire, comme dans le cas de membres du personnel disparus ou enlevés. Ces types d'incidents peuvent durer plusieurs années, et une organisation peut décider de désactiver la réponse à la crise même en l'absence de résolution. Les organisations doivent disposer d'un processus clair pour décider quand et comment désactiver et dissoudre les équipes de gestion de crise.

Prise en charge post-incident du personnel

La prise en charge des personnes touchées peut se prolonger au-delà de la réponse de crise mise en place par l'organisation. Les organisations peuvent avoir besoin de se préparer à fournir un soutien à long terme au personnel et aux autres personnes touchées par un événement.

À la suite d'un événement, le personnel touché peut avoir besoin d'un soutien de plusieurs façons, notamment :

- Accueil à la libération sous la responsabilité de l'organisation (en cas de détention, d'arrestation ou d'enlèvement).
- Prise en charge médicale et psychologique immédiate.
- Un soutien matériel immédiat, tel qu'un logement et d'autres équipements destinés à assurer son confort et son bien-être.
- Aide à la relocalisation ou à l'évacuation.
- Aide à la réunification de la famille.
- Gestion de la communication après la résolution de l'incident, conformément aux souhaits du membre du personnel touché, ce qui peut inclure des recommandations sur la manière de traiter les demandes des médias.
- Plan de retour au travail.
- Recommandations sur l'accès aux services de soutien, notamment les assurances et la prise en charge médicale et psychosociale à long terme.
- Recommandations sur la manière d'obtenir justice contre les auteurs.

Les personnes impliquées dans la gestion de l'incident ou autrement touchées par celui-ci (comme les membres de l'équipe du membre du personnel concerné), y compris leur famille, peuvent également avoir besoin d'un soutien à la suite d'un incident grave.

Une approche centrée sur la personne survivante permettra de s'assurer que le membre du personnel touché se sente capable de prendre ses propres décisions

concernant son rétablissement, tout en veillant à ne pas le submerger d'informations ou de choix trop nombreux, et en tenant compte de ses souhaits et de ses capacités (qui peuvent évoluer avec le temps).

- *Pour en savoir plus sur l'approche centrée sur la personne survivante, la prise en charge post-incident du personnel et l'assurance, voir le chapitre 5.4 sur le bien-être du personnel.*

Débriefing et examen a posteriori

Toutes les personnes directement impliquées dans la gestion de l'incident ou de la crise doivent avoir la possibilité de participer à un débriefing factuel. Cela peut également inclure des personnes qui étaient proches de la situation, mais qui n'ont pas été directement impliquées dans sa gestion. Toute crise, incident ou quasi-incident touchant l'organisation, ses programmes, ses partenaires ou ses sous-traitants mérite d'être analysé, et un examen a posteriori (parfois appelé examen post-incident) est largement considéré comme une bonne pratique. Pour les événements graves, les organisations peuvent envisager une évaluation plus approfondie et, idéalement, indépendante des raisons pour lesquelles la situation s'est produite, de la manière dont elle a été gérée et des raisons pour lesquelles elle a eu l'impact qu'elle a eu. À la suite de tout événement grave lié à la sécurité, il convient de procéder à un examen des politiques et procédures existantes en matière de sécurité et de sûreté.

Les questions clés à prendre en compte sont les suivantes :

- Les mesures de sécurité étaient-elles en place et comprises par le personnel ?
- Les mesures de sécurité ont-elles été respectées ?
- Les mesures de sécurité étaient-elles adaptées à la menace ?
- Des signes avant-coureurs d'une menace spécifique imminente ont-ils été observés et, si oui, ont-ils été pris en compte avant l'événement ?
- À l'inverse, n'y avait-il aucun signe avant-coureur, rendant l'événement imprévisible ?
- Le risque d'une menace spécifique avait-il été évalué avec précision et des mesures de sécurité appropriées avaient-elles été mises en place, mais l'événement s'est tout de même produit ?
- Les équipes de gestion de crise avaient-elles été préalablement identifiées et préparées ?

En substance, les organisations doivent s'efforcer de déterminer si l'analyse des risques et les stratégies d'atténuation des risques mises en œuvre présentaient des faiblesses ou des problèmes de conformité. Il est également recommandé de procéder à un examen du mécanisme de réponse aux crises afin que l'organisation

puisse apporter les ajustements nécessaires en vue de se préparer à d'éventuels incidents critiques ou crises futurs.

Il est important que les débriefings et les examens a posteriori soient menés avec tact et centrés sur les personnes survivantes. Cela implique de réfléchir aux informations qui peuvent être divulguées lors de ces sessions, notamment en ce qui concerne la violence physique et la violence sexuelle, par exemple, et à la manière dont celles-ci doivent être gérées et signalées.

Tout incident grave touchant une autre organisation opérant dans le même environnement mérite également attention et analyse. Cette analyse n'aboutira pas nécessairement à la conclusion que l'organisation est exposée à un risque accru. Il peut y avoir diverses raisons pour lesquelles ce qui est arrivé à une organisation a peu de chances d'arriver à une autre. Les capacités à mener une analyse raisonnable d'un incident touchant une autre organisation peut dépendre de la quantité d'informations fiables pouvant être obtenues.

Il est impératif que, si l'analyse post-crise indique des mesures de suivi (telles que des formations supplémentaires ou des modifications de l'analyse des risques et des procédures de sécurité), un plan d'action soit élaboré et un mécanisme de mise en œuvre (avec des responsabilités claires) soit mis en place pour garantir que les changements soient apportés. Dans de nombreux cas, le plan d'action n'est pas correctement mis en œuvre après la dissolution de l'équipe de gestion de crise et le retour de ses membres à leurs tâches habituelles. Les conclusions de l'examen a posteriori devraient idéalement être partagées avec le personnel, éventuellement avec différents niveaux de détail en fonction du degré d'implication dans l'incident. Les informations peuvent être transmises à d'autres organisations si elles les concernent, mais elles doivent être communiquées de manière à ne pas compromettre le personnel touché.

Révision du seuil de risque acceptable

Tout événement grave de sécurité, qu'il touche directement ou non une organisation, devrait généralement déclencher une révision du seuil de risque acceptable de cette organisation. Si l'incident implique des partenaires, l'organisation peut examiner si son exposition au risque est acceptable. Cet événement signifie-t-il que l'analyse initiale était erronée ? Indique-t-il que l'organisation a dépassé son seuil de risque acceptable ? Quelles en sont les conséquences pratiques ? Les mesures de sécurité peuvent-elles être renforcées afin de réduire le risque ? La stratégie de sécurité opérationnelle devrait-elle être modifiée, et ces modifications seront-elles efficaces ? Le personnel devrait-il être relocalisé hors des zones à haut risque ? Si des ajustements ou des changements sont nécessaires, du personnel doit être affecté à la mise en œuvre de ces changements et un calendrier doit être établi. Cela peut nécessiter une formation nouvelle ou supplémentaire.

C'est le moment opportun pour communiquer à l'ensemble du personnel la nouvelle évaluation de la situation en matière de sécurité, de la nature et du niveau de risque, ainsi que de l'efficacité probable des mesures de sécurité mises en place par l'organisation. Cela permet également d'informer le personnel de tout changement dans la situation/le contexte et de revoir les seuils de risque individuels.

Informations complémentaires

Recommandations et ressources

Bickley, S. (2017) *Gestion du risque sécurité: manuel de référence à l'attention des petites ONG*. European Interagency Security Forum (<https://gisf.ngo/resource/security-risk-management-a-basic-guide-for-smaller-ngos/>).

Buth, P. (2010) *Crisis management of critical incidents (en anglais, «Gestion de crise des incidents critiques»)*. European Interagency Security Forum (<https://gisfprod.wpengine.com/resource/crisis-management-of-critical-incidents/>).

Davidson, S. (2013a) *La famille avant tout: soutien et liaison en situation de crise*. European Interagency Security Forum (www.gisf.ngo/resource/family-first/).

Davidson, S. (2013b) *Gérer le message: gestion de la communication et des médias en cas de crise de sécurité*. European Interagency Security Forum (www.gisf.ngo/resource/managing-the-message/).

European Interagency Security Forum (2017) *Abduction and kidnap risk management (en anglais, «Gestion de risque en cas d'enlèvement et d'enlèvement contre rançon»)* (www.gisf.ngo/resource/abduction-and-kidnap-risk-management-guide/).

GISF (2021) *GISF – Remote crisis management course (en anglais, «GISF – Cours à distance sur la gestion de crise»)* (www.gisf.ngo/resource/gisf-remote-field-crisis-management-course/).

GISF (2022) *NGO security collaboration guide (en anglais, «Guide de collaboration en matière de sécurité des ONG»)* (<https://gisf.ngo/long-read/ngo-security-collaboration-guide/>).

GISF et Overseas Security Advisory Council (OSAC) (2023) *NGO crisis management exercise manual: a guide to developing and facilitating effective exercises (en anglais et en espagnol, «Manuel d'exercices de gestion de crise pour les ONG: guide pour élaborer et animer des exercices efficaces»)* (<https://gisf.ngo/resource/ngo-crisis-management-exercise-manual-a-guide-to-developing-and-facilitating-effective-exercises/>).

Insecurity Insight (n.d.a) *La gestion des informations sur les incidents de sécurité (GIIS)*. (<https://siim.insecurityinsight.org/>).

RedR UK, Insecurity Insight et European Interagency Security Forum (2017) *Manuel de la gestion de l'information en cas d'incident de sécurité (GIIS)* (<https://siim.insecurityinsight.org/tools-and-resources/handbook-guide-and-tools>).

Bases de données publiques sur les incidents de sécurité (en anglais)

Humanitarian Outcomes (n.d.) *Base de données sur la sécurité des travailleurs humanitaires (en anglais)* (www.aidworkersecurity.org/).

Insecurity Insight (n.d.b) *Aid in danger (en anglais, «Aide en danger»)* (<https://insecurityinsight.org/projects/aid-in-danger>).

Insecurity Insight (n.d.c) *Social media monitoring (en anglais, «Suivi des réseaux sociaux»)* (<https://insecurityinsight.org/projects/aid-in-danger/social-media-monitoring>).

INSO (n.d.) *Humanitarian Data Dashboard (en anglais, «Tableau de bord des données humanitaires»)* (<https://ngosafety.org/ngo-data-dashboard/>).

5 Les personnes engagées dans la gestion des risques de sécurité

5.1 Ressources humaines

La gestion des risques de sécurité dans le secteur humanitaire est une fonction multiforme qui implique un large éventail d'interactions à plusieurs niveaux et nécessite toute une gamme de compétences techniques, interpersonnelles et analytiques. Ce chapitre décrit l'évolution des profils, des qualifications, des compétences et des rôles des personnes qui gèrent la sécurité d'une organisation, ainsi que la manière dont la sécurité peut et doit influencer sur la gestion du personnel, depuis le recrutement jusqu'à la fin des contrats.

5.1.1 Évolutions de la fonction de gestion des risques de sécurité

Au fil des décennies, la gestion des risques de sécurité dans le secteur humanitaire a évolué, tout comme le corps de professionnels qui occupent aujourd'hui des postes dans la gestion des risques de sécurité. Le passage d'approches hautement protectrices, inspirées des modèles militaires et d'application de la loi, à des approches plus intégrées, axées sur la facilitation de l'action humanitaire, a donné naissance à un nouveau domaine professionnel : la sécurité humanitaire. Dans cette discipline émergente, les professionnels sont de plus en plus appréciés pour leur combinaison de compétences traditionnelles en matière de sécurité et leur compréhension de la programmation et des principes humanitaires.

Parmi les autres évolutions qui ont influencé le profil et les compétences du personnel de sécurité humanitaire, citons les défis liés à l'appétence au risque et aux seuils de risque plus élevés de certaines organisations, ainsi que la nécessité de développer des compétences en interne pour pouvoir travailler dans des environnements à menaces multiples et à haut risque, et gérer les situations de crise. Le recours plus fréquent à des partenariats avec d'autres organisations, ainsi que le renforcement de la collaboration en matière de sécurité en contextes de réponse, exigent des capacités à coordonner et à assurer la liaison entre un large éventail d'entités. En outre, le personnel de sécurité humanitaire est constamment confronté aux technologies émergentes, qui constituent à la fois des menaces potentielles pour la sécurité et des outils de gestion des risques de sécurité.

Enfin, les fonctions de gestion des risques de sécurité accordent de plus en plus d'importance aux compétences interpersonnelles et au leadership adaptatif, à mesure que les équipes deviennent plus diversifiées et inclusives et que les stratégies de sécurité se concentrent de plus en plus sur la sécurité centrée sur la personne et les facteurs de risque liés à l'identité.

► Voir le chapitre 1.1 pour plus d'informations sur la mise en place d'une culture de la sécurité positive.

5.1.2 Personnes occupant des fonctions dans la gestion des risques de sécurité

La gestion des risques de sécurité est façonnée par les structures générales et les politiques décisionnelles de l'organisation. Une petite organisation opérant dans une seule localité peut avoir un seul point focal pour les questions de sécurité. À l'inverse, une grande organisation internationale peut déployer des équipes de sécurité multinationales aux niveaux mondial, régional, national et infranational. Les rôles et responsabilités de ces professionnels peuvent varier, mais la plupart jouent des rôles techniques et consultatifs axés sur le soutien à la direction, avec une autorité décisionnelle limitée. Par exemple :

- Dans le cas des organisations internationales, un directeur principal de la sécurité, basé au niveau mondial, qui conseille la direction exécutive de l'organisation et supervise l'élaboration et la mise en œuvre des politiques de sécurité dans l'ensemble de l'organisation.
- Pour les organisations internationales, un conseiller et/ou une équipe de sécurité au niveau régional fournissant un soutien opérationnel en matière de gestion des risques de sécurité, des conseils techniques et une supervision des programmes de pays.
- Un point focal pour les questions de sécurité et/ou une équipe de sécurité au niveau du pays qui conseille la direction du pays et supervise la gestion des risques de sécurité - pour les organisations nationales, il s'agirait de leur siège social et de leur personnel de sécurité le plus expérimenté.
- Les points focaux pour les questions de sécurité au niveau local, dans les différents sites du programme, gèrent les incidents de sécurité et assurent les activités quotidiennes de gestion des risques de sécurité.

Selon l'organisation, ces postes peuvent porter différents titres, notamment directeur, conseiller, manager, coordinateur, agent ou point focal de la sécurité.

Il est important de souligner qu'il existe une grande diversité dans la manière dont les organisations structurent et mettent en œuvre leur gestion des risques de sécurité. Dans certains cas, cette responsabilité est intégrée dans les fonctions de gestion courantes et il n'existe pas de fonction distincte dédiée à la sécurité. Dans d'autres, l'autorité décisionnelle en matière de sécurité relève des fonctions de sécurité. D'autres organisations peuvent disposer, en complément ou à la place, de groupes de travail sur la sécurité, au sein desquels différentes fonctions se partagent les responsabilités en matière de gestion des risques de sécurité.

Pour structurer les rôles du personnel, il peut être utile de se référer au modèle «RACI»,⁷⁷ qui identifie, pour chaque domaine d'activité, la ou les personnes :

⁷⁷ Pour une analyse plus détaillée sur la manière dont le modèle RACI peut être utilisé dans la gestion des risques de sécurité, voir GISF (2024) *Développement de la stratégie et de la politique de gestion des risques de sécurité (GRS): Un guide interfonctionnel* (<https://gisf.ngo/resource/srm-strategy-and-policy-guide/>)

- **Responsable** - celui ou ceux qui mettent en œuvre le travail
- **Approbateur** - celui qui est en dernier ressort responsable de la tâche ou de la décision
- **Consulté** - ceux qui apportent leur contribution et leurs conseils
- **Informé** - ceux qui sont tenus informés des progrès ou des décisions, mais qui ne participent pas directement au travail.

Cette section présente un modèle consultatif de gestion des risques de sécurité, qui est l'un des plus courants dans le secteur humanitaire. Dans ce modèle, le personnel de sécurité est généralement responsable de la gestion des risques de sécurité, tandis que la redevabilité incombe à la direction. Remarque : bien que seule la « sécurité » soit mentionnée, dans la pratique, de nombreux rôles et responsabilités englobent à la fois la sûreté et sécurité.

► Voir le chapitre 3.1 pour plus de détails sur les structures de gouvernance et de sécurité.

Personnel cadre de sécurité

Les postes de cadre de sécurité au sein de la direction de l'organisation sont idéalement occupés par des professionnels hautement qualifiés et expérimentés dans la gestion des risques de sécurité, qui assurent la direction et assument plusieurs fonctions essentielles, notamment :

- Communiquer la vision, élaborer des politiques, des normes et des stratégies de sécurité, et créer des plans de gestion des risques de sécurité.
- Diriger les équipes et le personnel de sécurité.
- Contribuer à l'élaboration de programmes de formation à la sécurité à plusieurs niveaux.
- Mener des projets de recherche et de développement sur les tendances émergentes et les bonnes pratiques, et les intégrer dans les processus et procédures organisationnels.
- Élaborer les budgets de base consacrés à la sécurité.
- Élaborer et superviser les efforts de contrôle de la conformité et de l'efficacité en matière de sécurité.
- Représenter l'organisation dans les forums interagences mondiaux et participer à des discussions de haut niveau sur la gestion des risques de sécurité dans le secteur humanitaire.
- Rédiger des politiques de gestion de crise et participer à des équipes de gestion de crise.
- Établir des partenariats avec les parties prenantes de l'organisation afin d'intégrer la sécurité dans une approche plus large de gestion de risque organisationnelle.
- Examiner et améliorer les activités de sécurité afin de refléter l'évolution des contextes opérationnels, y compris les tendances en matière de données sur les incidents.

Certaines grandes organisations internationales ont mis en place des équipes de sécurité mondiale, dirigées par un directeur de la sécurité mondiale. Afin de répartir les responsabilités au sein de l'équipe, ces personnes peuvent couvrir différentes régions ou apporter une expertise spécifique et diriger des activités liées à cette zone, par exemple, la formation ou la sécurité de l'information.

Équipes et personnel de sécurité au niveau régional/du pays

Dans de nombreuses organisations, si la responsabilité première des décisions en matière de sécurité au niveau du pays incombe généralement au cadre senior de ce bureau (par exemple, le directeur de pays ou le directeur exécutif), les professionnels de la gestion des risques de sécurité jouent un rôle consultatif important et assument de nombreuses fonctions de gestion et de soutien, notamment :

- Conseiller les cadres seniors sur les meilleures pratiques de gestion des risques de sécurité et introduire des enseignements et des pratiques provenant d'autres contextes.
- Gérer et encadrer le personnel de sécurité moins expérimenté.
- Identifier les buts et objectifs de la gestion des risques de sécurité et élaborer des plans d'action alignés sur les plans stratégiques de l'organisation ou du programme de pays.
- Mettre en œuvre les normes, les directives, les procédures et la politique de sécurité, et veiller à leur révision et à leur respect.
- Collecter et analyser des informations afin d'identifier les tendances, d'adapter les mesures de gestion des risques de sécurité et de se préparer à d'éventuels scénarios futurs.
- Mettre en place et superviser des systèmes permettant d'enregistrer, d'analyser et de diffuser les informations en matière de sécurité ou d'incidents affectant le personnel et les opérations.
- Réaliser et examiner les évaluations des risques relatifs à la sécurité.
- Élaborer des plans, des protocoles, des procédures et des mesures visant à atténuer les risques identifiés.
- Soutenir les équipes de gestion de crise dans le traitement des incidents critiques et des situations de crise.
- Recommander et acquérir des équipements de sûreté et sécurité.
- Organiser des briefings et des formations à la sécurité.
- Représenter l'organisation dans les forums interagences sur la sécurité et les réunions de coordination aux niveaux régional/du pays.

Certaines organisations ont adopté une approche intégrée de gestion de la sécurité et des accès en combinant les deux fonctions.

- Voir le chapitre 3.2 pour une analyse plus détaillée du lien entre la gestion des risques de sécurité et les fonctions d'accès.

Dans certaines organisations internationales, il existe des conseillers ou des équipes de sécurité supplémentaires au niveau régional. Ces derniers exercent des fonctions similaires à celles énumérées ci-dessus et s'attachent principalement à conseiller la direction régionale et à soutenir les efforts déployés par les équipes de pays dans la région en matière de gestion des risques de sécurité.

Points focaux au niveau des bureaux locaux

Au niveau des bureaux locaux, les environnements à haut risque de sécurité justifient généralement la présence d'un membre du personnel de sécurité à temps plein. Dans les environnements à risque faible ou modéré, un point focal non dédié aux questions de sécurité peut remplir cette fonction en plus d'autres responsabilités (par exemple, administratives, logistiques ou RH). Cette personne gère généralement les tâches quotidiennes liées à la sécurité. Au niveau du bureau de pays et du bureau local, les responsabilités en matière de sûreté incombent généralement aussi aux points focaux pour les questions de sécurité.

La description de poste d'un point focal pour les questions de sécurité au niveau du bureau local peut inclure :

- Réaliser une analyse des risques liés à l'environnement opérationnel et envoyer des alertes de sécurité au personnel concerné.
- Contribuer à l'élaboration de stratégies d'atténuation des risques de sécurité, notamment des procédures opérationnelles standards, des directives et des plans d'urgence.
- Informer les nouveaux arrivants.
- Veiller à ce que l'ensemble du personnel du site soit tenu informé de l'évolution des conditions de sécurité.
- Signaler les incidents de sûreté et sécurité.
- Donner des conseils et gérer les équipements et fournitures de sécurité et de communication.
- Veiller au respect des procédures et des plans et signaler les violations ou les écarts en matière de sécurité.
- Gérer le personnel chargé de la sécurité, tel que les gardes, les opérateurs radio et autres points focaux pour les questions de sécurité.
- Former et encadrer les collègues afin de développer leurs compétences en matière de sécurité.
- Participer à l'élaboration du budget des dépenses de sécurité opérationnelle.
- Participer à la réponse aux incidents et à la gestion de crise, ainsi qu'aux analyses et examens a posteriori.
- Assurer la liaison et échanger des informations avec d'autres organisations humanitaires et les autorités.

Le point focal pour les questions de sécurité n'a pas nécessairement à assumer seul la responsabilité de la gestion des risques de sécurité. Une approche collective de la gestion de la sécurité est souvent bénéfique. Cela permet à un groupe de points focaux de gérer la charge de travail, de partager les procédures et plans de sécurité, et d'instaurer une culture de la sécurité positive au sein d'un site. Dans certaines organisations, un comité local de sécurité soutient le point focal et la sécurité est un sujet récurrent à l'ordre du jour des réunions programmatiques et opérationnelles.

5.1.3 Attributs et compétences clés

Profils, aptitudes et qualifications

Les compétences en sécurité peuvent être classées en deux grandes catégories : les compétences « techniques » et les compétences « non techniques ». Les compétences techniques font référence aux aspects plus techniques et opérationnels de la sécurité, tels que la manipulation des équipements de sécurité, la protection physique et les tactiques. Ces compétences sont souvent associées à une formation dans l'armée, la police ou les services de renseignement, où les individus ont pu acquérir des connaissances sur les armes, les tactiques militaires, les opérations policières et la lutte antiterroriste. Les compétences techniques peuvent également inclure des compétences en matière d'enquête ainsi que l'analyse des menaces et des risques.

Les compétences non techniques concernent les aptitudes interpersonnelles, telles que la compréhension des dynamiques sociales et culturelles, le travail au sein d'une équipe multiculturelle, ainsi que les compétences en matière de leadership, de mentorat et de formation, l'établissement de relations, la communication et la gestion. Dans le domaine de la gestion des risques de sécurité humanitaire, elles comprennent également une bonne compréhension des objectifs du programme, des mandats de l'organisation et des principes humanitaires. Compte tenu de la complexité des acteurs et des parties prenantes en contextes humanitaires, il est également nécessaire de créer et de maintenir des réseaux avec diverses communautés et d'être capable de comprendre et d'analyser différents contextes culturels, sociaux, géopolitiques et environnementaux, notamment les zones touchées par des conflits violents.

Ces dernières années, à mesure que la valeur des compétences non techniques et la reconnaissance des approches de sécurité fondées sur l'acceptation ont gagné en popularité, le profil et les compétences du personnel de sécurité ont évolué. Un professionnel de la gestion des risques de sécurité, doté à la fois de compétences techniques et interpersonnelles, et d'une solide expérience dans le secteur humanitaire, est le plus souvent le profil recherché. Cependant, la disponibilité de ces personnes peut être limitée dans de nombreux endroits. Pour remédier à cela, certaines organisations cherchent à renforcer leurs capacités internes en matière de sécurité en formant leur personnel actuel à des fonctions de sécurité. De plus en plus de membres du personnel se tournent vers la formation, les diplômes et les certifications pour développer leurs compétences et leurs connaissances, et démontrer leurs aptitudes.

► Pour quelques exemples de ressources de formation et de certifications, voir le chapitre 5.2.

Les aptitudes et compétences requises d'un professionnel de la gestion des risques de sécurité peuvent dépendre du type et du mandat de l'organisation, ainsi que du travail à accomplir. Elles peuvent également dépendre du contexte dans lequel l'organisation opère. Par exemple, dans un environnement marqué par un conflit actif et la présence de multiples acteurs militaires, où des mesures de protection et de dissuasion plus importantes sont nécessaires, des compétences techniques plus pointues et des connaissances militaires peuvent s'avérer utiles. Dans un environnement caractérisé par des problèmes socio-économiques et des dynamiques tribales, où la négociation de l'accès et la recherche de l'acceptation constituent les principales approches de gestion des risques de sécurité, une connaissance approfondie du contexte et de solides compétences interpersonnelles peuvent s'avérer nécessaires. Les contextes à forte criminalité peuvent exiger un éventail complet de compétences et d'aptitudes, notamment une expertise en sociologie, en criminologie et en gestion de la criminalité. Dans les bureaux ou les lieux où le respect des procédures de sécurité par le personnel s'avère particulièrement difficile, il peut être judicieux de recruter une personne qui soit proche du personnel (par sa nature, son parcours et ses caractéristiques personnelles) et qui possède de solides compétences interpersonnelles, ce qui lui permettra d'encourager un meilleur respect des protocoles de sécurité.

Pour les organisations internationales, il est essentiel de déterminer si un poste de sécurité doit être occupé par un ressortissant local ou étranger. Le personnel local a généralement une meilleure connaissance de l'environnement social, culturel et politique, et dispose de réseaux de contacts plus étendus. Cependant, il peut également rencontrer des difficultés s'il est perçu par certains acteurs comme étant aligné sur une partie au conflit ou affilié à des groupes locaux rivaux. Compte tenu de ses liens avec les communautés locales, il peut être plus vulnérable aux pressions exercées par les acteurs locaux. Le personnel qui n'est pas originaire du lieu peut avoir un point de vue et une perspective différents, et être mieux placé pour assurer la liaison avec toutes les parties prenantes. Il peut également manquer de connaissances locales, avoir une mauvaise compréhension de la culture et du contexte, et avoir des préjugés profondément ancrés. Le recrutement d'un membre du personnel originaire d'un pays voisin peut présenter des avantages et des défis. Même les membres du personnel originaires d'autres régions du pays peuvent être considérés et traités comme des étrangers dans certaines localités.

La sélection du personnel de sécurité doit être guidée par le contexte et les besoins spécifiques du poste, plutôt que par des profils ou des structures par défaut. À mesure que les situations évoluent et que le personnel de sécurité issu de divers horizons acquiert de nouvelles compétences, les organisations doivent rester flexibles et ouvertes à l'idée d'envisager un éventail plus large de candidats. Cette approche permet une meilleure adéquation entre les exigences du poste et les compétences croissantes au sein du vivier de talents, garantissant ainsi un recrutement plus inclusif, plus efficace et plus adaptable.

De nombreuses organisations s'efforcent d'accroître la diversité au sein de leurs équipes de sécurité, conscientes que cela peut améliorer la perception et l'engagement du personnel en matière de sécurité. Une représentation équilibrée des genres, des ethnicités et d'autres caractéristiques d'identité parmi le personnel de sécurité peut avoir des effets positifs, tels qu'une meilleure compréhension des expériences vécues par une main-d'œuvre diversifiée, une réduction des préjugés dans les évaluations des risques et les dispositifs de sécurité, et une résolution des problèmes plus innovante.

Les femmes dans la sécurité

Les femmes ont rarement occupé des postes de sécurité dans les organisations humanitaires, du moins jusqu'à récemment. La sous-représentation des femmes s'explique par plusieurs facteurs, notamment des barrières sociales et culturelles, ainsi que des perceptions négatives quant à leurs aptitudes et compétences. Ces perceptions découlent en grande partie des stéréotypes de genre et des idées rigides sur ce qui constitue un point focal pour les questions de sécurité efficace. Le nombre de femmes occupant des postes liés à la gestion des risques de sécurité dans les organisations humanitaires a toutefois considérablement augmenté ces dernières années, grâce à des politiques plus larges visant à favoriser un meilleur équilibre hommes-femmes et une représentation égale. Cela a eu de nombreux avantages, notamment une crédibilité accrue, des idées et des approches nouvelles, ainsi qu'une meilleure représentation et une meilleure compréhension des besoins en sécurité des travailleurs humanitaires femmes.

Compétences clés

Les compétences et aptitudes spécifiques des personnes occupant des fonctions de sécurité dépendent de l'organisation et du contexte, mais peuvent inclure celles énumérées dans le tableau 6.⁷⁸

Il est peu probable qu'une personne possède à elle seule toutes les compétences énumérées ici. C'est pourquoi de nombreuses organisations constituent des équipes de sécurité composées de personnes ayant des compétences diverses dans différents domaines.

78 L'INSSA a élaboré une liste des compétences fondamentales requises pour le personnel de sécurité : <https://inssa.org/certification>.

Tableau 6 Compétences clés du personnel de sécurité

Compétence	Description
Résolution de problèmes, esprit d'analyse, esprit critique et capacité d'adaptation	Capacités à analyser des situations complexes, à anticiper les risques potentiels et à élaborer des solutions efficaces afin de prendre des décisions éclairées dans des environnements dynamiques. À cela s'ajoutent des compétences en matière de gestion du changement afin d'adapter les approches et les plans de sécurité à l'évolution des menaces et aux changements organisationnels, garantissant ainsi une adaptation continue et une atténuation des risques.
Évaluation des risques et atténuation des risques	Capacités à identifier et analyser les risques de sécurité, ainsi qu'à élaborer des stratégies d'atténuation des risques.
Plan de sécurité	Capacités à élaborer des plans de sécurité, y compris des plans d'urgence.
Réponse aux incidents et gestion de crise	Maîtrise de la gestion des incidents et des crises.
Mesures de sécurité	Connaissances et capacités à mettre en œuvre des mesures de sécurité pour des menaces spécifiques ou des environnements à risque. Cela dépendra du contexte, mais peut inclure, par exemple, des mesures liées à la sécurité du site, aux menaces liées aux combats et aux risques d'enlèvement. Dans certains cas, des connaissances en premiers secours et en réponse aux traumatismes, en sécurité numérique ou des compétences en matière de détection et d'atténuation de la surveillance hostile peuvent être pertinentes.
Compétences en négociation et résolution des conflits	Compétences en négociation transactionnelle et résolution des conflits avec les collègues et les parties prenantes externes.
Compétences en communication et persuasion efficaces	Communication claire et convaincante pour transmettre les politiques de sécurité, coordonner les équipes et assurer la liaison avec les hauts responsables et les autorités et parties prenantes externes.
Travail d'équipe et collaboration	Capacités à bien travailler en équipe et à collaborer avec différents services de l'organisation.
Gestion financière et budgétaire	Compétences en gestion budgétaire pour garantir une allocation efficace des ressources afin d'atténuer les risques.
Compétences en présentation	Capacités à présenter des informations de manière claire et efficace à divers publics, notamment le personnel, les parties prenantes et les donateurs.
Gestion du cycle du projet	Comprendre les différentes phases de la gestion de projet, de la planification à l'évaluation, afin de mettre en œuvre des mesures de sécurité qui correspondent aux objectifs et au calendrier du projet.

Compétence	Description
Connaissances juridiques et réglementaires	Connaissance des lois et réglementations pertinentes afin d'assurer la conformité et d'aider les collègues à relever les défis juridiques dans différentes juridictions.
Sensibilité culturelle	Capacités à comprendre et à respecter les coutumes et les normes locales, et à adapter les efforts de sécurité en conséquence.
Technologies de l'information et de la communication (TIC)	Maîtrise des outils technologiques pour la communication sécurisée, la gestion des données et le signalement des incidents.
Maîtrise des données/analyse des données	Capacités à collecter, analyser et visualiser des données à l'aide d'outils logiciels et de technologies, qui peuvent aider, par exemple, à extraire des informations à partir d'ensembles de données afin d'identifier des tendances et de prendre des décisions fondées sur des données probantes.
Gestion des risques de l'entreprise	Connaissance approfondie des cadres et des pratiques de gestion des risques à l'échelle de l'organisation.
Compétences en formation	Capacités à renforcer les compétences et à former le personnel aux protocoles de sécurité, aux procédures d'urgence, à l'utilisation des équipements de protection et à d'autres sujets pertinents.

Bonnes pratiques en matière de communication interne

Une communication efficace est une compétence non technique essentielle à la réussite de la gestion des risques de sécurité dans les organisations. Pourtant, les professionnels de la sécurité ont souvent du mal à communiquer efficacement leur message aux autres membres de l'organisation et à susciter le changement. Le jargon technique, les explications complexes des risques et des formules, ainsi que les priorités divergentes peuvent créer des obstacles à la compréhension et à l'adhésion du personnel ne travaillant pas dans le domaine de la sécurité. Un manque d'empathie et de compréhension à l'égard du point de vue, des motivations et des défis auxquels sont confrontés les parties prenantes internes peut également constituer un obstacle à une collaboration efficace. Les dirigeants de l'organisation et le personnel non affecté à la sécurité seront probablement plus enclins à collaborer avec le personnel de sécurité qui les écoute attentivement et leur communique des solutions adaptées à leurs besoins d'une manière qu'ils comprennent.

Le personnel de sécurité peut relever les défis liés à la communication en :

- **Simplifiant le langage technique** - en évitant le jargon et les explications complexes, afin de rendre les informations plus faciles à comprendre.
- **Adaptant les messages au public** - en personnalisant la communication en fonction du niveau de compréhension et des préoccupations spécifiques du public.
- **Fournissant du contexte à l'aide d'exemples et d'anecdotes** - en utilisant des exemples concrets ou des anecdotes personnelles pour aider le personnel à comprendre pourquoi la sécurité est importante pour eux personnellement et pour leur travail.
- **Proposant des formations et en sensibilisant** - en organisant des sessions de formation ou des initiatives de sensibilisation qui clarifient la vision et les objectifs de la gestion des risques de sécurité au sein de l'organisation.
- **Maintenant une communication régulière et variée** - en utilisant différentes méthodes de communication et en partageant des mises à jour cohérentes, en soulignant les réussites pour booster le moral.
- **Faisant preuve d'empathie** - en entamant les conversations en faisant preuve d'empathie, en instaurant la confiance grâce à un dialogue ouvert et à une écoute active.
- **Encourageant la communication bidirectionnelle** - en invitant les collègues et les parties prenantes à donner leur avis afin de s'assurer qu'ils se sentent écoutés et en adaptant les stratégies en fonction de leurs contributions.
- **Utilisant la communication non verbale** - en étant attentif au langage corporel, au ton et aux expressions faciales, car ceux-ci peuvent renforcer ou entraver le message transmis.

► *Pour plus d'informations sur la communication en matière de sécurité au sein d'une organisation, voir le chapitre 5.3.*

Valeurs, principes et compétences interpersonnelles

En plus des compétences susmentionnées, le personnel occupant des fonctions liées à la sécurité peut s'appuyer sur des valeurs et des attributs tels que :

- **Apprentissage continu** - mise à jour active des connaissances et des compétences afin de rester à jour et pertinent.

- **Professionalisme** - apprécier et aspirer à la maîtrise d'un domaine professionnel et respecter les normes en matière de compétence, de diligence et d'éthique.
 - **Intelligence émotionnelle** - capacités à identifier et à gérer ses émotions, à faire preuve d'empathie envers les autres, à communiquer efficacement, à reconnaître différents points de vue et à désamorcer les conflits.
 - **Établir des relations** - interagir efficacement avec des collègues et un large éventail de réseaux externes, notamment l'ONU, d'autres organisations humanitaires, des entreprises privées, les autorités locales et le monde des affaires, en tant que sources d'informations et d'expertise.
 - **Résilience personnelle** - capacités physique, mentale et émotionnelle à supporter les problèmes et les difficultés et à s'imposer dans des situations stressantes dans des environnements changeants.
- Voir le chapitre 5.4 pour plus d'informations sur la résilience et la gestion du stress.

Remarque sur les principes humanitaires

La croyance et l'adhésion aux principes et valeurs humanitaires sont de plus en plus considérées comme une caractéristique importante d'un professionnel efficace de la gestion des risques de sécurité. La compréhension et l'adhésion à ces principes et valeurs permettent aux points focaux pour les questions de sécurité de communiquer plus efficacement avec le personnel des programmes et d'aligner les mesures de gestion des risques de sécurité sur les objectifs stratégiques globaux d'une organisation humanitaire. Il est donc conseillé de veiller à ce que le personnel de sécurité nouvellement recruté, en particulier celui qui découvre le secteur humanitaire, comprenne, adhère à ces valeurs et principes, soit capable de les appliquer et de les communiquer efficacement.

Compétences en management et leadership adaptatif

Les connaissances, l'expérience, les compétences interpersonnelles et sociales d'un manager sont essentielles pour façonner l'expérience collective d'une équipe et influencer sa réussite. Cela vaut également pour le personnel de sécurité. Un point focal pour les questions de sécurité qui cherche à apporter des changements ou à atteindre des objectifs de sécurité avec des méthodes de bulldozer, plutôt que de s'adapter et de collaborer, peut créer plus de problèmes que de solutions. Il est conseillé au personnel de sécurité d'adopter des approches collaboratives afin d'obtenir l'adhésion de tous et d'instaurer une culture de la sécurité positive, en

veillant à ce que l'objectif global soit de permettre aux collègues d'effectuer leur travail de la manière la plus sûre possible.

Le modèle de leadership adaptatif a suscité beaucoup d'intérêt ces dernières années et pourrait s'avérer particulièrement utile pour les postes de gestion des risques de sécurité. Cette approche utilise le diagnostic des problèmes, l'interruption et l'innovation pour traiter les problèmes et les obstacles dès qu'ils surviennent, ce qui est directement pertinent pour la gestion des risques dans des environnements internes et externes en constante évolution. Si une technique ou un processus ne donne pas les résultats escomptés, un leader adaptatif trouve de nouvelles stratégies qui peuvent fonctionner. Le changement adaptatif exige des leaders qu'ils communiquent efficacement aux gens ce qui reste inchangé (continuité) et ce qui doit changer. Le leadership adaptatif implique des stratégies telles que :

- Diagnostiquer et interpréter les problèmes dans une perspective globale.
- Reconnaître les pertes et en faire collectivement le deuil.
- Contrôler les niveaux de stress pour éviter de nuire au travail d'équipe et à la santé mentale des individus.
- Dépersonnaliser les conflits pour comprendre les différents points de vue.
- Déterminer activement ce qu'il faut conserver ou éliminer au sein des systèmes organisationnels.
- Encourager l'expérimentation et la prise de risque intelligente.
- Mener des évaluations rigoureuses afin d'affiner les systèmes et les processus.

5.1.4 Sécurité et gestion du personnel

La gestion du personnel est un élément essentiel de la gestion des risques de sécurité d'une organisation. Des employés satisfaits et motivés sont plus susceptibles d'être impliqués, dévoués et productifs. À l'inverse, des employés peu motivés et mécontents ont non seulement des performances médiocres sur leur lieu de travail, mais sont également susceptibles de devenir une source de risque pour l'organisation. L'une des nombreuses façons de mettre en place une équipe efficace et saine consiste à garantir un leadership et une clarté dans l'identité organisationnelle, les rôles, la communication, la prise de décision, la gestion des conflits et l'esprit d'équipe, et à créer un environnement de travail propice où les membres de l'équipe se sentent à l'aise et valorisés. Cela commence par la clarté des mandats et des contrats des employés et se poursuit à chaque étape de l'emploi d'un membre du personnel : recrutement, intégration, performances, développement et fin de contrat.⁷⁹

79 Pour plus de détails sur la manière dont la sécurité peut s'intégrer dans ces différentes phases, voir Davis, J. et al. (2020) 'Module 13, People management' in *Security to go: a risk management toolkit for humanitarian aid agencies*, 4th edition (en anglais, « Module 13, Gestion du personnel, La sécurité en pratique : boîte à outils de gestion de risque à l'attention des agences humanitaires », 4e édition). GISF (<https://gisf.ngo/resource/security-to-go/>)

La transparence et la clarté des dispositions contractuelles (par exemple, la résiliation anticipée des contrats) peuvent réduire les inquiétudes et les griefs du personnel. Il s'agit également d'un mécanisme important grâce auquel l'organisation peut clarifier le rôle de chaque membre du personnel dans le respect des règles et des recommandations en matière de sécurité. Grâce au processus RH, le personnel peut être informé des politiques, de la stratégie et de la structure de l'organisation en matière de sécurité, des responsabilités en la matière et des personnes à contacter pour obtenir du soutien. La clarté et la transparence des procédures disciplinaires, telles que les avertissements et les licenciements, sont primordiales en cas de non-respect des règles et des attentes en matière de sécurité.

Il est particulièrement important pour les organisations humanitaires de recruter les bonnes personnes. Des compétences inadéquates ou un manque de discernement peuvent non seulement nuire à l'efficacité opérationnelle, mais aussi accroître la vulnérabilité aux risques extérieurs. Il est également important que les profils de risque personnel soient pris en compte de manière proactive dans les décisions de recrutement afin de protéger le personnel, sans pour autant être indûment discriminatoires. Les offres d'emploi doivent être rédigées de manière non discriminatoire, en tenant compte des questions liées à l'identité et à l'inclusion. Lorsque certains profils personnels peuvent être exposés à un risque plus élevé que d'autres en raison du contexte et d'autres circonstances, cela peut être discuté au cours du processus de recrutement.

► Voir le chapitre 1.2 pour une analyse plus détaillée sur la manière dont les profils de risque personnel peuvent être pris en compte lors du recrutement.

La vérification pré-emploi est essentielle. Au minimum, les critères devraient viser à inclure une vérification du casier judiciaire, la présence/l'historique en ligne, la vérification des qualifications déclarées, les antécédents professionnels et une enquête sur les interruptions de plus d'un mois dans la carrière professionnelle. De nombreux donateurs internationaux exigent que les noms des membres du personnel soient vérifiés par rapport à une liste de personnes et d'entités sanctionnées, et que la preuve de cette vérification soit conservée dans les dossiers.

Les processus d'intégration peuvent préparer les nouveaux employés à l'environnement de sécurité dans lequel ils entrent. Un bon processus d'intégration tient compte de plusieurs niveaux d'orientation sur les politiques RH, la sécurité, les opérations, les programmes, la structure organisationnelle, le mandat, la mission et le niveau d'acceptation/d'appétence au risque, ainsi que le comportement personnel et son lien avec la sécurité. Cela peut inclure les implications potentielles des activités personnelles en matière de sécurité, y compris l'utilisation des médias sociaux. Dans les contextes à haut risque, il est conseillé d'organiser des briefings intensifs et des séances d'orientation sur la sécurité. L'intégration est le moment idéal pour une organisation de remplir son devoir d'informer son personnel des risques auxquels il peut être confronté et de s'assurer que celui-ci se sent à l'aise d'accepter ces risques.

► Voir le chapitre 1.1 pour plus d'informations sur le devoir d'information et sur les seuils de risque individuels.

Lorsque des employés quittent une organisation, en particulier en cas de retrait soudain, de licenciement ou de fermeture de bureau pour des raisons d'insécurité ou de financement, cela a des implications importantes en matière de sécurité. Il est essentiel de se préparer à ce type de scénarios, non seulement pour traiter le personnel de manière équitable, mais aussi pour veiller à ce que les informations en matière de sécurité soient transmises de la meilleure manière possible aux nouvelles recrues. Les défaillances dans la planification, comme celles observées lors des évacuations en Afghanistan en 2021 et au Soudan en 2023, peuvent exposer le personnel local à des risques de sécurité particulièrement élevés, mettant en évidence des défaillances éthiques et de sécurité potentiellement majeures. Des discussions précoces sur la fin des contrats et des entretiens de départ peuvent aider les organisations à conserver des connaissances précieuses, et le fait d'offrir un soutien aux employés qui quittent l'organisation peut atténuer les problèmes potentiels à venir.

Enfin, certains incidents de sécurité ont résulté d'un manque de mécanismes internes de traitement des griefs, et de nombreuses organisations négligent encore la nécessité de gérer les risques de sécurité internes. La mise en place de procédures ou de mécanismes de plainte pour le personnel offre un moyen officiel et sûr de signaler les inconduites, notamment la mauvaise gestion, la corruption, le harcèlement et les abus, sans crainte de représailles. Cela peut aider à identifier et à traiter les problèmes à un stade précoce, et favorise une culture de redevabilité et de confiance. Il s'agit également d'un élément fondamental dans la gestion des incidents de violence sexuelle touchant le personnel au sein d'une organisation.

Cela est étroitement lié à la sauvegarde, qui a fait l'objet d'une attention particulière ces dernières années dans le secteur humanitaire. La sauvegarde désigne l'ensemble des mesures prises par les organisations pour protéger les personnes, tant à l'intérieur qu'à l'extérieur de l'organisation, contre les préjudices, les abus, la négligence et l'exploitation (voir l'encadré ci-dessous).

Éléments clés de la sauvegarde

Politiques et procédures

- Politiques de sauvegarde solides qui décrivent l'engagement de l'organisation à prévenir l'exploitation sexuelle, les abus, le harcèlement et autres inconduites du personnel et du personnel associé.
- Mécanismes de signalement et procédures d'enquête clairs, confidentiels et sûrs pour traiter les préoccupations ou les incidents de sauvegarde.
- Sauvegarde intégrée dans les codes de conduite, les pratiques en matière de ressources humaines, la gestion des risques de sécurité et la conception des programmes.

Prévention

- Sélection et vérification minutieuses lors des processus de recrutement.
- Formation en sauvegarde obligatoire pour l'ensemble du personnel, des partenaires et des bénévoles.
- Sensibilisation à leurs droits et à la manière de signaler leurs préoccupations des communautés touchées.
- Évaluation et atténuation des risques de sauvegarde dans les zones couvertes par les programmes.

Réponse

- Approches centrées sur la personne survivante qui accordent la priorité aux droits, aux besoins et aux souhaits des personnes survivantes.
- Canaux de signalement confidentiels et mesures de protection des lanceurs d'alerte.
- Enquêtes équitables et rapides sur les allégations, menées par des enquêteurs qualifiés.
- Mesures de redevabilité transparentes et sanctions disciplinaires pour les cas d'inconduite avérés.

Informations complémentaires

Recherche et analyse

European Interagency Security Forum (2018) *Gérer la sécurité des travailleurs humanitaires aux profils diversifiés* (<https://gisf.ngo/resource/managing-the-security-of-aid-workers-with-diverse-profiles/>).

GISF et Humanitarian Outcomes (2024) *State of practice: the evolution of security risk management in the humanitarian space* (en anglais, «État des lieux: l'évolution de la gestion des risques de sécurité dans le domaine humanitaire») (https://humanitarianoutcomes.org/security_risk_mgmt_humanitarian_space_2024).

Heifetz, R.A., Linsky, M. et Grashow, A. (2009) *The practice of adaptive leadership* (en anglais, «La pratique du leadership adaptatif»). Harvard Business Review Press (www.hks.harvard.edu/publications/practice-adaptive-leadership-tools-and-tactics-changing-your-organization-and-world).

USAID Partner Liaison Security Operations («Opération de sécurité en liaison avec les partenaires») (PLSO) (2022) *Women in security. A study of barriers and enablers to entering and progressing within the security field in South Sudan* (en anglais, «Les femmes dans la sécurité. Étude sur les obstacles et les facteurs favorables à l'entrée et à la progression dans le secteur de la sécurité au Soudan du Sud») (<https://gisf.ngo/resource/women-in-security-a-study-of-barriers-and-enablers-to-entering-and-progressing-within-the-security-field-in-south-sudan/>).

Recommandations et outils

Centre de ressources et de support (n.d.) Centre de ressources et de support. (<https://safeguardingsupporthub.org/>).

Davis, J. et al. (2020) 'Module 13, People management' in *Security to go: a risk management toolkit for humanitarian aid agencies*, 4th edition (en anglais, «Module 13, Gestion du personnel, La sécurité en pratique: boîte à outils de gestion de risque à l'attention des agences humanitaires», 4e édition). GISF (<https://gisf.ngo/resource/security-to-go/>).

GISF (2024) *Développement de la stratégie et de la politique de gestion des risques de sécurité (GRS): Un guide interfonctionnel* (<https://gisf.ngo/resource/srm-strategy-and-policy-guide/>).

INSSA (n.d.) Certification (<https://inssa.org/certification>).

5.2 Formation à la sécurité

La formation à la sécurité dans le secteur humanitaire s'est considérablement développée au cours des dernières années et, bien qu'elle s'inspire des enseignements tirés des secteurs privé et public, elle est devenue un domaine de pratique unique et diversifié. Malgré de nombreuses recherches, l'élaboration de recommandations générales et les efforts visant à améliorer la qualité et la cohérence de la formation à la sécurité dans ce secteur,⁸⁰ il n'existe toujours pas d'approche standard en matière de formation à la sécurité.

Le chapitre suivant traite des approches existantes en matière de formation à la sécurité, notamment les avantages et les défis liés aux différents types de formation, ainsi que les considérations clés pour les organisations concernant les besoins fondamentaux et l'équité d'accès à ces ressources.

5.2.1 Pourquoi la formation à la sécurité est-elle importante ?

Bien que cette Revue des bonnes pratiques (RBP) se concentre sur le travail du personnel de sécurité, la plupart, voire la totalité, des décisions en matière de sécurité sont prises par les membres du personnel à titre individuel. C'est pourquoi tous les membres du personnel, quel que soit leur rôle, doivent être en mesure de prendre des décisions éclairées en matière de sécurité afin d'éviter les incidents et de réagir efficacement face aux menaces. La formation à la sécurité joue un rôle fondamental à cet égard et constitue un élément essentiel pour satisfaire au devoir de diligence et créer une culture de la sécurité positive.

5.2.2 Types de formation à la sécurité

La formation à la sécurité peut être divisée en trois catégories :

- Sensibilisation générale à la sûreté et sécurité, dispensée au personnel lors des séances d'intégration et des briefings.
- Formation aux compétences en sûreté et sécurité personnelles, telle que la formation «Sensibilisation en milieu hostile» (HEAT).
- Formation à la gestion des risques de sécurité pour le personnel ayant des responsabilités en matière de sécurité, qui peut inclure une formation à la gestion de crise.

Une quatrième catégorie potentielle est la formation à la gestion des risques de sécurité stratégique destinée aux dirigeants des organisations, généralement les

⁸⁰ Par exemple, le projet de formation en sûreté et sécurité des ONG mené par l'European Interagency Security Forum et InterAction (2014, en anglais) : <https://reliefweb.int/report/world/ngo-safety-and-security-training-project-how-create-effective-security-training-ngos>

cadres supérieurs et les directeurs de la sécurité. Elle aborde des questions telles que l'interaction entre la sécurité et d'autres processus organisationnels et la gestion de risque, ainsi que son intégration dans d'autres politiques et domaines de travail, en particulier le devoir de diligence. Ce niveau de formation est rare.

Sensibilisation à la sécurité : intégrations et briefings

Une formation de base de sensibilisation à la sûreté et sécurité est généralement dispensée au personnel au début de son emploi dans une organisation ou lorsqu'il arrive sur un nouveau lieu de travail. Ces sessions sont généralement brèves et visent à donner au personnel un aperçu général des politiques et procédures de sécurité de l'organisation, y compris les ressources et les points de contact, ainsi que les rôles et responsabilités clés (y compris les propres responsabilités des membres du personnel). En ce sens, les sessions de sensibilisation diffèrent de la plupart des formations en sûreté et sécurité personnelles, qui ont tendance à être plus génériques et ne couvrent pas toujours les procédures organisationnelles.

Les sessions de sensibilisation à la sécurité peuvent se concentrer sur des types de risques particuliers, souvent liés à un contexte spécifique, et peuvent également aborder des défis plus généraux, tels que les questions relatives aux risques liés à l'identité et d'autres préoccupations, par exemple les menaces numériques. Les sessions peuvent également couvrir les risques de sûreté, tels que la sûreté incendie, en particulier sur les sites des projets, bien que ceux-ci puissent parfois être traités séparément des discussions sur la sécurité, notamment lorsque les points focaux organisationnels pour la sécurité, la santé et la sûreté sont distincts. Ce type de sessions de sensibilisation peut se transformer en exercice fastidieux, en particulier si elles sont dispensées en ligne et n'offrent pas la possibilité de poser des questions.

Tableau 7 Briefings sur la sensibilisation à la sécurité : exemple de contenu

Exemple de contenu	Description
Approche de sécurité	Explication de l'approche de l'organisation en matière de sécurité, de son devoir de diligence envers son personnel, des risques auxquels son personnel est exposé et de l'attitude de l'organisation face au risque (c'est-à-dire son appétence au risque).
Politique de sécurité	Présentation de la politique de sécurité de l'organisation et d'autres politiques pertinentes, y compris les principes clés ainsi que les exigences de sécurité connexes et leur application.
Structure de gestion des risques de sécurité	Aperçu des rôles et responsabilités en matière de gestion de la sécurité au sein de l'organisation.

Exemple de contenu	Description
Attentes	Attentes de l'organisation à l'égard de chaque membre du personnel, notamment en ce qui concerne leur responsabilité vis-à-vis de leur propre sécurité et celle de leurs collègues, ainsi que les actions et comportements appropriés. Cela peut également couvrir ce que le personnel est en droit d'attendre de l'organisation en matière de sécurité, y compris le droit de se retirer ou de dire « non » s'il estime qu'une situation est dangereuse.
Sécurité des déplacements	Mesures de sécurité prises par l'organisation pour les déplacements.
Procédures d'urgence	Explication des procédures mises en place par l'organisation en cas d'urgence, comme l'aide médicale par exemple. Cela peut inclure la fourniture au personnel de toutes les informations nécessaires pour signaler un incident et demander de l'aide (par exemple, comment appeler le prestataire d'assurance médicale).
Compte rendu d'incident	Explication des incidents qui doivent être signalés et de la manière de les signaler.
Ressources	Le personnel dispose de ressources pertinentes, notamment des documents, des ressources en ligne, des manuels, des guides et du matériel de formation.

Adapté de Bickley, S. (2017) *Gestion du risque sécurité: manuel de référence à l'attention des petites ONG*. European Interagency Security Forum (<https://gisf.ngo/resource/security-risk-management-a-basic-guide-for-smaller-ngos/>).

Formation en sûreté et sécurité personnelles

Une formation plus approfondie en sûreté et sécurité personnelles peut être appropriée pour le personnel travaillant dans des lieux à haut risque. Ces cours sont généralement plus longs (certains peuvent durer plusieurs jours) et peuvent être dispensés par du personnel qualifié au sein d'une organisation ou par des prestataires de services externes.

Alors que les sessions de sensibilisation à la sécurité ont tendance à se concentrer sur la compréhension et le respect des protocoles de sécurité de l'organisation, la formation à la sécurité personnelle est souvent plus générique et se concentre généralement sur le développement de comportements et de compétences visant à assurer la sécurité du personnel et de ses collègues. Le tableau 8 ci-dessous présente quelques exemples d'objectifs d'apprentissage.⁸¹

81 Pour plus d'objectifs d'apprentissage en matière de sécurité personnelle, voir European Interagency Security Forum et InterAction (2014).

Tableau 8 Exemples d'objectifs d'apprentissage

Objectif	Description
Connaissance situationnelle	Prise en compte de l'environnement et des perceptions locales.
Conscience de l'aspect sécurité	Conscience et responsabilité personnelle des décisions et des actions susceptibles d'affecter la sécurité personnelle et organisationnelle.
Profil de risque personnel	Conscience de la façon dont chaque membre du personnel peut être perçu à travers son aspect physique ou ses actions, y compris toute démonstration de richesse ou de statut social, comportement confiant et posé, langage diplomatique et plein de tact, et attitude respectueuse envers les cultures et coutumes locales. Il est également important de préciser que les profils personnels sont parfois mal perçus ou ne peuvent pas être atténués au niveau individuel (par exemple en cas de ciblage ethnique ou d'attitudes négatives à l'égard des femmes).
Communication	Rester en contact avec ses collègues de manière appropriée et conforme aux attentes de l'organisation.
Réponse personnelle	Donner au personnel les moyens de répondre efficacement aux menaces, à l'hostilité, aux crises et au stress.

Le niveau de détail et la durée d'une formation à la sécurité personnelle sont généralement déterminés par le niveau de risque auquel un membre du personnel peut être confronté. La formation en sûreté et sécurité personnelles peut prendre plusieurs formes, mais elle devrait idéalement être adaptée à chaque organisation, aux besoins du personnel et au lieu concerné. Ce qui fonctionne pour une organisation ou un lieu peut ne pas convenir à une autre organisation ou à un autre lieu. Les formations à la sécurité sont devenues de plus en plus professionnelles et répandues ces dernières années (bien qu'avec des niveaux de qualité et de crédibilité variables), beaucoup considérant la formation « Sensibilisation en milieu hostile » (HEAT) comme la « référence absolue » en matière de formation à la sécurité personnelle dans les contextes à haut risque.⁸² Bien qu'il n'existe pas de format défini pour les cours HEAT, ceux-ci durent généralement de 3 à 5 jours et combinent des cours théoriques, des exercices et des scénarios de simulation plus approfondis, qui consistent généralement à placer les participants dans des situations stressantes réalistes à l'aide d'accessoires et d'acteurs.

82 HEAT est le type de formation prédominant, bien qu'il existe un certain nombre de variations, notamment la formation aux environnements hostiles et aux premiers secours (HEFAT) et la formation aux environnements hostiles (HET).

Beaucoup affirment que la composante simulation différencie HEAT des cours généraux sur la sûreté et sécurité personnelles. Les cours HEAT de qualité sont basés sur les principes de l'entraînement haute fidélité à l'exposition au stress (ou entraînement à l'inoculation de stress), développés dans le domaine de la psychologie. La recherche sur l'entraînement haute fidélité à l'exposition au stress dans des professions telles que la médecine et l'aviation soutient l'efficacité de cette formation lorsqu'elle est utilisée:

- transmet des connaissances et une familiarité avec l'environnement stressant afin de former des attentes précises ;
- transmet des connaissances sur les effets du stress sur le cerveau et le comportement, et sur la manière de contrôler ces réponses en toute sécurité; et
- renforce la confiance en les capacités de la personne à agir dans des scénarios progressivement plus stressants.

Les simulations HEAT permettent aux individus d'observer leurs réactions instinctives dans des situations extrêmement stressantes. Qu'ils aient tendance à réagir par la « lutte », la « fuite », la « paralysie » ou la « soumission » (c'est-à-dire capituler et se conformer), ils seront mieux armés pour gérer ces réponses dans des situations réelles. En mettant en pratique leurs compétences sous pression et dans le stress, les participants devraient mieux retenir et appliquer les connaissances acquises en cas de besoin.

Certains cours HEAT couvrent également les premiers secours en cas de traumatisme. La plupart des cours HEAT sont dispensés par des prestataires de services externes spécialisés. Dans certains contextes, des entités nationales proposent des cours HEAT ouverts à tous.

Outre les cours généraux de formation à la sécurité personnelle et les cours HEAT, il existe d'autres cours liés à la sécurité personnelle. L'ONU, par exemple, a mis au point une formation à la sécurité spécialement destinée aux femmes, appelée « Women's Security Awareness Training » (WSAT, formation à la sensibilisation des femmes à la sécurité).

Depuis la pandémie de Covid-19, davantage de cours sur la sûreté et sécurité personnelles sont proposés en ligne et sous forme de modules (avec ou sans animateur), certains prestataires faisant également la promotion de cours HEAT en ligne. Des cours gratuits en ligne sur la sécurité personnelle sont également de plus en plus disponibles sur les plateformes de formation destinées aux travailleurs humanitaires.⁸³ Certaines grandes organisations ont mis au point une formation à la sécurité interne en ligne.

83 Vous trouverez des exemples dans la section « Informations complémentaires » à la fin de ce chapitre.

Certaines organisations et certains organismes de formation ont opté pour une approche mixte, dans laquelle une partie de la formation est dispensée en ligne, suivie d'une partie en personne comprenant des exercices et des simulations.

Formation à la sécurité basée sur la simulation : inconvénients potentiels

La formation HEAT fait l'objet de controverses au sein de la communauté de la sécurité humanitaire. Bien qu'elle soit souvent décrite et considérée comme « la » formation à la sécurité incontournable pour travailler dans des zones à haut risque, et que certains employés attendent naturellement de leur employeur qu'il leur offre cette formation, sa disponibilité et son accessibilité limitées, ainsi que son coût élevé, en font un produit réservé à une poignée de travailleurs humanitaires (même si l'expansion du secteur a accru sa disponibilité ces dernières années). Bien qu'à ce jour, seules quelques études aient démontré l'efficacité des simulations HEAT,ⁱ les recherches sur la façon dont le cerveau réagit aux situations menaçantes indiquent que les informations cognitives apprises précédemment deviennent inaccessibles si elles ne sont pas consolidées par des expériences plus viscérales.ⁱⁱ

La qualité de la simulation d'un cours HEAT peut varier: certaines simulations sont bien gérées, soutenues par des psychologues et modérément stressantes, tandis que d'autres sont plus extrêmes et peuvent être physiquement et psychologiquement pénibles. Les cours de la formation visent à favoriser le maintien des compétences, mais s'ils sont poussés trop loin, en particulier sans soutien psychologique, le stress subi par les participants peut avoir l'effet inverse. Plus préoccupant encore est le risque de traumatisme ou de retraumatisation dans les simulations de formation à la sécurité, selon la sensibilité d'un participant à certains déclencheurs.

Si les simulations les plus extrêmes – les scénarios de prise d'otages, par exemple – sont désormais moins courantes dans le secteur humanitaire, le risque de nuire aux participants en les soumettant à des simulations stressantes reste préoccupant. Les bonnes pratiques suggèrent de viser des niveaux de stress modérés (afin de favoriser la formation de la mémoire) tout en veillant à ce que les scénarios de simulation soient clairement liés à des objectifs d'apprentissage spécifiques, et que les participants soient encouragés à se concentrer sur leur réaction aux facteurs de stress afin d'en apprendre davantage sur leurs propres réponses au stress.

Bien que le risque de préjudice ne puisse être totalement éliminé, les organismes de formation expérimentés ont mis en place des mesures de sauvegarde. Il s'agit notamment de faire remplir par un psychologue qualifié des questionnaires confidentiels sur les antécédents psychologiques et traumatiques avant la formation et d'offrir des consultations aux participants concernés avant la formation. Un psychologue peut également être présent sur place pour soutenir les participants pendant les simulations. Tous les formateurs, apprenants et acteurs doivent se sentir libres de quitter une simulation à tout moment s'ils estiment qu'elle dépasse leurs capacités. Enfin, un psychologue peut assurer le suivi de tout participant ayant éprouvé des difficultés pendant la formation afin de s'assurer de son bien-être. En général, toute simulation susceptible de générer du stress doit s'appuyer sur des acteurs bien formés, un personnel de soutien psychologique et des directives et règles claires.

- i Turner, C.R., Bosch, D. et Nolt, A.A.T. (2021) 'Self-efficacy and humanitarian aid workers' (en anglais, «L'auto-efficacité et les travailleurs humanitaires») *Journal of International Humanitarian Action* 6(1), 1–12 (<https://doi.org/10.1186/s41018-021-00092-w>) et Roberts, N.T. (2021) *Hostile environment awareness training for humanitarian aid workers: an outcome evaluation* (en anglais, «Formation «Sensibilisation en milieu hostile» pour les travailleurs humanitaires: évaluation des résultats»). Thèse de doctorat, Fuller Theological Seminary, École de psychologie.
- ii Arnsten, A.F. (2015) 'Stress weakens prefrontal networks: molecular insults to higher cognition' (en anglais, «Le stress affaiblit les réseaux préfrontaux: atteintes moléculaires aux fonctions cognitives supérieures») *Nature Neuroscience* 18(10), 1376–1385 (<https://doi.org/10.1038/nn.4087>) and McEwen, B.S. et Akil, H. (2020) 'Revisiting the stress concept: implications for affective disorders' (en anglais, «Revisiter le concept de stress: implications pour les troubles affectifs») *Journal of Neuroscience* 40(1), 12–21 (<https://doi.org/10.1523/JNEUROSCI.0733-19.2019>).

Formation à la gestion des risques de sécurité

Les formations en personne et en ligne à la gestion des risques de sécurité destinées au personnel humanitaire couvrent les aspects essentiels de la gestion de la sécurité, notamment comment identifier les risques et les atténuer, ainsi que comment répondre à des situations ou crises particulières, telles que la détention et l'enlèvement contre rançon. De plus en plus, ces formations prennent en compte les risques liés à l'identité et la manière de les intégrer dans la gestion des risques de sécurité.

Les formations sont généralement dispensées en externe, mais certaines organisations ont mis en place des systèmes internes pour former leur personnel à devenir des points focaux pour les questions de sécurité. Certains de ces cours font désormais partie

d'un programme de certification visant à reconnaître officiellement les aptitudes et les compétences du personnel de sécurité (voir la section «Informations complémentaires» à la fin de ce chapitre).

Des formations spécifiques sur différents aspects de la gestion des risques de sécurité sont également disponibles, telles que des formations sur le signalement des incidents, la conduite (défensive, sécurisée et de véhicules blindés) et la gestion de crise. Les cours comprennent des exercices sur table pouvant couvrir plusieurs bureaux situés à différents endroits au sein d'une organisation. Des prestataires de services externes proposent également des cours sur la gestion de crise, et des recommandations sur la manière d'élaborer et d'animer ce type de formation sont disponibles en ligne (vous trouverez quelques exemples dans la section «Informations complémentaires» à la fin de ce chapitre).

Il existe des exemples de formations stratégiques destinées aux cadres supérieurs, tels que les directeurs de la sécurité et les cadres supérieurs ayant des responsabilités en matière de sécurité, par exemple sur le devoir de diligence et les cadres de gestion du risque de sécurité. Cependant, les ressources de formation à la gestion des risques de sécurité destinées au personnel de sécurité cadre restent rares et l'essentiel de l'apprentissage est partagé par le biais d'organisations en réseau et à l'occasion d'événements et d'ateliers.

5.2.3 Défis

Malgré les progrès réalisés dans la formation à la sécurité des travailleurs humanitaires, des défis importants subsistent, notamment en matière de formation en sûreté et sécurité personnelles.

Tableau 9 Défis liés à la prestation de la formation à la sécurité

Zone	Défi
Disparités	Les travailleurs humanitaires nationaux, y compris ceux qui travaillent pour des organisations internationales, sont beaucoup moins susceptibles de recevoir une formation en sûreté et sécurité personnelles que leurs homologues internationaux.
Accès	Il y a un manque de formations à la sécurité accessibles localement et adaptées à la langue, ce qui rend plus difficile la mise à disposition de ressources aux travailleurs humanitaires nationaux. Les contraintes liées au lieu et au calendrier des cours peuvent également empêcher le personnel d'accéder à la formation de manière plus générale. En outre, certains s'inquiètent du fait que les cours HEAT sont désormais considérés comme la référence en matière de formation à la sécurité, alors qu'ils ne sont pas accessibles financièrement ou logistiquement à la plupart des travailleurs humanitaires, en particulier aux travailleurs humanitaires nationaux.

Zone	Défi
Efficacité	Malgré le recours à des formations à la sécurité personnelle pour préparer le personnel à travailler dans des zones à haut risque – en particulier les cours HEAT –, il existe peu de données publiées sur l'efficacité des différents types de formation à la sécurité personnelle. Si les études publiées confirment l'efficacité de ces formations, la plupart des rapports sur leur impact sont anecdotiques.
Coûts	Le coût des formations à la sécurité peut varier considérablement en fonction du contenu proposé au personnel et du lieu où elles sont dispensées. De nombreux personnels de sécurité sont contraints de décider qui peut suivre ces formations et qui ne le peut pas, en fonction des fonds disponibles.
Durabilité	Les formations ont tendance à être des expériences uniques. Même si certaines organisations exigent des remises à niveau tous les deux ou trois ans, la plupart des informations transmises sont rapidement oubliées sans une pratique régulière ou un lien clair avec les responsabilités professionnelles.
Qualité	L'absence de norme claire en matière de formation en sûreté et sécurité personnelles entraîne une grande disparité entre les cours proposés, tant au sein des organisations qu'auprès de prestataires de services externes. Les organisations qui ont moins de connaissances en gestion des risques de sécurité ou qui disposent de moins de ressources financières sont plus susceptibles de choisir par inadvertance des formations à la sécurité de moindre qualité pour leur personnel.
Pertinence	Certains cours sur la sécurité, en particulier ceux dispensés en ligne, ne sont pas adaptés à des contextes, programmes, organisations et individus spécifiques. Si cela rend la formation plus accessible, cela risque également de ne pas correspondre aux besoins et expériences particuliers des participants.
Diversité	Bien que des progrès aient été réalisés dans ce domaine, il existe toujours un manque de diversité parmi les formateurs, ce qui peut avoir une incidence sur leurs capacités à interagir efficacement avec divers groupes de travailleurs humanitaires et à adapter le contenu à leurs besoins.

Adapté de GISF et Humanitarian Outcomes (2024) *State of practice: the evolution of security risk management in the humanitarian space* (en anglais, «État des lieux: l'évolution de la gestion des risques de sécurité dans le domaine humanitaire») (www.humanitarianoutcomes.org/security_risk_mgmt_humanitarian_space_2024).

5.2.4 Considérations relatives aux bonnes pratiques

Les organisations doivent faire des efforts particuliers pour garantir que tous les membres du personnel aient accès à des possibilités d'apprentissage et à des formations à la sécurité, en particulier les membres du personnel les plus exposés aux risques de sécurité. Cela implique d'aller au-delà d'une simple évaluation des besoins en formation et de procéder à une évaluation à l'échelle de l'organisation des

niveaux de risque des différents membres du personnel, de leur accès à la formation à la sécurité et des mesures à prendre pour combler les lacunes identifiées. Cette démarche peut être complétée par la traduction des supports de formation dans les langues locales appropriées. Pour certaines organisations internationales, cela s'est traduit par une réduction de l'offre de cours HEAT afin de libérer des fonds pour financer une formation à la sécurité personnelle complète pour un plus grand nombre d'employés, en particulier ceux qui ne bénéficient normalement pas d'une telle formation.

Exemple de cas : La sécurité comme un droit

L'équipe de sécurité d'une organisation s'est attachée à promouvoir un environnement organisationnel qui considère la sécurité comme un droit. Cela implique d'informer le personnel sur ce qu'il est en droit d'attendre de l'organisation en matière de soutien à la sécurité et sur la manière de signaler ses préoccupations si ce qui est fourni dans la pratique ne correspond pas à ce qui lui a été promis. Cette démarche est renforcée par des formations et des actions de sensibilisation visant à donner au personnel les moyens d'exercer son droit à la sécurité.

La formation en ligne est devenue une ressource importante dans le secteur humanitaire. De plus en plus, des cours de formation à la sécurité sont disponibles à un coût modique ou gratuitement, avec différents niveaux de détail, couvrant de multiples aspects de la sécurité et dans un nombre croissant de langues. L'avènement de l'intelligence artificielle a accéléré le processus de développement et de traduction de nouveaux cours en ligne. Bien que la nature générique et la conception « standardisée » des cours en ligne – en particulier ceux qui sont accessibles gratuitement – restent un point faible, ces ressources peuvent servir d'introduction à la sécurité et être complétées par des formations plus détaillées et adaptées à l'organisation.

L'un des défis liés à la classification des formations à la sécurité en fonction des niveaux de risque contextuels est qu'elle peut entraîner des lacunes dans la couverture des menaces, telles que la violence interpersonnelle, qui sont plus susceptibles d'être abordées dans les formations personnelles sur les risques les plus élevés, mais qui concernent la plupart des employés, quel que soit leur lieu de travail. C'est pourquoi certaines organisations et certains organismes de formation ont adopté une approche modulaire de la formation, en désignant certains thèmes comme « fondamentaux » pour l'ensemble du personnel et en élaborant des modules supplémentaires en fonction des besoins individuels, du lieu, des menaces, de l'identité organisationnelle et des cadres.

Certains prestataires de formation externes proposent des cours sur mesure adaptés à des besoins particuliers. Ceux-ci peuvent être coûteux. La formation interne, bien qu'elle représente également un investissement organisationnel important en termes de financement et de personnel, permet aux cours de couvrir des situations spécifiques à l'organisation, telles que le type de programmation et les profils particuliers du personnel, et d'offrir une plus grande adaptabilité à des contextes et des défis particuliers. Il existe plusieurs ressources pour aider les organisations à développer des formations à la sécurité internes (voir « Informations complémentaires » à la fin de ce chapitre).

Plusieurs organisations ont opté pour une approche de formation des formateurs, qui leur permet de renforcer leurs capacités internes et d'offrir des formations sur mesure dans davantage de lieux. De telles approches posent des problèmes en matière de contrôle qualité et doivent faire l'objet d'un suivi rigoureux. La collaboration interagences et les investissements conjoints visant à offrir des formations à la sécurité adaptées au contexte aux travailleurs humanitaires locaux se sont également révélés utiles et peuvent réduire les coûts de formation.

Afin de renforcer les connaissances acquises lors des formations, certaines organisations ont intégré des références régulières aux questions de sûreté et sécurité dans le travail quotidien et ont mis en place des exercices périodiques de sûreté et sécurité. Pour les personnes chargées de la sécurité, certaines organisations ont mis en place un programme de mentorat et assigné des « devoirs » en rapport avec les responsabilités réelles des participants, leur permettant ainsi d'apprendre tout en travaillant. Par exemple, une agence de l'ONU offre 90 jours de formation sur le terrain au personnel de sécurité à la suite de son cours sur la sécurité.

Sécurité inclusive dans la formation

Il peut être difficile de discuter des risques différenciés en fonction des profils d'identité. La formation offre l'occasion de lutter contre les mythes et les préjugés dans ce domaine, et plusieurs formateurs ont profité de cet espace pour encourager le personnel à réfléchir au-delà de leurs propres profils d'identité. Vous trouverez ci-dessous une liste d'exemples illustrant la manière dont la sécurité inclusive a été abordée dans le cadre de la formation.

- Exemples concrets issus du groupe, anonymisés, partagés et analysés par l'animateur. Il peut être très instructif d'entendre ce à quoi les collègues sont confrontés au quotidien (y compris les menaces internes). Même s'il existe une certaine animosité envers ce profil particulier, la plupart des individus ne souhaitent pas que leurs collègues subissent un préjudice.

- Exercice de jeu de rôle dans lequel les participants sont invités à réfléchir aux risques encourus par des personnages imaginaires ayant des profils d'identité uniques dans des situations particulières.
- Le recrutement ciblé de formateurs issus de la diversité, qui offre aux participants l'occasion d'entendre directement les défis en matière de sécurité auxquels sont confrontés certains profils d'identité particuliers. Il peut également être utile pour les participants de voir des profils similaires occuper des postes d'influence et de respect (par exemple, des enseignants). En général, il est recommandé de combiner différents profils de formateurs (par exemple, en termes de genre, d'ethnicité, d'expérience et de compétences). La diversité des formateurs doit refléter la diversité des participants.

La formation à la sécurité d'une organisation couvre des questions telles que ce que le personnel à mobilité réduite peut faire aux points de contrôle ou lors de tir croisé, et comment leurs collègues peuvent les aider dans ces circonstances.

Tableau 10 Considérations pour le choix des prestataires de formation

Considération	Facteurs
Profil	Les valeurs, la motivation, l'éthique et la culture du prestataire de formation correspondent à celles de l'organisation et de son personnel. Idéalement, les équipes de formation sont constituées en tenant compte de toutes les compétences et expériences requises, notamment leurs capacités à collaborer de manière adéquate avec le personnel des programmes humanitaires.
Réputation et expérience	Les formateurs sont en mesure de fournir des références et des témoignages crédibles provenant d'autres organisations humanitaires, et possèdent les capacités et l'expérience nécessaires pour former des travailleurs humanitaires. L'expérience contextuelle est pertinente lorsque les cours se déroulent dans une zone géographique particulière. Une expérience dans l'enseignement ou une expertise technique dans des domaines spécifiques (par exemple, la violence sexuelle ou les traumatismes) peuvent également être importantes.

Considération	Facteurs
Contenu	Le contenu de la formation en sécurité est adapté aux types de risques auxquels le personnel de l'organisation est susceptible d'être confronté, ainsi qu'à son approche de sécurité globale. Il peut être judicieux de rechercher une formation comprenant des exercices de simulation, mais ceux-ci peuvent s'avérer trop agressifs ou inappropriés pour le personnel en formation. Le contenu couvre les compétences techniques et non techniques pertinentes. Certains cours peuvent se concentrer sur les risques à fort impact et à faible probabilité, tels que les enlèvements, et négliger les risques à faible impact mais à forte probabilité, tels que les conflits interpersonnels et le stress chronique.¹ Les cours plus avancés peuvent aborder le bien-être du personnel et la gestion du stress, ainsi que les risques liés à l'identité. De nombreuses organisations incluent une formation aux premiers secours. Celle-ci doit être adaptée au contexte et dispensée par un formateur possédant les qualifications nécessaires.
Coûts	Il est recommandé de comparer les coûts proposés par différents prestataires de formation, mais il convient également de tenir compte de la qualité et du contenu des formations proposées. En outre, il faut déterminer s'il est plus approprié de former un nombre réduit de membres du personnel dans le cadre de cours sur la sécurité plus intensifs et de meilleure qualité, ou d'opter pour une solution moins coûteuse qui touche plus de membres du personnel, en particulier ceux qui sont les plus à risque d'incidents de sécurité.
Identité de chaque formateur	Il est recommandé de tenir compte des compétences, des connaissances et de l'expérience individuelles des formateurs, et de déterminer s'il est possible de demander des formateurs particuliers. Le fait de disposer d'une équipe de formateurs diversifiée qui reflète les profils du personnel en formation (par exemple, tous les genres et toutes les ethnies pertinentes) peut encourager une plus grande participation et un plus grand engagement.
Lieu et langue	Le lieu et l'accessibilité de la formation sont des considérations particulièrement importantes, notamment les langues dans lesquelles la formation est dispensée et les coûts liés à la participation.

¹Pour plus d'informations sur les considérations relatives au contenu, voir : European Interagency Security Forum et InterAction (2014).

Adapté de Bickley (2017) *Gestion du risque sécurité : manuel de référence à l'attention des petites ONG*. European Interagency Security Forum (<https://gisf.ngo/resource/security-risk-management-a-basic-guide-for-smaller-ngos/>).

Exemple de cas : Principes de formation tenant compte des traumatismes

Une organisation qui dispense des formations en sûreté et sécurité personnelles internes avec des éléments de simulation a élaboré des principes de formation tenant compte des traumatismes pour son cours. Ces principes sont les suivants :

- **Sûreté** - les formateurs prennent des mesures pour que les participants se sentent en sécurité sur le plan psychologique et physique pendant la formation.
- **Fiabilité et transparence** - les formateurs informent à l'avance les participants de ce qu'ils peuvent attendre du cours, des simulations et des formateurs ; il n'y a pas de surprises et le personnel est informé à l'avance des sujets qui pourraient être des déclencheurs.
- **Soutien et connexion** - les formateurs s'efforcent de dialoguer individuellement avec les participants, qui travaillent ensemble en petits groupes ; des conseillers internes sont disponibles pendant le cours et des services externes de counseling sont proposés aux membres du personnel qui ont besoin d'un soutien supplémentaire.
- **Collaboration et réciprocité** - le cours est conçu pour encourager le partage d'expériences entre les participants.
- **Autonomisation, expression et choix** - le cours couvre les bonnes pratiques (plutôt que les « choses à faire et à ne pas faire ») et encourage les participants à examiner ce qui peut fonctionner pour eux dans différents contextes ; les participants peuvent se retirer d'un scénario qui leur semble dangereux ou qui dépasse leurs limites personnelles.
- **Justice sociale** - la formation reconnaît la dynamique de pouvoir entre les individus et aborde spécifiquement les questions d'identité et de risque ; afin d'éviter de perpétuer des stéréotypes préjudiciables, les lieux fictifs utilisés pour la formation ne ressemblent pas à des contextes ou à des personnes réels.
- **Résilience, croissance et changement** - le cours vise à renforcer la confiance des participants en leur donnant un sentiment de sécurité, de soutien et de validation ; les méthodes d'enseignement valident les réponses des participants ; toutes les simulations sont suivies d'une séance de débriefing au cours de laquelle les participants réfléchissent à ce qui a fonctionné pour eux et à ce qui n'a pas fonctionné.

Informations complémentaires

Recommandations

CICR (2021) *SAFE: Manuel de sécurité pour les humanitaires* (www.icrc.org/en/publication/4425-safe-manuel-de-securite-pour-les-humanitaires).

European Interagency Security Forum and InterAction (2014) *NGO Safety and Security Training Project: how to create effective security training for NGOs* (en anglais, «Projet de formation en sûreté et sécurité des ONG: comment créer une formation en sécurité efficace pour les ONG») (<https://reliefweb.int/report/world/ngo-safety-and-security-training-project-how-create-effective-security-training-ngos>).

GISF (2022a) *Kit de formation en sûreté et sécurité* (en anglais) (<https://gisfprod.wpengine.com/long-read/security-safety-training-pack/>).

GISF (2022b) *Inclusive security session plan*. Security and safety training pack (en anglais, «Plan de session sur la sécurité inclusive. Kit de formation en sûreté et sécurité.») (<https://gisf.ngo/long-read/security-safety-training-pack/3-training-resources/>).

GISF (2023) *NGO crisis management exercise manual: a guide to developing and facilitating effective exercises* (en anglais et en espagnol, «Manuel d'exercices de gestion de crise pour les ONG: guide pour élaborer et animer des exercices efficaces») (www.gisf.ngo/resource/ngo-crisis-management-exercise-manual-a-guide-to-developing-and-facilitating-effective-exercises/).

GISF (n.d.) 1. *Formation en matière de sécurité*. Guide interfonctionnel sur la sécurité des ONG (<https://gisf.ngo/toolbox-pwa-fr/resource/1-formation-en-matiere-de-securite/>).

Recherche et analyse

Arnsten, A. F. (2015) 'Stress weakens prefrontal networks: molecular insults to higher cognition' (en anglais, «Le stress affaiblit les réseaux préfrontaux: atteintes moléculaires aux fonctions cognitives supérieures») *Nature Neuroscience* 18(10), 1376–1385 (<https://doi.org/10.1038/nn.4087>).

Bickley, S. (2017) *Gestion du risque sécurité: manuel de référence à l'attention des petites ONG*. European Interagency Security Forum (<https://gisf.ngo/resource/security-risk-management-a-basic-guide-for-smaller-ngos/>).

Breckenridge, M.-J. et al. (2023) *Aid worker security report 2023 – Security training in the humanitarian sector: issues of equity and effectiveness* (en anglais, «Rapport sur la sécurité des travailleurs humanitaires 2023 – Formation en sécurité dans le secteur humanitaire: questions d'équité et d'efficacité»). Humanitarian Outcomes (www.humanitarianoutcomes.org/AWSR_2023).

GISF et Humanitarian Outcomes (2024) *State of practice: the evolution of security risk management in the humanitarian space* (en anglais, «État des lieux: l'évolution de la gestion des risques de sécurité dans le domaine humanitaire») (www.humanitarianoutcomes.org/security_risk_mgmt_humanitarian_space_2024).

Headington Institute (psychological support and research on HEAT, en anglais, «soutien psychologique et recherche sur HEAT»): <https://headington-institute.org/>

McEwen, B. S. et Akil, H. (2020) 'Revisiting the stress concept: implications for affective disorders' (en anglais, «Revisiter le concept de stress: implications pour les troubles affectifs») *Journal of Neuroscience* 40(1), 12–21 (<https://doi.org/10.1523/JNEUROSCI.0733-19.2019>).

Roberts, N. T. (2021) *Hostile environment awareness training for humanitarian aid workers: an outcome evaluation* (en anglais, «Formation «Sensibilisation en milieu hostile» pour les travailleurs humanitaires: évaluation des résultats»). Thèse de doctorat, Fuller Theological Seminary, School of Psychology.

Turner, C. R., Bosch, D. et Noltz, A. A. T. (2021) 'Self-efficacy and humanitarian aid workers' (en anglais, «L'auto-efficacité et les travailleurs humanitaires») *Journal of International Humanitarian Action* 6(1), 1–12 (<https://doi.org/10.1186/s41018-021-00092-w>).

UNDSS (2021) *Best practices for inclusive security training* (en anglais, «Pratiques exemplaires pour une formation en sécurité inclusive») (https://gisf.ngo/wp-content/uploads/2021/04/UNDSS_Best-Practices-for-Inclusive-Security-Training.pdf).

Ressources de formation

DisasterReady: www.disasterready.org/

GISF: <https://gisfprod.wpengine.com/training-events/>

IFRC: <https://ifrcstaysafe.org/stay-safe-e-course>

INSSA: <https://inssa.org/certification>

Kaya: <https://kayaconnect.org/>

UNDSS: <https://training.dss.un.org/thematicarea/category?id=6>

5.3 Communication sur la sécurité au sein de l'organisation

Dans les environnements complexes où opèrent les organisations humanitaires, une communication efficace des informations en matière de sécurité n'est pas seulement une nécessité procédurale : elle est également essentielle pour protéger le personnel et garantir la continuité du travail humanitaire. Plus un membre du personnel est bien informé, plus il est susceptible de comprendre et de respecter les processus de gestion des risques de sécurité mis en place par son organisation. De plus, des informations bien diffusées et de grande qualité peuvent contribuer à atténuer l'anxiété et l'incertitude qui accompagnent souvent le travail dans des environnements instables ou à haut risque.

5.3.1 Communication centrée sur la personne

Un principe clé dans la diffusion des informations en matière de sécurité consiste à adopter une approche à la fois centrée sur la personne et adaptée au public visé. Contrairement aux modèles traditionnels qui peuvent se concentrer sur les besoins de l'organisation, cette méthode donne la priorité aux préoccupations, vulnérabilités et exigences spécifiques des personnes à risque, tout en adaptant la méthode de communication au public cible. Que l'information soit partagée individuellement lors de briefings ou collectivement via des pages intranet ou des alertes SMS, leur contenu et leur mode de diffusion doivent être adaptés aux destinataires. Cette approche garantit non seulement le respect des protocoles de sécurité, mais implique également activement le personnel en rendant les informations pertinentes pour leur situation immédiate et leur sécurité personnelle.

Par exemple, lorsque l'on informe un membre du personnel des risques liés à un environnement à haut risque, il est essentiel de tenir compte de facteurs tels que son parcours, son expérience et son rôle au sein de l'organisation. Un briefing générique pourrait ne pas traiter de manière suffisante les risques particuliers auxquels est confrontée une employée voyageant seule dans une région conservatrice, ou un membre du personnel présentant des vulnérabilités sur le plan de la santé. Lorsque l'on s'adresse à des groupes plus importants via l'intranet ou les alertes SMS, les informations doivent être claires, accessibles et adaptées aux préoccupations communes du groupe, tout en tenant compte des considérations individuelles lorsque cela est nécessaire.

Le personnel de sécurité doit faire preuve de créativité dans la manière dont il partage les informations.⁸⁴ Il faut tenir compte de la langue, des formats et des canaux. Les supports visuels tels que les infographies, les cartes et les organigrammes peuvent aider à rendre les informations complexes plus faciles à comprendre, et un langage simple, des instructions

84 Le storytelling, par exemple, peut être un moyen efficace d'impliquer le personnel dans les formations en sécurité. Pour plus d'informations, voir Persaud, C. (2022) *Storytelling for learning: using engaging, ethical stories for effective security training* (en anglais, «Le storytelling au service de l'apprentissage : utiliser des récits captivants et éthiques pour une formation en sécurité efficace»). GISF (<https://gisf.ngo/blogs/storytelling-for-learning-using-engaging-ethical-stories-for-effective-security-training/>).

claires et l'absence de jargon technique peuvent considérablement améliorer l'efficacité de la communication.

En fin de compte, l'objectif de la communication sur la sécurité n'est pas seulement d'informer, mais aussi de responsabiliser. Le personnel doit être en mesure de comprendre non seulement ce qu'il doit faire, mais aussi pourquoi c'est important, car cela augmente les chances de conformité et contribue à instaurer une culture de la sécurité positive. En fournissant à leur personnel les informations ciblées dont il a besoin pour comprendre et gérer les risques auxquels il est confronté, les organisations peuvent l'aider à travailler en toute sécurité et efficacement, même dans les circonstances les plus difficiles.

- *Voir le chapitre 1.2 pour plus d'informations sur l'approche de sécurité centrée sur la personne.*
- *Voir le chapitre 1.1 pour plus d'informations sur la mise en place d'une culture de la sécurité positive.*

5.3.2 Modes de diffusion de l'information

L'efficacité de la diffusion des informations en matière de sécurité dépend en grande partie des canaux et des méthodes utilisés.

- **Pages web de l'organisation destinées au personnel (intranet).** Les intranets constituent un outil précieux pour diffuser des informations en matière de sécurité. Les organisations peuvent utiliser l'intranet pour publier régulièrement des mises à jour sur la situation en matière de sécurité, les changements dans les niveaux de risque et les mises à jour des protocoles de sécurité. Il peut également exister des pages spécifiques fournissant des conseils au personnel ayant des profils d'identité particuliers. Cependant, l'intranet dépend du bon fonctionnement des réseaux, qui ne sont pas toujours accessibles à l'ensemble du personnel.
- **E-mail.** L'e-mail reste un canal essentiel de diffusion de l'information au sein des organisations humanitaires. Pour être efficaces, les e-mails doivent être clairs, concis et structurés, et les informations importantes doivent être mises en évidence. Les indicateurs d'urgence, tels que les signalements prioritaires et les intitulés d'objet clairs, permettent de s'assurer que les messages critiques ne sont pas négligés. Des mises à jour régulières sont cruciales dans les situations en cours, tandis que la traduction dans les langues principales des membres du personnel évite les malentendus (parfois, fournir des liens vers des traducteurs d'IA peut être suffisant). Dans certaines circonstances, il peut être utile de demander au personnel de confirmer la réception et la compréhension des e-mails, en particulier pour les communications critiques.
- **Alertes par téléphone portable (telles que SMS ou applications comme Signal et WhatsApp).** Les alertes envoyées sur les téléphones portables constituent un moyen de communication direct et immédiat, garantissant que les informations essentielles sont transmises au personnel, même lorsqu'il est en déplacement ou qu'il travaille à distance. Ces alertes sont particulièrement utiles dans les situations où une diffusion rapide de l'information est nécessaire, par exemple lors d'une escalade soudaine de la violence ou

d'une catastrophe imprévue. Cependant, il est essentiel de trouver un équilibre dans la fréquence des alertes afin d'éviter de submerger le personnel avec un nombre excessif de messages, ce qui pourrait conduire à négliger des alertes importantes.

- **Briefings.** Les briefings sur les déplacements constituent un élément essentiel de la diffusion des informations en matière de sécurité, en particulier pour les membres du personnel qui s'appêtent à se rendre dans un environnement instable ou inconnu. La situation pouvant évoluer rapidement, il est important de fournir régulièrement des briefings actualisés sur la sécurité au personnel concerné. Les briefings ne doivent en aucun cas être ponctuels.

► Voir le chapitre 7.1 pour plus d'informations sur les recommandations relatives aux briefings, aux risques liés aux déplacements et aux mesures d'atténuation.

- **Rapports de situation (sitreps).** Les rapports de situation sont un outil essentiel pour tenir le personnel informé de la situation actuelle en matière de sécurité. Ces rapports doivent pouvoir être produits rapidement, être concis et s'attacher à fournir des informations actualisées sur la situation et faciles à comprendre. Un rapport de situation bien rédigé décrit non seulement l'environnement de sécurité actuel, mais souligne également les implications potentielles pour les opérations de l'organisation et les changements qui pourraient être nécessaires dans les procédures.

Les rapports de situation ont un format assez familier, mais doivent néanmoins être adaptés à leur public et à leur objectif. Les rapports de situation destinés au personnel de projet mettent l'accent sur les conseils pratiques et les risques immédiats, tandis que ceux destinés aux cadres supérieurs peuvent inclure une analyse plus large des tendances et des scénarios futurs potentiels.

- **Rapports.** En plus des mises à jour plus immédiates fournies par les rapports de situation, les organisations peuvent produire des rapports analytiques qui offrent un examen plus approfondi des tendances et des risques en matière de sécurité. Ces rapports peuvent être déclenchés par des changements importants de situation ou de contexte et sont conçus pour éclairer la prise de décision stratégique au sein de l'organisation. Les rapports analytiques peuvent également être périodiques, par exemple des évaluations mensuelles ou trimestrielles, et peuvent inclure divers médias et autres ressources.

Bien que ces rapports soient moins susceptibles d'entraîner des changements immédiats dans les procédures, ils jouent un rôle essentiel dans l'élaboration de la stratégie de sécurité à long terme de l'organisation. Par exemple, un rapport peut mettre en évidence les menaces émergentes dans une région particulière qui pourraient affecter les opérations futures de l'organisation, ce qui conduirait à une révision des évaluations des risques et des plans d'urgence. Compte tenu de la nature stratégique de ces rapports, il est essentiel qu'ils soient rédigés en tenant compte du public visé. Les cadres supérieurs, par exemple, peuvent avoir besoin d'une analyse plus détaillée de l'impact potentiel sur les opérations, tandis que le personnel opérationnel pourrait tirer profit de résumés axés sur les implications pratiques pour ses activités quotidiennes.

- Voir le chapitre 4.4 pour plus d'informations sur l'analyse des tendances en matière d'incidents de sécurité.
- Voir le chapitre 3.4 pour plus d'informations sur les mécanismes de suivi de la sécurité.

5.3.3 Gérer la surcharge d'informations

L'un des principaux défis liés à la diffusion des informations en matière de sécurité est le risque de surcharge d'informations, en particulier dans les environnements instables où les événements peuvent évoluer rapidement. Dans de telles situations, le volume considérable d'informations peut submerger le personnel, qui aura alors du mal à assimiler les mises à jour les plus importantes et à agir en conséquence. Un système de triage permet de hiérarchiser les informations en fonction de leur urgence et de leur pertinence.

Le système de triage doit être guidé par une série de questions et de considérations clés:

- **Importance opérationnelle.** La sûreté et sécurité du personnel seront-elles compromises si ces informations ne sont pas transmises immédiatement? Si oui, les partager immédiatement. Si ce n'est pas le cas, tenir compte des points ci-dessous.
- **Mise à jour de la situation.** Les informations indiquent-elles un effet potentiel sur la sécurité, pouvant nécessiter des précautions accrues? Si oui, informer le personnel concerné en temps utile. Si ce n'est pas le cas, tenir compte du point ci-dessous.
- **Changement de contexte.** Les informations indiquent-elles une tendance ou d'autres implications à plus long terme pour l'environnement du programme? Si oui, réfléchir au moment et à la manière les plus appropriés pour utiliser ces informations afin d'éclairer la prise de décision stratégique.

Chaque organisation devra réfléchir à la meilleure façon de transmettre les informations en matière de sécurité pour chaque niveau et veiller à ce que le personnel soit formé sur la manière et le moment de partager ces informations, ainsi que sur les personnes avec lesquelles les partager.

Pour les informations qui revêtent une importance immédiate et représentent une menace générale pour les membres du personnel, la priorité est de les diffuser aussi rapidement et largement que possible. Les méthodes traditionnelles de communication en matière de sécurité, telles que la chaîne de communication, peuvent être efficaces dans ces scénarios, mais de nombreuses organisations ont désormais également recours à la diffusion ou à la messagerie de groupe. Ces méthodes permettent une diffusion rapide des informations critiques, garantissant ainsi que tout le personnel concerné soit informé et puisse prendre les mesures appropriées sans délai.

Exemples de systèmes de triage pour le partage d'informations

- **Importance opérationnelle.** Une manifestation devant les bâtiments du Parlement du pays tourne à la violence. Informer le personnel qu'il doit éviter la zone. Utiliser des SMS, une chaîne de communication, la diffusion ou un groupe WhatsApp/Signal pour diffuser rapidement l'information au personnel travaillant dans cette zone.
- **Mise à jour de la situation.** Des manifestations sont prévues dans les prochains jours devant les bâtiments du Parlement. Envoyer un avis par e-mail et/ou l'intégrer dans les rapports de situation, les rapports de sécurité spécifiques et les procédures opérationnelles standards.
- **Changement de contexte.** Les manifestations ont conduit à la mise en place d'un gouvernement hostile aux organisations humanitaires. Incorporer les informations pertinentes dans les rapports de sécurité, les briefings ou les formations, et alimenter les processus d'analyse de la sécurité.

Chaîne de communication

Une chaîne de communication est un système hiérarchique utilisé pour diffuser rapidement des informations à un grand groupe. Elle commence par une personne qui contacte des individus clés, qui à leur tour informent les autres, créant ainsi un effet cascade jusqu'à ce que tout le monde soit atteint. Ce modèle est idéal pour les urgences ou les mises à jour urgentes, garantissant une communication rapide. Les chaînes de communication peuvent être manuelles, impliquant des appels directs, ou automatisés, utilisant un logiciel pour envoyer des messages au moyen d'appels, de SMS et d'e-mails.

Pour la communication au niveau opérationnel, l'introduction de la redondance est essentielle. Cela signifie que le personnel a accès à des méthodes de communication multiples et indépendantes, telles que les radios et les téléphones satellites, afin que la communication puisse se poursuivre même en cas de défaillance d'une méthode.

- Voir le chapitre 6.1 pour plus d'informations sur les différentes méthodes de communication et l'élaboration de plans de communication qui introduisent une redondance.

Pour les mises à jour de situation ou les changements de contexte qui ne nécessitent pas d'action immédiate mais qui ont des implications à plus long terme, une approche plus mesurée est souvent appropriée. Ces types de mises à jour doivent toujours être communiqués rapidement, mais l'accent doit être mis sur une analyse approfondie de la situation et de son impact potentiel sur la gestion des risques de sécurité de l'organisation.

Les mises à jour stratégiques de haut niveau peuvent être mieux communiquées au moyen de rapports formels ou de briefings exécutifs, tandis que les mises à jour opérationnelles peuvent être diffusées au moyen de canaux plus informels tels que des réunions d'équipe ou des groupes de chat. Les concepts plus approfondis et les informations en matière de sécurité peuvent être partagés lors de briefings et de sessions de formation. L'essentiel est de s'assurer que le mode de communication est adapté à l'urgence et à l'importance des informations, ainsi qu'aux préférences et aux habitudes du public visé.

Tableaux de bord et applications

Les organisations humanitaires utilisent de plus en plus des tableaux de bord et des applications mobiles personnalisées pour partager des informations en matière de sécurité.

Les tableaux de bord offrent au personnel une plateforme leur permettant d'accéder à des informations relatives à la sécurité, telles que les plans de sécurité, souvent sous une forme visuellement attrayante (comme des cartes thermiques) (*voir le chapitre 3.4 pour plus d'informations sur les tableaux de bord*).

Les applications mobiles peuvent fournir des mises à jour de sécurité en temps réel, permettre un signalement des incidents rapide et offrir des conseils sur des situations de sécurité spécifiques (comme les mesures à prendre aux points de contrôle). Elles peuvent également inclure des coordonnées d'urgence. Les applications peuvent être particulièrement utiles pour le personnel qui a besoin d'accéder à des informations en matière de sécurité lors de ses déplacements.

Vérification et surréaction prudente

L'exactitude et la fiabilité des informations en matière de sécurité sont d'une importance capitale. Il va sans dire que toutes les informations diffusées par l'organisation doivent avoir été vérifiées dans la mesure du possible. Cependant, dans des situations qui évoluent rapidement, il n'est pas toujours possible de vérifier entièrement les informations avant qu'elles ne doivent être communiquées. Dans de tels cas, le concept de surréaction prudente entre en jeu.

La surréaction prudente consiste à prendre des mesures préventives sur la base des informations disponibles, même si celles-ci n'ont pas été entièrement vérifiées, à condition que les risques potentiels justifient une telle approche. Par exemple, si un rapport non vérifié fait état d'une menace imminente pour la sécurité dans une zone particulière, il peut être prudent de suspendre temporairement les opérations ou de conseiller au personnel de se mettre à l'abri jusqu'à ce que davantage d'informations soient disponibles. L'essentiel est de communiquer l'information de manière à exposer clairement les raisons des mesures prises, tout en reconnaissant l'incertitude qui entoure la situation. Lors de la transmission de ces informations, il est essentiel d'anticiper les questions que le personnel est susceptible de se poser, telles que « Pourquoi ai-je besoin de savoir cela ? » et « Que dois-je faire ? ». En abordant ces questions dès le départ, les organisations peuvent contribuer à réduire la confusion et s'assurer que le personnel est prêt à prendre les mesures nécessaires en réponse à d'éventuelles menaces.

Révision et adaptation continues

Une communication efficace sur la sécurité au sein des organisations humanitaires repose largement sur un feedback et une adaptation continus. Le personnel de sécurité doit rechercher activement le feedback de ses collègues et l'intégrer afin de garantir que les informations fournies sont à la fois claires et utiles. À mesure que les environnements de sécurité et les menaces évoluent, les stratégies et les méthodes de communication utilisées doivent également évoluer. Il est essentiel de procéder à des révisions ou à des audits réguliers de ces pratiques, en impliquant tous les niveaux de l'organisation. Se tenir informé des nouvelles technologies de communication peut contribuer à améliorer l'efficacité et la portée des mises à jour de sécurité.

Informations complémentaires

Persaud, C. (2022) *Storytelling for learning: using engaging, ethical stories for effective security training* (en anglais, « Le storytelling au service de l'apprentissage: utiliser des récits captivants et éthiques pour une formation en sécurité efficace »). GISF (<https://gisf.ngo/blogs/storytelling-for-learning-using-engaging-ethical-stories-for-effective-security-training/>).

5.4 Bien-être du personnel

Un personnel et des équipes résilients sont essentiels à la résilience d'une organisation. Dans les environnements souvent très stressants du travail humanitaire, un soutien adéquat au bien-être mental et physique du personnel renforce cette résilience et les capacités du personnel à prendre les décisions judicieuses qui sont essentielles à une gestion des risques de sécurité efficace.

Ce chapitre met l'accent sur l'importance d'intégrer les considérations de santé physique et mentale dans la gestion des risques de sécurité et de soutenir le personnel avant, pendant et après les incidents critiques. Il propose des stratégies visant à préserver le bien-être du personnel et à renforcer la santé mentale et soutien psychosocial afin d'éviter des conséquences négatives à long terme. L'approche décrite peut être mise en œuvre par du personnel non médical, garantissant ainsi que tous les aspects liés au bien-être du personnel sont traités de manière efficace.

► *Ce chapitre porte principalement sur la santé mentale. Pour les considérations médicales physiques et les préparatifs nécessaires, voir le chapitre 5.5.*

5.4.1 Concepts clés

Résilience et bien-être

La résilience est « le processus et le résultat d'une adaptation réussie à des expériences de vie difficiles ou éprouvantes, notamment grâce à une flexibilité mentale, émotionnelle et comportementale et à une adaptation aux exigences externes et internes ». Aborder la résilience implique de soutenir le bien-être général afin de renforcer la capacité des individus et des équipes à gérer efficacement les chocs, tout en fournissant un soutien psychosocial immédiat et à long terme en réponse aux incidents (voir la figure 11).

La résilience des membres du personnel face à des environnements et des événements difficiles peut dépendre de divers facteurs, notamment la solidité des réseaux sociaux, des facteurs culturels et autres facteurs d'identité, la vision générale et le tempérament, ainsi que les mécanismes d'adaptation. Les capacités de résilience peuvent être développées et entretenues, et chaque individu possède son propre niveau de résilience, influencé par ses caractéristiques personnelles, ses attentes, son mode de vie et la conscience qu'il a de ses limites. L'environnement de travail joue également un rôle, avec des facteurs tels que les horaires de travail, les attentes, la charge de travail et les traumatismes vicariants potentiels qui affectent la résilience.

Figure 11 Facteurs favorisant la résilience

Même si de nombreux facteurs de stress échappent à leur contrôle, les organisations peuvent néanmoins favoriser la résilience en promouvant une culture de travail solidaire.

Dans le cadre d'une réponse humanitaire, les conditions de vie sont souvent difficiles, que le personnel réside dans une zone touchée par une crise ou dans des logements ou des tentes partagés de l'organisation. Pour les membres du personnel qui travaillent loin de leur domicile et de leur famille, les facteurs de stress en dehors des heures de bureau peuvent être plus importants, car ils ne bénéficient pas du soutien familial. Le personnel peut avoir du mal à distinguer clairement les limites entre le travail et la vie privée, et peut subir un stress accru en raison d'un accès limité au soutien familial. Le personnel résidant sur place peut être soumis à des pressions supplémentaires en tant que membres de la communauté touchée, les crises pouvant avoir des répercussions sur leurs familles, leurs amis et les infrastructures environnantes.

La mise en œuvre d'une approche de soutien par les pairs au sein d'une équipe et la sensibilisation des managers à l'importance de l'auto-soin et aux risques liés à la santé mentale peuvent considérablement renforcer la résilience tant individuelle qu'organisationnelle.

Le bien-être général d'une personne ne se limite pas à sa santé physique et à sa sûreté. La mesure dans laquelle la gestion des risques de sécurité prend en compte et soutient activement les dimensions mentales, émotionnelles et sociales peut faire une différence cruciale en termes de moral, de performances, de prise de décision et de résultats personnels. Un personnel bien formé prend de meilleures décisions en matière de sécurité et est mieux à même de faire face à des environnements et des incidents stressants.

Exemple de cas : Mettre l'accent sur des mécanismes d'adaptation sains

Une organisation a intégré la gestion du stress dans sa formation sur la santé et la sûreté et sécurité personnelles destinée à l'ensemble de son personnel. Au cours de cette session, le personnel apprend à reconnaître les signes de stress chez lui et chez les autres et discute de ses mécanismes d'adaptation. Chacun s'engage à adopter au moins un mécanisme d'adaptation sain sur lequel il se concentrera dans les mois suivant la formation. La session s'achève par un accord entre les participants sur les actions que l'organisation peut entreprendre pour améliorer le bien-être du personnel. Parmi les exemples, on peut citer l'installation de plantes dans les bureaux, la présence d'un médecin sur place un jour par mois pour des consultations sans rendez-vous, l'organisation d'un petit-déjeuner d'équipe une fois par semaine et la création d'un espace sûr où le personnel peut se détendre pendant ou à la fin de sa journée de travail. Les sessions contribuent à normaliser les conversations sur le bien-être et la santé, à mieux comprendre comment les équipes peuvent se soutenir mutuellement et à sensibiliser les membres du personnel à leurs propres mécanismes d'adaptation.

Le bien-être global d'une personne a été décrit comme comprenant six dimensions : physique, émotionnelle, sociale, intellectuelle, professionnelle/occupationnelle et spirituelle/religieuse. Ces dimensions sont interdépendantes, ce qui signifie que si un domaine est touché, cela peut avoir un impact sur les autres. Le personnel de sécurité doit comprendre et tenir compte de ces différentes dimensions et leur interdépendance, en particulier lors d'événements ou de périodes difficiles. Le personnel de sécurité peut également jouer un rôle important dans la promotion de la mise en œuvre, à l'échelle de l'organisation, d'initiatives en faveur du bien-être qui abordent ces six dimensions.

Pratiques favorisant le bien-être au travail

Les pratiques favorisant le bien-être au travail peuvent inclure la nomination d'un point focal pour les questions de bien-être ou la création d'un comité chargé d'organiser des activités physiques, des ateliers et des formations sur la gestion du stress et la santé mentale. Des pratiques telles que la promotion de la gratitude et de la reconnaissance et l'encouragement à prendre des pauses peuvent stimuler le moral et la productivité. Des politiques telles que l'interdiction d'envoyer des e-mails après les heures de travail, l'encouragement du personnel à prendre ses congés annuels et l'offre d'horaires de travail flexibles contribuent également au bien-être. La mise à disposition d'espaces dédiés à la méditation, au yoga et aux activités sociales peut aider les employés à se sentir valorisés et soutenus. Proposer des programmes de développement professionnel, d'éducation financière et de soutien au personnel dans des circonstances particulières, comme les nouveaux parents ou les personnes ayant des obligations religieuses, peut également favoriser le bien-être.

Stress et traumatisme

En raison de leur travail et de leur environnement, tous les travailleurs humanitaires sont exposés au stress. Cela inclut les professionnels de la sécurité et les dirigeants qui doivent régulièrement faire face à des incidents touchant d'autres personnes. Chaque individu vit et manifeste son stress différemment et développe des mécanismes d'adaptation individuels, en fonction de son profil personnel et de sa situation.

Il existe différents types de stress, qui peuvent être bons ou mauvais. Un bon stress aide les gens à se concentrer sur la tâche ou la situation à laquelle ils sont confrontés, mobilise leur énergie et les prépare à agir. Par exemple, avoir une échéance peut être source de stress, mais peut aussi aider à mener à bien une tâche. Dans les situations de tension ou de risque, les réactions de stress et de peur peuvent donner aux gens la concentration dont ils ont besoin pour survivre.

Cependant, lorsque le stress survient trop souvent, qu'il est trop intense ou qu'il dure trop longtemps, il devient néfaste. Tout stress consomme de l'énergie. Une série apparemment interminable de délais serrés ou une exposition continue à des situations ou des expériences à haut risque peuvent épuiser les réserves d'énergie. Lorsque plusieurs facteurs de stress surviennent en même temps, et en particulier lorsqu'ils sont prolongés, y compris des facteurs de stress corrosifs tels que la peur, l'incertitude et les conflits permanents, cela peut entraîner un stress cumulatif.

Il existe une différence entre le stress et le traumatisme. Les réponses normales au stress, appelées stress aigu, comme le mécanisme de survie «lutter ou fuir», sont désactivées lorsque la menace est passée. En cas de traumatisme, le corps reste en mode de survie et continue à répondre comme s'il était menacé, même après la disparition de la menace. Les événements traumatisants dépassent les capacités des gens à faire face et à gérer le stress.

Si une personne souffre d'un niveau continu de stress accru, ses mécanismes d'adaptation peuvent être dépassés, ce qui réduit ses capacités à supporter l'impact psychologique d'un événement traumatisant. Le stress et les traumatismes à long terme affectent également les capacités d'une personne à prendre des décisions.

Un traumatisme peut être le résultat d'un facteur de stress aigu (tel qu'un incident critique ou un événement mettant la vie en danger), d'un stress cumulatif ou d'une exposition continue au traumatisme d'autrui. Bien que les traumatismes soient courants, un seul événement indésirable, voire une série d'événements indésirables, n'entraîne pas nécessairement un traumatisme. Cela dépend plutôt de la manière dont une personne réagit et est équipée pour faire face à l'expérience, ce qui est étroitement lié aux ressources dont elle dispose ainsi qu'à ses expériences passées.

Les facteurs de stress pouvant entraîner un traumatisme sont très variés, et ce traumatisme peut survenir plusieurs heures, jours, semaines, mois, voire années après (le début de) l'événement. Ces facteurs de stress peuvent varier en intensité et entraîner un trouble de stress post-traumatique (TSPT) ou d'autres formes de traumatisme. Dans tous les cas, ils ont un impact sur la résilience des membres du personnel. Les organisations doivent être prêtes à offrir un soutien longtemps après la survenue d'un événement.

Traumatisme indirect

Les travailleurs humanitaires peuvent subir un traumatisme de manière indirecte de plusieurs façons. Le stress post-traumatique secondaire désigne des symptômes tels que les cauchemars ou l'anxiété qui apparaissent chez une personne exposée indirectement au traumatisme d'une autre personne, généralement par le biais de ses interactions avec la personne survivante du traumatisme ou de l'aide qu'elle lui apporte. Le traumatisme vicariant implique un changement profond de la vision du monde d'une personne, causé par une exposition indirecte répétée au traumatisme d'autrui. Il touche généralement les premiers intervenants, tels que les ambulanciers, mais peut également toucher d'autres personnes, par exemple le personnel des médias et des communications exposés de manière répétée à des contenus en ligne bouleversants.

5.4.2 Sécurité, santé mentale et soutien psychosocial

Les risques d'impact sur la santé mentale associés au travail humanitaire doivent être reconnus comme faisant partie du devoir de diligence d'une organisation. L'élaboration de stratégies localisées peut améliorer l'environnement de travail et renforcer la préparation à la réponse psychosociale afin de soutenir le personnel pendant et après les situations d'urgence et les incidents critiques. Cela peut s'appuyer sur une approche de santé mentale et soutien psychosocial (SMSPS), qui répond à la fois aux besoins en matière de santé mentale et aux facteurs sociaux affectant le bien-être des individus et des groupes en intégrant les soins psychologiques aux systèmes de soutien social. Il convient de noter que, tandis que le soutien psychologique se concentre sur la thérapie individuelle et la gestion des problèmes de santé mentale tels que l'anxiété ou la dépression, le soutien psychosocial est une approche plus large qui intègre à la fois les aspects psychologiques et sociaux du bien-être, en tenant compte de l'impact des relations, de l'environnement et de la communauté sur la santé mentale.

L'intégration des ressources de SMSPS dans les processus de gestion des risques de sécurité renforce la résilience du personnel et réduit le risque d'incidents liés au stress ou au burn-out. Cela peut impliquer :

- Promouvoir une culture solidaire qui réduit la stigmatisation et encourage le personnel à demander de l'aide avant que les problèmes ne s'aggravent et ne compromettent la sécurité.
- Identifier les besoins en SMSPS et les obstacles.
- Cartographier les services de santé mentale organisationnels et locaux et les prestataires en soutien psychosocial, approuvés par des cliniciens.
- Développer des stratégies de recrutement, de sélection et de supervision des services de soutien psychosocial.
- Établir des liens avec les ressources locales afin d'améliorer la gestion des incidents critiques en offrant un soutien psychosocial immédiat et adapté à la culture.
- Inclure des procédures de réponse psychosociale dans les plans de sécurité et les plans de gestion de crise.
- Former les dirigeants et les managers à répondre efficacement aux problèmes psychosociaux, notamment en matière de bien-être mental et de stratégies de renforcement de la résilience.
- Préparer et former le personnel à apporter des réponses psychosociales tenant compte des traumatismes lors d'incidents critiques, notamment la violence sexuelle.
- Intégrer les considérations relatives à la santé mentale dans les briefings et les formations à la sécurité.

► Voir le chapitre 5.2 pour plus d'informations sur la manière d'intégrer les considérations relatives à la santé mentale dans la formation à la sécurité.

Certains experts recommandent une approche de gestion de risque lié à la santé mentale, qui traite les risques psychologiques comme on traiterait les risques de sécurité, en utilisant les mêmes outils et cadres, en évaluant les risques psychologiques parallèlement aux risques de sécurité physique et en mettant en place des mesures d'atténuation et des plans d'urgence pertinents. En intégrant la santé mentale dans le cadre de gestion du risque de sécurité, les organisations peuvent renforcer leur résilience globale et gérer efficacement les risques de sécurité et les risques psychologiques.

Pour ce faire, elles peuvent commencer par cartographier les besoins et les capacités en SMSPS dans chaque site de l'organisation. Cette cartographie peut prendre en compte les facteurs de stress communs aux membres du personnel ayant des profils différents, ainsi que les problèmes et les besoins existants en matière de santé mentale parmi les membres du personnel. Elle peut inclure un examen des services, des prestataires, des installations et des programmes disponibles localement ou à distance (y compris les régimes d'assurance) et à qui ils s'adressent (en tenant compte, par exemple, des besoins du personnel en matière de langue et d'accessibilité). Les attitudes courantes, la culture organisationnelle et les mécanismes d'adaptation au stress, au burn-out, au traumatisme vicariant et au traumatisme post-incident sont également des éléments importants à prendre en considération.

Les informations recueillies grâce à cette cartographie peuvent être utilisées pour éclairer les initiatives d'une organisation en matière de soutien psychosocial et de bien-être. Voici quelques exemples de services de santé mentale et soutien psychosocial, tant formels (par le biais de professionnels externes et internes) qu'informels (tels que les groupes de soutien par les pairs).

Services de counseling et de thérapie:

- Programmes d'aide aux employés (PAE) (services confidentiels de counseling et de soutien fournis par des tiers pour les problèmes personnels et professionnels).
- Professionnels de santé mentale sur place (internes ou externes).
- Services de télémedecine (internes ou externes).
- Services spécialisés, tels que des psychiatres ou des thérapeutes, intervenant après un incident ou une crise.

Parmi les autres initiatives, on peut citer:

- Ateliers et formations en santé mentale.
- Programmes de gestion du stress.
- Formation aux premiers secours psychologiques.
- Programmes de soutien par les pairs.
- Ressources en ligne sur la santé mentale.

Il est important de revoir régulièrement les options de soutien en SMSPS afin de s'assurer qu'elles correspondent aux besoins et aux attentes du personnel et qu'elles sont pertinentes et accessibles pour le personnel issu de milieux culturels divers. Les bonnes pratiques suggèrent de ne pas se fier uniquement à un seul mécanisme de soutien, mais d'offrir une variété d'options adaptées à différents types de facteurs de stress et d'événements, afin de répondre efficacement à l'ensemble des besoins du personnel. Enfin, les services offerts en SMSPS doivent être clairement définis à l'avance par l'organisation, afin que le personnel sache à quels services il a accès et à quel type de soutien il peut s'attendre à la suite d'un incident critique.

Exemple de cas : Journées du bien-être

Après l'escalade de mai 2023 à Gaza, où le personnel avait traversé une période intense de frappes aériennes, une organisation a offert deux journées de bien-être à tout le personnel basé à Gaza. La plupart des employés avaient beaucoup de congés à prendre, mais ce congé bien-être était destiné à leur témoigner de la reconnaissance, et le personnel s'est senti motivé et pris en charge. Le bureau est resté ouvert pour les employés qui préféraient rester avec leurs collègues pour faire face à la situation.

5.4.3 Considérations générales relatives à la réponse

Les bonnes pratiques en matière d'approches de prise en charge post-incident du personnel et de suivi médical couvrent toute une série de considérations pratiques.

Veiller à ce que le personnel se sente soutenu

À la suite d'un incident ou d'un autre événement stressant, il est important que le personnel sente que l'organisation comprend que son expérience a été difficile et qu'elle a l'intention de le soutenir et de veiller à ce que les prochaines étapes se déroulent de la manière la plus harmonieuse possible. Pour ce faire, les organisations peuvent écouter le personnel concerné, répondre à ses besoins après l'incident et fournir des réponses aux questions initiales, tout en le mettant en relation avec les ressources nécessaires. Le personnel peut avoir besoin de temps pour assimiler les événements et les émotions liés à l'incident ou à la situation. Les organisations doivent encourager les personnes concernées à prendre le temps de se reposer, de prendre soin d'elles-mêmes et de rester en contact avec leurs proches. Il n'est pas rare que le personnel ait des besoins immédiats en santé physique ou mentale après un événement stressant. Une réponse structurée pour soutenir la santé mentale immédiatement après un incident, intégrant le soutien par les pairs et une direction et un management compatissants, réduira la probabilité qu'une personne ait besoin d'un soutien professionnel pour un traumatisme ultérieur.

Les considérations générales relatives à la prise en charge du personnel pendant ou après des incidents ou des événements très stressants comprennent les éléments suivants :

- **Messages de soutien au personnel.** Lorsque le personnel est confronté à des difficultés, le fait de recevoir des messages de soutien de la part des cadres supérieurs (dans leur langue maternelle) peut avoir un impact important. Les marques d'attention personnelles de la part des collègues peuvent également être source de réconfort. La communication peut se faire par SMS, sur les réseaux sociaux, par e-mail ou par téléphone, et peut inclure la possibilité pour le personnel concerné de répondre aux messages et de partager ses expériences.
- **Visites à l'hôpital.** Si un membre du personnel est hospitalisé loin de chez lui, organiser une visite par un autre membre du personnel ou une organisation partenaire peut atténuer son sentiment d'isolement.
- **Paquets de soins.** Des paquets de soins personnalisés pour le personnel touché par des incidents ou des conflits peuvent être mis en place par le personnel ou par des partenaires si l'organisation n'est pas en mesure d'accéder à certaines zones.
- **Équipe d'accueil.** Le fait de disposer d'une équipe d'accueil pour accueillir le personnel à son arrivée dans un lieu sûr peut faire une différence considérable. Cette équipe peut être présente pour aider le personnel arrivant après une évacuation, un incident critique ou une situation violente.
- **Informations post-incident.** Fournir un résumé écrit du soutien, des ressources, des assurances, des prestations et des conseils juridiques disponibles au personnel touché par un incident. Ce résumé peut être accompagné de conseils personnalisés prodigués par un représentant et des coordonnées d'une personne à contacter pour toute question de suivi.
- **Débriefing psychologique post-incident.** Le personnel responsable peut organiser un débriefing psychologique post-incident avec un psychologue agréé ou une autre personne qualifiée (voir ci-dessous).

► Voir le chapitre 4.4 pour plus de détails sur les débriefings post-incident.

Pendant la relocalisation et l'évacuation

Les organisations peuvent prendre des mesures pour s'assurer que le personnel se sente soutenu à la suite d'une relocalisation ou d'une évacuation, par exemple en veillant à ce que ses besoins immédiats soient satisfaits (fournitures essentielles, soins médicaux et aide à la communication). Cela comprend un soutien continu pendant leur séjour dans un lieu sûr, comme des contrôles réguliers, une aide pour l'organisation de la suite du déplacement et l'accès à des services médicaux et psychosociaux. L'objectif est de faire en sorte que le personnel se sente en sécurité, soutenu et connecté tout au long du processus de relocalisation et d'évacuation.

Approche centrée sur la personne survivante

Qu'il s'agisse d'aider le personnel victime d'un grave accident de la route, d'une agression sexuelle, d'une relocalisation pour échapper à une situation mettant sa vie en danger, d'un enlèvement ou d'un autre événement stressant, les organisations ont tout intérêt à adopter une approche centrée sur la personne survivante.

Les concepts clés de la prise en charge centrée sur la personne survivante sont les suivants:

- **Respect.** Respecter les souhaits et les choix de la personne survivante, la traiter avec dignité et comprendre que ses réactions peuvent être émotionnelles et différer des attentes des autres.
- **Confidentialité.** Ne partager les informations personnelles concernant la personne survivante que sur la base du « besoin de savoir » et demander son consentement avant de divulguer d'autres détails.
- **Autonomie.** Reconnaître le droit de la personne survivante à prendre ses propres décisions, en tenant compte du fait que l'autonomie peut être interprétée différemment selon les contextes culturels. Fournir des informations claires sur les procédures et les résultats potentiels afin de favoriser des choix éclairés.
- **Clarté et navigation.** La personne survivante peut être désorientée après l'incident et avoir besoin d'aide pour comprendre ce dont elle a besoin et comment obtenir du soutien.

Elle peut être bouleversée par l'expérience vécue et par la nécessité de prendre des décisions. Il est donc essentiel de lui apporter un soutien tout au long de ce processus. Une approche centrée sur la personne survivante donne la priorité aux besoins de la personne survivante sans l'accabler indûment de questions liées à l'emploi, aux actions en justice, aux procédures d'assurance et à la nécessité de s'y retrouver dans les mécanismes de soutien internes et externes. Cela implique de fournir un aperçu clair et concis des avantages et du soutien disponibles, et de désigner une personne de contact tout au long de la période de rétablissement. Au début, il peut s'agir d'un membre de l'équipe de gestion de l'incident ou d'un accompagnant de la personne survivante. À moyen ou long terme, ce soutien (congé d'urgence pendant la période d'incapacité de travail, retour au travail ou changement de parcours professionnel, par exemple) peut être confié à un supérieur hiérarchique, avec le soutien régulier d'un responsable des ressources humaines, d'un partenaire commercial ou d'un conseiller juridique, par exemple.

Le personnel responsable doit reconnaître que les préférences en matière de soutien peuvent varier. Pour certains, être soutenu peut signifier avoir quelqu'un avec qui partager ses expériences. D'autres peuvent apprécier la possibilité de rester occupés ou de se concentrer sur d'autres choses. Certains voudront prendre l'initiative dans toutes les actions de suivi et de réponse, tandis que d'autres auront des capacités ou aptitudes limitées à le faire et auront besoin d'un soutien organisationnel plus important.

Un défenseur externe des personnes survivantes peut être engagé pour soutenir les personnes survivantes/le personnel touché.

Une approche centrée sur la personne survivante se distingue d'une approche dirigée par la personne survivante, car elle comporte un certain contrôle afin d'éviter les décisions qui pourraient entraîner des risques supplémentaires. Tout en respectant autant que possible les souhaits de la personne survivante, une approche centrée sur la personne survivante permet des exceptions lorsque ses souhaits pourraient l'exposer, elle ou d'autres personnes, à un risque de préjudice supplémentaire.

5.4.4 Actions de réponse

Il est fréquent que les travailleurs humanitaires touchés par des incidents critiques ressentent une forme de « trahison institutionnelle » lorsque leur organisation, par ses actions ou son inaction, leur cause un préjudice supplémentaire ou semble même se ranger du côté des auteurs. Il est essentiel de veiller à ce que le personnel se sente pris en charge et écouté après un incident critique.

Intervention tenant compte du traumatisme subi

Une intervention tenant compte du traumatisme subi implique de comprendre les répercussions psychologiques et émotionnelles des traumatismes sur les individus et de veiller à ce que les réponses accordent la priorité à leur sûreté, leur bien-être et leur autonomisation, par exemple :

- **Sûreté** - garantir la sécurité physique et émotionnelle du personnel touché.
- **Confiance** - maintenir une communication claire et transparente afin d'instaurer la confiance.
- **Soutien par les pairs** - encourager le soutien par les pairs de la part des collègues, de la famille ou d'autres personnes ayant vécu des expériences similaires.
- **Collaboration et solidarité** - favoriser un esprit de partenariat et de collaboration dans le processus de rétablissement, en reconnaissant que la guérison est un effort commun.
- **Autonomie, expression et choix** - reconnaître les capacités des individus à défendre leurs propres intérêts et veiller à ce qu'ils aient la possibilité d'être entendus.
- **Considérations culturelles, historiques et de genre** - reconnaître que le profil de risque de chaque individu lui est propre et respecter les dimensions culturelles, historiques et de genre qui peuvent influencer son rétablissement.

- **Éviter la reviviscence du traumatisme** - faire attention au langage et aux actions afin d'éviter tout préjudice supplémentaire.
- **Éducation et sensibilisation** - former le personnel concerné aux effets des traumatismes sur la santé et le comportement des personnes touchées, et à la manière d'apporter une réponse appropriée.
- **Soutien aux aidants** - fournir des ressources et un soutien aux aidants, car ils sont exposés à un risque élevé de traumatisme secondaire.

- *Pour obtenir des recommandations générales sur la réponse aux incidents, voir le chapitre 4.4.*
- *Pour obtenir des recommandations plus détaillées sur la réponse aux incidents de violence sexuelle, voir le chapitre 7.7.*
- *Pour obtenir des recommandations plus détaillées sur les réponses aux enlèvements, voir le chapitre 7.9.*

Considérations et actions initiales

Immédiatement après un incident, il est recommandé d'assurer la sûreté physique du membre du personnel en le relocalisant dans un environnement sûr, si nécessaire et approprié, en lui apportant les premiers secours (y compris les premiers secours psychologiques) et en lui donnant accès à des soins médicaux professionnels (services physiques et psychosociaux). Cette mesure doit être suivie de près par l'élaboration d'un plan de sûreté personnelle sur mesure.

Étant donné que les répercussions médicales et psychologiques de l'incident peuvent ne pas être immédiatement apparentes, il est préférable que les options de soutien restent accessibles longtemps après l'incident.

Premiers secours psychologiques et soutien par les pairs

Le soutien par les pairs peut être un mécanisme efficace pour aider le personnel à traverser des périodes et des événements difficiles en favorisant un sentiment de compréhension commune et d'entraide. Cette approche permet au personnel d'apporter un soutien émotionnel et pratique immédiat à leurs collègues en détresse. La création d'un réseau de soutien peut s'avérer particulièrement utile dans les situations où un soutien psychosocial professionnel n'est pas immédiatement disponible. Le soutien par les pairs renforce non seulement la résilience, mais favorise également une culture de la compassion et de la solidarité au sein de l'organisation.

Les organisations doivent veiller à ce que tous les intervenants en cas d'incident, y compris les cadres supérieurs et les dirigeants, facilitent le soutien par les pairs et le leadership compatissant. Tout le personnel doit connaître les principes des premiers

secours psychologiques (PSP) (voir l'encadré ci-dessous), et toute personne susceptible d'interagir avec des collègues pendant et après des incidents critiques doit recevoir une formation de base aux PSP.

Principes des premiers secours psychologiques

Les trois principes fondamentaux sont :

- **Observer** - rechercher les signes de détresse ou les personnes qui pourraient avoir besoin d'un soutien particulier.
- **Écouter** - aborder la personne qui pourrait avoir besoin de soutien et lui demander la permission de l'aider ; l'écouter, essayer de la rassurer et l'aider à hiérarchiser ses besoins urgents ; respecter la confidentialité et son autonomie.
- **Mettre en relation** - donner des informations pratiques et aider la personne à entrer en contact avec les services de soutien (au sein de l'organisation ou auprès de ses proches, selon le cas).

Les PSP s'attachent à répondre aux besoins immédiats et à soulager la détresse en apportant un soutien compatissant destiné à aider les individus à faire face à l'impact émotionnel et psychologique d'un événement traumatisant. Il ne s'agit pas d'un traitement du trouble de stress post-traumatique (TSPT) ou d'autres troubles psychologiques. Ils visent à apporter réconfort et assurance, à écouter activement les préoccupations des personnes et à offrir une aide pratique pour répondre aux besoins immédiats, tels que la recherche d'un abri sûr ou de soins médicaux. Les PSP visent à valider les sentiments de la personne, en l'aidant à comprendre que ses réponses sont normales compte tenu des circonstances. Ils consistent à mettre les personnes en relation avec des réseaux de soutien, des ressources supplémentaires et des services de soutien professionnels, si nécessaire.

Pour être efficaces, les intervenants doivent être sensibles aux considérations culturelles, ethniques, religieuses, linguistiques, d'orientation sexuelle et d'identité de genre qui peuvent avoir une incidence sur l'expérience traumatique d'une personne et ses besoins en matière de rétablissement.

Il existe d'autres formes de soutien par les pairs, notamment les groupes de soutien, le mentorat, les systèmes de parrainage et les forums en ligne destinés aux travailleurs humanitaires actuels et anciens.

Plan de sûreté personnelle

Les plans de sûreté personnelle à la suite d'un incident traumatique identifient les moyens de rester en sécurité ou d'atténuer les préjudices supplémentaires, en fonction des besoins spécifiques en sûreté physique et psychologique de la personne survivante. Les éléments d'un plan de sûreté varient en fonction de l'incident, du membre du personnel et de l'organisation en question. Cependant, il peut généralement inclure :

- Mesures de sûreté immédiates, telles que la relocalisation dans un « lieu sûr », la mise en place de moyens de communication et de contacts d'urgence.
- Mesures de sécurité physique, telles que la mise à disposition d'un logement sûr et d'autres formes de soutien, notamment la présence d'un ami ou d'un collègue de confiance.
- Évaluation des risques liés à la menace et à toute vulnérabilité persistante du membre du personnel concerné.
- Mesures pour rester en sécurité à domicile (par exemple, serrures, alarme d'urgence, digicode à l'entrée).
- Mesures pour rester en sécurité dans d'autres lieux, tels que le lieu de travail et les lieux publics.
- Garantir l'accès aux documents importants tels que le passeport, le permis de conduire, la carte d'identité et la carte bancaire.
- Recommandations sur la conduite à tenir en cas de contact avec l'auteur, le cas échéant.
- Comment faire face aux déclencheurs psychologiques et émotionnels.
- Coordonnées en cas d'urgence.

Cette démarche peut être suivie d'une mise en relation du membre du personnel concerné avec les ressources appropriées, notamment un soutien médical et psychosocial (interne et externe). À plus long terme, les organisations peuvent envisager d'élaborer avec la personne concernée un plan de soutien qui lui permette de mieux comprendre le soutien, les prestations, les assurances et la prise en charge de longue durée dont elle peut bénéficier.

Actions à court terme

Une fois les besoins immédiats satisfaits, il peut être judicieux de procéder à une évaluation plus détaillée de la sûreté du membre du personnel concerné, d'adapter ses tâches, d'examiner les options en matière de mesures juridiques et judiciaires (telles que le signalement de l'incident à la police), de signaler l'incident conformément aux protocoles de l'organisation et de procéder à un débriefing psychologique. Il convient également de tenir compte des besoins des aidants et des personnes qui apportent leur soutien à la personne touchée.

Débriefing psychologique

À la suite d'un incident ou d'un événement, il peut être judicieux d'organiser un débriefing psychologique, c'est-à-dire une discussion structurée et animée visant à aider les personnes concernées à assimiler l'événement et à commencer à gérer leurs réponses émotionnelles. Cela implique généralement de réunir les personnes touchées par l'incident afin de discuter de ce qui s'est passé et de partager leurs réactions et leurs sentiments, puis d'organiser un soutien par les pairs et par des professionnels en santé mentale. Les objectifs du débriefing psychologique sont les suivants :

- aider les individus à donner un sens à l'événement et à leurs réactions à celui-ci ;
- normaliser leurs réponses émotionnelles ;
- donner des informations sur les réactions au stress et les stratégies d'adaptation ; et
- identifier les personnes qui pourraient avoir besoin d'un soutien supplémentaire.

Le débriefing est généralement proposé dans les 24 à 72 heures suivant l'événement afin de permettre aux participants d'exprimer leurs premières impressions et sentiments alors que l'événement est encore frais dans leur mémoire. Certains experts estiment que le débriefing psychologique ne devrait pas être obligatoire, car tout le monde ne tire pas profit d'une discussion immédiate sur l'incident, et pour certains, cela pourrait exacerber leur détresse. Cela dit, les croyances et la culture de l'obstination ou le stoïcisme qui prévalent dans le secteur humanitaire, ainsi que certaines attitudes culturelles spécifiques, peuvent parfois faire passer le fait d'admettre le besoin d'un soutien psychosocial pour une faiblesse. Pour remédier à cela, proposer un débriefing psychologique initial après un incident sous forme d'un « opt-out » (renoncer) plutôt que d'un « opt-in » (adhérer) peut considérablement augmenter la participation. De plus, le personnel peut craindre que le fait de reconnaître des blessures psychologiques puisse nuire à ses perspectives d'emploi. Pour remédier à cela, il peut être utile de rassurer le personnel en lui garantissant que le fait de demander un soutien ne compromettra pas ses opportunités d'emploi.

Soutenir le soutenant et les autres personnes touchées

Pendant et après la plupart des incidents critiques, l'attention se concentre sur les personnes survivantes, mais le soutien doit également s'étendre au-delà du membre du personnel directement touché et peut inclure l'offre d'une assistance aux témoins et à l'équipe au sens large. Les personnes qui interviennent en cas d'incident (à tous les niveaux de l'organisation) peuvent avoir besoin d'un soutien spécifique. Le stress cumulatif et le traumatisme vicariant sont des facteurs importants à prendre en compte, en particulier pour les personnes qui apportent leur soutien lors d'incidents réussis.

Les personnes qui ont besoin d'un soutien supplémentaire peuvent se voir offrir un congé pour se rétablir, un accès à un soutien psychosocial et une aide pour gérer leur charge de travail en dehors de l'incident. D'autres interventions efficaces consistent à offrir un accès à des ressources en santé mentale, telles que des services de counseling et des groupes

de soutien, des ateliers de gestion du stress, et à favoriser un environnement de travail solidaire où les employés peuvent discuter ouvertement de leurs préoccupations. Des vérifications régulières et la création d'occasions pour les employés de s'adonner à des pratiques de pleine conscience ou à des techniques de relaxation peuvent aider à gérer le stress et à prévenir le burn-out, en veillant à ce que tous les employés soient équipés pour faire face aux défis du lieu de travail et aux pressions personnelles.

Assistance postérieure à long terme

À plus long terme, il peut être judicieux de continuer à suivre le bien-être du membre du personnel par des vérifications régulières, d'adapter le plan de sûreté si nécessaire et de veiller à ce qu'il ait accès à un soutien psychosocial et à des soins médicaux continus, notamment à une thérapie tenant compte des traumatismes subis, si nécessaire. Cela peut être consigné dans un plan de soutien détaillé. À ce stade, il peut également être utile de fournir des recommandations plus détaillées sur les voies juridiques et judiciaires, ainsi que d'envisager des options de retour au travail.

Plan de soutien général

Selon la gravité de l'incident, le personnel touché peut avoir besoin d'une assistance postérieure à long terme. Le personnel responsable peut élaborer un plan de soutien complet avec le membre du personnel touché. Ce plan doit être flexible et centré sur la personne survivante, et inclure des évaluations et des traitements médicaux et psychologiques, une assistance postérieure, une réinsertion professionnelle et une transition vers des services à long terme tels que les services de santé nationaux. Le plan doit être sensible et ouvert aux facteurs culturels et aux voies de rétablissement préférées du membre du personnel touché, qui peuvent inclure des méthodes de guérison traditionnelles.

Les organisations doivent clairement définir l'étendue, le coût et la durée du soutien qu'elles sont en mesure et désireuses de fournir à la suite d'un incident, afin de gérer les attentes.

Le soutien à long terme aux personnes survivantes et au personnel impliqué dans des incidents graves peut également nécessiter :

- des aménagements dans les obligations professionnelles;
- une communication pleine de tact sur les absences;
- des vérifications régulières pour répondre aux préoccupations persistantes;
- la notification aux compagnies d'assurance, le cas échéant et avec le consentement des personnes concernées;
- une aide financière pour les personnes touchées et le personnel de soutien (par exemple, les membres de l'équipe de réponse); et
- un soutien pour les blessures à apparition tardive (par exemple, le TSPT ou les traumatismes crâniens).

Il peut être utile - et pour certaines organisations, il s'agit d'une politique standard - de conserver la documentation des rapports médicaux et autres sur le diagnostic des blessures afin d'orienter le soutien à long terme.

Exemple de cas : Échecs dans l'assistance postérieure

À la suite d'un incident critique grave, un travailleur humanitaire international a dû subir plusieurs évaluations psychologiques et psychiatriques, et soumettre huit rapports avant que son diagnostic de TSPT ne soit accepté par son employeur. Les rapports ultérieurs incluaient des diagnostics de dépression. De plus, le membre du personnel a dû fournir 12 rapports médicaux avant que l'organisation n'accepte de reconnaître que ses blessures étaient liées à une blessure par balle subie lors de l'incident. Ce processus n'était pas seulement difficile pour la personne concernée, mais il a également entraîné une perte de confiance des autres membres du personnel dans la volonté de l'organisation de les soutenir s'ils étaient blessés dans le cadre de leur travail dans des contextes à haut risque.

Justice et recours juridique

Lorsque des membres du personnel ayant subi des violences souhaitent obtenir justice par le biais de mécanismes juridiques formels, les organisations doivent être prêtes à les conseiller sur les options juridiques qui s'offrent à eux, notamment sur les implications d'un signalement aux autorités locales et sur les définitions juridiques de l'infraction pénale dans ce contexte. Les organisations doivent avoir une compréhension approfondie de l'environnement juridique dans lequel elles opèrent, notamment savoir à quel poste de police s'adresser en cas d'incident et connaître les exigences en matière de signalement (y compris les délais), et avoir établi des relations avec des juristes professionnels locaux de confiance qui peuvent fournir des conseils préalables et une assistance immédiate. Si un membre du personnel choisit d'intenter une action en justice, une organisation peut examiner dans quelle mesure elle est prête à fournir les types de soutien suivants (et comment) :

- Accompagner le membre du personnel concerné quand il va porter plainte, lors des entretiens et pour rassembler des preuves.
- Assurer une représentation juridique appropriée.
- Fournir des informations pratiques sur l'arrestation, les procédures judiciaires et les sanctions potentielles.

- Offrir un soutien psychosocial continu pour aider à surmonter le traumatisme lié aux procédures judiciaires.
- Expliquer les procédures et les délais, et veiller à ce que le personnel puisse prendre des décisions éclairées en matière de poursuites judiciaires.
- Mettre en place des services juridiques, médicaux et psychologiques en cas d'incident, notamment la collecte de preuves médico-légales.

Considérations à prendre en compte lorsque les auteurs présumés sont des membres du personnel

Dans les cas où l'auteur présumé est un membre du personnel, par exemple, en cas de violence sexuelle ou d'autres préjudices infligés à un autre membre du personnel, une organisation peut envisager les actions suivantes :

- **Devoir de diligence** - définir et fournir un soutien juridique, médical et psychosocial à l'auteur présumé de l'infraction, et déterminer quand ce soutien doit prendre fin.
- **Enquête interne** - lancer une enquête interne afin de recueillir des informations pour établir les faits, en veillant à faire preuve de sensibilité et de neutralité, et en faisant appel à des enquêteurs indépendants et qualifiés.
- **Procédures judiciaires** - être prêt à soutenir le personnel tout au long des procédures judiciaires et réfléchir aux conséquences de l'intervention des autorités locales ; ces considérations sont particulièrement importantes dans les contextes où les peines sont sévères et les conditions de détention mauvaises.

► Voir le chapitre 7.7 pour d'autres exemples et considérations en cas d'incident de violence sexuelle, ainsi que pour une analyse plus détaillée sur les enquêtes internes.

Retour au travail

Le retour au travail après un incident grave peut être difficile. Il est important de reconnaître que la réintégration est un processus propre à chaque individu et qu'elle peut prendre beaucoup de temps. Le moment du retour au travail doit être flexible, en tenant compte du fait que certaines personnes peuvent souhaiter reprendre leurs fonctions immédiatement, tandis que d'autres peuvent avoir besoin de plus de temps. Ce processus doit être géré avec tact, en proposant éventuellement d'autres postes ou en discutant des options de retraite si la personne choisit de ne pas revenir. Les organisations doivent s'assurer que les autres membres du personnel savent comment soutenir leurs collègues qui reviennent, tout en les aidant à surmonter l'impact émotionnel que l'incident a pu avoir sur eux.

5.4.5 Assurance et prestations

Aperçu de l'assurance

Les organisations doivent être prêtes à couvrir les coûts financiers de la réponse aux incidents touchant leur personnel. La plupart des organisations le font en souscrivant des polices d'assurance qui couvrent un large éventail de risques. Toutefois, certaines organisations ont opté pour des régimes d'auto-assurance, dans lesquels l'organisation assume le risque financier associé à certains événements, tels que les prestations de santé des employés, l'indemnisation des travailleurs ou les dommages matériels, en utilisant ses propres ressources pour payer les demandes d'indemnisation.

Il est important de garder à l'esprit que l'assurance offre une indemnisation, et non une protection. Elle n'empêchera pas la maladie ou les blessures, mais elle peut aider à atténuer les conséquences financières d'un incident. L'assurance ne couvrira également que les pertes incluses dans les conditions générales spécifiques de l'assureur. En fin de compte, ce que les compagnies d'assurance offrent, c'est un niveau de protection économique qui atténue les répercussions des événements négatifs en transférant le risque d'une perte économique importante à la compagnie d'assurance, en échange d'une prime.

Les accidents et incidents de sûreté et sécurité peuvent avoir des conséquences financières importantes pour le personnel concerné, sa famille et l'organisation. Il y a des coûts immédiats, tels que l'évacuation médicale et les soins d'urgence, qui peuvent rapidement atteindre des sommes très importantes. Il existe également des coûts potentiels à long terme, tels que ceux résultant d'un handicap permanent (par exemple à la suite de la perte d'un membre) et des besoins en soins de longue durée. Certaines polices d'assurance prévoient l'intervention d'un spécialiste en gestion de risque pour aider à la mise en place d'une réponse, ainsi que la prise en charge des coûts liés à des incidents tels que la détention illégale, l'évacuation pour cause d'insécurité et l'enlèvement.

Le devoir de diligence d'une organisation consiste à offrir une compensation financière au personnel concerné en cas de blessure, de maladie, de décès ou d'autres événements de la vie. Comme la plupart des organisations ne peuvent pas couvrir ces coûts elles-mêmes, elles ont recours à une assurance pour offrir cette compensation. Pour les organisations internationales, cette responsabilité s'applique également au personnel national. Le fait que la couverture d'assurance de certaines organisations internationales ne s'étende pas à tous les membres du personnel devient donc un grave problème opérationnel et éthique. L'assurance est un outil qui peut aider l'employeur à s'acquitter de sa responsabilité, mais elle ne devrait pas constituer l'intégralité du soutien qu'une organisation apporte au personnel touché.

Les travailleurs humanitaires doivent être informés des détails de la couverture d'assurance fournie par leur organisation (à l'exception éventuelle des polices d'assurance spéciales pour les situations d'urgence, par exemple la couverture en cas d'enlèvement et demandes de rançon). Le personnel a le droit de se renseigner sur la couverture d'assurance qui lui est fournie et de demander des informations complémentaires. Si le préjudice psychologique et le handicap peuvent être pris en compte dans l'indemnisation des frais médicaux et des accidents du travail, ce n'est pas automatique. L'organisation devra peut-être s'assurer que ces aspects sont pris en compte, et ne pas simplement supposer qu'ils le sont, en particulier si les documents organisationnels mentionnent spécifiquement le soutien en santé mentale.⁸⁵

Exemple de cas : Évaluation de l'accès et de l'éligibilité

Une organisation a cartographié l'accès et l'éligibilité à l'aide médicale et à l'évacuation. Outre la transparence qu'elle offre au personnel en matière de couverture, cette vue d'ensemble permet à l'organisation d'identifier les lacunes et les recoupements en matière d'assurance et d'améliorer l'équité.

L'organisation a d'abord identifié les groupes bénéficiaires :

- Personnel des programmes de pays
- Personnel international
- Personnel du siège
- Travailleurs à distance
- Invités en déplacement ne faisant pas partie du personnel (par exemple, membres du conseil d'administration)

Pour chaque groupe, l'aperçu répertorie les détails relatifs à l'accès à un prestataire d'aide médicale et à la couverture d'assurance applicable :

- Accès à un prestataire d'aide médicale
 - Qui?
 - Quand?
 - Informations, conseils et orientations? Oui/Non
 - Soins médicaux de routine/électifs?
 - Aide médicale en cas d'accident/maladie? (par exemple: Oui, lors de déplacements internationaux pour raisons professionnelles)
 - Évacuation médicale en cas d'accident/maladie (par exemple: Oui, lors de déplacements internationaux pour raisons professionnelles)

85 Reilly, L. (2024) 'Is your mental health covered? Insurance for psychological injury' (en anglais, « Votre santé mentale est-elle couverte? Assurance pour les dommages psychologiques »). Bond (www.bond.org.uk/news/2024/05/is-your-mental-health-covered-insurance-for-psychological-injury/).

- Que couvre l'organisation? (Détails sur le soutien fourni gratuitement et le soutien pour lequel des frais seront encourus)
- Couverture d'assurance applicable
 - Informations générales (sur l'aide au paiement, la soumission des demandes d'indemnisation)
 - Soins médicaux de routine/électifs dans le pays (par exemple, couverture médicale locale, couverture d'assurance maladie mondiale, aucune couverture fournie par l'organisation)
 - Soins médicaux de routine/électifs en dehors du pays (voir ci-dessus)
 - Soins médicaux en cas d'accident ou de maladie lors de déplacements internationaux pour raisons professionnelles (par exemple, assurance accidents déplacements professionnels, assurance maladie mondiale)
 - Évacuation médicale en cas d'accident ou de maladie lors de déplacements internationaux pour raisons professionnelles (voir ci-dessus)

Lacunes et absence d'assurance maladie nationale

Pour offrir un soutien adéquat aux travailleurs humanitaires nationaux, il faut non seulement leur garantir l'accès à l'aide médicale et leur donner droit à celle-ci, mais aussi leur offrir des avantages plus larges tels que la couverture et l'accès à un soutien psychosocial, une assurance-vie, des prestations pour handicap, une indemnisation des accidents du travail et des allocations de formation et de perfectionnement/éducation rémunérées. L'aide à l'évacuation des travailleurs humanitaires nationaux reste toutefois difficile, car elle peut nécessiter beaucoup plus de négociations avec les prestataires de services d'évacuation et requiert des visas et d'autres autorisations administratives, en plus des coûts financiers liés à l'assurance. Dans certains cas, les régimes d'assurance locaux sont soit indisponibles, soit inabordables. Certains transporteurs internationaux peuvent offrir une couverture aux ressortissants locaux, mais cela dépend du pays et de l'assureur.

Comme il n'est pas envisageable de ne souscrire aucune assurance, les organisations peuvent :

- Opter pour un régime d'auto-assurance, si cela est possible, dans le cadre duquel l'organisation met de côté des fonds pour couvrir les risques et les réclamations potentiels au lieu de souscrire une assurance auprès d'un prestataire externe.
- Négocier des extensions de police d'assurance (mondiales).
- Proposer une somme forfaitaire pour la couverture médicale.

- Appuyer les demandes d'indemnisation ou d'aide financière en cas de maladie, de blessure ou de décès, au cas par cas.
- Mettre en place un système d'assurance coopératif interne avec un fonds d'assurance alimenté par une somme forfaitaire versée par l'organisation, à laquelle s'ajoutent les cotisations des employés participants.
- Offrir des soins de santé gratuits à tous les employés à titre d'avantage social (comme c'est souvent le cas dans les organisations d'aide médicale).

Il est probable que, dans les pays exposés aux dangers naturels, l'assurance médicale nationale ne fonctionnera pas en temps de crise et qu'il faudra envisager d'autres solutions.

► *Pour plus d'informations sur les considérations relatives aux urgences médicales, voir le chapitre 5.5.*

Polices d'assurance courantes

Les besoins en assurance varient d'une organisation à l'autre. L'assurance doit être considérée comme un élément d'une stratégie d'atténuation des risques et, comme tout autre élément, elle nécessite une évaluation complète des risques afin d'en apprécier pleinement l'importance. La plupart des organisations ont souscrit des polices d'assurance offrant les types de couverture suivants (la liste ci-dessous n'est pas exhaustive):

- Assurance maladie standard.
- Assurance accident standard, y compris en cas de décès ou de mutilation accidentels.
- Assurance pour handicap, partiel ou total, à long terme ou à court terme.
- Assurance médicale d'urgence, comprenant la couverture des frais d'évacuation médicale et des soins d'urgence sur place et pendant le transport.
- Assurance contre les risques de guerre: il s'agit souvent d'une police distincte ou d'un supplément payant couvrant les blessures ou les décès causés par des « actes de guerre ou de terrorisme » (voir la section « Clauses d'exclusion » ci-dessous pour plus d'informations).
- Assurance risques spéciaux, couvrant l'expertise technique en gestion de crise et les imprévus afin de faciliter la libération des otages en toute sécurité.
- Assurance responsabilité civile générale/professionnelle: l'une des polices d'assurance les plus courantes qui couvre les coûts liés aux réclamations pour dommages matériels ou corporels causés à des tiers, par exemple en cas de chute dans les locaux de l'organisation.
- Assurance responsabilité civile automobile et assurance flotte/automobile: polices couvrant les responsabilités juridiques et financières telles que la responsabilité civile, les collisions et la couverture complète, ainsi que la protection contre un éventail plus large de risques, y compris les dommages causés aux véhicules.

- Indemnisation des accidents du travail : permet aux employés blessés au travail de bénéficier de prestations médicales et salariales. L'indemnisation des bénévoles étrangers étend la couverture aux employés travaillant à l'étranger, y compris les risques supplémentaires et le rapatriement. Les régimes locaux garantissent le respect des réglementations locales en matière d'assurance et offrent les protections nécessaires aux travailleurs dans certains pays.
- Assurance responsabilité civile professionnelle : couvre les entreprises contre les réclamations pour négligence, erreurs ou omissions dans les services ou conseils qu'elles fournissent.
- Assurance des dirigeants et administrateurs : protège les dirigeants et administrateurs contre les pertes financières personnelles, les frais juridiques et les enquêtes réglementaires.
- Assurance responsabilité civile liée aux pratiques d'emploi : couvre les employeurs contre les réclamations liées à la discrimination au travail, au harcèlement, au licenciement abusif et à la rupture de contrat de travail.
- Assurance vol et détournements : protège les entreprises contre les pertes financières dues au vol, à la fraude ou au détournement de fonds par des employés ou des tiers.
- Cyber-assurance : couvre les pertes financières résultant de violations de données, de cyberattaques et d'autres incidents liés à la cybersécurité.
- Assurance de biens – couvre les dommages ou la perte d'actifs physiques tels que les bâtiments et les équipements en cas d'incendie, de vol ou d'autres risques.
- Assurance contre la violence politique et le terrorisme : couvre les pertes résultant de violences à caractère politique, notamment les guerres, les émeutes et les « actes terroristes ».

Clauses d'exclusion

Il est essentiel que les organisations lisent attentivement les clauses en petits caractères et se renseignent explicitement sur ce qui est couvert et ce qui ne l'est pas, afin de déterminer clairement l'étendue des lacunes dans la couverture d'assurance qu'elles seraient susceptibles de devoir couvrir elles-mêmes. Les polices d'assurance peuvent ne pas s'appliquer dans certaines conditions, et les détails et l'interprétation de ces clauses d'exclusion peuvent revêtir une importance cruciale. Les organisations peuvent se retrouver sous-assurées et contraintes de couvrir elles-mêmes des coûts imprévus.

La couverture d'assurance peut exclure les risques de guerre au sens large (certains types de risques de guerre ou d'actes malveillants, en particulier les « actes de terrorisme » tels que les attentats à la bombe dans les lieux publics), sauf si l'organisation a ajouté une clause relative aux risques de guerre à son contrat d'assurance ou souscrit un contrat distinct. Même avec une clause relative aux risques de guerre, les compagnies d'assurance peuvent exclure certaines zones de guerre de leur couverture. Certaines de ces zones de guerre sont prédéterminées par l'assureur. Les assureurs peuvent également ajouter

certain pays à leur clause d'exclusion soit lors du renouvellement du contrat, soit même pendant la durée du contrat existant, par notification écrite (les détails à ce sujet figureront dans le contrat et la plupart des courtiers peuvent aider les organisations à comprendre les termes spécifiques du contrat).

Une assurance souscrite dans un pays faisant l'objet d'une clause d'exclusion peut ne pas couvrir les blessures, maladies, décès ou handicaps résultant directement d'un «acte de guerre/terrorisme». Cela signifie que le décès d'un membre du personnel causé par un véhicule percuté par un drone armé n'est pas couvert par l'assurance, contrairement au décès d'un membre du personnel causé par un accident de la route. Les primes à payer pour ajouter des pays à la clause d'exclusion de l'assurance («rachat de cette assurance») peuvent être très élevées. Si l'organisation souhaite néanmoins employer du personnel dans ce pays, une option pourrait être de «s'auto-assurer», par exemple en s'engageant à indemniser le personnel travaillant ou se déplaçant dans ce pays à hauteur du montant que la compagnie d'assurance aurait couvert si le pays n'avait pas été exclu de la couverture.

Autres exemples d'exclusions:

- La couverture s'applique uniquement pendant les missions professionnelles (par exemple en Somalie, mais pas pendant une période de repos et de détente à Nairobi).
- La couverture s'applique uniquement pendant les heures de travail (par exemple jusqu'à 18 heures, mais pas après ni pendant les week-ends).
- La couverture s'applique uniquement si l'organisation dispose de certaines clauses de sécurité écrites, telles que le principe de non-paiement des rançons.
- La couverture exclut le personnel sous contrat à durée déterminée, le personnel originaire de certains pays ou les bénévoles.

Il est également important d'identifier ce qui peut être considéré comme une «condition préexistante» et qui n'est donc pas couvert, par exemple les troubles de santé mentale ou physiques. Une organisation doit discuter de son processus de recrutement et de diligence raisonnable avec son courtier/prestataire d'assurance.

Considérations relatives à l'assurance

- **Former le personnel.** Le personnel doit comprendre l'étendue de la couverture accident et assurance lorsqu'il travaille et se déplace pour le compte de l'organisation, ainsi que l'impact potentiel sur toute assurance personnelle qu'il pourrait avoir (par exemple, les polices d'assurance-vie (telles que celles souscrites dans le cadre d'un prêt hypothécaire) devenant caduques s'il travaille dans une zone à haut risque).
- **Couverture au début et à la fin du contrat de travail.** Les organisations doivent savoir précisément quand la couverture commence et prend fin. Il est important de déterminer si le membre du personnel est couvert s'il ne perçoit pas encore de salaire ou s'il n'a pas encore commencé sa mission, par exemple. Il convient également

que l'organisation et la personne concernée sachent clairement à quel moment la couverture cesse après la fin de la mission. Ceci est important pour les blessures psychologiques, qui peuvent se manifester longtemps après un incident.

- **Primes.** Les organisations peuvent souvent négocier avec leur courtier pour obtenir des primes moins élevées si elles peuvent démontrer que des mesures d'atténuation des risques appropriées sont en place (par exemple, des politiques, des procédures et des formations à la sécurité). Certains prestataires offrent un crédit qui peut être utilisé pour améliorer les mesures de gestion des risques de sécurité.
- **Équité dans la couverture.** Lorsque l'on aborde la question des polices d'assurance au sein des organisations internationales, il est essentiel de traiter les disparités et les défis potentiels qui peuvent surgir entre le personnel national et le personnel international. Ces disparités se manifestent souvent dans l'accès aux soins de santé et aux services d'urgence, tels que les évacuations médicales et la qualité des services de santé internationaux par rapport aux services de santé nationaux.

Informations complémentaires

Analyse

Barkwill, D. (2022) *Letter of recommendation: reversing the mental health pandemic amongst aid workers* (en anglais, « Lettre de recommandation : inverser la pandémie de santé mentale chez les travailleurs humanitaires »). AidEx (<https://gisf.ngo/resource/letter-of-recommendation-reversing-the-mental-health-pandemic-amongst-aid-workers/>).

Reilly, L. (2024) 'Is your mental health covered? Insurance for psychological injury' (en anglais, « Votre santé mentale est-elle couverte ? Assurance pour les dommages psychologiques »). Bond (www.bond.org.uk/news/2024/05/is-your-mental-health-covered-insurance-for-psychological-injury/).

Recommandations

European Interagency Security Forum (2017) *Abduction and kidnap risk management* en anglais, « Gestion de risque en cas d'enlèvement et d'enlèvement contre rançon » (<https://gisf.ngo/resource/abduction-and-kidnap-risk-management-guide/>).

European Interagency Security Forum (2019) *Gérer la violence sexuelle à l'encontre du personnel humanitaire : prévention, préparation, réponse et suivi* (<https://gisf.ngo/resource/managing-sexual-violence-against-aid-workers/>).

Linnell, H. (2017) *Guide to selecting appropriate crisis management insurance* (en anglais, « Guide pour choisir une assurance en gestion de crise adaptée »). European Interagency Security Forum (www.gisf.ngo/resource/guide-to-selecting-appropriate-crisis-management-insurance).

Organisation mondiale de la Santé, War Trauma Foundation et World Vision International (2011) *Les premiers secours psychologiques : Guide pour les acteurs de terrain*. Organisation mondiale de la Santé (www.who.int/publications/i/item/9789241548205).

5.5 Considérations médicales et de santé

Étant donné que les incidents de sécurité impliquent souvent des dommages physiques pour le personnel, la gestion des risques de sécurité doit nécessairement tenir compte des considérations médicales d'urgence, en particulier lorsque le travail s'effectue dans des contextes instables ou en situation de conflit actif. Même en l'absence de violence, les problèmes de santé sont inévitables, qu'il s'agisse d'exposition à des maladies, d'aggravation de maladies chroniques ou de blessures mortelles, et nécessitent des mécanismes clairs de prévention, de préparation et de réponse. Ce chapitre décrit les éléments essentiels nécessaires à la gestion des risques et incidents médicaux, notamment la préparation, les premiers secours, les réponses d'urgence et le transfert médical. Ces recommandations peuvent aider les organisations à identifier les mesures à prendre pour répondre au mieux aux défis médicaux. Toutefois, ce chapitre n'est pas exhaustif et les organisations sont encouragées à consulter des prestataires médicaux afin d'élaborer les politiques et protocoles les mieux adaptés à leur personnel et à leur contexte spécifique.

5.5.1 Prévention et atténuation des risques

Bon nombre des défis médicaux auxquels sont confrontées les organisations peuvent être évités. De même, les capacités à répondre efficacement aux problèmes sanitaires et médicaux dépend souvent de considérations non médicales, notamment les évaluations de santé avant le départ, une solide sûreté du personnel et la mise en place de cadres détaillés à l'intention des cadres supérieurs sur la manière de gérer les incidents médicaux.

Une réponse rapide et appropriée aux urgences sanitaires nécessite une bonne compréhension des risques sanitaires et médicaux qui pèsent sur le personnel et le paysage des soins de santé environnant. Cela implique d'inclure les risques sanitaires et médicaux pertinents dans les exercices d'évaluation des risques et de cartographier les ressources en soins de santé disponibles pour aider à gérer les urgences médicales.

Remarque sur la santé et la sûreté au travail

La santé et la sûreté au travail désignent les mesures, pratiques et politiques visant à protéger la santé, le bien-être et la sûreté des personnes sur leur lieu de travail, ainsi que du grand public. Elles comprennent la promotion et le maintien du bien-être physique et mental des travailleurs, la prévention des maladies et des accidents liés au travail, ainsi que l'inspection régulière des lieux de travail afin de détecter les dangers potentiels.

La santé et la sûreté au travail sont souvent codifiées dans la législation gouvernementale et couvrent de nombreuses mesures différentes qui dépassent le cadre de la présente RBP. Cependant, ce chapitre examine certaines considérations sanitaires particulièrement pertinentes pour la gestion des risques de sécurité, en mettant l'accent notamment sur les bonnes pratiques en matière de préparation et de réponse aux urgences médicales. Pour obtenir des recommandations plus détaillées, consultez les ressources spécialisées en matière de santé et de sûreté au travail, telles que celles de l'Organisation internationale de normalisation *ISO 45001:2018: Systèmes de gestion de la santé et de la sûreté au travail* (www.iso.org/iso-45001-occupational-health-and-safety.html).

Évaluation des risques sanitaires locaux et des capacités locales

Avant de lancer les activités du programme, il convient de se poser certaines questions, notamment sur les conditions sanitaires générales et les tendances dans la zone d'opérations, ainsi que sur les principaux risques susceptibles d'entraîner des urgences médicales. Voici les plus courants :

- maladies infectieuses (par exemple, hépatite, paludisme, choléra) ;
- blessures causées par les conflits armés (par exemple, blessures par balle et blessures causées par les mines terrestres et les frappes aériennes) ;
- blessures causées par des agressions (par exemple, coups de couteau, passage à tabac) ;
- blessures causées par des accidents de la route ;
- maladies non transmissibles ou problèmes de santé chroniques chez le personnel, tels que le diabète ou l'hypertension ; et
- problèmes de santé mentale.

Les risques seront amplifiés si l'accès aux services de santé dans la zone est limité ou inexistant. Les évaluations doivent donc inclure une cartographie des ressources médicales disponibles (par exemple, hôpitaux, ambulances, prestataires de soins de santé et médicaments ou fournitures médicales) et une évaluation de leur capacité à soutenir la réponse aux incidents et à répondre aux besoins spécifiques du personnel. Ces évaluations devraient inclure un accès rapide aux centres de crise pour victimes de viol et à d'autres structures offrant des soins spécialisés et une prophylaxie post-exposition au VIH (PEP) aux personnes survivantes d'agression sexuelle.

► Pour plus d'informations sur les risques de violence sexuelle, voir le chapitre 7.7.

Au minimum, les organisations devraient disposer des coordonnées d'urgence de prestataires locaux réputés ainsi que de l'emplacement des centres de soins tertiaires les plus proches. Il est également important d'identifier les prestataires qui sont disponibles 24 heures sur 24 et 7 jours sur 7 pour les soins physiques et psychologiques. Pour le soutien en santé mentale, les organisations peuvent envisager à la fois des services disponibles localement et à distance.

► *Pour plus de détails sur les risques et le soutien en santé mentale, voir le chapitre 5.4.*

Il convient de noter que le prestataire de soins de santé le plus proche et/ou le plus fiable peut être une ONG médicale. Il est conseillé au personnel d'encadrement d'établir des relations avec les principaux prestataires de services de santé. Cela peut accélérer la prestation des soins et améliorer leur qualité en cas d'urgence.

Certificat médical d'aptitude

Si l'organisation affecte des membres du personnel (et les personnes à charge qui les accompagnent) dans un lieu éloigné de leur domicile, elle a la responsabilité de veiller à ce que leurs besoins en matière de santé puissent y être satisfaits. Un processus de certificat médical d'aptitude permet d'évaluer l'aptitude à exercer la fonction (c'est-à-dire une évaluation de la santé au travail) et l'aptitude à assumer la nouvelle affectation (c'est-à-dire que les besoins actuels en matière de santé peuvent être satisfaits dans le pays d'affectation). Les règles relatives à ce qu'il est acceptable ou non de demander aux employés varient selon les juridictions, et les organisations doivent également indiquer clairement comment ces informations seront utilisées et par qui. L'examen peut inclure une analyse ciblée des antécédents médicaux de la personne (santé physique et mentale), des traitements en cours, des médicaments pris et des facteurs de risque de maladie grave ou de blessure. De nouveaux certificats peuvent être demandés avant de nouvelles affectations ou après des changements importants dans l'état de santé d'un membre du personnel ou dans les conditions de risque sur le lieu de travail. Le personnel peut également être encouragé à mettre à jour son certificat médical en cas de changement de son état de santé ou de ses besoins potentiels pendant la durée de l'affectation. Cette évaluation devra être effectuée par des professionnels qualifiés et devra être traitée de manière confidentielle (voir ci-dessous).

Si les antécédents médicaux d'un membre du personnel nécessitent un plan d'atténuation des risques, son médecin peut travailler avec lui pour identifier un plan approprié et réalisable à proposer à l'organisation. Dans le cadre de ce processus, le personnel doit être informé de tout obstacle potentiel à l'accès aux soins de santé pendant l'affectation, y compris la possibilité d'un retard ou d'une prise en charge rudimentaire. Un plan général peut être communiqué de manière confidentielle aux dirigeants de pays (selon le principe du «besoin de savoir») afin de garantir sa mise en œuvre sans contrainte ni difficulté excessive. Voici quelques exemples:

- Un membre du personnel a besoin d'un médicament qui n'est pas disponible localement. Cependant, son médecin traitant accepte de lui prescrire une provision d'un an à utiliser pendant son séjour sur place.
- L'enfant d'un membre du personnel souffrant d'une grave allergie aux arachides accompagnera sa famille dans le cadre d'une affectation à l'international. La famille a été formée à l'utilisation d'un auto-injecteur d'épinéphrine et s'engage à toujours en emporter deux avec elle lors de ses déplacements. Elle a également reçu des informations sur l'alimentation locale et sur la manière d'éviter toute exposition accidentelle aux arachides.

Comme pour les autres protocoles de sûreté et sécurité, le personnel doit comprendre clairement qu'il est tenu de se conformer à tous les conseils médicaux et sanitaires pendant sa mission, y compris, par exemple, les politiques exigeant la vaccination ou la prise de médicaments antipaludiques.

Il est important de veiller à ce que toutes les informations médicales soient transmises soit dans un document confidentiel que l'organisation conservera en toute sécurité, soit directement sur un portail en ligne sécurisé (celui de l'organisation ou d'un prestataire de services externe), soit par e-mail crypté avec des fichiers protégés par un mot de passe.

Confidentialité médicale

Il est conseillé à chaque organisation d'établir des directives et des attentes en matière de confidentialité médicale, notamment en ce qui concerne l'existence éventuelle de protocoles différents selon l'environnement et l'accès aux prestataires de soins médicaux. Le personnel doit être informé de ces mesures et savoir clairement qui a accès à ses informations médicales et dans quelles circonstances celles-ci peuvent être divulguées à des tiers.

Les informations médicales personnelles doivent rester strictement confidentielles, sauf dans des circonstances exceptionnelles prédéfinies. Il est recommandé de former le personnel concerné à la confidentialité médicale et à la protection des données. Personne d'autre ne doit avoir accès aux informations médicales d'un membre du personnel sans son consentement explicite.

Le personnel chargé de domaines tels que la santé et la sûreté peut parfois avoir besoin de demander des informations médicales supplémentaires pour étayer sa prise de décision. En cas d'urgence médicale, le personnel de soutien peut étendre la confidentialité médicale aux dirigeants de l'organisation sur une base limitée, en cas de nécessité absolue.

Capacités et pratiques permanentes

En fonction des risques évalués, les mesures d'atténuation peuvent nécessiter la mise en place ou le renforcement des capacités de l'organisation à répondre aux urgences médicales et l'élaboration des volets médicaux des plans de réponse en cas de crise et de gestion des incidents.

Si les risques sanitaires et médicaux sont élevés et que les ressources sanitaires externes disponibles sont faibles, les organisations doivent déterminer si elles disposent des capacités de base pour prendre en charge leur personnel en cas d'incident. Ne pas disposer de telles capacités constituerait un manquement au devoir de diligence.

Les capacités sanitaires et médicales peuvent comprendre les éléments suivants :

- **Mesures préventives.** Réduire le risque médical dès le départ, par exemple en mettant en place des protocoles de sécurité rigoureux et en coordonnant les équipes de logistique et d'approvisionnement afin de garantir un accès continu aux fournitures nécessaires.
- **Protocoles et procédures.** Créer et réévaluer régulièrement les protocoles de gestion des incidents médicaux, y compris les responsabilités et les protocoles spécifiques en matière de signalement (par exemple, les évacuations médicales, y compris le transport et la coordination avec les services d'évacuation locaux et internationaux).
- **Capacités en matière de premiers secours.** Proposer une formation aux premiers secours (notamment la réanimation cardio-pulmonaire (RCP) et tout besoin spécifique aux environnements reculés), des trousse de premiers secours dans tous les bureaux (y compris les espaces de travail partagés, les sites de projet, les entrepôts, les résidences du personnel et les véhicules) et des recommandations (identifier un point focal pour les questions médicales, chargé de la gestion des trousse, y compris des évaluations périodiques pour vérifier leur contenu et leurs dates d'expiration).
- **Fournitures médicales d'urgence et logistique.** Déterminer les autres fournitures médicales d'urgence nécessaires, telles que les kits de prophylaxie post-exposition au VIH, et comment les obtenir ou y avoir accès (en les stockant directement ou en passant par une autre entité), et veiller à ce qu'elles soient réapprovisionnées en temps opportun.
- **Éducation à la santé.** Proposer une éducation à la santé, par exemple sous forme de webinaires/briefings du personnel sur les épidémies, et élaborer un plan d'éducation continue à la santé sur les risques identifiés. Cela devrait inclure les risques pour la santé mentale.
- **Avantages médicaux.** Évaluer et optimiser les avantages médicaux offerts à l'ensemble du personnel, tant sur le plan physique que mental, afin de répondre aux besoins du personnel et d'améliorer l'équité (en particulier dans le cas des travailleurs humanitaires nationaux).

- **Aide médicale externe.** Identifier et passer des contrats avec des prestataires externes d'aide médicale afin de fournir des informations, des conseils et des orientations en matière de santé physique et mentale, et prendre des dispositions avec un prestataire/une clinique pour les soins de routine/électifs, le transport médical urgent/d'urgence et l'accès aux soins de santé (voir la section 5.5.2 ci-dessous pour plus de détails). Établir et entretenir des relations avec les prestataires et les établissements de soins de santé locaux pour le soutien et les orientations.
- **Télémédecine.** Mettre en œuvre des solutions de télémédecine, lorsque cela est approprié et possible, afin d'offrir des consultations à distance avec des professionnels de santé, en particulier dans les zones où l'accès aux établissements de santé est limité.

Liste de contrôle de la santé sur le lieu de travail

Voici quelques mesures clés que les organisations peuvent mettre en place pour protéger la santé de leur personnel :

- Encourager les bilans de santé individuels réguliers/annuels
- Mettre à disposition des trousseaux de premiers secours dans tous les bureaux, résidences et véhicules
- Former le personnel aux premiers secours
- Aider le personnel dans l'accès aux médicaments et prévoir des mesures d'urgence en cas de perte
- Certificat médical pour les déploiements et les déplacements du personnel
- Plans d'atténuation des risques médicaux pour le personnel présentant des risques sanitaires accrus
- Webinaires sur les risques pertinents/limités dans le temps, tels que les épidémies
- Recommandations sur la confidentialité médicale et la protection des données, et formation au traitement des informations personnelles
- Personnes à contacter en cas d'urgence (pour le personnel et leurs familles)
- Visites médicales du travail dans les bureaux et/ou les bureaux à domicile
- Conseils d'experts en ergonomie sur les équipements de bureau
- Un plan d'accessibilité et d'inclusion des personnes en situation de handicap
- Ajustements en matière d'inclusivité et d'accessibilité dans les bureaux et autres espaces organisationnels (accessibilité physique et technologique)
- Accès à la télémédecine

- Accès aux services de santé mentale en général, ainsi qu'à un soutien spécialisé à la suite d'un incident
- Plans de sécurité, y compris les risques sanitaires et leur atténuation
- Briefings écrits ou oraux sur la santé avant le départ et rapports sanitaires spécifiques au lieu de destination (internes ou fournis par un prestataire d'aide médicale externe)
- Une série de ressources pour le personnel (dans les langues pertinentes), notamment l'accès à des applications de premiers secours, des recommandations écrites et des coordonnées, avec des instructions claires sur la manière d'obtenir de l'aide en cas d'urgence
- Couverture d'assurance par un prestataire commercial ou autre dispositif en cas d'incident

Plus le risque d'urgence médicale est élevé (par exemple dans les zones de conflit actif ou lors d'épidémies), plus une organisation doit s'efforcer de soutenir et de former son personnel, de se préparer aux incidents et de mettre en place des mesures de réponse appropriées et rapides.

Exemple de bonnes pratiques : Intégrer la santé pendant les situations de sécurité

Après le début des violents affrontements au Soudan en avril 2023, qui ont entraîné l'effondrement du système de santé à Khartoum, une organisation a mis en place des consultations de télémedecine pour le personnel. Cela comprenait des conseils via la télémedecine pour la femme enceinte d'un membre du personnel avant et pendant l'accouchement, ainsi que l'identification des pharmacies disposant d'insuline en stock et l'organisation de la livraison à un membre du personnel atteint de diabète.

5.5.2 Préparation

Préparation aux urgences médicales

Afin de garantir des réponses rapides et appropriées en cas d'urgence médicale et d'évacuation, il est essentiel de se concentrer sur la préparation médicale avant que les incidents ne se produisent. Il est tout aussi important d'encourager le personnel à signaler rapidement toute maladie ou blessure. Par exemple, une organisation préférera qu'un membre du personnel signale rapidement une douleur abdominale intense plutôt que de se retrouver dans une situation où ce membre du personnel

s'effondre en raison d'une appendicite perforante pendant son transit. Il est souvent possible d'éviter des conséquences plus graves si le personnel signale rapidement les problèmes et demande de l'aide. En veillant au respect de la confidentialité médicale, les organisations peuvent contribuer à améliorer le signalement, car le personnel aura davantage confiance dans le responsable médical désigné.

Dans certaines circonstances, les problèmes médicaux peuvent être traités avec l'aide d'un prestataire d'aide médicale externe. Un prestataire d'aide n'est pas une compagnie d'assurance, bien que certaines compagnies d'assurance puissent fournir (une partie de) l'aide médicale et l'aide à l'évacuation dans le cadre de leur offre. Les prestataires peuvent être rémunérés par la compagnie d'assurance (si le prestataire d'aide a conclu un accord de facturation directe avec celle-ci), par l'organisation (au moyen d'une garantie de paiement) ou par le membre du personnel.

Si un membre du personnel est blessé ou tombe malade pendant son travail, il faut prévoir un moyen de couvrir les frais associés. Cela peut se faire au moyen de polices d'assurance appropriées. Cependant, cela peut s'avérer difficile pour les petites organisations locales qui fonctionnent avec des budgets serrés et dans des endroits où le marché de l'assurance commerciale est limité (voire inexistant). Dans de tels cas, les organisations pourraient se tourner vers des régimes d'auto-assurance ou vers le soutien de donateurs et de partenaires.

► *Voir le chapitre 5.4 pour plus d'informations sur l'assurance.*

Les services de soutien que les prestataires de services de sécurité et d'aide médicale peuvent fournir comprennent :

- un accès 24 heures sur 24 et 7 jours sur 7 au centre d'assistance le plus proche, en cas d'urgence et pour des conseils quotidiens ;
- des conseils et des informations d'experts en matière de médecine, de sécurité et de déplacements ;
- des alertes médicales et de sécurité des déplacements en temps réel spécifiques à un lieu donné ;
- des listes de contrôle pour les déplacements ; et
- des coordonnées à jour en cas d'urgence.

Avec ou sans aide médicale externe, il est recommandé aux organisations de veiller à ce qu'il existe un point de contact au sein de l'organisation pour les questions médicales.

Exemple de cas : Attentat à la bombe dans un restaurant à Islamabad, au Pakistan, en 2008

En 2008, des kamikazes ont pris pour cible un restaurant italien fréquenté par des étrangers à Islamabad, blessant le personnel d'au moins deux organisations humanitaires. Ces deux organisations disposaient de prestataires d'aide médicale qui ont identifié le même hôpital à Islamabad. L'une d'elles s'était rendue à l'hôpital, avait ouvert un compte et établi une relation. Son personnel a été amené au triage de l'hôpital dans l'heure qui a suivi l'attaque. La deuxième organisation s'est rendue à l'hôpital et a demandé que son personnel soit admis conformément à la procédure de son prestataire médical. L'hôpital a demandé une confirmation de la capacité de paiement de l'organisation. Le traitement de cette demande a pris plusieurs heures, et le personnel n'a été admis à l'hôpital qu'une fois cette procédure terminée.

Outre la préparation aux problèmes de santé physique, les organisations doivent également mettre en place des ressources et des protocoles pour fournir un soutien en santé mentale. Cela nécessite une réflexion approfondie, compte tenu du coût psychologique des interventions dans des environnements violents et de l'accès limité aux prestataires de soins en santé mentale dans de nombreux contextes.

Les besoins en santé mentale peuvent prendre différentes formes :

- Les membres du personnel qui ont des besoins permanents en santé mentale et qui nécessitent des soins et un soutien continu (par exemple, des médicaments et du counseling).
- Les membres du personnel qui souffrent de problèmes de santé mentale tels que le stress ou le TSPT résultant directement d'expériences liées au travail.
- Les membres du personnel dont les troubles de santé mentale préexistants sont exacerbés ou aggravés par les exigences et les défis de leur environnement de travail.

Chacun gère le stress et réagit aux chocs différemment. Les individus peuvent manifester toute une gamme d'émotions, allant d'émotions extrêmes à une absence totale d'émotions. Il est également normal d'exprimer ses émotions de manière intermittente. Le soutien psychosocial apporté par des professionnels, ainsi que par des pairs formés et des dirigeants bienveillants, peut réduire le risque de troubles psychologiques graves, tels que le TSPT.

Ce que l'organisation est en mesure d'offrir en termes de soutien en santé mentale doit idéalement être évalué de manière approfondie et clairement présenté au personnel avant qu'un incident ne se produise. Cette offre peut varier en fonction des besoins et des souhaits des membres du personnel concernés.

- *Voir le chapitre 5.4 pour des recommandations plus détaillées sur le soutien en santé mentale pour le personnel.*

Formation aux premiers secours

Les premiers secours prodigués rapidement, correctement et de manière appropriée, avec le matériel adéquat, constituent la meilleure mesure d'atténuation pour réduire l'impact d'une urgence médicale. Dans les environnements reculés ou aux ressources limitées, la formation aux premiers secours doit se concentrer sur les soins immédiats et efficaces lorsque l'aide médicale professionnelle n'est pas immédiatement disponible. Il s'agit notamment d'une formation aux premiers secours axée sur les traumatismes, qui permet d'évaluer rapidement les blessures et l'état des patients, d'administrer les traitements appropriés, tels que le maintien des voies respiratoires, de la respiration et de la circulation (ABC) et le contrôle des hémorragies, de gérer efficacement la douleur et d'assurer le transport des patients en toute sécurité. Il est essentiel de comprendre les impacts environnementaux sur la santé, car des facteurs tels que les températures extrêmes et le mal d'altitude peuvent à la fois causer et aggraver des problèmes médicaux et des blessures. De plus, les travailleurs humanitaires peuvent être formés à l'utilisation de «l'adaptation ingénieuse», qui consiste à improviser des solutions avec un minimum de ressources, en utilisant éventuellement des matériaux naturels pour stabiliser et traiter la personne touchée jusqu'à ce qu'une intervention professionnelle soit possible. La formation spécialisée en premiers secours destinée aux travailleurs humanitaires (souvent dispensée dans le cadre de la formation «Sensibilisation en milieu hostile») tient compte de la gamme (et de la gravité) des urgences médicales (en mettant particulièrement l'accent sur les blessures) auxquelles le personnel humanitaire peut être confronté, l'accès limité aux services médicaux et les défis environnementaux aggravants (naturels et humains) qui rendent les traitements plus difficiles.

- *Voir le chapitre 5.2 pour plus d'informations sur la formation «Sensibilisation en milieu hostile».*

Équipement de premiers secours pour les environnements reculés ou à ressources limitées

Outre une formation complète, la disponibilité d'un équipement de premiers secours approprié (en quantité suffisante) est essentielle pour une réponse médicale efficace dans les zones reculées où l'accès aux services de santé professionnels est limité, voire inexistant. Vous trouverez ci-dessous une liste indicative. Celle-ci n'est pas exhaustive et les organisations doivent demander l'avis d'un spécialiste sur les articles à stocker et la formation à dispenser en fonction du contexte et des besoins de leur personnel.

Réponse à un événement médical majeur

- **Bandages pour traumatismes.** Bandages stériles et absorbants pour le pansement des plaies (y compris les pansements thoraciques et les bandages triangulaires pour écharpes).
- **Attelles.** Pour immobiliser les fractures et stabiliser les membres blessés.
- **Agents hémostatiques.** Agents spécialisés pour favoriser la coagulation sanguine et contrôler les saignements.
- **Garrots.** Pour contrôler les hémorragies graves au niveau des membres.
- **Défibrillateur.** En cas d'arrêt cardiaque.
- **Pansements hydrogels pour brûlures.** Pour soigner les brûlures.

Nettoyage et désinfection des plaies

- **Solutions antiseptiques.** Pour nettoyer les plaies et prévenir les infections.
- **Compresse de gaze stériles.** Utilisées pour le pansement des plaies.
- **Pansements adhésifs.** Pour panser les coupures et écorchures mineures.
- **Pommade antibiotique.** Pour le traitement topique des plaies afin de prévenir les infections.
- **Pellicule plastique.** Pour une protection temporaire supplémentaire des plaies.

Évacuation et transport

- **Civière.** Civières portables pour transporter des personnes blessées sur des terrains accidentés.
- **Couvertures.** Pour apporter chaleur et confort aux blessés. Les couvertures métallisées et isothermiques conservent la chaleur corporelle et apportent de la chaleur.
- **Trousses médicales portatives.** Trousses compactes contenant des médicaments et des fournitures essentiels.

Équipement de protection individuelle (EPI)

- **Gants.** Gants à usage unique pour maintenir l'hygiène et prévenir la contamination croisée.
- **Masques chirurgicaux.** Pour se protéger contre les agents pathogènes et les contaminants présents dans l'air.
- **Protection des yeux.** Lunettes de sécurité ou lunettes de protection contre les débris et les éclaboussures.

Fournitures supplémentaires

- **Ruban adhésif médical.** Pour fixer les bandages et les pansements.
- **Ciseaux.** Ciseaux de qualité médicale pour couper les bandages et les vêtements.
- **Lampes de poche.** Sources lumineuses portables pour l'évaluation des blessures dans des conditions de faible luminosité.

Il est essentiel de veiller à la disponibilité et à l'entretien adéquat des fournitures de premiers secours afin d'assurer des soins rapides et efficaces dans des environnements difficiles. Il convient de noter que les traitements plus complexes, en particulier l'administration de médicaments, doivent être effectués sous la supervision d'un médecin. Dans les situations d'urgence, cela peut être fait à distance.

5.5.3 Réponse aux urgences médicales

La programmation de l'aide se fait souvent dans des zones où l'accès à des soins médicaux rapides est limité. Il est essentiel de répondre rapidement aux urgences médicales, car tout retard dans le traitement peut avoir de graves conséquences. Cette section fournit des recommandations sur les compétences, l'équipement et les protocoles nécessaires pour permettre une réponse efficace. Tous les protocoles doivent être développés et élaborés par du personnel ou des consultants possédant une expertise médicale.

► *Les sections suivantes traitent des risques médicaux physiques. Voir le chapitre 5.4 pour plus d'informations sur les risques psychologiques et les bonnes pratiques.*

Réponse immédiate

Alors que la plupart des protocoles humanitaires de premiers secours et de réponse se concentrent sur les blessures traumatiques (c'est-à-dire les blessures physiques graves qui surviennent soudainement et nécessitent des soins médicaux immédiats), d'autres types d'urgences médicales peuvent également nécessiter une réponse immédiate, notamment les arrêts cardiaques, les noyades et les coups de chaleur, par exemple. Les organisations doivent réfléchir aux urgences médicales auxquelles leur personnel doit être prêt à faire face, en fonction du contexte et de la situation

du personnel. Il est recommandé aux organisations de mettre en place des plans et des protocoles pour gérer les crises médicales, notamment des procédures de triage rapide, d'évacuation sanitaire primaire et de transport.

Les étapes clés pour venir en aide à une personne souffrant d'un traumatisme physique ou d'une autre urgence médicale sont les suivantes :

- Assurer la sûreté des lieux et utiliser un EPI approprié avant de commencer toute évaluation ou tout traitement.
- Évaluer et traiter rapidement les menaces immédiates pour la vie, telles que les hémorragies graves ou l'obstruction des voies respiratoires.
- Décider si un transfert vers un niveau de soins supérieur est nécessaire et lancer le processus de transfert.
- Fournir des informations sur l'état du patient à l'établissement d'accueil.
- Choisir un mode de transport approprié en fonction des besoins du patient et des ressources disponibles.
- Poursuivre les soins et le suivi pendant le transport.

L'objectif est de répondre aux besoins critiques immédiats et de stabiliser le patient afin qu'il puisse être transféré vers un établissement médical, dans le délai critique de « l'heure décisive » en cas de blessure traumatique.

D'autres éléments à prendre en compte dans la gestion des événements médicaux majeurs sont les suivants :

- **Communication d'urgence.** Cela implique d'établir une communication efficace pour coordonner les efforts de réponse et demander de l'aide, au moyen de radios, de téléphones satellites et de dispositifs de signalisation.
- **Évacuation médicale (MEDEVAC).** Des compétences de base en navigation et en lecture de cartes peuvent faciliter le transport rapide des patients vers des établissements médicaux ou des points d'évacuation. Il est également recommandé d'équiper les véhicules du projet de fournitures de base afin de pouvoir transporter le personnel blessé ou malade.
- **Évaluation et amélioration continues des protocoles de réponse aux incidents médicaux.** Cela peut inclure de recueillir le feedback des équipes de réponse afin d'adapter les stratégies en fonction des enseignements tirés et de l'évolution des défis.

- **Documentation et compte rendu.** Documenter et signaler les incidents, y compris les quasi-accidents et les enseignements tirés, à des fins de suivi et d'analyse des incidents, d'assurance et pour tout besoin d'information externe en matière de soins médicaux et de suivi. Le cas échéant, et en garantissant la confidentialité, cela peut être lié au compte rendu d'incident de sécurité d'une organisation.

Considérations pour les organisations humanitaires intervenant dans un scénario impliquant un grand nombre de victimes

Les scénarios impliquant un grand nombre de victimes, qui peuvent aller de catastrophes liées à des dangers naturels, à des accidents ou actes de violence à grande échelle, exigent une action rapide et efficace et peuvent rapidement submerger les systèmes de santé. Cela peut impliquer de prendre en compte des questions qui vont au-delà des soins médicaux immédiats, notamment des aspects liés à la gestion opérationnelle, à la coordination et à l'éthique.

- **Sûreté et sécurité.** Assurer la sûreté des intervenants et sécuriser le lieu de l'incident. Être conscient des menaces ou dangers secondaires potentiels.
- **Évaluation rapide et triage.** Évaluer rapidement l'ampleur de l'incident et mettre en place un système de triage afin de traiter en priorité les victimes en fonction de la gravité de leurs blessures.
- **Gestion des ressources.** Répartir efficacement le personnel, les fournitures et l'équipement afin d'en tirer le meilleur parti. Envisager de demander des ressources supplémentaires dès le début.
- **Communication et coordination.** Établir des lignes de communication claires entre les organisations qui interviennent, les hôpitaux et les centres de commandement. Coordonner les efforts afin d'éviter les doublons et les lacunes dans les réponses.
- **Information du public.** Coordonner une communication cohérente et opportune avec le public et les médias au sujet de l'incident et des efforts de réponse.
- **Documentation.** Mettre en place des systèmes permettant de suivre les patients, les ressources utilisées et les actions entreprises à des fins d'analyse ultérieure et d'éventuelles poursuites judiciaires.
- **Sensibilité culturelle.** Connaître et respecter les pratiques culturelles et religieuses, notamment en ce qui concerne le traitement des défunts.

- **Prise de décision éthique.** Être prêt à faire des choix éthiques difficiles concernant l'allocation de ressources limitées.
- **Soutien psychosocial.** À plus long terme, fournir des ressources en santé mentale aux personnes touchées, à leurs familles et aux intervenants.

Assistance postérieure

Un plan de sûreté et de soutien bien structuré est essentiel pour assurer l'assistance postérieure à long terme des travailleurs humanitaires qui ont été victimes d'un incident médical grave. Ce plan doit donner la priorité à la sûreté et au bien-être de la personne, en lui garantissant l'accès à un soutien médical et psychosocial continu, adapté à ses besoins et à ses souhaits spécifiques (une approche de soins à long terme centrée sur la personne survivante est recommandée). Le soutien médical à long terme peut inclure des examens réguliers et l'accès à des soins spécialisés si nécessaire, tandis que le soutien psychosocial peut inclure du counseling ou une thérapie pour traiter les traumatismes psychologiques et prévenir les effets psychologiques à long terme. Il est essentiel d'être transparent avec le personnel concerné quant à l'étendue et à la durée du soutien.

La réintégration au travail doit être gérée avec soin afin de favoriser le rétablissement du membre du personnel concerné. Cela peut impliquer des modalités de travail flexibles, un retour progressif aux fonctions ou une réaffectation à des tâches moins exigeantes. Maintenir une communication régulière avec la personne afin d'évaluer son confort et ses progrès, en procédant à des ajustements si nécessaire.

► *Pour des recommandations plus détaillées sur l'assistance postérieure centrée sur la personne survivante pour le personnel touché, voir le chapitre 5.4.*

Informations complémentaires

Recommandations et ressources

Center for Substance Abuse Treatment (US) (2014) 'Ch 1: Trauma-informed organizations' in *Trauma-Informed Care in Behavioral Health Services*. Treatment Improvement Protocol (TIP) Series, No. 57 (en anglais, « Centre pour le traitement de la toxicomanie (États-Unis) (2014) « Chapitre 1: Organisations tenant compte des traumatismes » dans Soins tenant compte des traumatismes dans les services de santé comportementale. Série de protocoles d'amélioration des traitements (TIP), n°57 ») (www.ncbi.nlm.nih.gov/books/NBK207201/).

Croix-Rouge américaine (n.d.) First aid training (en anglais, « Formation aux premiers secours ») (www.redcross.org/take-a-class/first-aid/first-aid-training).

DeMers, G. et Wightman, J. (2019) 'Mass casualty preparedness and response' in F.G. (en anglais, « (2019) « Préparation et réponse en cas d'accident impliquant un grand nombre de victimes » chez F.G. ») O'Connor, E.B. Schoomaker et D.C. Smith (éditions) *Fundamentals of military medicine* (« Principes fondamentaux de la médecine militaire »). Borden Institute (<https://medcoeckapwstorprd01.blob.core.usgovcloudapi.net/pfw-images/dbimages/Fund%20och%2034.pdf>).

DeNolf, R.L. et Kahwaji, C.I. (2022) *EMS mass casualty management* (en anglais, « Gestion des accidents impliquant un grand nombre de victimes dans les services d'urgence médicale »). StatPearls (www.ncbi.nlm.nih.gov/books/NBK482373/).

Organisation internationale de normalisation (2018) *ISO 45001:2018: Systèmes de gestion de la santé et de la sûreté au travail - exigences avec mode d'emploi* (www.iso.org/iso-45001-occupational-health-and-safety.html).

Organisation mondiale de la Santé (2022) *Guide: mass casualty preparedness and response in emergency units* (en anglais, « Guide : préparation et réponse en cas d'accident impliquant un grand nombre de victimes dans les services d'urgence »). ReliefWeb (<https://reliefweb.int/report/world/guide-mass-casualty-preparedness-and-response-emergency-units>).

Rural Health Information Hub (n.d.a) *Emergency preparedness and response for mass casualty incidents* (en anglais, « Préparation et réponse d'urgence en cas d'incidents impliquant un grand nombre de victimes ») (www.ruralhealthinfo.org/toolkits/emergency-preparedness/4/mass-casualty-incidents).

Rural Health Information Hub (n.d.b) *Partners and collaborators for emergency preparedness and response* (en anglais, « Partenaires et collaborateurs pour la préparation et la réponse d'urgence ») (www.ruralhealthinfo.org/toolkits/emergency-preparedness/1/partners-collaborators).

US Centers for Disease Control and Prevention (2024) *CDC Yellow Book: health information for international travel 2024* (en anglais, « CDC Yellow Book: informations sanitaires pour les voyages internationaux 2024 ») (www.cdc.gov/yellow-book/index.html).

6 Technologie et sécurité

6.1 Gestion de la sécurité de l'information et des communications

Ce chapitre traite des considérations relatives à la gestion de l'information sensible et au transfert sécurisé des informations, ainsi que des mesures à prendre lorsque les moyens de communication habituels sont perturbés. Après un aperçu de la sécurité de l'information, il aborde les communications sécurisées et les éléments essentiels d'un plan de communication.

6.1.1 Sécurité de l'information

La sécurité de l'information désigne les mesures et pratiques visant à protéger l'information sensible contre tout accès non autorisé, toute violation et toute utilisation abusive. Cela implique notamment de garantir la confidentialité, l'intégrité et la disponibilité des données, en particulier dans les environnements où les informations peuvent être essentielles à la sûreté et à l'efficacité des opérations. Pour les organisations humanitaires, cela implique souvent de sauvegarder les données personnelles, les détails opérationnels et autre information sensible qui, s'ils étaient compromis, pourraient mettre en danger des personnes ou des opérations. Les informations concernant les membres du personnel, les activités de l'organisation, les bénéficiaires de l'aide et les contacts peuvent toutes être utilisées à des fins malveillantes. Dans certains cas, les informations ne sont pas destinées à être partagées avec l'extérieur. Dans d'autres cas, les informations peuvent simplement être mal interprétées ou sorties de leur contexte.

Les dossiers sensibles pour les organisations peuvent inclure :

- Documents relatifs à chaque membre du personnel, tels que les salaires et les évaluations des performances.
- Informations personnelles confidentielles, telles que les dossiers médicaux.
- Informations spécifiques à l'organisation (par exemple, dossiers bancaires, documents juridiques et accords avec les gouvernements).
- Évaluations opérationnelles (par exemple, évaluations des risques, cartographie des acteurs, rapports de situation et compte rendus d'incidents, qui peuvent être perçus comme de l'espionnage).
- Informations sur les mouvements de personnel.
- Comptes rendus de réunions.
- Informations relatives aux programmes, notamment les détails concernant les bénéficiaires de l'aide.

- Informations sur les finances et la gestion des espèces.
- Inventaires des actifs (véhicules, équipement de bureau, radios).

Les dossiers médicaux, l'identité du personnel et des bénéficiaires de l'aide, ainsi que les plans opérationnels dans les zones de conflit constituent des exemples typiques de documents sensibles. Une mauvaise gestion de ces informations peut avoir de graves conséquences, notamment des risques pour la sûreté des personnes et la crédibilité de l'organisation. Parmi les problèmes courants, on peut citer le stockage inapproprié des documents, l'absence de sécurisation des fichiers numériques et le laxisme des procédures d'élimination de l'information sensible. Une mauvaise gestion interne peut facilement entraîner des accès non autorisés ou des fuites de données accidentelles.

Dans certains contextes, il existe également un risque élevé de surveillance de la part d'acteurs étatiques, de groupes criminels ou d'autres parties intéressées par les opérations des organisations humanitaires. Cela peut inclure la surveillance des communications, le piratage des systèmes ou la surveillance physique.

Les organisations peuvent prendre plusieurs mesures pour renforcer la sécurité de l'information.

- Les **politiques et procédures opérationnelles** de sécurité de l'information sont essentielles dans tous les contextes opérationnels. Ces documents définissent ce qui constitue une « information sensible », qui est autorisé à la consulter et comment elle doit être stockée, communiquée, transportée, insensibilisée ou détruite. En fait, le personnel responsable doit évaluer l'impact que pourrait avoir l'accès à ces informations par du personnel non autorisé. Par exemple, quelles seraient les conséquences si l'ordinateur personnel d'un membre du personnel contenant des informations et des images personnelles était consulté par les autorités du pays hôte hostiles à son arrivée dans le pays ?
- Des **protocoles** peuvent être mis en place pour la gestion des données, le contrôle des accès, la réponse aux incidents et le plan d'urgence. Ceux-ci doivent également répondre à des défis spécifiques, tels que la gestion des informations dans des environnements à haut risque ou en cas d'urgence. Ces protocoles peuvent également servir de base aux communications externes, notamment les relations avec les médias, les déclarations officielles et les publications sur les réseaux sociaux.
- Un moyen essentiel de protéger les informations consiste à conserver des **copies de sauvegarde** à plusieurs endroits. Cela permet de se prémunir contre la perte (mais pas contre le vol). Il convient de conserver à la fois des copies numériques et papier des documents essentiels. Les bonnes pratiques en matière de protection des informations sur support papier comprennent le traitement approprié des documents, le stockage sécurisé et les méthodes de destruction

appropriées. Dans certains cas, il peut être nécessaire de détruire rapidement les documents sensibles (par exemple en les déchiquetant et en supprimant de manière sécurisée les fichiers numériques), il est donc conseillé de réduire au minimum la documentation sur place. Limiter l'accès à l'information sensible à un nombre restreint de personnes peut offrir un niveau de sécurité supplémentaire.

- **La formation du personnel** est cruciale. L'ensemble du personnel doit être sensibilisé à l'importance de la sécurité de l'information, à la manière de reconnaître et de traiter les informations sensibles, ainsi qu'aux risques spécifiques liés à la communication dans le contexte opérationnel. Cela est particulièrement important pour le personnel ayant accès à de l'information sensible ou qui est régulièrement en contact avec des acteurs externes ou gère les interactions avec les médias, comme le personnel chargé de la communication.

Les bonnes pratiques en matière de sécurité de l'information comprennent également la gestion des communications et de la sécurité numérique, ainsi que la gestion des risques liés à la surveillance hostile. La sécurité des communications est traitée plus en détail dans les sections suivantes de ce chapitre, tandis que la sécurité numérique est abordée en détail au chapitre 6.2. Pour plus d'informations sur la surveillance hostile, voir le chapitre 7.5.

6.1.2 Planification des communications

Les capacités à communiquer avec les autres sont l'un des piliers fondamentaux de la sécurité et revêtent une importance particulière dans les environnements à haut risque. Les procédures et plans de sécurité ne peuvent être mis en œuvre sans les capacités à communiquer. En cas d'urgence, les capacités à communiquer rapidement avec d'autres parties peuvent faire la différence entre la vie et la mort. À ce titre, un plan de communication est tout aussi important pour la sécurité qu'une évaluation des risques, et l'élaboration d'un bon plan de communication doit être prise tout aussi au sérieux.

Un bon plan de communication est adapté à l'organisation et répond à ses besoins spécifiques dans le contexte dans lequel elle opère. Les plans de communication doivent être personnalisés pour chaque organisation, chaque bureau et même chaque projet. L'intégration de la sécurité des communications dans les politiques de sécurité plus générales de l'organisation permet de garantir une approche cohérente dans toutes les opérations.

Considérations initiales

Les considérations suivantes devraient éclairer le plan de communication de tout projet, bureau ou organisation.

Taille et budget de l'organisation

Si des plans localisés peuvent suffire aux petites organisations, les grandes entités disposant de plusieurs bureaux ont besoin de stratégies globales et compatibles

pour garantir une communication inter-bureaux efficace et rentable. L'objectif est d'optimiser les capacités de communication dans l'ensemble de l'organisation. L'évolutivité est cruciale : les plans doivent être adaptables afin de satisfaire à la croissance ou à la contraction futures, et évoluer au fur et à mesure que les besoins de l'organisation changent.

Les considérations budgétaires sont cruciales. Les petites organisations consacrent généralement une part plus importante de leur budget global à la communication (en raison des coûts élevés liés à la technologie et aux infrastructures), tandis que les grandes organisations dépensent davantage par employé, mais une part moins importante du budget global de l'organisation. Il est essentiel d'établir un budget réaliste, tant en termes de dépenses par employé que de pourcentage du budget de fonctionnement global. L'évolutivité à long terme peut justifier des investissements initiaux plus importants dans des solutions durables.

Contexte opérationnel

Un plan de communication distinct peut être nécessaire pour chaque contexte opérationnel. Un plan de communication qui fonctionne dans un environnement urbain et professionnel peut ne pas convenir à une zone rurale reculée, et un plan de communication destiné à un environnement urbain et professionnel dans un pays peut ne pas fonctionner dans un environnement similaire dans un autre pays. De même, un plan de communication conçu pour un bureau fixe peut ne pas convenir à une équipe mobile.

Le coût et la visibilité des équipements de communication, tels que les radios et les téléphones satellites, peuvent en faire des cibles attrayantes pour le vol ou d'autres activités criminelles. Ce risque doit être pris en compte dans le choix des moyens de communication, parallèlement aux mesures de sécurité visant à l'atténuer, telles que le stockage sécurisé, le contrôle des accès et la formation régulière du personnel à l'utilisation et à la manipulation sécurisées des équipements.

Infrastructures existantes

Optimiser l'utilisation des infrastructures de communication existantes permet d'élargir les options et la flexibilité d'un plan de communication, tout en minimisant les coûts. Cependant, il convient de mener des recherches sur la fiabilité des infrastructures existantes, car tout ce qui échappe au contrôle direct de l'organisation peut être sujet à des interruptions ou à des défaillances.

- Communications mobiles :
 - identifier les fournisseurs de services mobiles dans la zone ;
 - évaluer la couverture des antennes-relais ;
 - déterminer si les appareils de communication mobiles doivent être intégrés au plan et utilisés.

- Communications par Internet:
 - identifier les fournisseurs d'accès Internet locaux ;
 - évaluer les débits de données ;
 - évaluer les coûts associés aux services Internet.
- Communications radio:
 - vérifier si un réseau radio existant est disponible ;
 - évaluer si l'organisation doit mettre en place sa propre infrastructure.
- Infrastructure électrique:
 - évaluer les systèmes électriques existants ;
 - déterminer la tension disponible et si elle répond aux exigences ;
 - évaluer la nécessité d'alimentations électriques de secours ;
 - déterminer si des batteries sont nécessaires pour l'alimentation portative ou de secours ;
 - si des batteries sont nécessaires, élaborer un plan pour leur recharge et leur entretien.

Les communications peuvent être surveillées par les gouvernements, les fournisseurs de services et d'autres acteurs. La sécurité de l'information, c'est-à-dire faire attention à qui a accès à quelles informations et comment elles sont partagées, est primordiale. C'est également un élément important pour décider quel équipement utiliser et quand.

Exemple de cas : Planification en cas de perturbation des infrastructures

En 2024, Starlink (un fournisseur privé d'accès Internet par satellite) a annoncé qu'il allait mettre fin à ses services Internet au Soudan, invoquant l'absence d'autorisation d'exercer dans ce pays. Cette décision a alarmé les organisations humanitaires qui dépendaient de Starlink pour communiquer dans un contexte de conflit et de coupures des télécommunications. Elles ont exhorté Starlink à reconsidérer sa décision, soulignant le rôle essentiel du service dans la coordination de l'aide et la communication avec les personnes dans le besoin.

Considérations environnementales et autres types d'urgences

Les équipements de communication sont susceptibles de tomber en panne dans des environnements soumis à des températures extrêmes. Les conditions très chaudes ou très froides nécessitent des équipements de communication conçus pour résister

à des températures extrêmes ou équipés de mécanismes de refroidissement ou de chauffage supplémentaires. Dans les environnements très humides, un système de déshumidification peut être nécessaire. Dans les environnements très pluvieux, une protection supplémentaire peut être nécessaire pour empêcher toute infiltration d'eau. Dans les environnements très sales ou poussiéreux, les appareils équipés de ventilateurs et de pièces mobiles peuvent présenter des dysfonctionnements s'ils ne sont pas correctement nettoyés et protégés.

En cas d'urgence, le volume d'appels peut augmenter considérablement, car les gens cherchent à prendre des nouvelles de leurs proches ou à obtenir de l'aide. Cela peut entraîner une saturation du réseau, rendant difficile la connexion des appels, qu'il s'agisse de lignes fixes ou de réseaux mobiles. Si les réseaux de télécommunications sont compromis, les alertes d'urgence nationales risquent de ne pas être diffusées efficacement, ce qui complique encore davantage la communication en cas d'urgence.

Structure administrative et organisationnelle

Les bureaux ou les équipes comptant moins d'employés auront généralement besoin de moins d'équipements de communication que ceux qui en comptent davantage. D'autres facteurs entrent également en ligne de compte. Le personnel travaillera-t-il uniquement depuis un bureau ou sera-t-il amené à se déplacer? Quel mode de transport utilisera-t-il et voyagera-t-il en équipe ou seul? Une petite équipe de cinq personnes dont chaque membre se rend chaque jour dans un lieu différent aura besoin de plus de ressources qu'une équipe de 20 personnes qui ne se déplace qu'une fois par semaine vers un seul lieu en groupe. Cependant, si les cinq membres de l'équipe devaient se rendre une fois par semaine sur un site particulier et pouvaient chacun se rendre sur un nouveau site un jour différent, les ressources de communication liées aux déplacements pourraient être partagées, ce qui réduirait le coût global. Cela montre comment la structure administrative et organisationnelle, et pas seulement le nombre ou la taille des effectifs, peut déterminer les besoins en matière de communication.

Considérations relatives au temps

La durée du programme est un facteur crucial dans l'élaboration d'un plan de communication. Il n'est peut-être pas judicieux d'investir massivement dans des infrastructures de communication fixes pour une programmation à court terme. Si l'organisation a l'intention d'occuper un bureau pendant plusieurs années, les coûts initiaux liés à l'investissement dans un plan de communication solide sont plus justifiés.

Considérations réglementaires

Il est important d'identifier les équipements de communication autorisés par les autorités locales. Par exemple, les systèmes de communication par satellite peuvent nécessiter un enregistrement spécial et peuvent être interdits dans certaines juridictions. Bien que les organisations humanitaires puissent demander une dérogation, en particulier si elles travaillent ou collaborent avec l'ONU, l'approbation n'est pas garantie et doit être demandée avant d'importer des appareils de communication dans le pays. Savoir quels équipements de communication sont légaux peut éviter des erreurs coûteuses.

Exemple de cas : Choisir le bon équipement

Il est également important de déterminer quels équipements de communication sont généralement utilisés dans certains contextes et par qui. En 2023, une organisation humanitaire opérant dans l'est de l'Ukraine a été prise pour cible par inadvertance par l'armée russe. Un examen a posteriori a révélé que l'organisation humanitaire avait été confondue avec une cible militaire ukrainienne parce qu'elle disposait d'une antenne parabolique Starlink sur le toit de son bâtiment. Les seuls autres systèmes Starlink présents dans la région étaient exploités par des unités militaires ukrainiennes.

Coordination interagences

Dans de nombreuses zones opérationnelles à haut risque, les services de télécommunications peuvent être fournis par le Cluster des télécommunications d'urgence (ETC pour son sigle en anglais). L'ETC est un réseau mondial qui collabore avec diverses organisations afin de fournir des services de communication partagés lors de situations d'urgence humanitaire. Cela comprend l'offre d'options de communication vocale et d'autres services essentiels aux organisations humanitaires, aux autorités nationales et aux communautés touchées, en particulier lorsque les infrastructures de communication existantes sont compromises ou indisponibles. Le groupe de travail local de l'ETC, ou le Programme alimentaire mondial (PAM) en tant qu'agence chef de file de l'ETC, peut fournir des informations sur les services disponibles dans la zone d'opération. Les risques pesant sur les services de l'ETC sont similaires à ceux qui pèsent sur les autres services de télécommunications, notamment en matière de vulnérabilité des infrastructures et de perturbations. Dans certaines régions, les organisations peuvent avoir la possibilité de participer au système radio de l'ONU, ou des fréquences spécifiques peuvent avoir été attribuées aux ONG.

Partenaires de communication choisis

L'étape suivante de l'élaboration d'un plan de communication consiste à déterminer les personnes et les organisations qui doivent communiquer entre elles. Chacun de ces groupes aura probablement besoin d'un plan de communication distinct, mais pas nécessairement d'un équipement de communication distinct.

Communications internes

Les communications internes sont les plus simples, car l'organisation contrôle entièrement les équipements, les méthodes et les politiques. Elles sont également les plus faciles à corriger en cas de problème. Les communications internes peuvent

être les plus coûteuses, car l'organisation doit prendre en charge tous les frais liés à l'achat d'équipements, à la maintenance et à la formation.

Lorsqu'elle élabore un plan de communication interne, l'organisation doit d'abord déterminer qui et quels groupes doivent communiquer entre eux. Si plusieurs membres d'une petite équipe se rendent séparément dans un endroit situé dans le pays, un plan de communication peut être élaboré pour définir la manière dont chaque membre de l'équipe communiquera avec les autres. Un deuxième plan de communication pourrait décrire la manière dont cette équipe communique avec les autres équipes, tandis qu'un troisième pourrait détailler la manière dont ces équipes communiquent avec leur siège social. Un plan de communication distinct pourrait définir comment chaque individu ou groupe communique avec les parties prenantes internes concernées.

Communications externes

Les communications externes englobent toutes les interactions avec des personnes ou des groupes extérieurs à l'organisation. Il peut s'agir notamment des bénéficiaires de l'aide, des représentants des communautés locales, des organisations partenaires, des entités gouvernementales, des organismes de financement et des agences de l'ONU. Il est conseillé d'élaborer des plans de communication pour chaque entité. Dans certains contextes, les organisations humanitaires peuvent être amenées à adopter le plan de communication ou l'équipement utilisé par l'entité externe. Ce n'est pas toujours le cas, mais avant d'élaborer un plan de communication, identifier les parties prenantes externes et les systèmes qu'elles utilisent peut permettre à l'organisation d'économiser du temps et de l'argent à long terme.

► Voir le chapitre 4.4 pour plus d'informations sur les communications en cas de crise.

Communications d'urgence

Un plan de communication d'urgence doit décrire plusieurs méthodes permettant aux individus et aux équipes de contacter les services d'urgence, tant au niveau national qu'au sein de l'organisation. Tous les pays et tous les contextes ne disposent pas de numéros de téléphone nationaux standardisés pour les services d'urgence, et des dispositions doivent être prises en cas de panne des réseaux téléphoniques.

L'organisation devra généralement adopter les méthodes, plans et protocoles de communication définis par les services d'urgence. Il est donc utile de bien comprendre ces protocoles avant d'élaborer un plan de communication d'urgence pour l'organisation.

6.1.3 Équipements de communication

Cette section présente les principaux types d'équipements de communication qu'une organisation peut envisager dans le cadre de sa planification.

Types d'équipements

Radios hautes fréquences

Fonctionnant à des fréquences comprises entre 3 et 30 mégahertz (MHz), les radios à hautes fréquences (HF) (par exemple, les équipements portatifs, embarqués dans des véhicules ou installés dans des stations de base) sont généralement utilisées par les radioamateurs, le personnel militaire et les organisations humanitaires, y compris l'ONU. Les organisations humanitaires ont progressivement cessé d'utiliser les radios HF à mesure que les technologies mobiles et satellitaires se sont généralisées et sont devenues moins coûteuses.

Le principal avantage de ces systèmes radio réside dans le fait qu'ils réfléchissent les signaux de communication dans la haute atmosphère, ce qui permet des transmissions à plus longue portée. Les radios HF sont ainsi capables de communiquer entre elles à des centaines de kilomètres de distance. Les principaux inconvénients des communications radio HF sont que les perturbations atmosphériques peuvent perturber le signal (par exemple, les conditions météorologiques et la lumière du soleil). De plus, les systèmes radio HF nécessitent généralement un niveau élevé d'expertise pour leur installation, leur maintenance et leur utilisation, ce qui peut impliquer des investissements dans la formation (par exemple, pour la manipulation du matériel et l'utilisation d'un langage codé : les communications non cryptées peuvent être interceptées par toute personne disposant d'une radio fonctionnant avec les mêmes réglages et la même fréquence). Ces radios nécessitent généralement une grande antenne, ce qui peut augmenter la visibilité du véhicule et le rendre susceptible d'être pris pour cible par des acteurs hostiles, volé ou confondu avec un équipement militaire.

Tableau 11 Considérations relatives à la sécurité des équipements de communication par radio HF

Type	Avantages	Inconvénients/vulnérabilités
Radio de véhicule	● Alimentée par le véhicule (la radio est allumée lorsque le véhicule est en marche) ● Peut communiquer sur de plus longues distances ● Accessible à tous les occupants du véhicule	● La qualité du signal peut dépendre de l'emplacement du véhicule ● Nécessite généralement un niveau de connaissances élevé pour pouvoir résoudre les problèmes ● Les besoins d'entretien peuvent être plus importants en raison des conditions de conduite ● Coûts initiaux élevés ● Doit fonctionner aux deux extrémités pour permettre la communication ● Peut nécessiter un permis d'exploitation

Type	Avantages	Inconvénients/vulnérabilités
Radio portable	• Plus petite qu'une radio de véhicule • Portable - non reliée à l'alimentation électrique du véhicule • Peut être utilisée sans infrastructure existante	• Nécessite un niveau élevé de connaissances pour être configurée et utilisée correctement • Nécessite des piles, qui peuvent s'épuiser • L'équipement est lourd • Coût initial élevé • Doit fonctionner aux deux extrémités pour permettre la communication • Peut nécessiter un permis d'exploitation
Station de base par radio	• Utilise l'alimentation existante (prise murale ou générateur) • Peut communiquer sur de très longues distances • Accessible à tous • Ne dépend d'aucune infrastructure existante autre que l'alimentation électrique	• Nécessite un niveau élevé de connaissances pour être configurée et entretenue • Doit fonctionner aux deux extrémités pour que la communication puisse s'établir • Coût initial élevé • Peut nécessiter un permis d'exploitation

Radios à très hautes fréquences et à ultra hautes fréquences

Les radios à très hautes fréquences (VHF) fonctionnent sur la bande de 30 à 300 MHz, et les radios à ultra hautes fréquences (UHF) fonctionnent entre 300 MHz et 3 gigahertz (GHz). Ces radios sont utilisées par un large éventail de personnes, allant des militaires, policiers et autres services d'urgence jusqu'aux amateurs.

Le principal avantage des radios VHF et UHF réside dans leur capacité à assurer une communication instantanée dans un format simple à utiliser et relativement économique. Le principal inconvénient est que les radios VHF et UHF ont généralement besoin d'une ligne de mire directe, et que la communication peut donc être difficile dans les zones urbaines avec de grands bâtiments, par exemple, ou dans les régions montagneuses où le terrain obstrue le chemin direct entre les radios.

Bien que la distance maximale de communication radio VHF et UHF varie en fonction du fabricant, de la puissance, de l'antenne et d'autres facteurs, les radios VHF et UHF portatives doivent se trouver à quelques centaines de mètres à quelques kilomètres les unes des autres, sinon elles ne pourront pas communiquer. Les radios UHF fonctionnent généralement mieux en milieu urbain, car leur bande de fréquences pénètre mieux les murs et autres obstacles que les radios VHF. Les radios VHF sont généralement mieux adaptées aux communications extérieures de longue portée. Les radios VHF et UHF ne constituent pas un bon choix pour les communications trans-horizon, à moins d'utiliser des répéteurs.

Tout comme les radios HF, les radios VHF et UHF fonctionnent sur un mode point à point, ce qui signifie qu'une radio communique directement avec une autre sans avoir besoin d'un intermédiaire pour relayer la transmission. Cependant, des répéteurs peuvent être utilisés comme intermédiaires, acceptant la transmission d'une radio et la retransmettant pour étendre la portée du signal. Comme les radios HF, les signaux parcourent de longues distances et, s'ils ne sont pas cryptés, peuvent être interceptés par toute personne disposant d'une radio fonctionnant avec les mêmes réglages et la même fréquence. De même que les radios HF, ces systèmes nécessitent une expertise pour être configurés, entretenus et utilisés.

Tableau 12 Considérations relatives à la sécurité des équipements de communication par radios VHF et UHF

Type	Avantages	Inconvénients/vulnérabilités
Radio de véhicule	- Alimentée par le véhicule (la radio est allumée lorsque le véhicule est en marche) - Peut communiquer sur plusieurs kilomètres - Accessible à tous les occupants du véhicule	- Pour obtenir un bon signal, le véhicule doit se trouver à portée du récepteur choisi - Nécessite certaines connaissances pour la configuration (mais pas pour l'utilisation) - Les besoins d'entretien peuvent être plus importants en raison des conditions de conduite - Doit fonctionner aux deux extrémités pour permettre la communication - Peut nécessiter un permis d'exploitation
Radio portative	- Plus petite qu'une radio de véhicule - Portative - non reliée à l'alimentation électrique du véhicule - Peut être utilisée sans infrastructure existante	- Nécessite des piles, qui peuvent s'épuiser - Portée limitée (environ 8 kilomètres ou moins, selon les conditions) sans répéteur - Doit fonctionner aux deux extrémités pour permettre la communication - Peut nécessiter un permis d'exploitation
Station de base par radio	- Utilise l'alimentation existante (prise murale ou générateur) - Peut communiquer sur des distances plus longues que les radios portatives - Accessible à tous - Ne dépend d'aucune infrastructure existante autre que l'alimentation électrique	- Nécessite un niveau de connaissances modéré pour être configurée et utilisée correctement - Doit fonctionner aux deux extrémités pour que la communication puisse s'établir - Peut nécessiter un permis d'exploitation

Type	Avantages	Inconvénients/vulnérabilités
Répéteur	• Étend la portée de la communication en rediffusant la transmission radio • Nécessite une alimentation électrique, mais aucune autre infrastructure existante • Ne nécessite aucune intervention humaine une fois configuré	• Peut être coûteux • Nécessite une alimentation électrique et un espace pour l'installation • Peut nécessiter de nombreux répéteurs pour établir un réseau de communication étendu • Nécessite un niveau de connaissances modéré pour la configuration et l'entretien, mais pas pour le fonctionnement • Peut nécessiter un permis d'exploitation

Appareils mobiles

Les appareils mobiles nécessitent un réseau mobile existant qui répète la transmission d'un appareil mobile à un autre le long du réseau ou, selon la situation, via Internet. Les principaux avantages des appareils mobiles sont la généralisation de l'équipement, le coût relativement faible, l'étendue de l'infrastructure existante et la facilité d'utilisation. Les principaux inconvénients sont la dépendance vis-à-vis des infrastructures existantes (sans couverture mobile, les appareils ne peuvent pas communiquer) et le fait que les opérateurs de téléphonie mobile agissent comme intermédiaires dans la chaîne de communication, ce qui leur permet d'intercepter et éventuellement de surveiller les communications. De nombreux gouvernements ont le pouvoir de couper les communications mobiles ou d'en surveiller étroitement l'activité. Beaucoup exigent également l'enregistrement obligatoire des cartes SIM, ce qui implique généralement de fournir des informations personnelles, notamment une pièce d'identité valide, pour activer la carte. Enfin, si de nombreuses communications vocales et de données sont cryptées, ce qui empêche la majorité des utilisateurs d'intercepter les communications et de les écouter, il n'est pas toujours possible de garantir la sécurité des communications vis-à-vis des opérateurs de téléphonie mobile ou des pouvoirs publics.

Tableau 13 Considérations relatives à la sécurité des équipements de communications mobiles

Type	Avantages	Inconvénients/vulnérabilités
Téléphone portable (voix)	• Équipement peu coûteux et universellement utilisé • Faibles besoins en formation • Nécessite un signal mobile moins puissant pour la communication vocale que pour la communication de données	• Nécessite de disposer d'une couverture par le réseau mobile et d'un forfait actif • Peut faire l'objet d'une surveillance par les pouvoirs publics • Peut être interrompu à tout moment par les pouvoirs publics • Peut être perturbé par des dangers naturels ou d'autres facteurs environnementaux • Risque accru de saturation du réseau en cas d'urgence
Téléphone portable (données)	• Équipement peu coûteux et universellement utilisé • Faibles besoins en formation • Le flux d'informations et le débit de données peuvent être très élevés, ce qui permet de communiquer de grandes quantités de données en peu de temps	• Nécessite de disposer d'une couverture par le réseau mobile et d'un forfait actif • Peut faire l'objet d'une surveillance par les pouvoirs publics • Peut être interrompu à tout moment par les pouvoirs publics • Peut être perturbé par des dangers naturels ou d'autres facteurs environnementaux
Hotspot mobile	• Faibles coûts des équipements • Plusieurs appareils peuvent communiquer via un seul hotspot • Certains hotspots peuvent utiliser plusieurs réseaux mobiles, ce qui permet une meilleure couverture	• Nécessite de disposer d'une couverture par le réseau mobile et d'un forfait actif • Peut faire l'objet d'une surveillance par les pouvoirs publics • Peut être interrompu à tout moment par les pouvoirs publics • Peut être perturbé par des dangers naturels ou d'autres facteurs environnementaux

Type	Avantages	Inconvénients/vulnérabilités
Appareil intelligent	• L'appareil se connecte directement au réseau mobile sans avoir besoin d'un autre appareil comme intermédiaire • Les appareils peuvent être de tailles diverses (de très petits à très grands) • Les appareils peuvent être intégrés à des équipements existants (écran intelligent installé dans un véhicule, par exemple)	• Nécessite de disposer d'une couverture par le réseau mobile et d'un forfait actif • Peut faire l'objet d'une surveillance par les pouvoirs publics • Peut être interrompu à tout moment par les pouvoirs publics • Peut être perturbé par des dangers naturels ou d'autres facteurs environnementaux • Les options de communication sont presque toujours limitées aux options logicielles installées sur l'appareil

Appareils filaires

Les appareils filaires (ou fixes) se connectent entre eux via un réseau de câbles existant (souterrain, aérien, sous-marin). Le principal avantage des appareils filaires est qu'ils permettent généralement de transmettre de grandes quantités de données vocales ou numériques de manière fiable et rapide. Ils peuvent également être plus fiables que les appareils mobiles, car la connexion filaire doit être interrompue pour que le service soit interrompu, tandis que les appareils mobiles dépendent de la puissance du signal provenant d'une connexion à distance à une antenne-relais. L'inconvénient des connexions filaires est qu'elles ne peuvent pas être déplacées et ne sont donc pas portatives. De plus, l'infrastructure existante des connexions filaires n'est pas aussi répandue que celle des antennes-relais de téléphonie mobile, et les réparations en cas de panne peuvent prendre plus de temps.

Tableau 14 Considérations relatives à la sécurité des équipements de communication filaires

Type	Avantages	Inconvénients/vulnérabilités
Téléphone fixe	• Plus difficile à intercepter que les appels vocaux sur téléphone mobile • Facile à utiliser • Les téléphones fixes traditionnels, en particulier les modèles analogiques, ne nécessitent pas de source d'alimentation externe pour fonctionner	• Totalement non crypté • Disponibilité en baisse • Peut être interrompu à tout moment par les pouvoirs publics • Peut être perturbé par des dangers naturels ou d'autres facteurs environnementaux

Type	Avantages	Inconvénients/vulnérabilités
Accès commuté	• Fournit un accès par modem à Internet	• Disponible uniquement dans certains lieux reculés • Dépend des lignes téléphoniques existantes • Débit très lent • Peut être perturbé par des dangers naturels ou d'autres facteurs environnementaux
Ligne d'abonné numérique (DSL)	• Plus rapide que l'accès commuté • Faible coût • Largement disponible • Peut utiliser des routeurs wifi afin que plusieurs appareils puissent communiquer sur une seule ligne	• Dépend des lignes téléphoniques existantes • Peut faire l'objet d'une surveillance par les pouvoirs publics • Peut être interrompu à tout moment par les pouvoirs publics • Peut être perturbé par des dangers naturels ou d'autres facteurs environnementaux
Câble	• Transferts de données très rapides • Plus fiable que la DSL • La connexion peut être ralentie pendant les heures de pointe • Peut utiliser des routeurs wifi afin que plusieurs appareils puissent communiquer sur une seule ligne	• Dépend des lignes câblées existantes (initialement destinées à la télévision par câble) • Peut faire l'objet d'une surveillance par les pouvoirs publics • Peut être interrompu à tout moment par les pouvoirs publics • Peut être perturbé par des dangers naturels ou d'autres facteurs environnementaux
Fibre	• Transferts de données très rapides • Connexion la plus fiable • Peut être coûteux • Moins sujette aux pannes ou aux ralentissements • Peut utiliser des routeurs wifi afin que plusieurs appareils puissent communiquer sur une seule ligne	• S'appuie sur des lignes à fibre optique • Peut faire l'objet d'une surveillance par les pouvoirs publics • Peut être interrompu à tout moment par les pouvoirs publics • Peut être perturbé par des dangers naturels ou d'autres facteurs environnementaux

Appareils de communication par satellite

Les appareils de communication par satellite communiquent via un réseau de satellites (ou une constellation de satellites) plutôt que via des antennes-relais. L'avantage est qu'un satellite peut couvrir une zone au sol beaucoup plus vaste qu'une antenne-relais. Les appareils de communication par satellite sont également plus difficiles à perturber et les pouvoirs publics n'ont généralement pas les capacités

d'interrompre les services comme ils peuvent le faire avec les appareils mobiles ou d'autres réseaux terrestres.

Les deux principaux inconvénients des appareils satellitaires sont que l'antenne de l'appareil doit avoir une ligne de mire directe vers le ciel (ils ne peuvent donc pas être utilisés à l'intérieur d'un bâtiment, à moins qu'une antenne ne soit placée à l'extérieur) et que les appareils et les services sont plus coûteux que ceux des communications mobiles. Il est également important de reconnaître qu'ils ne sont pas totalement à l'abri du contrôle des pouvoirs publics ou d'autres formes d'interférence (y compris les perturbations ciblées). Certains pouvoirs publics interdisent totalement les appareils de communication par satellite, d'autres imposent des restrictions à certains opérateurs et d'autres encore exigent que tous les appareils satellitaires soient enregistrés. Enfin, l'un des principaux risques liés aux communications par satellite est la dépendance vis-à-vis des opérateurs de services satellitaires, qui peuvent décider de mettre fin brusquement à leurs services. Si cela constitue un défi pour tous les services de communication, ce problème est plus prononcé dans le domaine des communications par satellite en raison du nombre limité d'opérateurs.

Tableau 15 Considérations relatives à la sécurité des équipements de communication par satellite

Type	Avantages	Inconvénients/vulnérabilités
Téléphone satellite	• Couverture quasi universelle • Permet d'appeler n'importe quel téléphone	• Certains opérateurs offrent une meilleure couverture que d'autres • Le service peut être coûteux • Le téléphone doit avoir une ligne de mire directe vers le ciel • Peut être illégal dans certaines juridictions, ou nécessiter une licence/autorisation
Appareil satellite Push-To-Talk (PTT)	• Couverture quasi universelle • Le signal peut être plus fiable qu'avec un téléphone satellite • Permet de parler avec plusieurs personnes à la fois (comme un système radio)	• Certains opérateurs offrent une meilleure couverture que d'autres • Le service peut être coûteux • L'appareil doit avoir une ligne de mire directe vers le ciel • Peut être illégal dans certaines juridictions ou nécessiter une licence/autorisation • Nécessite un niveau de connaissances modéré pour être configuré

Type	Avantages	Inconvénients/vulnérabilités
Radiobalise/ balise de détresse	• Couverture quasi universelle • Le signal peut être plus fiable qu'avec un téléphone satellite ou un appareil Push-To-Talk • Peut être entièrement crypté • La transmission en micro-rafales ne nécessite pas de signal actif continu	• Certains opérateurs offrent une meilleure couverture que d'autres • L'appareil doit avoir une ligne de mire directe vers le ciel • Peut être illégal dans certaines juridictions ou nécessiter une licence/autorisation • Généralement limité à de petites quantités de données (SMS, petits fichiers, une seule photo) ou uniquement à des informations de localisation • L'envoi et la réception des messages peuvent être lents
Internet par satellite	• Couverture en pleine expansion • Accès Internet complet • Possibilité de connecter plusieurs appareils à une seule connexion	• Certains opérateurs offrent une meilleure couverture que d'autres • Le service peut être coûteux • L'appareil doit avoir une ligne de mire directe vers le ciel • Peut être illégal dans certaines juridictions, ou nécessiter une licence/autorisation • Nécessite un niveau de connaissances modéré pour être configuré

6.1.4 Choisir l'équipement et établir un plan

Une fois que l'on a acquis une connaissance de base des types d'équipements de communication et que l'on a identifié les besoins de l'organisation en matière de communication, il est temps de commencer à élaborer un plan de communication.

Choisir des équipements sécurisés

On demande souvent au personnel de sécurité quels sont les moyens et les équipements de communication les plus sûrs. La réponse dépend du lieu, des circonstances et du moment, car la technologie évolue rapidement. Les bonnes pratiques recommandent de procéder à des évaluations des risques approfondies afin de sélectionner les outils de communication adaptés aux besoins opérationnels et au contexte, ainsi que de mettre en place des redondances pour se prémunir contre les défaillances de communication.

Les organisations peuvent également envisager des options de cryptage lors du choix des équipements de communication. Le cryptage peut être utilisé sur la plupart des équipements de communication, y compris les systèmes radio, les appareils filaires et les communications par satellite. Le cryptage peut améliorer considérablement

la sécurité des communications, mais nécessite un équipement ou un logiciel compatible. L'utilisation de communications cryptées peut être soumise à des réglementations.

Il est conseillé aux organisations qui utilisent des protocoles de cryptage de les mettre à jour et de les auditer régulièrement afin de faire face aux nouvelles menaces et vulnérabilités. L'adoption d'une approche de sécurité à plusieurs niveaux, combinant le cryptage avec d'autres mesures telles que les contrôles d'accès et l'authentification sécurisée des utilisateurs, offre une défense plus solide contre les violations de sécurité potentielles. Il peut être approprié d'utiliser des codes pour communiquer une information sensible. Ce point est abordé brièvement dans les sections ci-dessous.

Créer un plan de communication : introduire la redondance nécessaire

Les plans de communication doivent intégrer une redondance, c'est-à-dire qu'ils doivent garantir que la communication reste fonctionnelle même en cas de défaillance d'un élément. Un plan PACE (Primary, Alternate, Contingency, and Emergency) est conçu pour maximiser la redondance des communications et ainsi réduire les risques. Le plan PACE décrit l'ordre dans lequel les différentes méthodes de communication doivent être utilisées. Par exemple, les téléphones portables peuvent être désignés comme principale (Primary) méthode de communication. Si cette méthode échoue, l'équipe passe alors à la méthode alternative (Alternate, par exemple, la radio VHF), puis à la méthode de secours (Contingency, par exemple, la communication par satellite) si celui-ci échoue également.

Il existe deux principes clés dans un plan PACE. Tout d'abord, PACE fait référence aux types de communication, et non aux appareils eux-mêmes. Par exemple, deux appareils qui dépendent tous deux des réseaux mobiles ne peuvent pas servir de méthodes principale et secondaire dans un plan PACE, car une interruption du réseau mobile rendrait les deux inutilisables. La seule exception concerne les communications radio, car les systèmes radio ne dépendent pas d'un intermédiaire : deux systèmes radio VHF ou HF complets peuvent servir de méthodes de communication distinctes dans le cadre d'un plan PACE. Cependant, chaque système doit être entièrement indépendant. S'il existe un point de défaillance unique, tel qu'une station de base par radio partagée dans un bureau, ces systèmes ne sont pas considérés comme des systèmes distincts.

Le deuxième principe est que le plan PACE est appliqué de manière séquentielle : chaque étape n'est utilisée que si la méthode précédente échoue, ce qui garantit un processus de communication structuré et fiable. Par exemple, si la principale méthode de communication est le téléphone portable, celle-ci doit être le premier choix dans toutes les situations. Une situation d'urgence ne nécessite pas automatiquement de passer à l'option « Urgence » (Emergency) du plan PACE. L'équipe passe à la méthode alternative uniquement lorsque la méthode principale échoue, et de même, elle passe à la méthode de secours uniquement lorsque la méthode alternative échoue, et ainsi de suite.

Vous trouverez ci-dessous quelques exemples de plans PACE. Il convient de noter que chaque section du plan PACE comporte un type de communication différent, même si plusieurs appareils sont utilisés pour communiquer au sein de ce type.

Tableau 16 Exemple de plan PACE (bureau principal)

P/A/ C/E	Type	Appareil	Utilisation(s) principale(s)
P	Filaire	• Internet par câble via un opérateur commercial avec couverture Wi-Fi dans tout le bâtiment	• Communication de données • Accès Internet • Communication vocale
A	Mobile	• Sauvegarde mobile pour connexion Internet par câble • Téléphone portable • Hotspot mobile	• Communication vocale • Communication de données • Accès Internet
C	Satellite	• Connexion Internet de secours par satellite vers certains points Wi-Fi et certains membres du personnel	• Communication de données • Accès Internet
E	Radio VHF	• Station de base par radio	• Communication vocale d'urgence

Tableau 17 Exemple de plan PACE (site reculé mais fixe)

P/A/ C/E	Type	Appareil	Utilisation(s) principale(s)
P	Satellite	• Connexion Internet par satellite avec Wi-Fi dans tout le bâtiment • Téléphone satellite	• Communication de données • Accès Internet • Communication vocale
A	Radio HF	• Station de base par radio • Radios de véhicule	• Communication vocale
C	Radio VHF	• Station de base par radio • Radios portatives	• Communication vocale
E	Mobile	• Téléphone portable	• Communication vocale d'urgence nécessitant un trajet de 20 minutes en voiture jusqu'à une zone couverte par le réseau mobile

Tableau 18 Exemple de plan PACE (équipe mobile)

P/A/ C/E	Type	Appareil	Utilisation(s) principale(s)
P	Mobile	• Téléphone portable • Hotspot mobile	• Communication vocale • Communication de données • Accès Internet
A	Radio VHF	• Radios de véhicule • Radios portatives	• Communication vocale
C	Satellite	• Téléphone satellite • Radiobalise de détresse	• Communication vocale • Notification d'urgence
E	Aucun	• N/A	• N/A

Un plan PACE réduit les risques, mais ne peut jamais les éliminer complètement. Dans certaines situations et dans certains lieux, il peut s'avérer peu pratique, voire impossible, de disposer de quatre types de communication distincts dans un plan PACE (voir le tableau 18 avec le dernier exemple de plan PACE). Dans ce cas, il est possible de réduire davantage les risques en augmentant le nombre d'appareils d'un type de communication particulier, car cela fournit autant de sauvegardes que possible à un point de défaillance unique.

Remarque sur les communications via des applications

Il est de plus en plus courant d'utiliser des applications tierces pour envoyer des messages texte et passer des appels vocaux ou vidéo. Ces outils de communication via des applications sont très répandus et faciles à utiliser. Cependant, les applications ne peuvent pas occuper une place distincte dans un plan PACE, car elles dépendent du matériel sur lequel elles sont installées. Ainsi, un téléphone portable n'occupera qu'un seul espace sur le plan PACE, même s'il dispose de trois applications de communication différentes. *Pour une analyse plus détaillée sur les communications via les applications, voir le chapitre 6.2 – La sécurité dans un monde numérique.*

Formation du personnel

Une fois le plan PACE élaboré, un programme de formation peut être mis en place afin de s'assurer que tous les membres du personnel comprennent quand utiliser chaque moyen de communication et qu'ils maîtrisent l'utilisation de chaque appareil. Le programme de formation dépendra généralement des types de communication et des appareils utilisés. Si très peu de membres du personnel devront probablement être formés à l'utilisation d'un téléphone portable, la plupart d'entre eux auront besoin d'instructions sur l'utilisation de certains logiciels ou d'autres applications sur le téléphone. En revanche, très peu de membres du personnel (voire aucun) seront immédiatement capables de configurer et d'utiliser un système radio HF. Il est recommandé de veiller à ce que tout le personnel soit formé à l'utilisation de tous les moyens de communication prévus dans le plan PACE et s'entraîne régulièrement à les utiliser.

Les questions à prendre en compte lors de l'élaboration de la formation comprennent l'identification de la personne qui va dispenser la formation, le budget (temps et argent) nécessaire pour que le personnel maîtrise l'utilisation de tous les équipements et le niveau de connaissances technologiques requis pour chaque type d'utilisateur. Certains équipements de communication sont si complexes qu'ils peuvent nécessiter une ou plusieurs personnes à temps plein pour leur configuration et leur entretien.

La formation initiale sur les équipements de communication peut faire partie du processus d'intégration, suivie d'une remise à niveau régulière. Des formations ponctuelles peuvent aider à identifier les faiblesses et à habituer le personnel à mettre en œuvre le plan PACE. Par exemple, un membre du personnel de sécurité d'une organisation internationale coupait le Wi-Fi lorsqu'il se rendait dans un bureau national afin de tester la réaction du personnel.

Il est également utile de veiller à ce que le personnel soit formé aux pratiques de communication sécurisées, notamment à la reconnaissance des menaces et au traitement approprié de l'information sensible. Des exercices réguliers permettent au personnel de rafraîchir ses compétences, notamment en matière de mise en marche, d'utilisation et d'entretien des équipements, de résolution des problèmes de base et de vérification du chargement et du bon stockage des équipements.

Entretien des équipements

Tous les équipements de communication sont susceptibles de tomber en panne au fil du temps et devront, à un moment donné, être remplacés. Il s'agit d'un élément important à prendre en compte lors de l'élaboration d'un plan de communication. Les fabricants devraient être en mesure de fournir une estimation du délai de remplacement (c'est-à-dire la durée prévue pour le remplacement d'un appareil donné). Les organisations devraient essayer de planifier le remplacement de tous les appareils afin d'estimer les besoins budgétaires à long terme et d'anticiper les perturbations dans les communications.

Outre l'équipement lui-même, les éléments d'entretien courants à budgétiser comprennent les batteries de rechange, les chargeurs de batterie, les antennes ou autres périphériques, les étuis pour téléphones ou les protections d'écran, ainsi que tout autre accessoire nécessaire au bon fonctionnement de l'équipement.

Exemple de cas : L'importance de l'entretien

Pour des raisons de coût, une organisation a décidé de ne pas utiliser le satellite comme principal moyen de communication, préférant le réserver comme solution de secours en cas d'urgence. Un audit de son infrastructure de téléphonie par satellite a révélé qu'environ 40 % des batteries étaient déchargées et que 40 % des téléphones avaient besoin d'une mise à jour du logiciel.

Tous les équipements de communication, quelle que soit leur place dans le plan PACE, doivent être testés régulièrement. Les tests doivent être effectués au moins une fois par semaine sur les équipements de communication qui ne sont pas utilisés régulièrement, et quotidiennement sur les équipements de communication qui sont utilisés tous les jours. En plus des tests de routine, les appareils doivent idéalement être testés avant tout déplacement prévu et avant l'arrivée du personnel sur un nouveau site. Par exemple, si une équipe se rend sur un site, tous les appareils du plan PACE peuvent être testés pour s'assurer qu'ils fonctionnent avant le départ de l'équipe, puis testés à nouveau à l'arrivée. Cela ne doit pas nécessairement être trop contraignant, mais il est conseillé d'envoyer un simple SMS ou de passer un appel test pour vérifier la connexion. Outre l'équipement lui-même, il est recommandé de tester régulièrement les batteries et autres équipements périphériques.

Protection des équipements de communication

Les équipements de communication ont des paramètres de fonctionnement et des besoins de protection différents. Tout équipement électronique branché sur une prise électrique doit être protégé contre les coupures de courant et les surtensions ou surintensités. Dans un environnement chaud, les équipements doivent généralement être équipés d'un mécanisme permettant de les refroidir, tandis que ceux qui fonctionnent dans un environnement très froid peuvent devoir être maintenus à une température élevée. L'un des plus grands défis pour les équipements de communication dans les véhicules est de les garder propres et exempts de poussière. Les exigences en matière de protection doivent être prises en compte dans le budget et planifiées.

- *Pour plus d'informations sur les précautions à prendre contre le vol, voir le chapitre 7.2 - Sécurité du site.*

- *Pour plus d'informations sur les précautions à prendre contre l'interception des communications ou l'intrusion numérique, voir le chapitre 6.2 - La sécurité dans un monde numérique.*

6.1.5 Bonnes pratiques en matière de méthodes de communication

Communication claire et sécurisée

Les principes clés de la discipline opérationnelle en matière de communication sont la clarté, la concision, la rapidité et la pertinence. Il est impératif que le personnel soit conscient des risques liés à la communication de certains types d'informations et qu'il soit formé à cet égard, en particulier lorsqu'il utilise des méthodes non cryptées.

Procédures d'utilisation de la radio

La clarté et la concision des communications radio sont assurées par l'utilisation de mots de procédure (ou «prowords») et de signaux de communication (tels que «Terminé!» ou «Répétez!»). La clarté est améliorée lorsque:

- les messages sont préparés à l'avance;
- les messages sont présentés point par point;
- les utilisateurs cessent de parler lorsqu'ils n'ont rien à ajouter;
- les utilisateurs s'expriment par des phrases courtes, dans un langage simple et standard, plutôt que dans les dialectes locaux; et
- les utilisateurs ne parlent pas trop vite, surtout lorsque le destinataire doit noter le message, et parlent sur un ton normal (crier peut nuire à la qualité de la réception).

Il existe un protocole radio internationalement reconnu pour les situations d'urgence (avec de nombreuses variations locales). L'appelant demande l'autorisation d'utiliser la fréquence en répétant trois fois «MAYDAY MAYDAY MAYDAY» ou «PAN PAN PAN», généralement suivi de «ALL STATIONS». Il existe une obligation absolue d'accepter les appels d'urgence et d'interrompre les conversations en cours. Un message de sécurité qui n'indique pas une menace pour la vie ou les biens (par exemple, un avis de troubles civils dans une ville qui doit donc être évitée) peut être lancé en répétant «SÉCURITÉ, SÉCURITÉ, SÉCURITÉ».

Procédures de communication d'urgence

Les procédures de communication d'urgence doivent être établies à l'avance et régulièrement mises en pratique par tous les membres du personnel. L'encadré ci-dessous donne des indications sur les informations essentielles à communiquer en cas d'urgence, quel que soit le mécanisme de communication utilisé. La mise en pratique de cette séquence peut contribuer à réduire les erreurs en cas d'urgence.

Comment communiquer en cas d'urgence

Communiquer les informations dans le format et l'ordre indiqués ci-dessous :

1. Qui vous êtes.
2. Votre organisation.
3. Votre position (par exemple, votre position GPS ou les routes ou villes principales les plus proches).
4. Type d'urgence (par exemple, accident de mine, sous les tirs ou évacuation médicale).
5. Nombre de personnes blessées.
6. Activité négative actuelle : est-il possible d'effectuer un sauvetage en toute sécurité à l'heure actuelle ?
7. Activité négative passée.
8. Prochaine heure de communication.
9. Comment contacter l'appelant (par exemple, numéro de téléphone ou fréquence radio).
10. Autres informations.

► Pour plus de recommandations sur le signalement des incidents, voir le chapitre 4.4.

Il est également important que les membres du personnel vérifient régulièrement tous les contacts et procédures d'urgence afin que chacun soit en mesure de contacter le personnel approprié en cas d'urgence. Cela peut se faire, par exemple, au moyen d'appels mensuels de vérification.

En période de crise, les décideurs peuvent être submergés par tant d'informations qu'il leur est impossible de distinguer les faits des rumeurs. Pour être efficace, il est important de limiter les communications aux seules questions d'importance directe. Là encore, cela peut être réalisé grâce à la formation et à la discipline.

Communiquer une information sensible

Lorsqu'il communique une information sensible, le personnel doit tenir compte des facteurs suivants :

- **Évaluer la nécessité de communiquer.** Avant de partager une information sensible, évaluer s'il est nécessaire de divulguer cette information et à qui elle doit être communiquée. S'assurer que le partage est justifié et approprié.

- **Vérifier l'autorisation du destinataire.** Confirmer que tous les destinataires sont autorisés à recevoir l'information. Cela permet d'empêcher tout accès non autorisé et de garantir le respect des réglementations en matière de confidentialité.
- **Limiter le partage d'informations.** Ne partager que le minimum d'informations nécessaires à la communication. Éviter de fournir des détails superflus qui pourraient augmenter le risque d'exposition. Toutes les personnes ayant accès à ces informations doivent comprendre et respecter la confidentialité.
- **Choisir les canaux de communication appropriés.** Choisir la méthode de communication la plus sûre et la plus appropriée. Pour l'information sensible, privilégier les réunions privées en face à face ou les plateformes de messagerie sécurisées plutôt que les équipements de communication non cryptés ou les forums publics.
- **Documenter soigneusement les communications.** Conserver des traces précises des communications impliquant de l'information sensible, en notant qui a été informé et ce qui a été discuté. Cela peut contribuer à garantir la redevabilité et la transparence.
- **Gérer le consentement.** Si les informations concernent une personne en particulier ou sa situation, il est recommandé d'obtenir son consentement pour partager ses informations personnelles et d'être transparent quant aux personnes qui peuvent avoir accès à ces informations et à quelles fins.

Le personnel peut être sensibilisé au fait que, même dans les meilleures circonstances, les communications peuvent être interceptées, et qu'il doit donc faire attention à ce qu'il communique. Dans les environnements à haut risque, il est judicieux d'encourager le personnel à s'exprimer de manière modérée, factuelle et impartiale. Lorsque le personnel risque d'être pris pour cible, il convient de coder certaines informations susceptibles de révéler sa position ou ses déplacements, par exemple en utilisant des mots codés pour désigner les bureaux, les personnes, les itinéraires et les points de passage, les véhicules et les types de marchandises. Cette pratique est courante, mais rarement bien gérée et, par conséquent, peu efficace. Elle nécessite des briefings minutieux et des accords préalables. Idéalement, les mots ou expressions codés sont appris par cœur (plutôt qu'écrits dans un livre de codes) et changés régulièrement. Pour les événements politiquement sensibles, les expressions métaphoriques peuvent permettre un démenti plausible. Un code qui est déchiffré peut constituer une vulnérabilité majeure. Un trop grand nombre de mots codés peut semer la confusion parmi le personnel.

Informations complémentaires

Recommandations et ressources

Cluster des télécommunications d'urgence (n.d.) *Services & activities* (en anglais, « Services et activités ») (www.etcluster.org/services-activities).

Davis, J. et al. (2020) 'Module 9, Communications and information security' in *Security to go: a risk management toolkit for humanitarian aid agencies* (en anglais, « Module 9, Sécurité des communications et de l'information dans La sécurité en pratique: boîte à outils de gestion des risques à l'attention des agences humanitaires », 4e édition), 4th edition. GISF (<https://gisf.ngo/resource/security-to-go/>).

European Interagency Security Forum (2010) *The information management challenge: a briefing on information security for humanitarian non-governmental organisations in the field* (en anglais, « Le défi de la gestion de l'information : briefing sur la sécurité de l'information pour les organisations non gouvernementales humanitaires sur le terrain ») (<https://gisf.ngo/resource/the-information-management-challenge/>).

GISF (n.d.) *Communications technology hub* (<https://gisf.ngo/communications-technology-and-humanitarian-delivery/>).

PAM (n.d.) Cluster des télécommunications d'urgence (www.wfp.org/emergency-telecommunications-cluster).

6.2 La sécurité dans un monde numérique

Ce chapitre traite des risques numériques et de leurs conséquences concrètes pour les travailleurs humanitaires. Il donne un aperçu des mesures d'atténuation possibles ainsi que des défis croissants posés par les informations préjudiciables, telles que les informations erronées, la désinformation, la mauvaise information et les discours de haine.

6.2.1 Sécurité numérique

Les technologies mondiales d'accès permettent d'élargir la portée, d'améliorer l'acheminement de l'aide et la stabilité opérationnelle, et permettent aux populations touchées de partager leurs expériences et leurs points de vue. Les progrès réalisés dans le domaine des technologies mobiles, notamment la 4G et la 5G, ont permis d'accélérer la transmission des données et d'augmenter les capacités de bande passante, tandis que les équipements satellitaires de nouvelle génération, tels que Starlink, ont considérablement élargi les possibilités de travailler en ligne dans des endroits très reculés, en offrant un accès Internet fiable, rapide et abordable.

Ces évolutions technologiques comportent également des risques accrus pour les organisations humanitaires, leur personnel et leurs opérations, ainsi que pour les populations qu'elles servent. L'augmentation du nombre et de la gravité des cyberattaques et autres menaces numériques (telles que le piratage, la surveillance, les abus en ligne et les fuites de données) signifie que chaque utilisateur individuel doit être équipé pour se protéger, protéger ses appareils, ses communications et ses données contre les menaces numériques. Il est de plus en plus important pour les organisations humanitaires de mettre en place des pratiques de sécurité numérique complètes.

Sécurité numérique

Dans le cadre du présent chapitre, la sécurité numérique désigne la protection et la sauvegarde des travailleurs humanitaires qui utilisent ou sont concernés par les outils et technologies numériques. Cela inclut les préjudices liés à l'information ainsi que la « cybersécurité », c'est-à-dire les aspects techniques liés à la sécurité des ordinateurs, des appareils mobiles, des applications, des données et des services d'accès dont dépendent les travailleurs humanitaires.

Les menaces numériques qui pèsent sur les organisations humanitaires sont nombreuses et multiples. La sécurité des appareils mobiles, l'utilisation de réseaux et de sources Internet non fiables et potentiellement hostiles, l'interception de données et de

communications numériques, ainsi que la sécurité physique des appareils et des données requièrent toute notre attention. La sphère numérique offre également des possibilités de collecte de renseignements à des entités potentiellement hostiles ou malveillantes. Bien que la sécurité numérique relève souvent du domaine informatique, le personnel de sécurité participe de plus en plus aux discussions sur la sécurité numérique, car les menaces numériques peuvent avoir des implications importantes en matière de sécurité physique pour les travailleurs humanitaires. Par exemple, le piratage ou l'accès non autorisé à des données sensibles, telles que des itinéraires de voyage ou des informations personnelles, peut entraîner des attaques physiques ciblées, des enlèvements contre rançon et du harcèlement de la part d'acteurs hostiles. Le cyberespionnage et la surveillance peuvent permettre à des acteurs étatiques et non étatiques de surveiller les déplacements et les communications des travailleurs humanitaires, les rendant vulnérables à des interceptions ou à des embuscades.

La diffusion d'informations erronées ou de désinformation via des canaux numériques peut également inciter à l'hostilité ou à la violence de la part des communautés locales ou des groupes armés, mettant directement en danger le personnel. Le vol d'appareils contenant des données critiques peut entraîner des violations qui compromettent la sécurité des opérations, mettant ainsi à risque les travailleurs humanitaires et les communautés locales. L'intersection entre la sécurité numérique et la sécurité physique est donc cruciale, car toute faille dans la sécurité numérique peut avoir de graves conséquences dans le monde réel. Le personnel de sécurité doit comprendre les types de menaces numériques auxquelles les travailleurs humanitaires peuvent être confrontés et savoir comment collaborer avec d'autres équipes de l'organisation pour atténuer les risques numériques, notamment en encourageant les pratiques d'hygiène numérique parmi le personnel.

6.2.2 Menaces numériques et risques liés à la cybersécurité

La nature des menaces numériques peut varier en fonction du niveau de la cible, qui peut être un individu, une organisation spécifique ou le secteur humanitaire dans son ensemble. Bien qu'il y ait souvent des recoupements (par exemple, des individus peuvent devenir des victimes lorsque leur organisation est prise pour cible), il est utile pour les organisations de discuter des risques spécifiques et de mettre en œuvre des mesures visant à atténuer les menaces à ces trois niveaux. Cela peut s'avérer particulièrement utile en ce qui concerne les risques liés aux informations préjudiciables.

Acteurs de menaces

Les menaces numériques peuvent provenir d'un éventail d'acteurs ayant des motivations différentes (par exemple économiques, idéologiques ou stratégiques). En voici quelques exemples :

- **Cybercriminels.** Individus, petits groupes, gangs ou grandes organisations et entreprises criminelles principalement motivés par l'appât du gain et qui recherchent des cibles d'opportunité. Certains ont également des motivations idéologiques ou politiques.

- **Acteurs étatiques.** Les organisations humanitaires opérant dans des zones de conflit ou des régions soumises à de fortes tensions politiques peuvent être prises pour cible, accidentellement ou intentionnellement, par des gouvernements et des acteurs étatiques étrangers. Les entités gouvernementales opérant dans la sphère numérique sont généralement motivées par des considérations de sécurité nationale et d'autres préoccupations politiques, et peuvent être tout à fait capables de mener à bien des cyberattaques et des opérations de surveillance numérique, ainsi que des campagnes d'influence préjudiciables en ligne.
- **Acteurs armés non étatiques.** À mesure que les ressources numériques deviennent de plus en plus accessibles, leur utilisation potentielle par des acteurs armés non étatiques augmente. Ces groupes peuvent utiliser les mêmes tactiques que les cybercriminels à des fins lucratives, mais aussi pour recueillir des renseignements et exploiter les informations à des fins idéologiques et politiques. Ils peuvent recourir à des campagnes d'influence en ligne, à la désinformation et à d'autres attaques ciblées pour nuire aux activités d'une organisation ou à son image auprès des communautés locales.
- **Autres.** Les employés mécontents ou les personnes qui nourrissent de la rancœur envers l'organisation ou certains membres du personnel peuvent constituer une menace dans la sphère numérique, tout autant que dans la vie réelle. Les influenceurs des réseaux sociaux ayant des agendas politiques peuvent utiliser leurs plateformes pour diffuser des informations préjudiciables sur les organisations humanitaires ou le secteur humanitaire dans son ensemble. Les menaces peuvent également provenir du public influencé par ces influenceurs ou par des campagnes en ligne.

Types de menaces numériques

Voici une liste de certains des défis en matière de sécurité numérique auxquels les travailleurs humanitaires peuvent être confrontés. Ceux-ci peuvent se chevaucher ou se produire simultanément, mais tous peuvent potentiellement se traduire par des risques de sécurité physique.

Tableau 19 Types de menaces numériques

Menace	Description
Harcèlement et discours de haine en ligne	Le harcèlement et les menaces en ligne, y compris les discours de haine, visent souvent les travailleurs humanitaires issus de groupes marginalisés ou en relation directe avec le public. Il peut s'agir de campagnes ciblées diffusant des contenus incendiaires ou péjoratifs visant à inciter à la violence ou à nuire à la crédibilité et à la sûreté de travailleurs humanitaires individuels, d'une organisation particulière ou de la communauté humanitaire dans son ensemble.
Usurpation d'identité	Vol d'informations personnelles.
Ingénierie sociale	Manipulation d'individus afin qu'ils divulguent des informations confidentielles, souvent au moyen d'interactions apparemment anodines.

Menace	Description
Informations erronées, désinformation et mauvaise information	La diffusion d'informations préjudiciables sur les organisations humanitaires, leur personnel ou leur travail, qui nuisent à leur crédibilité, à la confiance dont elles jouissent et à leur efficacité opérationnelle. Il peut s'agir de campagnes en ligne ou de fuites de données qui portent atteinte à la réputation de l'organisation ou des travailleurs humanitaires à titre individuel. Si ces informations préjudiciables peuvent être délibérément orchestrées, elles peuvent également se propager de manière organique sur les réseaux sociaux.
Hameçonnage et escroqueries par e-mail	Ces techniques sont conçues pour voler des identifiants, introduire des logiciels malveillants ou obtenir un accès non autorisé à de l'information sensible. Ces risques se sont étendus aux appareils mobiles sous la forme de hameçonnage par SMS ou « smishing ». Les escroqueries améliorées par l'intelligence artificielle (IA), telles que les attaques de « vishing » (hameçonnage par appel vocal, dans lesquelles l'IA est utilisée pour cloner la voix d'une personne connue de la cible), sont également en augmentation.
Escroqueries et fraudes en ligne	Escroqueries financières visant les organisations et les travailleurs humanitaires à titre individuel, souvent au moyen de pratiques trompeuses en ligne.
Piratage et intrusions dans les systèmes	Ces actes visent à accéder aux systèmes organisationnels ou à les perturber, souvent dans le but de voler des données sensibles ou de causer des dommages opérationnels.
Vol de données	Vol de données organisationnelles sensibles, notamment des informations sur les bénéficiaires de l'aide, des documents financiers et des communications confidentielles.
Attaques par ransomware et logiciels malveillants	Introduction de logiciels malveillants, notamment des ransomwares (rançongiciels), afin de verrouiller les systèmes ou les données jusqu'au paiement d'une rançon ou d'endommager purement et simplement les systèmes.
Cyberespionnage et surveillance	La surveillance et le contrôle exercés par des acteurs étatiques ou non étatiques, en particulier dans les régions où les activités des organisations humanitaires sont considérées avec suspicion, peuvent inclure : l'interception de communications et d'informations sur les lieux de distribution de l'aide ; le suivi des déplacements ou la géolocalisation du personnel ou des bénéficiaires de l'aide ; ou l'identification du personnel, pouvant aboutir à d'autres cyberattaques, voire à des atteintes physiques. Il existe des cas avérés d'acteurs étatiques utilisant des logiciels espions contre des organisations. <i>Pour plus de détails sur la surveillance hostile et les mesures d'atténuation associées, voir le chapitre 7.5.</i>

6.2.3 Ciblage en ligne de membres du personnel particuliers

Les attaques en ligne, en particulier via les réseaux sociaux et autres plateformes, peuvent entraîner le harcèlement, l'abus, l'intimidation et le chantage directs des

travailleurs humanitaires. Le ciblage direct est une menace croissante et sérieuse, en particulier pour les personnes occupant des fonctions en contact avec le public ou issues de groupes sous-représentés ou marginalisés (par exemple, les femmes et les personnes qui s'identifient comme LGBTQI+).⁸⁶ Le harcèlement peut prendre diverses formes, notamment le cyberharcèlement, le doxing (publication en ligne d'informations privées sans consentement) et l'imposture malveillante. La cyber-traque (ou traque en ligne) peut se traduire par des messages persistants et menaçants, tandis que le doxing peut exposer au public des informations personnelles sensibles (telles que l'adresse du domicile et des détails sur la famille). L'imposture (ou usurpation) malveillante, qui consiste pour les pirates à créer de faux profils afin de tromper ou de ternir la réputation de la victime, peut gravement nuire aux relations personnelles et professionnelles ainsi qu'à la crédibilité.

Exemple de cas : Harcèlement en ligne au Moyen-Orient

Un blog jordanien a publié des photos de profil provenant d'applications de rencontres gay, ce qui a suscité une vive réaction de la part du public et exposé les personnes dont les photos ont été publiées à des risques immédiats et importants, notamment l'ostracisme social, le harcèlement et d'éventuelles poursuites judiciaires. Cet incident souligne l'importance de la sécurité numérique et les conséquences potentielles de l'exposition numérique dans des environnements hostiles. Il souligne également la nécessité pour les organisations humanitaires de fournir des directives claires à leur personnel sur la protection de leur identité en ligne, ainsi que l'importance de surveiller les espaces en ligne locaux afin de détecter les menaces potentielles et de prendre des mesures proactives pour atténuer les risques.

Source : Kumar, M. (2017) *Digital security of LGBTQI aid workers: awareness and response* (en anglais, « Sécurité numérique des travailleurs humanitaires LGBTQI : sensibilisation et réponse »). GISF (<https://gisfprod.wpengine.com/resource/digital-security-of-lgbtqi-aid-workers-awareness-and-response/>).

Les attaques en ligne peuvent avoir des effets psychologiques profonds sur leurs cibles, entraînant du stress, de l'anxiété et un sentiment généralisé de vulnérabilité. L'impact peut être encore plus grave lorsque les informations personnelles sont utilisées comme une arme dans des environnements hostiles à certaines identités ou

86 Pour des exemples plus détaillés des risques numériques auxquels sont confrontés les travailleurs humanitaires LGBTQI+, voir Kumar, M. (2017) *Digital security of LGBTQI aid workers: awareness and response* (en anglais, « Sécurité numérique des travailleurs humanitaires LGBTQI : sensibilisation et réponse »). GISF (<https://gisfprod.wpengine.com/resource/digital-security-of-lgbtqi-aid-workers-awareness-and-response/>).

affiliations, ou lorsque les travailleurs humanitaires sont déjà confrontés à des risques importants en raison de la nature de leur travail.

Ces attaques directes sont également plus difficiles à détecter pour les organisations, et les auteurs peuvent même être des collègues de la victime. L'ensemble du processus d'une menace numérique (identification de la cible, recherche des vulnérabilités, prise de contact avec la victime, mise en œuvre de la menace, résolution du problème) peut se dérouler entièrement en ligne, ce qui le rend difficile à détecter pour toute personne qui n'est pas directement concernée.

Pour atténuer ces risques, les organisations peuvent proposer une formation à la sécurité numérique complète qui couvre les comportements sûrs en ligne, la manière de reconnaître et de répondre aux risques en ligne (tels que le harcèlement et l'exploitation) et la manière de gérer les identités et les empreintes numériques. Les travailleurs humanitaires peuvent être encouragés à utiliser des comptes sécurisés, à activer des paramètres de confidentialité stricts sur les réseaux sociaux et à envisager l'utilisation de pseudonymes pour protéger leur identité. Il est également conseillé aux organisations de mettre en place des politiques solides pour lutter contre l'exploitation numérique, en proposant des directives claires sur la manière de traiter les incidents de harcèlement et en offrant des espaces sûrs où les employés concernés peuvent faire part de leurs préoccupations ou signaler des incidents.

Des services de soutien doivent être mis à la disposition des personnes concernées, notamment des ressources en santé mentale pour aider les employés à faire face à l'impact psychologique d'être pris pour cible, ainsi qu'une aide juridique pour traiter toute violation potentielle de la vie privée ou de la sécurité. En créant un réseau de soutien solide et en favorisant une culture de sensibilisation à la sécurité numérique, les organisations peuvent contribuer à protéger leur personnel contre la menace croissante des attaques en ligne et de leurs conséquences potentiellement graves.

► Voir le chapitre 5.4 pour plus d'informations sur bien-être du personnel, notamment le soutien en santé mentale.

Répondre à une attaque directe en ligne

Voici les mesures qu'une organisation peut envisager de prendre à la suite d'une attaque en ligne contre une personne.

- **Identifier l'agresseur.** Identifier l'agresseur et ses actions, si possible.
- **Évaluer les plateformes compromises.** Identifier les plateformes ou appareils compromis et réinitialiser les mots de passe. Modifier les noms d'utilisateur et les identifiants si nécessaire.
- **Contenir les informations indésirables.** Contacter les réseaux sociaux ou les opérateurs de télécommunications afin de contenir la propagation de contenus indésirables. Veiller à sécuriser les communications lors de cette démarche.

- **Avertir les institutions financières.** Si nécessaire, informer les banques ou les institutions financières en cas de demandes d'argent ou de menaces.
- **Protéger l'intégrité de l'organisation.** Minimiser l'impact sur l'organisation afin d'éviter de mettre en danger d'autres membres du personnel ou de nuire à la réputation de l'organisation.
- **Informers les autorités compétentes.** Selon la situation, alertez les autorités compétentes, par exemple la police locale ou l'ambassade (si un ressortissant étranger est concerné).
- **Communiquer avec le personnel.** Informer le personnel qu'il doit signaler toute nouvelle menace directement au service de sécurité et aux autres responsables.
- **Envisager une évacuation ou une relocalisation.** Si la situation dégénère en menace physique, envisager d'évacuer ou de relocaliser les personnes concernées.
- **Limiters la révélation d'informations.** Ne partager que les informations nécessaires pour contenir la menace, en évitant la révélation de détails sensibles.
- **Documenter l'incident.** Conserver des traces écrites détaillées de toutes les communications, menaces et actions entreprises. Cela peut s'avérer utile à des fins juridiques et de protection future.
- **Offrir un soutien psychosocial.** Proposer des services de counseling ou tout autre soutien psychosocial au personnel concerné.
- **Engager une campagne de contre-information.** Si les informations erronées ou le harcèlement sont publics, envisager une réponse officielle contrôlée afin de contrer les fausses rumeurs et de préserver la crédibilité.
- **Réviser et renforcer les protocoles de sécurité.** Une fois l'incident résolu, réviser et mettre à jour les protocoles de sécurité numérique afin d'éviter que cela ne se reproduise à l'avenir.
- **Suivi continu.** Continuer le suivi de la présence en ligne de la victime et des plateformes associées afin de détecter toute nouvelle menace ou tout nouveau harcèlement.

6.2.4 Informations préjudiciables

Les informations préjudiciables (informations erronées, désinformation, mauvaise information et discours de haine) constituent désormais une menace sérieuse pour

les organisations humanitaires. Avec l'essor des réseaux sociaux, des images et vidéos générées par l'IA, et le nombre croissant de sites Web alternatifs de partage d'informations, ce type de menace ne fera qu'augmenter en fréquence, en ampleur et en gravité.

Les informations partagées en contextes de crise humanitaire peuvent devenir préjudiciables par le biais de plusieurs mécanismes différents, décrits plus en détail ci-dessous, et peuvent impliquer un large éventail d'acteurs externes ayant des intentions, des cibles et des moyens de diffusion de l'information différents. La confiance dans les institutions, les autorités et les sources d'information traditionnelles est affaiblie, laissant la place à d'autres sources d'information, notamment les réseaux sociaux. Si les plateformes alternatives peuvent amplifier des voix qui, autrement, ne seraient pas entendues, elles peuvent également permettre à des informations préjudiciables de se propager sans contrôle et d'atteindre un public sans précédent, y compris les parties prenantes de l'action humanitaire.

Il est important de garder à l'esprit que les sources d'informations préjudiciables peuvent être des acteurs avec lesquels les organisations humanitaires ne collaborent généralement pas, tels que les entreprises de la tech, le secteur privé, les plateformes de réseaux sociaux, les influenceurs et les utilisateurs lambda.

Définitions clés

Les informations erronées désignent des informations inexacts ou fausses qui sont diffusées sans intention de tromper. Elles résultent souvent d'un malentendu, d'une erreur ou d'un manque de vérification adéquate, plutôt que d'une tentative délibérée d'induire en erreur. Elles se distinguent de la désinformation, qui désigne une information délibérément fausse ou trompeuse. La mauvaise information est une information vraie qui est sortie de son contexte d'origine ou manipulée de manière à induire en erreur ou à causer un préjudice. Le discours de haine désigne tout contenu qui cible un groupe ou un individu en fonction de ses caractéristiques intrinsèques, telles que l'ethnicité, la religion ou le genre.⁸⁷

Impact sur la sécurité

Les organisations humanitaires privilégient souvent l'acceptation comme approche fondamentale de gestion des risques de sécurité, fondée sur une réponse basée sur des principes qui respecte les principes de neutralité, d'indépendance, d'humanité et d'impartialité. Les informations préjudiciables sont particulièrement dangereuses car elles peuvent nuire à la perception d'une réponse fondée sur des principes parmi les parties prenantes, souvent indépendamment de toute action entreprise par l'organisation ou son personnel. Ces informations peuvent également être utilisées pour manipuler l'opinion publique, façonner les discours et nuire à la crédibilité des organisations humanitaires. En voici quelques exemples :

87 Pour une analyse détaillée des définitions, voir Wardle, C. (2024) *A conceptual analysis of the overlaps and differences between hate speech, misinformation and disinformation* (en anglais, «Analyse conceptuelle des recoupements et des différences entre discours de haine, informations erronées et désinformation»). Département du Maintien de la paix (ONU) (<https://peacekeeping.un.org/en/new-report-finds-understanding-differences-harmful-information-is-critical-to-combatting-it>).

- **Propager de fausses informations.** Les acteurs peuvent diffuser de fausses informations afin de discréditer les organisations humanitaires, en les présentant comme partiales ou motivées par des considérations politiques, voire comme servant de couverture à des activités d'espionnage. Cela suscite la méfiance, sape le soutien public et justifie les restrictions d'accès aux zones de crise. Même les vraies informations sur les efforts d'aide peuvent être manipulées. Après les tremblements de terre de 2023 en Turquie, une histoire selon laquelle le Croissant-Rouge turc vendait des tentes s'est répandue et amplifiée sur les réseaux sociaux, alimentant les critiques à l'égard de la réponse du gouvernement à la catastrophe. Cette manipulation a sapé la confiance du public tant envers le gouvernement qu'envers le Croissant-Rouge turc.⁸⁸
- **Accusations d'inconduite.** Les campagnes de désinformation peuvent accuser à tort les travailleurs humanitaires de crimes ou d'inconduite, tels que la corruption ou la collaboration avec les forces ennemies, ce qui nuit à leur réputation et peut entraîner des répercussions juridiques ou opérationnelles, voire leur expulsion. Les organisations humanitaires peuvent elles-mêmes être accusées de diffuser des informations erronées ou de la désinformation.
- **Diffuser de fausses informations.** La désinformation, telle que les fausses informations sur les distributions ou autres interventions partagées en ligne, peut semer la confusion, perturber les opérations et nuire à la confiance entre les organisations et les communautés. Les fausses informations exploitant les sensibilités culturelles ou religieuses, telles que les rumeurs sur les campagnes de vaccination, peuvent inciter à la violence contre les travailleurs humanitaires et perturber les opérations critiques. La désinformation peut également créer de fausses perceptions de biais dans la distribution de l'aide.
- **Discréditer les rapports humanitaires.** Les acteurs étatiques peuvent utiliser les informations erronées pour saper la crédibilité des rapports documentant les violations des droits humains ou les crises, les qualifiant souvent de «faux» afin d'en rejeter les conclusions. À titre d'exemple, le Myanmar a nié l'existence d'une crise humanitaire touchant la population rohingya.
- **Imposture.** Les acteurs peuvent pirater les communications des organisations humanitaires afin de diffuser directement de fausses informations.
- **Utiliser l'information comme une arme.** Des acteurs hostiles peuvent pirater des systèmes de données afin de modifier des archives ou de divulguer une information sensible, sapant ainsi la crédibilité de l'organisation ou ciblant des groupes spécifiques. En 2022, un piratage a exposé les données de plus de 515 000 personnes vulnérables, les mettant en danger et nuisant à la confiance accordée au CICR.⁸⁹

88 Insecurity Insight (2023) *The role of social media in the spreading of the Turkish Red Crescent Tent Sale Story in Türkiye* (en anglais, «Le rôle des réseaux sociaux dans la diffusion de l'histoire de la vente de tentes du Croissant-Rouge turc en Turquie»). Social Media Monitoring (en anglais, «Suivi des réseaux sociaux») (<https://insecurityinsight.org/wp-content/uploads/2023/08/The-Spreading-of-the-Turkish-Red-Crescent-Tent-Sale-Story.pdf>).

89 CICR (2022) *Cyberattaque contre le CICR: le point sur ce que nous savons* (www.icrc.org/en/document/cyber-attack-icrc-what-we-know).

- **Inciter à la violence et aux discours de haine.** Les publications sur les réseaux sociaux peuvent être utilisées pour inciter à la violence ou à d'autres comportements négatifs à l'égard du personnel humanitaire, des lieux, des biens et des opérations. Les discours de haine, qui ciblent des groupes en fonction de leur identité, constituent une préoccupation réelle et immédiate.

Exemple de cas : Exemples de désinformation en Ukraine

La désinformation a des répercussions sur tous les aspects, depuis la sécurité personnelle et la réputation des organisations humanitaires individuelles jusqu'à la perception générale du secteur humanitaire et ses capacités à atteindre ses objectifs humanitaires et à mettre en œuvre ses programmes.

Pendant le conflit en Ukraine, des acteurs affiliés à la Russie ont utilisé la désinformation pour entraver et manipuler les opérations humanitaires. Un exemple notable est la diffusion de fausses informations sur les itinéraires d'évacuation. Des chaînes Telegram pro-russes ont faussement affirmé que l'armée ukrainienne bloquait certains itinéraires d'évacuation ou que ces itinéraires étaient attaqués. Ces informations ont semé la confusion et la peur parmi les civils, les incitant à éviter d'emprunter les itinéraires d'évacuation sûrs ou à retarder leur départ des zones dangereuses.

Le CICR a également été confronté à une importante campagne de désinformation visant ses efforts humanitaires en Ukraine, lorsque des acteurs affiliés à la Russie ont diffusé de fausses informations, affirmant notamment que l'organisation était impliquée dans l'évacuation forcée d'Ukrainiens vers la Russie et qu'elle avait ouvert des bureaux dans le sud de la Russie afin de filtrer les Ukrainiens. Ces accusations sans fondement, qui ont été diffusées sur les réseaux sociaux et ont parfois été reprises par les médias grand public, visaient à discréditer le travail du CICR auprès des Ukrainiens et à compromettre ses opérations.

Sources: Center for Civilians in Conflict (2023) *When words become weapons: the unprecedented risks to civilians from the spread of disinformation in Ukraine* (en anglais et en ukrainien, « Quand les mots deviennent des armes: les risques sans précédent pour les civils liés à la propagation de la désinformation en Ukraine ») (<https://civiliansinconflict.org/publications/research/when-words-become-weapons-the-unprecedented-risks-to-civilians-from-the-spread-of-disinformation-in-ukraine>) ; CICR (2022) *Ukraine: addressing misinformation about ICRC's activities* (non disponible en français, « Ukraine: lutter contre la désinformation concernant les activités du CICR ») (www.icrc.org/en/document/ukraine-addressing-misinformation-about-icrcs-activities).

Évaluation des risques liés aux informations préjudiciables

En plus de veiller à ce que les menaces numériques, y compris les informations préjudiciables, soient intégrées dans les processus d'évaluation des risques existants, les organisations devraient doter le personnel responsable, tel que celui chargé des réseaux sociaux, des outils nécessaires pour prendre directement en compte les risques liés aux informations préjudiciables.

► Voir le chapitre 4.1 pour plus d'informations sur les évaluations des risques.

Vous trouverez ci-dessous un exemple de processus d'évaluation des risques liés aux informations potentiellement préjudiciables, adapté de l'outil d'évaluation des informations erronées / de la désinformation de Médecins sans Frontières.⁹⁰

- **Comprendre la cible.** Qui est la cible (personne, programme, organisation, secteur) et comment est-elle ciblée?
- **Comprendre l'objectif.** Les informations préjudiciables sont-elles partagées dans l'intention de nuire, ou deviennent-elles préjudiciables de manière organique en raison d'une mauvaise interprétation et d'un partage généralisé?
- **Comprendre la source.** Les informations proviennent-elles d'une source particulière (par exemple, un groupe ou un influenceur)? S'agit-il d'informations totalement nouvelles ou ont-elles déjà été diffusées auparavant?
- **Classer.** Ce contenu présente-t-il un risque faible ou élevé? (Voir le tableau 20.)
- **Évaluer.** Quel type de risque cela représente-t-il? (Voir le tableau 21.)

Tableau 20 Classification des risques liés au contenu

Faible	Moyen	Élevé	Urgent
Malentendu inoffensif / information erronée sans gravité	Informations erronées pouvant causer un préjudice	Informations délibérément préjudiciables impliquant l'organisation ou son personnel	Propagande ciblée contre l'organisation ou son personnel

90 Voir GISF (2023) *Online risk to real-life harm: disinformation and social listening workshop resources* (en anglais, «Risques en ligne et préjudices dans la vie réelle: ressources pour un atelier sur la désinformation et l'écoute sociale») (www.gisf.ngo/resource/online-risk-to-real-life-harm-disinformation-and-social-listening-workshop-resources/).

Tableau 21 Évaluation du risque lié au contenu

	Faible	Moyen	Élevé	Urgent
Gravité	Aucun risque réel de préjudice ou de menace	Risque modéré de préjudice	Risque indirect de préjudice réel	Menace directe de préjudice réel
Degré	Peu d'attention	Reprise modérée, quelques commentaires	Attention considérable en peu de temps	Se propage
Cible	Pas de cible spécifique	Impact indirect sur l'organisation et son personnel	Impact direct sur l'organisation et son personnel	Cible directement l'organisation et son personnel
Source	Source ayant une portée limitée	Localisée en mouvement, ponctuelle	Coordonnée, ciblée	Réseaux à forte portée

Mesures d'atténuation

Une fois les risques liés aux informations préjudiciables évalués, plusieurs mesures d'atténuation sont possibles, comme indiqué ci-dessous. Ces mesures doivent être soigneusement évaluées et adaptées aux risques spécifiques, car ce qui fonctionne bien dans un cas peut aggraver la situation dans un autre.

- **Évaluer le paysage de l'information.** Comprendre où et comment les communautés cibles obtiennent leurs informations en identifiant les sources et les canaux de communication de confiance. Cela permet de cibler et de contrer les discours préjudiciables avant qu'ils ne se propagent massivement.⁹¹ Les organisations doivent veiller à ce que l'analyse et la cartographie des acteurs incluent les personnes ou les groupes susceptibles d'influencer la propagation d'informations préjudiciables.
- **Élaborer et mettre en œuvre des stratégies de communication.** Concevoir des stratégies de communication solides qui incluent le suivi des réseaux sociaux afin d'identifier les contenus positifs et négatifs pertinents pour l'organisation, son travail et le secteur humanitaire dans son ensemble. Créer une forte présence sur les réseaux sociaux, sur des plateformes pertinentes dans le contexte, en les mettant régulièrement à jour avec des contenus positifs, honnêtes et transparents qui mettent

⁹¹ À cette fin, une évaluation de l'écosystème de l'information peut s'avérer utile. Voir, par exemple, Internews (2015) *Mapping information ecosystems to support resilience* (en anglais, « Cartographier les écosystèmes de l'information pour soutenir la résilience ») (https://internews.org/wp-content/uploads/legacy/resources/Internews_Mapping_Information_Ecosystems_2015.pdf).

en avant les messages clés et les principes humanitaires. «Verified» ou «Vérifié», par exemple, est une initiative lancée par l'ONU en collaboration avec Purpose pour lutter contre les informations erronées liées au Covid-19.

- **Suivre les contenus préjudiciables et les changements d'opinions.** Investir dans des initiatives «d'écoute» des réseaux sociaux afin de suivre l'évolution des sentiments au fil du temps et de signaler les contenus négatifs avant qu'ils ne se transforment en une menace réelle pour la sécurité.⁹² Les organisations peuvent également utiliser des ressources publiques qui suivent et analysent les contenus afin d'identifier les menaces potentielles, les informations préjudiciables et les opinions du public susceptibles d'affecter la sécurité et l'efficacité des efforts d'aide.⁹³
- **Sensibiliser et former le personnel.** Offrir au personnel une formation aux compétences numériques, en mettant l'accent sur la manière de traiter les contenus frauduleux et de gérer leur empreinte en ligne. Encourager le personnel à agir comme les yeux et les oreilles de l'organisation en ligne, en signalant les risques potentiels.
- **Construire des réseaux solides.** Développer des réseaux solides avec des partenaires tant à l'intérieur qu'à l'extérieur du contexte humanitaire afin d'assurer un soutien mutuel et la vérification des informations. Les relations préexistantes peuvent atténuer les risques d'atteinte à la réputation et permettre le partage rapide de la contre-information. Établir des relations avec les médias locaux et les stations de radio peut également être un moyen efficace de diffuser des informations précises sur les activités humanitaires dans la zone.
- **Sensibiliser.** Établir des partenariats avec d'autres organisations, des décideurs politiques et les médias afin de sensibiliser le public aux contenus préjudiciables et de faire pression sur les réseaux sociaux pour qu'ils agissent de manière responsable.
- **Définir clairement les rôles et les responsabilités et établir une collaboration entre les équipes.** Veiller à ce que les rôles et les responsabilités soient clairement définis en matière de suivi et de documentation des informations préjudiciables ou susceptibles de l'être, à ce que le personnel soit correctement formé et soutenu, et à ce qu'il existe des protocoles clairs précisant quand et comment les informations pertinentes seront partagées avec d'autres services de l'organisation, notamment avec le personnel de sécurité.

En général, il est conseillé aux organisations de mettre en place une stratégie pour répondre efficacement aux incidents liés à des informations préjudiciables. Les actions de réponse peuvent inclure les éléments suivants :

- **Signaler les contenus préjudiciables.** Utiliser les outils de signalement des plateformes de réseaux sociaux pour signaler les contenus préjudiciables et contacter directement les entreprises de réseaux sociaux afin d'accélérer le processus d'examen et de suppression.

92 Iacucci, A. (2023) *Social Listening* (en anglais, «Écoute sociale»). Diaporama. GISF (<https://gisf.ngo/resource/online-risk-to-real-life-harm-disinformation-and-social-listening-workshop-resources/>).

93 Par exemple, Insecurity Insight (n.d.) *Social media monitoring* (en anglais, «Suivi des réseaux sociaux») (<https://insecurityinsight.org/projects/aid-in-danger/social-media-monitoring>).

- **Vérifier les faits et diffuser la contre-information.** Envisager de collaborer avec des organismes de vérification des faits afin de vérifier les informations et élaborer la contre-information pour corriger les fausses informations. Pour que la contre-information soit efficace, il faut comprendre les principaux nœuds et liens par lesquels l'information s'est initialement propagée, et cibler ces mêmes réseaux. Cette approche peut aider à maintenir la confiance et la crédibilité tout en empêchant la propagation d'informations erronées. Toutefois, dans certains cas, il peut être préférable de ne pas attirer davantage l'attention sur les fausses informations.
- **Rétablir la confiance après des campagnes d'information préjudiciables.** Mettre l'accent sur le rétablissement de la confiance avec les communautés touchées grâce à une communication transparente et à un engagement concret. Cela peut notamment consister à démontrer comment l'organisation protège les données qu'elle collecte sur les populations ciblées et d'autres acteurs locaux, et qu'elle a pris en considération les préjudices et risques potentiels si ces données tombaient entre de mauvaises mains.
- **Collaborer avec les autorités.** Si le contenu représente une menace immédiate, envisager d'en informer les forces d'application de la loi ou les autorités compétentes.

Répondre aux incitations à la violence sur les réseaux sociaux

Les incitations à la violence sur les réseaux sociaux sont interdites par la plupart des plateformes, y compris Meta (Facebook et Instagram), qui dispose de normes communautaires contre ce type de contenu. Si une organisation constate des publications incitant à la violence, elle peut utiliser les outils de signalement de la plateforme ou contacter directement l'entreprise pour signaler que le contenu enfreint les normes communautaires ou pourrait causer un préjudice potentiel, ce qui entraînera un examen et une éventuelle suppression. Fournir des informations détaillées devrait contribuer à accélérer le processus d'examen. Si le contenu représente une menace immédiate, les forces d'application de la loi ou les autorités compétentes doivent être informées, le cas échéant, afin de garantir une réponse rapide.

Les activités de suivi peuvent inclure :

- Signaler les contenus susceptibles de devenir préjudiciables à l'avenir afin d'assurer un suivi continu.

- Consigner les mesures prises et les résultats obtenus à la suite d'un incident afin d'éclairer les futures évaluations des risques, les mesures d'atténuation des risques et les mesures de réponse.
- Procéder à un examen a posteriori afin d'identifier les enseignements à tirer pour améliorer les efforts futurs, comme cela serait fait pour un incident de sécurité critique.

6.2.5 Les technologies de communication numérique et leurs risques

De nombreux risques découlent de l'utilisation de réseaux non fiables, c'est-à-dire généralement tout réseau qui n'est pas sous le contrôle de l'organisation. Tout réseau dont le niveau de sécurité est inconnu peut être considéré comme intrinsèquement non sécurisé. La section suivante présente une liste indicative des risques associés aux technologies de communication numérique. Elle ne prétend pas être exhaustive, mais fournit plutôt des informations sur les domaines de préoccupation courants.

Réseaux mobiles

Les réseaux mobiles présentent des failles de sécurité inhérentes, notamment une vulnérabilité aux accès non autorisés et à l'interception de données, en particulier lorsque la surveillance réglementaire est laxiste ou compromise.

L'un des principaux risques liés à l'utilisation des réseaux mobiles est la possibilité pour des parties hostiles d'intercepter les flux de données. Ces parties peuvent être des gouvernements locaux, des gangs, des organisations criminelles ou des États ayant accès aux réseaux des opérateurs. Cette interception pourrait entraîner la fuite de communications sensibles ou de données opérationnelles, telles que la localisation du personnel et les mouvements opérationnels.

Wi-Fi public

Les sources Wi-Fi publiques, telles que le Wi-Fi gratuit ou payant dans les aéroports, les cafés et les hôtels, constituent un moyen courant et souvent nécessaire de connexion à Internet pour le personnel en déplacement. Le principal vecteur d'attaque est celui des attaques de type « man-in-the-middle » (MITM), dans lesquelles un tiers malveillant espionne le réseau, intercepte ou interfère avec les communications.

Il n'y a aucun moyen de savoir si un opérateur de réseau Wi-Fi a configuré son réseau de manière sécurisée, et le risque d'une attaque MITM réussie augmente lorsque ce n'est pas le cas.

Il existe également le risque qu'un acteur malveillant mette en place un « jumeau maléfique », c'est-à-dire un faux réseau Wi-Fi qui utilise le même nom qu'une source Wi-Fi légitime, amenant les utilisateurs à se connecter involontairement au faux réseau. L'attaquant sera alors en mesure d'intercepter tout le trafic Internet sur ce faux réseau Wi-Fi. Par défaut, les téléphones et les appareils peuvent se connecter

automatiquement aux réseaux Wi-Fi « connus », ce qui signifie qu'un attaquant pourrait mettre en place ce même réseau dans un aéroport et que des dizaines, voire des centaines d'appareils pourraient s'y connecter passivement.

Fournisseurs d'accès Internet locaux

Les fournisseurs d'accès Internet (FAI) locaux peuvent fournir une connexion Internet plus rapide et plus stable pour les bureaux permanents ou à long terme, ainsi que pour les sites de projets à court terme. Il est toutefois recommandé de rester prudent avec ces connexions et de prendre des mesures pour les sécuriser.

Si les FAI eux-mêmes ne constituent probablement pas une menace importante, tout système ou appareil connecté à Internet est exposé à des risques d'attaque. Les FAI pourraient être infiltrés par des cybercriminels ou des acteurs étatiques, ce qui pourrait entraîner l'interception de communications et de données sensibles. La mise en place de niveaux de cryptage supplémentaires peut renforcer la protection.

Risques liés à l'IA

Les outils d'IA présentent à la fois des opportunités et des défis pour les organisations humanitaires. Pour les travailleurs humanitaires, les défis comprennent le risque de violation des données et la propagation de contenus biaisés ou inexacts. Des acteurs hostiles peuvent utiliser l'IA pour amplifier les informations erronées, mener des attaques de phishing (hameçonnage) ou même déployer une surveillance basée sur l'IA pour suivre et cibler les travailleurs humanitaires. Ces risques soulignent la nécessité de faire preuve de prudence et de respecter strictement les protocoles de sécurité lors de toute interaction avec l'IA, tant en termes d'utilisation des outils d'IA que de protection contre les menaces liées à l'IA provenant d'acteurs hostiles. L'utilisation des systèmes d'IA dans le ciblage militaire suscite également des inquiétudes croissantes, notamment en raison du risque d'erreurs d'identification et de frappes erronées. Des organisations telles que le CICR attirent l'attention sur ce risque.ⁱ

ⁱ Viveros Álvarez, J.S. (2024) 'The risks and inefficacies of AI systems in military targeting support' (en anglais, « Les risques et les inefficacités des systèmes d'IA dans le soutien au ciblage militaire ») *Droit et politiques humanitaires*, CICR (<https://blogs.icrc.org/law-and-policy/2024/09/04/the-risks-and-inefficacies-of-ai-systems-in-military-targeting-support/>).

Stations de recharge publiques

Les stations de recharge publiques, telles que celles situées dans les aéroports, les gares et les hôtels, comprennent des prises électriques murales standard et des ports de recharge USB. Le risque accru est spécifiquement lié aux ports de recharge USB.

Le «juice jacking» consiste à introduire un petit dispositif dans un port de recharge USB compromis afin d'envoyer des commandes à un téléphone, une tablette ou tout autre appareil branché pour être rechargé. Cela peut potentiellement être utilisé pour installer des logiciels malveillants ou permettre à un pirate d'accéder à distance à l'appareil. Lorsqu'il n'est pas possible d'accéder à une prise électrique murale pour recharger un appareil, un bloqueur de données USB peut être branché sur le port de recharge USB avant utilisation afin de se protéger contre une éventuelle attaque de type «juice jacking».

6.2.6 Maîtrise du risque de sécurité et hygiène numérique

Mesures d'atténuation organisationnelles

Évaluation des besoins technologiques

Afin de comprendre les menaces auxquelles une organisation et son personnel peuvent être confrontés, et afin de mettre en œuvre des mesures d'atténuation des risques appropriées, il est important d'identifier les technologies susceptibles d'être utilisées par le personnel dans le cadre de son travail, ainsi que les différents risques liés aux différents types de projets. Pour ce faire, il est nécessaire de comprendre la portée du programme et les activités numériques de toutes les parties prenantes. Cette évaluation des besoins technologiques porterait sur les équipements et les appareils de communication, ainsi que sur les logiciels et les applications.

Les organisations ont généralement moins de contrôle et de visibilité sur les appareils à usage personnel, bien que ceux-ci puissent présenter les mêmes risques. Les organisations peuvent gérer les risques associés aux appareils personnels en formant leur personnel aux bonnes pratiques d'hygiène numérique (quel que soit l'appareil utilisé), en établissant des protocoles régissant l'utilisation des appareils personnels à des fins professionnelles et en limitant l'accès à l'information sensible sur les appareils personnels.

Évaluations des risques

Pour évaluer efficacement les risques, il est préférable d'adopter une approche collaborative et interdisciplinaire. Les équipes informatiques peuvent se concentrer sur l'évaluation des menaces potentielles liées au matériel, aux logiciels et aux systèmes, tandis que les responsables peuvent examiner les logiciels utilisés par leurs équipes afin d'identifier les vulnérabilités. Le personnel chargé de la communication peut effectuer une «analyse du contexte numérique» afin de comprendre comment les différentes parties prenantes sont susceptibles d'utiliser les médias numériques, tandis que le personnel de sécurité peut identifier les failles de sécurité et les relier à des menaces physiques plus larges découlant de l'exposition numérique. Le personnel de programme peut évaluer les

risques d'abus, de ciblage criminel ou de manipulation liés aux aspects numériques de leurs programmes, tels que les transferts d'espèces, le plaidoyer ou la collecte de données. Il est essentiel de reconnaître que, tout comme les menaces physiques, les menaces numériques ne touchent pas tout le monde de la même manière. Toute évaluation des risques devra être inclusive et tenir compte de la manière dont les différents profils d'identité peuvent influencer sur les risques numériques.

Les organisations doivent également garder à l'esprit qu'il existe des recoupements entre la sécurité numérique du personnel, celle de l'organisation et celle des communautés concernées. Une faille dans un domaine aura des répercussions sur les autres, et toute évaluation des risques et toutes les mesures d'atténuation doivent tenir compte de leur interdépendance.⁹⁴

Les travailleurs humanitaires peuvent également subir des dommages collatéraux lors d'une attaque numérique visant un tiers qui détient les données de leur organisation ou dont celle-ci utilise les services. Cet aspect doit également être pris en compte dans toute évaluation des risques. Enfin, les organisations sont tenues de se conformer aux réglementations applicables en matière de protection des données (telles que le règlement général sur la protection des données (RGPD) de l'Union européenne).

► Voir le chapitre 4.1 pour plus d'informations sur les évaluations des risques.

Protocoles de sécurité reproductibles

Les protocoles aident les utilisateurs à se comporter et à effectuer des opérations de manière sécurisée et cohérente. Le fait de veiller à ce que les protocoles soient simples et reproductibles (c'est-à-dire standardisés, bien documentés et faciles à suivre de la même manière à chaque fois) permet de garantir leur respect systématique. Les protocoles peuvent inclure des procédures pour demander et acquérir des appareils, signaler les appareils perdus ou volés, obtenir une connexion Internet et adopter de bonnes pratiques en matière de comportement des utilisateurs.

VPN et sécurité Web

Les Virtual private network (réseaux privés virtuels, VPN) et les outils de sécurité Web protègent les appareils, les données et les communications des utilisateurs finaux lorsqu'ils sont en déplacement et utilisent des réseaux non sécurisés. Un VPN crypte les données lorsqu'elles quittent l'appareil d'un utilisateur afin qu'elles restent protégées et masquées aux acteurs malveillants lorsqu'elles transitent par des réseaux Wi-Fi, des réseaux mobiles et Internet non sécurisés. La sécurité Web se présente généralement sous la forme d'un filtrage du contenu Web et constitue une première ligne de défense essentielle contre les logiciels malveillants, les sites Web malveillants, les attaques de phishing et autres menaces en ligne. Associée à un outil VPN qui crypte le trafic Internet, elle peut offrir une protection et une sécurité importantes aux utilisateurs finaux et à leurs données.

94 Pour en savoir plus, voir Davis, J. et al. (2020) 'Module 4, Digital security' in *Security to go: a risk management toolkit for humanitarian aid agencies* (en anglais, «Module 4, Sécurité numérique dans La sécurité en pratique: boîte à outils de gestion de risque à l'attention des agences humanitaires»), 4^e édition. GISF (<https://gisf.ngo/resource/security-to-go/>).

Il est recommandé d'utiliser des sites Web cryptés SSL qui affichent le symbole du «cadenas» lorsque l'on se connecte à un réseau Wi-Fi non sécurisé. De nombreux sites Web gouvernementaux, en particulier dans les pays où se déroule la majeure partie de l'aide humanitaire, ont déjà été piratés par le passé et ne sont pas configurés pour utiliser le cryptage. La prudence est donc de mise.

La prudence est donc de mise. Les solutions de sécurité d'entreprise offrent des fonctionnalités avancées, complètes et à l'échelle de l'organisation pour protéger les données et les utilisateurs d'une organisation, même sur des réseaux distants ou non sécurisés. Ces outils comprennent le «Zero Trust» (ou principe «Ne jamais faire confiance, toujours vérifier»), le «SSE (secure service edge)», qui est une solution de sécurité fournie dans le cloud et le «SASE (secure access service edge)», qui est une architecture de sécurité basée sur le cloud. Les solutions d'entreprise vont au-delà du cryptage individuel des sites Web en offrant un cadre de sécurité plus large pour protéger l'ensemble de l'écosystème numérique d'une organisation.

Outils de communication basés sur des applications

Lorsque l'on évalue les risques et les avantages des différentes applications et plateformes de communication, trois éléments sont à prendre en compte.

- **Quel est le niveau de sécurité de l'application ?** Les applications open source hébergées dans des pays dotés de lois strictes en matière de protection de la vie privée et de bonnes pratiques de sécurité seront plus sûres que les applications propriétaires hébergées dans des pays où le gouvernement contrôle le réseau et où les lois sur la protection de la vie privée sont ignorées ou non appliquées.
- **À qui appartiennent les données générées par l'application ?** Les données sont-elles stockées uniquement sur l'appareil lui-même ? Les données sont-elles stockées sur les serveurs d'une entreprise privée, d'un organisme gouvernemental ou d'une organisation à but non lucratif ? Il est important de savoir où se trouvent les données et quel chemin elles empruntent afin d'évaluer correctement la sécurité d'une application particulière.
- **Qu'est-ce qui est actuellement disponible ou utilisé dans les pays d'opération ?** Une application hautement sécurisée peut s'avérer être un mauvais choix si elle n'est pas disponible au téléchargement dans un pays donné, si elle ne peut pas être installée sur les appareils utilisés par la majorité du personnel ou si elle est peu familière ou difficile à utiliser.

Gestion des appareils mobiles

Une plateforme de gestion des appareils mobiles (MDM, de l'anglais «mobile device management») suit et protège les appareils mobiles. La MDM permet la gestion à distance centralisée des appareils, y compris la possibilité d'effacer les données sensibles des appareils perdus ou volés. Si cela n'est pas possible, crypter les appareils et utiliser des mots de passe forts et des dossiers privés est une bonne mesure.

Sécurité physique des appareils

La sécurité physique est un aspect important de la protection des personnes, des appareils et des données. Si des acteurs malveillants parviennent à mettre la main sur un appareil, ils sont susceptibles de le compromettre. Le risque de fuite de données est considérablement réduit si les fichiers sont cryptés, si les appareils sont protégés par un mot de passe et s'ils ne sont jamais laissés sans surveillance. Signaler dès que possible la perte ou le vol d'un appareil aux équipes informatiques et de sécurité permet de réagir rapidement afin d'atténuer l'impact potentiel. Il peut arriver que le personnel soit tenu de remettre temporairement ses appareils aux autorités pour inspection. En cas de suspicion de manipulation frauduleuse ou si l'appareil quitte le champ de vision du membre du personnel pendant un certain temps, les services informatiques et de sécurité voudront en être informés.

Bien qu'ils ne soient pas toujours pratiques, les sacs de Faraday peuvent protéger les appareils mobiles contre d'éventuelles attaques pendant les déplacements. Les ondes électromagnétiques, telles que celles utilisées pour le Wi-Fi et les communications mobiles, ne peuvent pas pénétrer le sac, ce qui permet de bloquer les tentatives de connexion indésirables ou la surveillance des appareils mobiles.

Pratiques d'hygiène numérique

L'hygiène numérique désigne les pratiques standard visant à maintenir la sécurité numérique et à atténuer les risques numériques. L'hygiène numérique peut contribuer à maintenir un niveau de sécurité numérique constant en encourageant des comportements et des protocoles appropriés et reproductibles. Vous trouverez ci-dessous quelques suggestions de pratiques d'hygiène numérique saines, qui peuvent être intégrées aux protocoles de sécurité et aux formations en sécurité d'une organisation.⁹⁵

Utiliser des mots de passe forts et l'authentification multifacteur

- **Créer des mots de passe forts.** Le personnel peut créer des mots de passe forts et complexes en utilisant une combinaison de caractères et les mettre à jour régulièrement, en évitant de réutiliser les mêmes mots de passe pour plusieurs comptes. Une bonne pratique consiste à utiliser «trois mots aléatoires» pour créer des mots de passe faciles à mémoriser mais sécurisés.
- **Utiliser l'authentification multifacteur.** L'authentification multifacteur offre un niveau de protection supplémentaire contre le vol ou le piratage des mots de passe.

Installer les mises à jour des appareils et des applications

- **Toujours tout mettre à jour.** Veiller à ce que tous les systèmes d'exploitation et toutes les applications installées soient mis à jour avant tout déplacement. Si possible, utiliser un système de gestion des appareils mobiles pour mettre à jour automatiquement les appareils et les applications.

95 Pour plus de recommandations, voir ACT Alliance (2019) *Basic cyber security. A guide for all to manage digital security* (en anglais, «Cybersécurité de base. Un guide pour tous sur la gestion de la sécurité numérique.») (https://gisf.ngo/wp-content/uploads/2021/10/ACT_Digital_Security_Guidelines_2019.pdf).

Renforcer la protection des appareils

- **Sécuriser les paramètres de l'appareil.** Les appareils ne sont généralement pas livrés dans leur état le plus sécurisé. Les organisations doivent donc établir des normes de renforcement de la protection des appareils dans le cadre de leurs politiques de sécurité. Le personnel peut mettre en œuvre le renforcement de la protection des appareils en configurant des codes d'accès sécurisés, en désactivant les applications et services inutiles, en activant le cryptage des appareils, en activant les modes de verrouillage et en désactivant les communications sans fil lorsqu'elles ne sont pas nécessaires.

Réduire au minimum l'utilisation des applications et des réseaux sociaux

- **Limiter l'utilisation des applications.** Chaque application installée représente une vulnérabilité potentielle. Il est conseillé de réduire au minimum l'utilisation d'applications inutiles, surtout en déplacement, et d'envisager de supprimer celles dont on n'a pas besoin.
- **Utiliser des applications de communication sécurisées.** Les applications de communication cryptées de bout en bout sont préférables, mais une évaluation approfondie peut être menée afin de déterminer l'application la plus sûre à utiliser dans différents contextes.
- **Précautions à prendre sur les réseaux sociaux.** Éviter de publier sur les réseaux sociaux pendant un déplacement, car cela peut entraîner des fuites d'informations. Désactiver les services de localisation et vérifier les paramètres de confidentialité et de partage de toutes les applications.
- **Métadonnées des photos.** Désactiver les paramètres de localisation pour prendre des photos et supprimer les métadonnées des images avant de les partager.

Renforcer la sécurité des e-mails

- **Être prudent avec les e-mails.** Éviter de cliquer sur des liens ou d'ouvrir des pièces jointes provenant de sources inconnues. Vérifier l'adresse e-mail de l'expéditeur, en particulier lorsqu'il s'agit d'une information sensible.

Gérer et crypter les données

- **Crypter les données sensibles.** S'assurer que tous les fichiers sensibles sont cryptés avant de les stocker ou de les partager. Anonymiser les informations d'identification personnelle.
- **Sécuriser le partage de fichiers.** Utiliser des méthodes sécurisées pour partager des fichiers, telles que des services d'e-mails cryptés ou des plateformes sécurisées de partage de fichiers.
- **Sauvegarder les données.** Sauvegarder régulièrement les données importantes sur un support sécurisé et crypté afin d'éviter toute perte.
- **« Nettoyer au fur et à mesure ».** Réfléchir à l'utilisation des données lors de déplacements d'un endroit à un autre : des données telles que des photos, qui peuvent être utilisées et partagées en toute sécurité dans un endroit, peuvent présenter des risques de sécurité si elles sont vues dans un autre endroit. Pour atténuer ces risques, envoyer les photos nécessaires par des moyens électroniques sécurisés, puis les supprimer rapidement de l'appareil.

- **Supprimer les données.** Supprimer les données de manière sécurisée lorsqu'elles ne sont plus nécessaires.
- **Vérifier et contrôler l'accès.** Vérifier régulièrement l'exactitude des données, contrôler l'accès et conserver les pistes de vérification afin de garantir que seul le personnel autorisé puisse accéder aux données critiques. Le personnel doit faire particulièrement attention au type de données qu'il collecte, à la manière dont il les stocke et aux personnes qui y ont accès. Le personnel de sécurité peut collecter et avoir accès à des informations personnelles très sensibles sur le personnel et d'autres acteurs, et doit être conscient du risque que ces informations soient utilisées pour nuire à l'organisation, à son personnel, aux personnes qu'elle tente d'aider ou à ses opérations, même si elles sont partagées avec des acteurs légitimes, tels que des acteurs étatiques.⁹⁶

Utiliser Internet en toute sécurité

- **Utiliser des VPN sur les réseaux Wi-Fi publics.** Toujours utiliser un VPN pour accéder à Internet via un réseau Wi-Fi public.
- **Éviter les sites Web non sécurisés.** Savoir reconnaître et éviter les sites Web qui ne sont pas sécurisés par le protocole HTTPS (un protocole sécurisé conçu pour envoyer des données entre un navigateur Web et un site Web).

Signaler les incidents

- **Suivre les protocoles de signalement établis.** Signaler les incidents de sécurité numérique suspects, tels que les tentatives de phishing ou les violations potentielles de données.

Les organisations devraient envisager de mettre en place des sessions de formation et des séminaires afin d'améliorer les compétences numériques et de couvrir les bonnes pratiques en matière d'hygiène numérique pour le personnel, tant au niveau organisationnel que personnel, y compris sur les réseaux sociaux. Des rappels et des mises à jour réguliers sur les nouvelles menaces numériques sont essentiels pour garantir que les travailleurs humanitaires restent vigilants et bien préparés à se protéger eux-mêmes et leurs collègues dans l'espace numérique.

Informations complémentaires

Recommandations et outils en matière de sécurité numérique

Access Now (2020) *Digital security helpline: Self-doxing guide* (en anglais, « Assistance téléphonique en matière de sécurité numérique : guide pour se dédoxer soi-même ») (<https://gisf.ngo/resource/access-now-digital-security-helpline-self-doxing-guide/>).

ACT Alliance (2019) *Basic cyber security. A guide for all to manage digital security* (en anglais, « Cybersécurité de base. Un guide pour tous sur la gestion de la sécurité numérique. ») (https://gisf.ngo/wp-content/uploads/2021/10/ACT_Digital_Security_Guidelines_2019.pdf).

⁹⁶ À titre d'exemple, le HCR a partagé des informations personnelles concernant des réfugiés Rohingyas avec le gouvernement bangladais, qui les a à son tour transmises aux autorités du Myanmar. Voir Human Rights Watch (2021) *UN shared Rohingya data without informed consent* (en anglais, « L'ONU a partagé des données sur les Rohingyas sans leur consentement éclairé ») (www.hrw.org/news/2021/06/15/un-shared-rohingya-data-without-informed-consent)

Davis, J. et al. (2020) 'Module 4, Digital security' in *Security to go: a risk management toolkit for humanitarian aid agencies* (en anglais, « Module 4, Sécurité numérique dans La sécurité en pratique : boîte à outils de gestion de risque à l'attention des agences humanitaires »), 4e édition. GISF (<https://gisf.ngo/resource/security-to-go/>).

Front Line Defenders (n.d.) Security in-a-box (outils et tactiques de sécurité numérique) (<https://securityinabox.org/fr/>).

GISF (2021) 'Module 2: Information management' in *Keeping up with COVID-19: essential guidance for NGO security risk managers* (en anglais, « Module 2: Gestion de l'information », dans *Se tenir informé sur la COVID-19: conseils essentiels pour les responsables du risque de sécurité des ONG*) (<https://gisfprod.wpengine.com/resource/keeping-up-with-covid-19-essential-guidance-for-ngo-security-risk-managers-module-2-information-management/>).

GISF (n.d.a) Resources & background materials (DCS) (en anglais, « Ressources et documents de référence (DCS) ». *Digital cyber security*. (en anglais « Cybersécurité numérique ») (www.gisf.ngo/themes/digital-cyber-security/resource-background-materials-dcs/).

GISF (n.d.b) 2. *Sécurité numérique*. Guide interfonctionnel sur la sécurité des ONG (<https://gisf.ngo/toolbox-pwa-fr/resource/2-securite-numerique/>).

GISF (n.d.c) *Digital security resources* (en anglais, « Ressources sur la sécurité numérique »). *Communications technology and humanitarian delivery* (en anglais, « Technologies de communication et acheminement de l'aide humanitaire ») (www.gisf.ngo/themes/communications-technology-and-humanitarian-delivery/digital-security-resources/).

Tactical Tech (n.d.) *Holistic security manual* (en anglais, « Manuel de sécurité holistique ») (<https://holistic-security.tacticaltech.org/index.html>).

Recherches et analyses sur la sécurité numérique

Al Achkar, Z. (2021) 'Digital risk: How new technologies impact acceptance and raise new challenges for NGOs' (en anglais, « Risques numériques : comment les nouvelles technologies influencent l'acceptation et posent de nouveaux défis aux ONG ») sur le site du GISF (éd.) *Achieving safe operations through acceptance: challenges and opportunities for security risk management* (en anglais, « Assurer la sécurité des opérations grâce à l'acceptation : défis et opportunités pour la gestion des risques de sécurité ») (<https://gisf.ngo/resource/achieving-safe-operations-through-acceptance/>).

CICR (2022) « Cyberattaque contre le CICR: le point sur ce que nous savons ». 24 juin (www.icrc.org/en/document/cyber-attack-icrc-what-we-know).

GISF (2023a) *The intersection of technology and human security* (en anglais, « L'intersection entre technologie et sécurité humaine »). Podcast. Evolving NGO security risk management (« Évolution de la gestion des risques de sécurité des ONG ») (www.gisf).

ngo/resource/evolving-ngo-security-risk-management-ep4-the-intersection-of-technology-and-human-security-gisf-podcast/).

GISF (2023b) *Humanitarian security in an age of uncertainty: the intersection of digital and physical risks* (en anglais, «La sécurité humanitaire à l'ère de l'incertitude: l'intersection des risques numériques et physiques») (www.gisf.ngo/resource/humanitarian-security-in-an-age-of-uncertainty-the-intersection-of-digital-and-physical-risks/).

Human Rights Watch (2021) 'UN shared Rohingya data without informed consent' (en anglais, «L'ONU a partagé des données sur les Rohingyas sans leur consentement éclairé»), 15 juin (www.hrw.org/news/2021/06/15/un-shared-rohingya-data-without-informed-consent).

Kumar, M. (2017) *Digital security of LGBTQI aid workers: awareness and response* (en anglais, «Sécurité numérique des travailleurs humanitaires LGBTQI: sensibilisation et réponse»). European Interagency Security Forum (<https://gisfprod.wpengine.com/resource/digital-security-of-lgbtqi-aid-workers-awareness-and-response/>).

Rodenhäuser, T., Staehelin, B. et Marelli, M. (2022) 'Safeguarding humanitarian organizations from digital threat' (en anglais, «Sauvegarde des organisations humanitaires contre la menace numérique») *Droit et Politiques humanitaires*, CICR (<https://blogs.icrc.org/law-and-policy/2022/10/13/safeguarding-humanitarian-organizations-from-digital-threats/>).

Viveros Álvarez, J.S. (2024) 'The risks and inefficacies of AI systems in military targeting support' (en anglais, «Les risques et les inefficacités des systèmes d'IA dans le soutien au ciblage militaire») *Droit et Politiques humanitaires*, CICR (<https://blogs.icrc.org/law-and-policy/2024/09/04/the-risks-and-inefficacies-of-ai-systems-in-military-targeting-support/>).

Ressources sur les informations préjudiciables

Blake, J. (2020) *Disinformation and security risk management for NGOs* (en anglais, «Désinformation et gestion des risques de sécurité pour les ONG»). GISF (www.gisf.ngo/blogs/disinformation-and-security-risk-management-for-ngos/).

Center for Civilians in Conflict (CIVIC) (2023) *When words become weapons: the unprecedented risks to civilians from the spread of disinformation in Ukraine* (en anglais et en ukrainien, «Quand les mots deviennent des armes: les risques sans précédent pour les civils liés à la propagation de la désinformation en Ukraine») (<https://civiliansinconflict.org/publications/research/when-words-become-weapons-the-unprecedented-risks-to-civilians-from-the-spread-of-disinformation-in-ukraine/>).

CICR (2021) *Harmful information – misinformation, disinformation and hate speech in armed conflict and other situations of violence: ICRC initial findings and perspectives on adapting protection approaches* (en anglais, «Informations préjudiciables – informations erronées, désinformation et discours de haine dans les conflits armés et autres situations de violence: premières conclusions et perspectives du CICR sur l'adaptation des approches de

protection») (<https://shop.icrc.org/harmful-information-misinformation-disinformation-and-hate-speech-in-armed-conflict-and-other-situations-of-violence-icrc-initial-findings-and-perspectives-on-adapting-protection-approaches-pdf-en.html>).

CICR (2022) *Ukraine: addressing misinformation about ICRC's activities* (non disponible en français, «Ukraine: lutter contre la désinformation concernant les activités du CICR») (<https://www.icrc.org/en/document/ukraine-addressing-misinformation-about-icrcs-activities>).

CICR (2023) *Comment la mésinformation et la désinformation nuisent au travail humanitaire du CICR au Burkina Faso* (www.icrc.org/en/document/burkina-faso-how-misinformation-disinformation-harm-humanitarian-action).

GISF (2023c) *Online risk to real-life harm: disinformation and social listening workshop resources* (en anglais, «Risques en ligne et préjudices dans la vie réelle: ressources pour un atelier sur la désinformation et l'écoute sociale») (www.gisf.ngo/resource/online-risk-to-real-life-harm-disinformation-and-social-listening-workshop-resources/).

Insecurity Insight (2023) 'The role of social media in the spreading of the Turkish Red Crescent Tent Sale Story in Türkiye' (en anglais, «Le rôle des réseaux sociaux dans la diffusion de l'histoire de la vente de tentes du Croissant-Rouge turc en Turquie») *Social Media Monitoring* (en anglais, «Suivi des réseaux sociaux») (<https://insecurityinsight.org/wp-content/uploads/2023/08/The-Spreading-of-the-Turkish-Red-Crescent-Tent-Sale-Story.pdf>).

Insecurity Insight (n.d.) *Social media monitoring* (en anglais, «Suivi des réseaux sociaux») (<https://insecurityinsight.org/projects/aid-in-danger/social-media-monitoring>).

Internews (2015) *Mapping information ecosystems to support resilience* (en anglais, «Cartographier les écosystèmes de l'information pour soutenir la résilience») (https://internews.org/wp-content/uploads/legacy/resources/Internews_Mapping_Information_Ecosystems_2015.pdf).

Tiller, S., Devidal, P. et van Solinge, D. (2023) *The fog of war and information* (en anglais, «Le brouillard de la guerre et de l'information»). Analyse de MSF (<https://analysis.ocb.msf.org/the-fog-of-war-and-information/>).

Wardle, C. (2024) *A conceptual analysis of the overlaps and differences between hate speech, misinformation and disinformation* (en anglais, «Analyse conceptuelle des recoupements et des différences entre discours de haine, informations erronées et désinformation»). Département du Maintien de la paix (ONU) (<https://peacekeeping.un.org/en/new-report-finds-understanding-differences-harmful-information-is-critical-to-combating-it>).

7 Gestion des menaces spécifiques et des situations à risque

7.1 Sécurité des déplacements

Les travailleurs humanitaires sont souvent exposés à des risques accrus lorsqu'ils se déplacent. Il est donc essentiel de mettre en place une gestion de risque lié aux déplacements efficace, non seulement pour maintenir l'accès aux zones critiques, mais aussi pour garantir la sûreté, la sécurité et la confiance de ceux qui se déplacent. La gestion de ces risques est une responsabilité partagée entre l'organisation et son personnel, et nécessite des politiques globales, une formation approfondie et des plans d'urgence solides. En mettant l'accent sur la sûreté et sécurité, les organisations humanitaires peuvent continuer à se rendre dans les environnements les plus difficiles pour mener à bien leur travail. Ce chapitre traite des considérations générales relatives à la sécurité des déplacements et présente les bonnes pratiques à adopter pour différents modes de transport.

7.1.1 Considérations générales

Politique de gestion de risque lié aux déplacements

Une politique de gestion de risque lié aux déplacements bien définie sert de base à toutes les pratiques de sécurité des déplacements, transformant ainsi un chaos potentiel en une préparation structurée.

Une politique complète de gestion de risque lié aux déplacements comprend généralement les éléments suivants :

- **Normes et procédures cohérentes.** Une politique de gestion de risque lié aux déplacements définit des normes et des procédures claires et cohérentes tant pour l'organisation que pour les individus. Elle peut inclure l'identification des risques potentiels, l'établissement de protocoles visant à atténuer ces risques et la définition de procédures de réponse d'urgence. La clarté apportée par ces politiques favorise une approche unifiée de la gestion de risque lié aux déplacements, permettant aux organisations d'identifier et d'atténuer les risques avant qu'ils ne se concrétisent.
- **Gestion centralisée ou décentralisée.** Les organisations doivent examiner attentivement quels aspects de la gestion de risque lié aux déplacements sont mieux traités de manière centralisée et lesquels sont mieux gérés au niveau local. Cette décision peut être fondée sur les ressources disponibles et les risques spécifiques associés à chaque scénario de déplacement. Par exemple, si les données relatives à la sûreté aérienne peuvent être gérées de manière centralisée, le choix des compagnies aériennes et des itinéraires appropriés peut être mieux géré au niveau local par du personnel connaissant les conditions locales.
- **Droits des personnes en déplacement et seuils de risque personnel.** Les droits des personnes en déplacement peuvent être clairement définis dans la politique, notamment en ce qui concerne les seuils de risque personnel. Il est recommandé

d'informer le personnel de son droit de se retirer d'une mission ou d'un déplacement s'il estime que les risques sont trop élevés. Cela permet non seulement de protéger les personnes, mais aussi de garantir que les déplacements sont effectués par des personnes pleinement préparées et confiantes dans leurs capacités à gérer les risques.

► Voir le chapitre 1.1 pour plus d'informations sur les seuils de risque personnel.

- **Briefings de sécurité avant le déplacement.** Les briefings de sécurité préparent les personnes à leur déplacement en leur fournissant des informations essentielles, notamment l'itinéraire et d'autres détails sur le déplacement, les risques spécifiques au contexte et les risques personnels, les réponses appropriées à ces risques, ainsi que des recommandations sur les documents et articles à emporter. Les briefings portent généralement aussi sur les directives organisationnelles, les politiques internes pertinentes, les contacts d'urgence et les informations sur l'assurance voyage et les services d'assistance. Ces briefings peuvent être organisés de différentes manières, notamment sous forme de documents, de vidéos ou de discussions avec les points focaux pour les questions de sécurité, et doivent être adaptées au type de déplacement et au profil de risque personnel de la personne.
- **Formation.** Les exigences de l'organisation en matière de déplacements, y compris les formations obligatoires, doivent être clairement énoncées dans les politiques de déplacement, les contrats des employés et les plans de sécurité. Les organisations doivent veiller à ce que les formations et les briefings ne soient pas réservés exclusivement aux déplacements à l'international, mais soient également accessibles au personnel résident susceptible de se déplacer dans différentes zones d'un même pays.

► Voir le chapitre 5.2 pour plus d'informations sur la formation.

La mise en place d'une politique complète de gestion de risque lié aux déplacements crée un cadre protecteur qui permet au personnel de se déplacer en toute confiance et en toute transparence. Cette politique peut également être utilisée pour traiter les questions d'éthique et d'environnement, promouvoir des pratiques durables et garantir des mises à jour régulières et la prise en compte du feedback des personnes qui se déplacent. Cela permet non seulement d'améliorer la sûreté et l'efficacité des opérations humanitaires, mais aussi de démontrer l'engagement de l'organisation en faveur de la sûreté de son personnel, ce qui renforce la confiance et le moral des employés.

Systèmes d'autorisation de déplacement

Un système d'autorisation de déplacement bien structuré est un élément essentiel de la gestion de risque lié aux déplacements. Les organisations doivent déterminer quelle autorisation est nécessaire pour chaque type de déplacement, ce qui peut dépendre de plusieurs facteurs, notamment les niveaux de risque et la distance à parcourir. Le système idéal est durable et pertinent, tout en apportant une valeur ajoutée et en améliorant la gestion de risque. Un système trop complexe ou trop gourmand en ressources peut devenir contraignant, tandis qu'un système trop simpliste risque de ne pas offrir une protection adéquate.

Un système d'autorisation de déplacement comprend plusieurs éléments clés, notamment les suivants :

- **Processus de demande formalisé.** Le processus d'autorisation de déplacement commence par une demande officielle dans laquelle les personnes soumettent des itinéraires détaillés indiquant leurs destinations, l'objet et la durée du déplacement, ainsi que les activités prévues. Cela permet de s'assurer que toutes les informations pertinentes sont saisies et examinées avant que l'autorisation ne soit accordée.
- **Évaluation des risques.** Chaque demande de déplacement doit faire l'objet d'une évaluation des risques afin d'évaluer les risques potentiels liés au déplacement et à la destination, notamment l'instabilité politique, les menaces pour la santé, les dangers environnementaux et les problèmes de sécurité locale. Cela permet également aux personnes de signaler toute considération personnelle dont il faut tenir compte.
- **Préparation des voyageurs.** Veiller à ce que les personnes soient bien préparées et disposent des outils et ressources nécessaires, tels qu'une assurance voyage, une trousse médicale et des fonds d'urgence.
- **Débriefing après déplacement.** Un système efficace d'autorisation de déplacement comprend généralement un débriefing après déplacement. Il peut être utile que les personnes fassent part de leurs expériences à leur retour, en signalant tout incident ou observation susceptible d'éclairer les évaluations des risques ou les ajustements à faire dans la pratique.

Autres considérations

- **Capacités internes de gestion de risque lié aux déplacements.** Certaines organisations ont investi dans des capacités internes pour gérer les déplacements et atténuer les risques liés aux déplacements, par exemple en affectant du personnel dédié à la réservation des vols. Cela nécessite un budget soutenu et des ressources spécialisées, mais peut s'avérer très efficace pour garantir une gestion proactive et complète des risques liés aux déplacements.
- **Responsabilité partagée.** L'organisation et la personne qui se déplace ont une responsabilité conjointe en matière de sûreté et sécurité du déplacement. L'organisation est chargée de créer et de maintenir un système et un environnement permettant de gérer les déplacements en toute sécurité, ainsi que de mettre en place les moyens nécessaires pour répondre et soutenir les personnes en cas de problème. La personne qui se déplace est tenue d'écouter les briefings et de respecter les consignes et les exigences.
- **Profil de risque personnel.** Le profil de risque personnel d'un employé peut jouer un rôle important dans la gestion des risques liés aux déplacements et doit être pris en compte dans la planification et la préparation. Par exemple, les membres du personnel souffrant de problèmes de santé peuvent avoir besoin d'accéder à des médicaments indispensables.

7.1.2 Modes de transport

Le choix du mode de transport doit être guidé par une analyse complète des risques. Par exemple, même si un vol d'une heure avec une compagnie aérienne dont les antécédents en matière de maintenance sont douteux peut présenter certains risques, il peut néanmoins s'agir d'une option plus sûre qu'un trajet de 10 heures par la route à travers le pays. Les sections suivantes doivent être considérées dans ce contexte.

Transport aérien

Le transport aérien présente plusieurs risques que les organisations doivent être prêtes à gérer. Il s'agit notamment de problèmes liés à la santé, tels que la thrombose veineuse profonde (TVP), ainsi que de risques de sécurité, tels que les détournements d'avion ou les accidents aériens. Les voyageurs peuvent être stressés par les retards, la perte de bagages et les procédures complexes de contrôle de sécurité.

- **Sûreté et choix de la compagnie aérienne.** Toutes les compagnies aériennes ne sont pas égales en termes de navigabilité et de qualité de maintenance. Plusieurs organismes commerciaux évaluent les compagnies aériennes à l'échelle mondiale, et ces informations peuvent être utilisées pour prendre des décisions éclairées. Au minimum, les organisations doivent examiner les procédures et les antécédents des compagnies aériennes en matière de sûreté avant de les utiliser.
- **Utilisation des compagnies aériennes humanitaires.** Le Service aérien d'aide humanitaire des Nations unies (UNHAS) et d'autres compagnies aériennes humanitaires fournissent des services essentiels dans de nombreux environnements difficiles. Les organisations qui souhaitent utiliser les services aériens de l'ONU ou des ONG doivent bien connaître leur mode de fonctionnement, y compris les règles et réglementations locales, qui peuvent différer considérablement de celles des transporteurs nationaux.
- **Briefings et soutien aux personnes en déplacement.** Les personnes en déplacement doivent généralement gérer elles-mêmes bon nombre des risques liés au transport aérien, mais les organisations peuvent néanmoins leur fournir des directives et des briefings complets. Les plans d'urgence traitent des problèmes courants tels que les retards de vol, la perte de bagages ou les changements dans les conditions de sécurité. Les agences commerciales peuvent proposer des services tels que des alertes individuelles et le suivi des bagages.

Liste de contrôle pour la sûreté aérienne et maritime

Assurer la sûreté et l'entretien des avions et des navires peut être crucial pour la réussite d'un voyage. Voici quelques éléments à prendre en compte, en particulier pour les navires affrétés par l'organisation :

- **Historique d'entretien** - vérifier que l'avion ou le navire a fait l'objet d'un entretien régulier et approprié.

- **Pièces de rechange pour les navires** - vérifier la disponibilité des pièces de rechange essentielles, notamment un deuxième moteur et une batterie de rechange, en cas de panne mécanique en mer.
- **Systèmes de navigation et de communication** - évaluer la fonctionnalité des systèmes de navigation et de communication afin de garantir un fonctionnement fiable pendant le trajet.
- **Équipement de sûreté** - vérifier l'équipement de sûreté, tel que les gilets de sauvetage, les dispositifs de signalisation de détresse, les torches, les extincteurs en état de marche, les masques à oxygène d'urgence, les rames de rechange pour les canots de sauvetage.
- **Carburant** - vérifier que la quantité de carburant est suffisante, notamment la réserve au-delà des besoins prévus pour le voyage, afin de tenir compte des retards ou des détours imprévus.
- **Poids de la cargaison** - confirmer que le poids de la cargaison se situe dans les limites de sûreté du navire et qu'il est correctement réparti pour assurer l'équilibre.

Déplacements routiers

Les déplacements routiers restent le moyen de transport le plus courant pour les organisations humanitaires, mais c'est aussi l'un des plus dangereux. Les risques liés aux déplacements routiers sont nombreux et variés, allant des accidents de la route et des barrages routiers aux embuscades armées et au mauvais état des infrastructures routières. Les déplacements routiers peuvent impliquer de longs trajets sur des terrains difficiles, dans des conditions météorologiques imprévisibles et dans des régions où l'insécurité est élevée. La gestion de ces risques nécessite une planification minutieuse, des systèmes solides et une attention particulière à la sûreté et sécurité du personnel et des ressources. Les considérations suivantes peuvent s'avérer cruciales:

- **Flottes de véhicules et maintenance.** Les flottes de véhicules des organisations humanitaires sont généralement variées et comprennent des SUV, des berlines, des camions et des motos d'âges et de kilométrages divers. L'état et le contrôle technique de ces véhicules sont primordiaux. Des contrôles d'entretien réguliers, notamment des inspections des pneus, des freins et des équipements de sûreté, doivent être obligatoires. Les organisations doivent également s'assurer que les véhicules sont équipés d'éléments essentiels tels que des roues de secours, des crics, des trousseaux de premiers secours et des appareils de communication.
- **Visibilité.** Il peut être nécessaire de réfléchir au degré de visibilité souhaité par l'organisation lors de ses déplacements, conformément à sa stratégie de sécurité dans le contexte donné. Les organisations qui souhaitent être visibles en tant qu'acteurs humanitaires devront s'assurer que tous leurs véhicules sont clairement identifiables grâce à des couleurs et des logos (cela peut également s'appliquer à d'autres types de transport, tels que les bateaux).

- **Compétences au volant et formation des conducteurs.** Les compétences, le moral et l'adhésion aux valeurs de l'organisation des conducteurs peuvent être essentiels pour garantir la sécurité des trajets. Les conducteurs doivent connaître les normes et pratiques locales en matière de conduite, qui peuvent varier considérablement d'un pays à l'autre. Il est conseillé de former les conducteurs et d'évaluer régulièrement leurs performances. Dans les zones de conflit ou de criminalité, il peut être nécessaire de former les conducteurs à la sécurité et à la conduite défensive, notamment à la conscience situationnelle, à l'évaluation des risques et aux manœuvres d'évitement.
 - **Systèmes de contrôle des déplacements.** De nombreuses organisations utilisent des registres/feuilles de présence pour gérer le personnel et les ressources lors des déplacements routiers. Les systèmes de contrôle des déplacements (MovCon) permettent de suivre les personnes en déplacement et de gérer les ressources, avec des déclencheurs d'alerte et des plans d'urgence en cas de retard ou de disparition du personnel. Ces systèmes doivent être adaptés au contexte et mis à jour en permanence.
 - **Suivi numérique et enregistrement des déplacements.** Les dispositifs numériques de suivi et d'enregistrement des déplacements installés dans les véhicules offrent des fonctionnalités de sûreté améliorées et des mesures détaillées des trajets, notamment le suivi en direct des véhicules. Cependant, il est essentiel que ces systèmes soient soumis à une surveillance et à des protocoles appropriés. Ils doivent être intégrés dans la stratégie globale de gestion de risque lié aux déplacements et s'appuyer sur une capacité de réponse solide en cas d'urgence.
 - **Protocoles et briefings relatifs aux déplacements routiers.** Les organisations doivent établir des protocoles clairs pour les déplacements routiers, notamment des directives sur les limitations de vitesse, les pratiques de conduite sûres et les procédures d'urgence. Les briefings préalables au départ destinés aux personnes qui se déplacent couvrent les risques spécifiques associés au trajet, les conditions routières, la situation en matière de sécurité dans la zone ainsi que les normes et attentes culturelles locales.
 - **Plan d'urgence pour les déplacements routiers.** Compte tenu de la nature imprévisible des déplacements routiers, il est essentiel de prévoir un plan d'urgence. Les organisations doivent disposer de protocoles clairs pour répondre à des incidents tels que les pannes de véhicules, les barrages routiers et les embuscades, les itinéraires alternatifs, les contacts d'urgence et les procédures de relocalisation/évacuation du personnel. Dans les zones à haut risque, les organisations peuvent également envisager de recourir à des convois ou à des escortes de sécurité.
- Voir le chapitre 4.2 pour plus d'informations sur les escortes armées.
- **Coordination avec les autorités et les communautés locales.** La police locale, l'armée et les dirigeants communautaires peuvent être une source d'informations précises et actualisées sur l'état des routes, les menaces pour la sécurité et d'autres facteurs pertinents. D'autres organisations humanitaires, notamment les agences de l'ONU, peuvent également fournir ce type d'informations. Les communautés locales peuvent apporter une aide précieuse pendant le déplacement, par exemple en surveillant l'état des routes et en apportant leur aide en cas d'accident.

- **Considérations environnementales.** Les organisations doivent être conscientes de l'impact environnemental de leurs activités. Cela implique notamment de réduire au minimum l'utilisation de véhicules, de diminuer les émissions et de veiller à ce que les déchets soient éliminés de manière appropriée. Il peut être judicieux de réaliser des études d'impact environnemental avant d'entreprendre des opérations de transport routier à grande échelle ou d'envisager l'achat ou la mise au rebut de véhicules.

Transports publics

Pour le personnel qui ne réside pas dans la zone, la décision d'utiliser les transports publics, tels que les bus ou les taxis, doit être fondée sur une évaluation des risques approfondie. Dans certaines circonstances, notamment dans des contextes à très haut risque ou lorsque le profil personnel de certains membres du personnel les expose à un risque accru, cette considération peut également s'appliquer au personnel résident. Pour les destinations à faible risque, les personnes en déplacement peuvent être informées des options de transport sûres, notamment sur la manière d'identifier les prestataires de services agréés et réputés. Dans les zones à haut risque, il peut être préférable d'éviter complètement les transports publics. Les organisations doivent disposer de politiques claires concernant les trajets domicile-travail de leur personnel, notamment sur la question de savoir si l'organisation organisera ou prendra en charge le transport, plutôt que de simplement déconseiller l'utilisation des transports publics sans proposer d'alternatives.

Points de contrôle

Les interactions aux points de contrôle peuvent aller de favorables à hostiles. Les personnes en déplacement peuvent être harcelées, intimidées ou menacées par les individus qui contrôlent les points de contrôle, en particulier si ces derniers se laissent facilement provoquer ou sont sous l'influence de l'alcool ou de stupéfiants. Les points de contrôle peuvent être accueillants et fournir des informations précieuses sur l'état des routes. La manière dont le personnel interagit avec les personnes aux points de contrôle peut influencer non seulement leur propre trajet, mais aussi la manière dont les autres travailleurs humanitaires seront traités par la suite.

Il est essentiel que le personnel évalue rapidement le type et l'emplacement de chaque point de contrôle, ainsi que l'état d'esprit des personnes qui les gèrent et y travaillent. Les points de contrôle sont généralement situés aux carrefours, sur les ponts, aux cols de montagne et aux entrées ou sorties des villes. Les objectifs des points de contrôle varient et peuvent inclure le contrôle de la circulation et la sécurité.

Dans le cas d'un seul véhicule, le chef de groupe peut faire office de porte-parole s'il parle la langue locale. Dans le cas d'un convoi, un chef peut être désigné pour chaque véhicule, idéalement la personne la plus expérimentée qui maîtrise la langue locale. Les conducteurs jouent souvent un rôle clé dans les premières interactions, car ils sont généralement les premiers à entrer en contact avec les gardes aux points de contrôle. Tous les membres de l'équipe doivent connaître le contenu du chargement et être cohérents dans leurs explications concernant la mission de leur organisation et l'objet de leur déplacement. Il peut être judicieux que les passagers aient sur eux une pièce d'identité rédigée dans la langue locale et éviter, si possible, de remettre les passeports. S'il est demandé au personnel d'entrer dans un poste de garde, la règle est de rester ensemble et de ne pas laisser le véhicule sans surveillance.

- Voir le chapitre 7.4 pour plus d'informations sur la manière de traiter le harcèlement à l'encontre du personnel.

Sûreté routière

Les organisations peuvent prendre en compte les éléments suivants dans le cadre de leurs politiques relatives aux déplacements routiers.

- Interdiction des armes (conformément à la politique de l'organisation et aux principes humanitaires)
 - La plupart des organisations humanitaires n'autorisent pas les armes à bord des véhicules ou autres moyens de transport, sauf dans les situations impliquant la coercition. Le personnel responsable doit veiller à ce que cette politique soit claire et visible (par exemple, autocollants avec des symboles représentant des armes à feu barrées).

- Engagement avec des acteurs armés
 - Évaluer et définir la position de l'organisation concernant le recours à des escortes armées et à d'autres acteurs armés ou la collaboration avec ceux-ci. Cela peut avoir des implications sur les politiques interdisant les armes à bord des véhicules de l'organisation (en particulier pour les avions et les bateaux, où toute protection armée ne peut se trouver dans un navire séparé).
- Transport de passagers ou de marchandises non affiliés
 - Élaborer une politique pour le transport de passagers ou de marchandises non affiliés.
 - Fournir des documents plastifiés dans les langues locales afin de communiquer cette politique.
 - Autoriser des exceptions pour des raisons pratiques (par exemple, guides, hospitalité, urgences médicales).
 - Anticiper les exigences culturelles (par exemple, les femmes voyageant avec des proches masculins dans certains contextes).
- Exonération de responsabilité
 - Placer dans les véhicules un document d'exonération de responsabilité exemptant l'organisation de toute responsabilité en cas d'incidents imprévus.
 - Reconnaître l'efficacité variable de ces documents en fonction des lois et des circonstances locales.
 - Tenir compte des aspects pratiques et des problèmes d'acceptation potentiels liés à la mise en œuvre de cette politique.

Déplacements par voie navigable

Bien que souvent nécessaires dans des contextes humanitaires, comme lors d'inondations ou pendant la saison des pluies, les déplacements par voie navigable peuvent comporter de nombreux risques. La gestion de ces risques nécessite une planification minutieuse.

- **Choix de l'embarcation.** Les organisations doivent utiliser des embarcations adaptées aux conditions spécifiques qu'elles rencontreront, qu'il s'agisse de rivières, de lacs ou d'eaux côtières. L'état de l'embarcation, y compris son historique d'entretien et son équipement de sûreté, doit être soigneusement inspecté avant toute utilisation. Avant chaque déplacement, vérifier que le niveau de carburant est suffisant et qu'il y a une réserve.

- **Compétences et formation de l'équipage.** Les compétences de l'équipage sont aussi importantes que l'état de l'embarcation. Vérifier que les membres d'équipage possèdent les permis, certificats et expérience nécessaires pour exploiter l'embarcation en toute sécurité. Cela comprend la formation aux procédures d'urgence, à la navigation et à la communication (voir l'encadré ci-dessous).
 - **Équipement de sûreté.** Les embarcations doivent être pourvues d'équipements de sûreté essentiels, notamment de gilets de sauvetage, de dispositifs de signalisation de détresse, d'extincteurs et de rames de rechange.
 - **Risque de piraterie.** Des précautions supplémentaires peuvent être nécessaires dans les régions connues pour des actes de piraterie. Il s'agit notamment de choisir des embarcations dotées de dispositifs de sécurité avancés, tels que des systèmes de surveillance et des équipements de communication sécurisés. Dans certains cas, une protection armée peut s'avérer nécessaire pour protéger l'embarcation et ses occupants.
- Voir le chapitre 4.2 pour plus d'informations sur le recours à la protection armée.
- **Plan d'urgence.** Des protocoles clairs peuvent être mis en place pour répondre aux situations d'urgence, telles que les pannes mécaniques, les conditions météorologiques extrêmes et les attaques de pirates. Ces protocoles peuvent inclure des itinéraires alternatifs, des contacts d'urgence et des procédures d'évacuation du personnel.
 - **Considérations environnementales.** Les déplacements par voie navigable peuvent avoir lieu dans des écosystèmes sensibles et les organisations peuvent être amenées à tenir compte de leur impact sur l'environnement. Il s'agit notamment de réduire au minimum la pollution, d'éviter de perturber la faune locale et de veiller à ce que les déchets soient éliminés de manière appropriée.
 - **Coordination avec les autorités locales.** Les garde-côtes, les autorités portuaires et les responsables locaux peuvent fournir des informations sur les conditions maritimes, les menaces pour la sécurité et d'autres facteurs pertinents.

Liste de contrôle des qualifications et compétences de l'équipage

Lorsque les organisations affrètent des avions ou des embarcations, il est important de tenir compte des qualifications de l'équipage.

- **Permis et certificats**
 - S'assurer que le pilote/capitaine et l'équipage possèdent les permis et certificats valides pour leurs fonctions et le type d'embarcation utilisé.
- **Compétences mécaniques et préparation aux situations d'urgence**
 - Évaluer les compétences mécaniques de l'équipage et sa préparation à gérer des situations imprévues.
- **Maîtrise de la langue**
 - S'assurer que l'équipage maîtrise les langues indispensables à la communication pendant le déplacement et en cas d'urgence.

Déplacements atypiques

Dans les régions difficiles d'accès et reculées, les moyens de transport conventionnels peuvent s'avérer peu pratiques, voire impossibles à utiliser, et le personnel peut être amené à se déplacer à pied ou à dos d'animal. Les considérations suivantes sont importantes pour gérer efficacement les risques associés.

- **Cartographie des itinéraires et évaluation des risques.** Les itinéraires doivent être minutieusement cartographiés afin d'éviter les zones dangereuses. Cela peut impliquer d'évaluer le terrain, d'identifier les menaces potentielles et de prévoir des points de repos et des sources d'eau. Le personnel peut avoir besoin d'une formation spéciale pour faire face à des menaces potentielles, telles que des rencontres avec des animaux sauvages ou des groupes hostiles.
- **Préparation de la personne.** Les personnes qui se déplacent doivent être préparées aux défis physiques et mentaux que peut présenter ce moyen de déplacement. Elles doivent notamment s'assurer d'avoir l'équipement et les provisions adaptés au terrain et au climat, et être formées aux techniques de survie, aux premiers secours et aux communications d'urgence.
- **Protocoles de communication.** Les personnes en déplacement doivent être équipées d'appareils de communication fiables, tels que des téléphones satellites ou des radios bidirectionnelles. Des contacts réguliers doivent être établis avec le bureau compétent de l'organisation. Dans les zones où les infrastructures de communication

sont limitées ou inexistantes, les organisations peuvent être amenées à mettre en place d'autres méthodes pour suivre et assister les personnes en déplacement, par exemple en faisant appel à des guides locaux.

► Voir le chapitre 6.1 pour plus d'informations sur les communications.

- **Coordination avec les communautés locales.** Les communautés locales peuvent partager des informations et des ressources pour s'orienter en terrain difficile et écarter toute menace pour la sécurité, mais aussi apporter leur aide en cas d'urgence.
- **Plan d'urgence.** Des protocoles clairs doivent être mis en place pour répondre aux situations d'urgence, telles que les blessures, les pannes d'équipement et les rencontres avec des groupes hostiles. Les protocoles peuvent couvrir les itinéraires alternatifs, les contacts d'urgence et les procédures d'évacuation du personnel.

► Voir le chapitre 5.5 pour plus d'informations sur les urgences médicales.

Convois

Un convoi est un groupe de véhicules voyageant ensemble, principalement à des fins de protection, de soutien ou d'efficacité. En contextes humanitaires, les convois sont utilisés pour transporter des marchandises, du personnel ou du matériel à travers des zones présentant des risques de sécurité ou des défis logistiques. Ils peuvent être composés de véhicules appartenant à une seule organisation ou être organisés avec d'autres acteurs.

Dans les zones à faible risque, la taille d'un convoi peut être moins importante tant qu'il existe une communication fiable entre tous les véhicules (par exemple, à l'aide de radios ou de talkies-walkies). Toutefois, dans les environnements complexes ou à haut risque, la taille et la structure d'un convoi doivent être soigneusement étudiées. Si voyager en convoi peut réduire les risques grâce à la force du nombre, cela peut également présenter des dangers, comme celui d'être pris pour une colonne militaire, et attirer une attention indésirable. En règle générale, un convoi comprend un véhicule de tête, un corps principal où sont placés les biens de valeur et un véhicule de queue. Dans certaines situations, un véhicule de reconnaissance ou véhicule-cible peut être utilisé, maintenant une distance de sécurité et un contact radio avec le reste du convoi derrière lui. Le chef du convoi se trouve généralement dans le véhicule de tête, tandis qu'une autre personne expérimentée se trouve dans le véhicule de queue.

Avant le départ, le chef du convoi doit s'assurer que tous les véhicules ont été contrôlés quant à leur état, leur niveau de carburant, leur équipement et la présence des documents nécessaires. Il est conseillé aux conducteurs et aux chefs de convoi d'être pleinement informés des règles applicables au convoi, notamment en matière de vitesse, de distance à respecter, de protocoles de communication et de procédures à suivre dans divers scénarios, tels que les points de contrôle ou les pannes de véhicules. La distance entre les véhicules est cruciale ; ils doivent généralement être suffisamment proches pour maintenir un contact visuel, mais suffisamment éloignés pour éviter d'être pris dans le

même incident. La distance appropriée peut varier en fonction du terrain, des conditions météorologiques et de sécurité, et peut devoir être ajustée au cours du trajet.

7.1.3 Considérations relatives à la sécurité personnelle pendant le transport

Les aéroports, les ports et les gares routières et ferroviaires peuvent présenter des risques de sécurité importants. Ces lieux sont souvent la cible d'activités criminelles, et les voyageurs peuvent être vulnérables en raison de leur méconnaissance de l'environnement local et des conditions de sécurité. Les organisations peuvent prendre des mesures proactives pour réduire ces risques.

Les briefings avant départ doivent porter sur la situation en matière de sécurité de la destination, les exigences légales et administratives pertinentes (telles que les obligations vaccinales), les risques potentiels liés aux aéroports, ports, gares routières et ferroviaires, et inclure les coordonnées du personnel de sécurité local. De plus, les briefings peuvent porter sur les points suivants :

- **Options de transport sûres.** Des recommandations peuvent être données sur les options de transport depuis les aéroports, les ports et les gares routières et ferroviaires jusqu'à la destination finale. Cela peut inclure la fourniture de listes de services ou de stations de taxi légitimes, d'applications de transport réputées et l'organisation d'une prise en charge par une personne désignée. Il est recommandé d'utiliser les véhicules de l'organisation, car les chauffeurs connaissent souvent bien les conditions locales et peuvent fournir un moyen de transport sûr et fiable.
- **Mesures de sécurité personnelle.** Les personnes en déplacement peuvent recevoir des conseils sur les mesures de sécurité personnelle à adopter pendant leur transport, comme garder leurs objets de valeur hors de vue, rester vigilantes à leur environnement et éviter toute interaction avec des inconnus. Les organisations peuvent également mettre à la disposition des personnes en déplacement des dispositifs de sécurité personnelle, tels que des sifflets d'alarme ou des dispositifs de localisation. Il peut être nécessaire d'informer les personnes en déplacement sur la manière de transporter leurs bagages de manière sécurisée, notamment en les gardant à portée de vue à tout moment, en utilisant des cadenas et en évitant de transporter de grosses sommes d'argent ou des objets de valeur. Il peut être judicieux d'étiqueter les bagages sans indiquer de détails personnels qui pourraient être utilisés par des criminels.
- **Passer les contrôles de sécurité.** Les personnes en déplacement peuvent avoir besoin de recommandations pour passer les contrôles de sécurité dans les aéroports et les gares. Il peut s'agir de comprendre les restrictions relatives aux bagages à main, de savoir quels documents sont requis et à quel moment, et d'être au courant des mesures de sécurité spécifiques. Les personnes en déplacement doivent également être informées des risques liés à la cybersécurité lors des contrôles de sécurité dans les aéroports, ainsi que des précautions à prendre pour protéger l'information sensible.

- **Traiter avec les autorités.** Dans certains cas, les personnes en déplacement peuvent être interrogées ou faire l'objet d'autres types d'interactions potentiellement difficiles avec les autorités. Les organisations pourront faire des recommandations sur la manière de gérer ces situations, notamment en se montrant coopératif et patient, en étant honnête et en sachant quand demander une aide juridique ou consulaire. Les personnes en déplacement doivent connaître leurs droits et les lois locales régissant leur séjour.

Liste de contrôle générale de sûreté et sécurité opérationnelles en déplacement

Lors de la planification des déplacements du personnel, en particulier dans des environnements complexes, les considérations générales suivantes doivent être prises en compte :

- Conditions météorologiques
- Conditions de sécurité dans différents lieux
- Autorisation des autorités
- Plans d'urgence
- Identification (personnes et véhicules)
- Assurance raisonnable que le mode de transport, tel qu'une embarcation, n'est pas également utilisé pour mener des activités illicites, telles que la contrebande

7.1.4 Hôtels et logements temporaires

Les personnes en déplacement peuvent avoir besoin de passer la nuit dans des hôtels ou des logements temporaires. Lorsqu'il n'a pas été possible de planifier à l'avance, le personnel doit savoir comment évaluer la sécurité du logement et demander des changements si nécessaire.

- **Infrastructure de sécurité des hôtels.** Les hôtels qui prennent les mesures suivantes sont généralement mieux équipés pour répondre aux situations d'urgence et assurer la sécurité de leurs clients : personnel de sécurité, réception ouverte 24h/24, systèmes de contrôle d'accès complets et systèmes de sécurité incendie visibles et opérationnels.
- **Choix de la chambre.** Les personnes en déplacement doivent choisir des chambres situées dans des couloirs très fréquentés et offrant une bonne visibilité. Il convient d'éviter les chambres facilement accessibles aux intrus ou situées dans des zones isolées. Les points d'accès, y compris les portes et les fenêtres, doivent être vérifiés pour s'assurer qu'ils sont en bon état de fonctionnement et qu'ils peuvent être verrouillés en toute sécurité.

Les considérations à prendre en compte pendant un séjour sont les suivantes :

- **Préparation aux situations d'urgence.** Les personnes en déplacement doivent se familiariser avec les procédures d'urgence de leur logement, repérer les issues les plus proches et s'assurer qu'elles ont accès à une trousse d'urgence de base (comprenant une lampe torche, des fournitures de premiers secours et les numéros d'urgence). Elles doivent également connaître l'emplacement des extincteurs et des autres équipements de sûreté.
- **Interactions avec les visiteurs.** Les personnes en déplacement doivent faire preuve de prudence lorsqu'elles interagissent avec les visiteurs dans leur logement. Elles peuvent notamment refuser l'accès à des personnes dont l'identité ou les intentions ne sont pas claires, telles que de nouvelles connaissances, du personnel de services et de livraison non sollicités. Si un visiteur semble suspect, le personnel de sécurité (tel que la sécurité de l'hôtel) doit être immédiatement averti.
- **Signaler tout problème.** Tout problème concernant la sécurité des chambres d'hôtel ou le comportement du personnel de l'hôtel ou d'autres clients doit être signalé sans délai à la direction de l'hôtel. Les organisations peuvent indiquer aux personnes en déplacement comment signaler ces problèmes si nécessaire, notamment en contactant les autorités locales et le personnel de sécurité de l'organisation.
- **Considérations culturelles.** Les personnes en déplacements doivent être attentives aux normes et aux attentes culturelles locales lorsqu'elles séjournent dans des hôtels ou dans des logements temporaires. Cela peut inclure le respect des coutumes locales en matière d'habillement, de comportement et d'interactions avec le personnel de l'hôtel.

► Voir le chapitre 7.2 pour plus d'informations sur la sécurité du site.

7.1.5 Plan d'urgence et gestion d'incident

Il est essentiel de mettre en place un plan d'urgence et une gestion d'incident solides. Pour cela, il est important d'élaborer, de réviser et de mettre à jour régulièrement des plans complets pouvant être rapidement mis en œuvre en cas de réponse d'urgence. Cela implique généralement d'identifier les risques potentiels liés aux déplacements (en accordant une attention particulière aux profils de risque personnels), d'élaborer des stratégies pour atténuer ces risques et d'établir des protocoles de réponse aux incidents. Des formations et des exercices réguliers peuvent contribuer à la préparation.

► Voir le chapitre 4.3 pour plus d'informations sur le plan d'urgence.

- Voir le chapitre 4.4 pour plus d'informations sur la réponse aux incidents.
- Voir le chapitre 5.4 pour plus d'informations sur le bien-être du personnel.
- Voir le chapitre 5.5 pour plus d'informations sur les considérations médicales.

Informations complémentaires

Recommandations et ressources

Bickley, S. (2017) *Gestion du risque sécurité: manuel de référence à l'attention des petites ONG*. European Interagency Security Forum (www.gisf.ngo/resource/security-risk-management-a-basic-guide-for-smaller-ngos/).

Comité permanent interorganisations (IASC) (2013) *IASC non-binding guidelines on the use of armed escorts for humanitarian convoys* (en anglais, «Directives non contraignantes du IASC relatives à l'utilisation d'escortes armées pour les convois humanitaires») (<https://reliefweb.int/report/world/iasc-non-binding-guidelines-use-armed-escorts-humanitarian-convoys>).

Davis, J. et al. (2020) 'Module 10, Travel safety: airports, vehicles and other means of transport' in *Security to go: a risk management toolkit for humanitarian aid agencies* (en anglais, «Module 10, Sûreté lors des déplacements: aéroports, véhicules et autres moyens de transport dans La sécurité en pratique: boîte à outils de gestion de risque à l'attention des agences humanitaires»), 4e édition. GISF (<https://gisf.ngo/resource/security-to-go/>).

GISF (2024) 3. *Voyages et déplacements*. Guide interfonctionnel pour la sécurité des ONG (<https://gisf.ngo/toolbox-pwa-fr/resource/3-voyages-et-deplacements/>).

Organisation internationale de normalisation (2021) *ISO 31030:2021: Gestion de risque lié aux déplacements - Conseils aux organisations* (www.iso.org/standard/54204.html).

7.2 Sécurité du site

La sécurité du site peut dissuader ou empêcher les intrusions, retarder les attaques et atténuer les effets d'un incident dans les environs immédiats d'un site.⁹⁷ Ce chapitre porte principalement sur les bureaux et les résidences destinés au personnel vivant loin de chez lui. Il est toutefois également nécessaire de prendre en considération la sécurité du site où le personnel passe beaucoup de temps, tels que les sites de projet, les camps de réfugiés, les bâtiments scolaires, les établissements médicaux et les points de distribution. Des mesures de sécurité du site peuvent parfois également s'avérer nécessaires autour des domiciles privés du personnel.

7.2.1 Choix du site

La protection du site commence par l'identification et la sélection d'un emplacement approprié, en gardant à l'esprit que le choix idéal existe rarement. En plus de l'espace, du prix et d'autres critères, les forces et les faiblesses physiques d'un site peuvent être évaluées du point de vue de la sécurité: ce qui est acceptable, ce qui doit être amélioré et combien cela coûterait. Cela permet à une organisation d'évaluer la pertinence d'un site, de détailler et de négocier les autorisations nécessaires pour apporter des modifications avant de signer un bail.

Approches de sécurité

Dans toute évaluation de la sécurité physique, qu'il s'agisse de choisir un site ou d'ajouter de nouvelles mesures de sécurité physique, il est important de tenir compte des perceptions et des attitudes de la communauté locale à l'égard de ces mesures. Par exemple, la construction d'un mur de 2,5 mètres peut être conseillée du point de vue de la protection, mais peut éveiller les soupçons ou perturber l'espace local. Cette «optique d'acceptation» peut s'appliquer à tous les exemples de bonnes pratiques présentés dans ce chapitre.

Considérations relatives au profil individuel

Lors du choix des bureaux et des logements, il est important de tenir compte des profils et des besoins personnels du personnel et des visiteurs potentiels. Cela peut contribuer à créer un environnement de travail sûr, inclusif et favorable.

Dans certains contextes, il peut être culturellement inapproprié ou potentiellement dangereux pour les femmes de vivre seules. Dans de tels cas, des solutions de logement partagé conformes aux normes sociales et répondant aux besoins des collègues féminines peuvent être appropriées. Il peut être conseillé de prévoir des logements séparés pour le personnel masculin et féminin, en fonction du contexte culturel et social. Les exigences en matière d'accessibilité pour le personnel en situation de handicap constituent également un élément important à prendre en considération. Offrir des

97 Les risques changent radicalement en cas d'insurrection ou de guerre, où des mesures supplémentaires sont requises. Ces questions sont examinées plus en détail au chapitre 7.10.

options de logement privé ou partagé qui respectent l'identité de genre et l'orientation sexuelle peut contribuer à atténuer les risques et à garantir un environnement accueillant.

Consulter divers groupes de personnel lors du choix des sites peut aider à garantir que leurs besoins sont correctement pris en compte.

► Voir le chapitre 1.2 pour plus d'informations sur les considérations relatives à la sécurité inclusive.

Critères physiques

Les organisations peuvent tenir compte de divers critères physiques lors du choix d'un site. Ceux-ci peuvent inclure les éléments suivants :

- **Résilience structurelle.** Il est conseillé aux organisations de s'assurer que les bâtiments sont suffisamment solides et résistants pour supporter les effets des conditions météorologiques extrêmes et autres risques environnementaux, notamment les inondations et les glissements de terrain. Cela peut impliquer de vérifier l'intégrité structurelle du bâtiment, la qualité des matériaux et l'efficacité des systèmes de drainage dans la zone.
- **Lieu.** Les organisations ont tout intérêt à éviter les zones qui offrent des possibilités de dissimulation et de fuite, par exemple celles où la végétation est dense ou les ruelles étroites et mal éclairées. Les zones comportant de nombreux bâtiments inoccupés, endommagés ou abandonnés peuvent également présenter des risques. Dans les situations de conflit armé actif, les critères de sélection des sites tiendront souvent compte de la distance par rapport aux cibles militaires potentielles et de l'accès à des abris. Si les considérations de sécurité peuvent conduire à choisir des quartiers aisés, des enclaves diplomatiques ou des communautés fermées, ces choix peuvent donner une image élitiste, susceptible d'affecter la perception de l'organisation.
- **Périmètre de sécurité.** Un double périmètre, où un immeuble ou un appartement est situé à l'intérieur d'un complexe ou d'une zone fermée plus vaste, est généralement préférable. Un périmètre géré efficacement peut dissuader les accès non autorisés et fournir une alerte précoce en cas d'intrusion.
- **Évacuation d'urgence.** Dans quelle mesure le personnel et les visiteurs peuvent-ils évacuer facilement le bâtiment ou ses environs immédiats en cas d'urgence, par exemple en cas d'incendie ? Tenir compte des issues de secours, vérifier si la conception du bâtiment facilite l'évacuation rapide et en toute sécurité de tous les occupants et si les pompiers locaux peuvent accéder efficacement au site.
- **Étage.** Il est souvent conseillé de louer un espace de bureau ou un appartement au-dessus du rez-de-chaussée afin de réduire la vulnérabilité face aux intrus. Cependant, les étages supérieurs peuvent être inaccessibles aux équipements d'urgence et difficiles à évacuer. Si le toit est accessible, par exemple depuis un bâtiment voisin,

occuper l'appartement situé juste en dessous peut augmenter les risques.

- **Accessibilité.** Veiller à ce que les entrées, les sorties et les espaces communs soient accessibles aux personnes à mobilité réduite et à ce que les procédures d'urgence tiennent compte de leurs besoins. Il est conseillé de vérifier si le bâtiment est équipé de rampes, d'ascenseurs et de toilettes accessibles.
- **Parking sécurisé.** Il peut être prudent de vérifier que le site dispose d'un parking sécurisé : l'aire de stationnement est bien éclairée, surveillée par des caméras de sécurité et protégée par des points d'accès contrôlés, tels que des portails ou des barrières. Un parking sécurisé est un aspect important de la sécurité globale des locaux, en particulier pendant les heures creuses. Les places de stationnement peuvent également présenter des risques dans les zones de conflit actif, qui sont abordés plus en détail ci-dessous.

► *Voir le chapitre 7.10 pour d'autres considérations relatives aux sites situés dans des zones de combat actif.*

Propriété, occupation et location de bâtiments

- **Propriété du bâtiment.** Les organisations doivent vérifier à qui appartient le bâtiment, par exemple s'il s'agit d'un particulier, d'une banque, d'un magasin ou d'une organisation religieuse. Comprendre l'identité du propriétaire et son rôle potentiel au sein de la communauté peut donner un aperçu de la manière dont ses affiliations pourraient avoir un impact sur l'image et les activités de l'organisation.
- **Occupation et location.** Lorsque l'on évalue un immeuble, il est conseillé de tenir compte des autres occupants ou locataires des locaux. La présence d'autres locataires peut contribuer à une meilleure vigilance et offrir une certaine protection collective. Cependant, les autres locataires peuvent également présenter des risques, en particulier s'ils sont ou pourraient devenir eux-mêmes des cibles. Un site dédié à un seul locataire est susceptible d'être mieux contrôlé par l'organisation.
- **Autres organisations.** Il est parfois possible de gagner en sécurité et en efficacité lorsque plusieurs organisations humanitaires occupent des sites au même endroit ou à proximité les uns des autres. Les agences de l'ONU, par exemple, regroupent souvent leurs bureaux dans une même zone afin de renforcer la sécurité et de réduire les coûts. Certaines ONG ont également adopté cette approche. Cependant, les sites regroupés peuvent se transformer en communautés fermées, isolant potentiellement les organisations du reste de la communauté, ou donner l'impression d'une association étroite entre les organisations, ce qui peut avoir un impact sur la perception et l'acceptation locales. La concentration de cibles potentielles dans une seule zone signifie qu'une attaque peut avoir un impact beaucoup plus important si elle réussit.

Le quartier

Il est conseillé d'examiner les environs, idéalement dans un rayon d'au moins 1,5 km, afin d'avoir une vision globale du quartier. Les éléments clés à prendre en compte sont les suivants :

- **La stabilité et la cohésion sociale de la population résidente.** Une forte cohésion sociale peut être le signe d'un système de surveillance de quartier informel et fiable, avec des résidents vigilants et soucieux de la sécurité. Une faible cohésion sociale peut indiquer un manque d'intérêt pour la sécurité des voisins, ce qui peut permettre à des inconnus d'accéder facilement au site.
- **La nature du quartier.** La plupart des habitants sont-ils des résidents locaux ou le quartier est-il fréquenté par un grand nombre de travailleurs ou de voyageurs de passage ? Moins la population est locale, plus il sera facile pour des inconnus de s'introduire dans le quartier sans attirer l'attention.
- **Disponibilité des autorités locales et des services de secours.** Déterminer l'emplacement de la caserne de pompiers et des postes de police les plus proches, ainsi que les résidences des personnalités locales influentes. Identifier les zones les plus fréquemment patrouillées par la police.
- **Mesures de contrôle d'accès.** Tenir compte du type de contrôle d'accès utilisé par les résidents locaux, notamment la manière dont ils entrent et sortent des bâtiments et s'il existe des systèmes physiques ou virtuels/informatiques. Des gardes sont-ils postés à l'extérieur des maisons ? Les maisons de la zone sont-elles lourdement fortifiées ?
- **Niveaux de criminalité.** La criminalité peut être un facteur important, sachant que les niveaux de criminalité peuvent être élevés tant dans les zones riches que dans les zones moins riches. Quelle que soit la richesse de la zone, les organisations et leur personnel doivent éviter de donner une image d'opulence. Le choix d'un emplacement à proximité d'un poste de police dépend du contexte et des relations entre la police et la communauté locale.

En général, entretenir de bonnes relations avec les voisins, sans être intrusif, peut constituer une mesure de sécurité du site importante. Le simple fait d'établir une relation de base peut augmenter la probabilité que les voisins agissent s'ils remarquent quelque chose de suspect.

7.2.2 Renforcement du site

Pour ce qui est de la sécurité physique des lieux de travail et des résidences, une rubrique intitulée « Dissuader, détecter, retarder et réagir » peut s'avérer utile.⁹⁸ Cette rubrique peut inclure : l'ajout d'éléments rendant plus difficile l'accès à un bâtiment, tels que des murs, des barrières et des contrôles d'accès ; la suppression d'éléments qui empêchent

98 GISF (2024) 1. *Plans de sécurité*. Guide interfonctionnel sur la sécurité des ONG (<https://gisf.ngo/toolbox-pwa-fr/resource/1-plans-de-securite/>).

de voir les intrus potentiels et l'ajout de caméras, d'alarmes et de gardes ; la mise en place d'une pièce sécurisée qui peut retarder l'accès des intrus au personnel ; et la mise en place de procédures pour réagir rapidement en cas de détection d'intrusions. Les sections suivantes traitent ces mesures en détail.

Le périmètre extérieur

Les facteurs suivants doivent être pris en compte lors de l'évaluation de la sécurité du périmètre extérieur d'un site.

- **Cadre.** Si la végétation entourant le bâtiment offre des possibilités d'accès ou des cachettes potentielles, les organisations peuvent envisager de la tailler, de la couper ou de la remplacer par des buissons épineux. Les déchets ou les gravats à proximité du périmètre pourraient aider un agresseur à surveiller ou à accéder au bâtiment, ou entraver la réponse du personnel de sécurité. Il est également conseillé d'enlever rapidement tout débris susceptible de dissimuler des engins explosifs.
- **Murs et portes.** La construction de murs autour du site peut renforcer la sécurité. Les bonnes pratiques recommandent généralement que ceux-ci mesurent au moins 2,5 mètres de haut et soient renforcés par des mesures supplémentaires telles que des barbelés ou du verre brisé sur leur partie supérieure. Il peut également être nécessaire de s'occuper des arbres ou autres objets à proximité qui pourraient permettre d'escalader les murs. Les portes, qui constituent des points potentiellement vulnérables, doivent être correctement sécurisés et équipés de judas permettant de vérifier visuellement l'identité des visiteurs. Dans certains contextes, il peut être prudent de disposer d'un point de sortie secondaire, mais sécurisé.
- **Éclairage et visibilité.** Un éclairage amélioré peut dissuader les menaces potentielles, mais il convient de veiller à trouver un équilibre entre l'amélioration de la visibilité et le fait d'attirer l'attention. L'éclairage ne doit pas non plus avoir d'impact négatif sur les voisins. Les lampes à détecteur de mouvement qui s'allument lorsqu'elles détectent un mouvement peuvent être une bonne option, à condition qu'elles disposent d'une alimentation électrique constante. Dans les zones sujettes aux coupures de courant, d'autres sources d'énergie telles que des générateurs ou des lampes solaires peuvent être envisagées. La décision d'afficher le logo de l'organisation sur le périmètre extérieur dépendra de la question de savoir si l'organisation a déterminé que la visibilité dans le contexte donné renforce ou nuit à sa sécurité. Dans les environnements où l'organisation est bien considérée, l'affichage du logo peut être approprié, accompagné de traductions dans la langue locale.
- **Sites inoccupés.** Lorsque des sites sont inoccupés pendant un certain temps, les organisations peuvent mettre en place des mesures visant à donner l'illusion d'une activité, par exemple en allumant et éteignant régulièrement les lumières et en ajustant les volets afin de dissuader les intrus potentiels.
- **Conformité avec les pratiques locales en matière de sécurité.** Il peut être judicieux d'adopter des niveaux de protection similaires à ceux des autres bâtiments situés à proximité, même si les niveaux de risque perçus ne semblent pas le justifier.

- **Contrôle du stationnement et de l'accès des véhicules.** Les modalités de stationnement doivent être conçues de manière à empêcher l'accès non autorisé des véhicules au site et à réduire les risques d'attaques contre les véhicules. En cas de risques tels que vandalisme, vol de voiture, violence collective ou attentat à la bombe, il est préférable de garer les véhicules dans des endroits sécurisés, par exemple à l'intérieur d'un complexe. Il est également conseillé de s'assurer que le site choisi dispose d'un nombre suffisant de places de stationnement et que les véhicules sont verrouillés lorsqu'ils ne sont pas utilisés. Il convient d'établir des procédures opérationnelles pour le contrôle des clés des véhicules, les modalités de stationnement et l'utilisation en cas d'urgence. Les modalités de stationnement et de ravitaillement en carburant doivent faciliter le départ du site. Cela peut impliquer de s'assurer que les véhicules sont pleinement ravitaillés en carburant à la fin de chaque journée et stationnés de manière à permettre un chargement et un départ rapides.

Prévention du crime par l'aménagement du milieu

La prévention du crime par l'aménagement du milieu (CPTED) vise à améliorer la sécurité du site en modifiant l'environnement physique afin d'influencer les comportements et de réduire les occasions de commettre des crimes. Cet aspect est souvent négligé lors de la conception ou de la rénovation d'installations, ou lorsque des solutions de sécurité sont mises au point au fil du temps. Les stratégies CPTED comprennent les éléments suivants :

- **Surveillance naturelle.** Améliorer la visibilité extérieure et intérieure afin de démasquer les auteurs potentiels d'actes répréhensibles et renforcer le sentiment de sûreté des usagers légitimes. Cela implique de gérer avec soin l'aménagement paysager, l'éclairage et l'emplacement des fenêtres et des entrées afin d'obtenir une vue dégagée et de réduire les possibilités de dissimulation.
- **Contrôle naturel des accès.** Utilisation d'éléments physiques tels que des structures, des barrières, des aménagements paysagers, des éclairages et des panneaux de signalisation pour diriger l'accès vers des points spécifiques et contrôlables.
- **Renforcement territorial.** Définition des espaces publics, semi-publics et privés à l'aide d'éléments physiques tels que des bâtiments, des clôtures et des aménagements paysagers. Cela encourage les occupants à s'opposer aux intrus et les rend plus facilement identifiables.
- **Entretien.** Éviter les signes visibles de désordre tels que les vitres cassées, les graffitis et les équipements abandonnés, qui peuvent donner une impression d'abandon et de négligence, et inciter à la criminalité.

- **Bornes et barrières anti-chocs.** Placées stratégiquement, les bornes peuvent restreindre l'accès des véhicules tout en permettant la circulation des piétons. Les bornes peuvent être fixes, amovibles ou rétractables. Les barrières anti-chocs peuvent offrir une protection renforcée contre les menaces liées aux véhicules et sont généralement conçues pour résister à des impacts à grande vitesse. Les options comprennent des barrières en béton armé, des bornes en acier et des systèmes de câbles. Les bornes peuvent être intégrées dans le système global de sécurité du périmètre, en complément des murs et des portes.
- **Intégration des mesures de sécurité du périmètre.** En associant des barrières physiques à d'autres mesures de sécurité, les organisations peuvent mettre en place une défense à plusieurs niveaux. Il est essentiel d'aligner ces mesures de sécurité du périmètre sur les objectifs de sécurité plus larges de l'organisation, notamment en favorisant l'acceptation et la bonne volonté de la population locale, afin de garantir une approche cohérente et globale de la sauvegarde du personnel et des actifs.

Le périmètre intérieur

Il est conseillé aux organisations d'évaluer chaque site du point de vue d'un intrus, en identifiant tous les points faibles potentiels, en particulier les portes et les fenêtres, mais aussi les portes de garage et les caves.

- **Portes d'entrée.** Les organisations devraient s'assurer que les portes d'entrée sont solides, y compris les cadres et les charnières. Si la porte est vitrée, envisager de la remplacer. L'installation d'un support optique (judas), d'une serrure principale et d'une serrure auxiliaire sur les portes extérieures peut renforcer la sécurité. Pour renforcer la sécurité interne, les organisations peuvent envisager d'installer une chaîne de sûreté et un pêne dormant coulissant ou une barre solide sur la porte. Des cadenas robustes, placés en haut et en bas de la porte avec des anneaux soudés, peuvent offrir une protection supplémentaire. Enfin, il est conseillé de placer les boutons d'alarme ou les téléphones loin des portes d'entrée afin d'empêcher un intrus d'en bloquer l'accès.
- **Fenêtres.** Les organisations peuvent sécuriser les fenêtres, en particulier celles du rez-de-chaussée, à l'aide de barreaux, de grilles ou de volets, à condition qu'ils soient faciles à ouvrir de l'intérieur en cas d'urgence. Si les fenêtres des étages supérieurs sont accessibles de l'extérieur, il peut être utile de les sécuriser à l'aide de barreaux ou de grilles. Il est important de veiller à ce qu'ils ne puissent pas être facilement dévissés ou retirés de l'extérieur.
- **Routine nocturne.** Il peut être conseillé de fermer les rideaux la nuit afin d'empêcher les intrus d'observer qui se trouve à l'intérieur du bâtiment et combien de personnes s'y trouvent. Le personnel peut laisser une lumière allumée lorsqu'il quitte les lieux afin de donner l'impression que quelqu'un se trouve encore à l'intérieur. Il convient de vérifier que toutes les serrures et tous les verrous fonctionnent correctement et de les verrouiller systématiquement à la tombée de la nuit ou avant d'aller se coucher.

- **Sortie alternative en cas d'urgence.** En cas d'incendie, d'intrusion ou d'émeute, il est conseillé de prévoir une sortie alternative du bâtiment. Cette issue de secours, y compris les protections des fenêtres, doit être facilement accessible depuis l'intérieur, en tenant compte des profils personnels de l'ensemble du personnel (tels que les besoins en matière de mobilité). Si des barreaux sont déjà installés aux fenêtres, les organisations peuvent envisager de les modifier afin de permettre une sortie facile depuis l'intérieur. Cela peut impliquer de fixer les barreaux sur un côté à l'aide d'une charnière et de les sécuriser avec un cadenas, en veillant à ce que les occupants puissent accéder rapidement à la clé en cas d'urgence.
- **Alarmes anti-effraction et télévision en circuit fermé (CCTV).** Bien que les alarmes anti-effraction et les caméras CCTV soient peu courantes dans de nombreux contextes d'aide humanitaire, les organisations pourraient néanmoins envisager de les utiliser pour renforcer la sécurité. Ces deux dispositifs dépendent généralement d'une alimentation électrique, même si certaines alarmes anti-effraction fonctionnent sur piles. Les caméras CCTV peuvent avoir un effet dissuasif limité, à moins que les intrus ne soient conscients de leur présence et de leur fonction, et qu'il y ait un risque raisonnable qu'ils soient pris sur le fait. Les dispositifs de sécurité à haut débit sonore, qui fonctionnent à distance et de manière directionnelle, émettent un son insupportable qui peut empêcher les intrus, voire les foules en émeute, de pénétrer plus avant dans les locaux. Ils sont généralement équipés d'une protection anti-sabotage et fonctionnent à piles.

Considérations élémentaires en matière de sûreté incendie

Pour prévenir les risques d'incendie, il faut tenir compte des points suivants :

- Installer des détecteurs de fumée et de monoxyde de carbone et placer des extincteurs dans la cuisine et à chaque étage. Les incendies d'origine électrique et ou liés aux hydrocarbures nécessitent un extincteur à CO₂ ou à poudre ; pour les autres types d'incendie, utiliser un extincteur à mousse ou à eau.
- Vérifier les extincteurs et les faire réviser au moins une fois par an.
- Identifier les issues de secours et s'assurer qu'elles peuvent être ouvertes instantanément lorsqu'elles sont verrouillées de l'intérieur.
- Organiser régulièrement des exercices d'évacuation, en particulier si le taux de rotation du personnel est élevé.
- S'assurer que les appareils de chauffage au gaz sont correctement ventilés et vérifier qu'ils sont équipés de thermocouples (dispositifs qui empêchent l'alimentation en gaz de s'activer sans veilleuse ou autre source d'allumage). Les appareils de chauffage sans thermocouples ne doivent pas être laissés sans surveillance et ne doivent pas être utilisés la nuit.

- Désigner officiellement des personnes formées pour veiller à ce que le personnel en situation de handicap bénéficie d'une assistance en cas d'urgence (parfois appelé «système de jumelage») ; ces personnes doivent être des membres du personnel qui passent la majeure partie de leur temps sur le site.
- Placer les plans d'évacuation de manière à ce qu'ils soient bien visibles, mais pas des passants, et éventuellement, coder l'identification des pièces de manière à aider le personnel et les visiteurs, sans pour autant servir de guide potentiel aux intrus.

Pièces sécurisées

Une pièce sécurisée peut servir de refuge essentiel aux occupants en cas d'urgence, leur offrant une protection contre les intrus jusqu'à l'arrivée des secours. La plupart des pièces sécurisées ne sont pas conçues pour résister aux impacts de bombes ou d'obus.

- **Emplacement et accessibilité.** Une pièce sécurisée doit être facilement accessible et idéalement située au cœur du bâtiment pour permettre un accès rapide. Il est également possible de transformer les étages supérieurs en zones sûres en sécurisant les escaliers à l'aide de grilles de verrouillage pendant les périodes sensibles, comme la nuit.
- **Éléments de sécurité.** La pièce sécurisée devrait idéalement être équipée de portes renforcées et de fenêtres sécurisées afin de dissuader les intrus. Un téléphone ou une radio d'urgence devrait être disponible pour appeler à l'aide. Les organisations peuvent envisager d'installer des systèmes de communication avec une alimentation sans interruption pour maintenir la connexion en cas de coupure de courant. Une liste des numéros de téléphone importants, notamment ceux des services d'urgence et des équipes internes de réponse, peut être affichée bien en évidence dans la pièce sécurisée.
- **Fournitures d'urgence.** La pièce sécurisée doit être approvisionnée en fournitures essentielles pour subvenir aux besoins des occupants en cas d'urgence. Il peut s'agir de trousse de premiers secours, d'une petite quantité d'eau, de denrées alimentaires non périssables et de produits d'hygiène. Des chaises, des matelas et de la literie peuvent être ajoutés au cas où le personnel devrait se réfugier pendant une période prolongée ou y passer la nuit. Les denrées périssables et les médicaments doivent être vérifiés et remplacés régulièrement.
- **Formation et exercices.** Des sessions de formation et des exercices réguliers (y compris des scénarios simulés) permettent aux occupants du bâtiment de se familiariser avec l'emplacement, la disposition et les procédures de la pièce sécurisée, notamment comment y accéder rapidement et quoi faire lorsqu'ils s'y réfugient en cas d'urgence.

- **Protocoles de communication.** Il est conseillé d'établir des protocoles de communication clairs au sein de la pièce sécurisée, décrivant les procédures à suivre pour contacter les services d'urgence et coordonner les interventions externes. Il est préférable de désigner des personnes chargées d'établir la communication avec les autorités et de fournir des informations actualisées sur la situation. Une hiérarchie de communication peut contribuer à rationaliser la diffusion des informations et la prise de décision.

► *Pour en savoir plus sur la sécurité des communications, voir le chapitre 6.1.*

7.2.3 Gestion des risques de sécurité du site

Sensibilisation individuelle

La sécurité du site est la responsabilité de tous. Tout le monde, y compris les réceptionnistes, les standardistes, les agents d'entretien et les jardiniers, doit être vigilant et signaler tout élément inhabituel ou suspect, ainsi que tout manquement aux procédures de sécurité (par exemple, des portes ou des fenêtres laissées ouvertes ou des clés laissées à la vue de tous). Dans le cas des propriétés résidentielles, cela concerne tous les résidents (y compris les membres de la famille). Ces personnes doivent recevoir des consignes leur recommandant de ne pas laisser entrer des inconnus dans les locaux, de ne pas donner d'informations à des appelants inconnus, de ne pas donner de détails sur la disposition des bureaux et de ne pas autoriser la reproduction de leurs clés. Les réceptionnistes peuvent jouer un rôle clé en contrôlant les visiteurs et les appels téléphoniques, ainsi que les lettres et les colis livrés, et peuvent être formés pour signaler tout élément ou toute personne qui leur semble suspect.

Gardes

Les organisations humanitaires font parfois appel à des gardes pour surveiller leurs résidences, leurs entrepôts et leurs bureaux. Ces gardes peuvent être embauchés directement ou engagés par l'intermédiaire d'un prestataire local. Ils peuvent s'avérer inefficaces s'ils ne sont pas formés, mal instruits, mal payés, mal équipés ou mal gérés. Malheureusement, cela n'est pas rare dans de nombreux contextes où s'inscrivent les activités humanitaires. Il n'est pas rare non plus de trouver un lit dans le poste de garde des complexes des organisations humanitaires, ce qui augmente le risque que le garde s'endorme pendant son service. Pendant la journée, les gardes peuvent être occupés à d'autres tâches et être distraits. Lors du recrutement de gardes, il est important de fournir un cahier des charges clair et de l'intégrer au contrat.

Pour le recrutement et le management des gardes, il convient de tenir compte des éléments suivants :

- Obtenir des références fiables et, si possible, recruter du personnel dans le voisinage immédiat. Cela permet de s'assurer qu'ils connaissent bien le quartier et ses occupants réguliers, ce qui peut les motiver davantage à identifier les malfaiteurs potentiels.

- Vérifier les compétences linguistiques des recrues potentielles. Les principaux occupants d'un bâtiment doivent être en mesure de communiquer avec le garde.
- Recruter et déployer suffisamment de gardes pour détecter les intrusions et pour qu'ils puissent se soutenir mutuellement dans leur travail.
- Veiller à ce que les gardes reçoivent une présentation complète de l'organisation.
- Si le garde doit porter une arme (létale ou non), les circonstances dans lesquelles il peut l'utiliser doivent être régies par le contrat signé avec la personne ou le prestataire de services de garde et refléter la politique de sécurité de l'organisation. Il est recommandé que ces politiques soient examinées par le conseiller juridique de l'organisation. Les organisations peuvent inclure des clauses contractuelles interdisant la consommation de substances nocives (par exemple l'alcool) pendant le service et l'exercice d'activités annexes susceptibles d'affecter les performances du garde.
- Fournir l'équipement, les instructions et la formation nécessaires. L'équipement peut comprendre des vêtements de pluie, des lampes torches, un sifflet ou tout autre dispositif d'alarme, ainsi qu'une radio portative ou un téléphone séparé dans le poste de garde.
- Fournir un registre contenant des instructions sur la manière de le tenir et de signaler toute activité suspecte, ainsi qu'une liste des numéros de téléphone importants.
- Fournir des instructions claires et une formation sur la manière de traiter les visiteurs et sur les mesures à prendre si les gardes rencontrent un intrus.
- Fournir des instructions claires sur la surveillance des environs, la patrouille du complexe et les règles concernant les portails, les portes, les fenêtres et les clés.
- Les gardes n'ont généralement accès qu'au périmètre extérieur (et non intérieur), en particulier dans les locaux résidentiels. Dans les immeubles de bureaux, ils doivent généralement avoir accès aux couloirs, aux escaliers et au toit, mais pas nécessairement aux bureaux eux-mêmes.
- Dans les zones où le risque d'intrusion ou de braquage est élevé, envisager d'alterner les inspections de routine avec des rondes à des heures moins prévisibles. Il peut être utile de répartir les gardes, en plaçant au moins l'un d'entre eux dans un endroit où il ne peut être facilement observé et maîtrisé, par exemple sur un toit-terrasse.
- Spécialement dressés pour assurer la garde, les chiens peuvent constituer un excellent moyen d'alerte précoce en cas d'intrusion et ont souvent un effet dissuasif. Cependant, un chien peut être dangereux pour les personnes qu'il ne connaît pas, et des mesures de maîtrise du risque peuvent être nécessaires pour protéger les visiteurs légitimes et le personnel.

Contrôle des accès

Le contrôle des accès commence par la mise en place de mesures clés de gestion. Les organisations peuvent également utiliser des cartes d'accès magnétiques, des serrures à code (systèmes électroniques à bouton-poussoir qui ne permettent l'entrée qu'aux personnes connaissant le code), des lecteurs magnétiques, des cartes à puce ou des dispositifs biométriques. Les bureaux plus grands, généralement situés dans les grandes villes, peuvent contrôler les accès en installant des portes ou des tourniquets fonctionnant avec des cartes magnétiques. Idéalement, il faudrait mettre en place des contrôles de gestion pour tous ces éléments. Les systèmes peuvent être coûteux et peuvent tomber en panne en cas de coupure de courant ou de dysfonctionnement du mécanisme.

Clés du site

Les organisations peuvent tenir un registre complet des clés et de leurs détenteurs, et veiller à ce que le nombre de clés en circulation soit strictement contrôlé. En cas de doute quant à la sécurité des clés, il est conseillé de changer les serrures. Les clés peuvent être étiquetées à l'aide d'un code afin qu'elles ne puissent pas être facilement identifiées. Les doubles des clés doivent être conservés en lieu sûr dans un coffre à clés verrouillé muni d'une vitre pouvant être brisée en cas d'urgence.

Tout le personnel ayant accès aux clés, y compris le personnel de maison, doit être informé des protocoles de gestion des clés, par exemple, garder les clés sur soi plutôt que de les laisser sur un bureau, dans une voiture ou dans un manteau ou un sac sans surveillance. En règle générale, la reproduction des clés est interdite, sauf instruction contraire expresse de la direction de l'organisation, et toute perte de clés doit être immédiatement signalée.

Une gestion trop stricte des clés peut présenter certains dangers. Par exemple, le personnel risque de ne pas pouvoir s'échapper d'un bâtiment en feu s'il n'a pas accès à la clé de la porte de sortie de secours. De même, une réponse suite à un appel d'urgence d'un collègue pourrait être retardée si les clés du véhicule sont sous clé.

En ce qui concerne les visiteurs, le contrôle d'accès remplit généralement deux fonctions : établir l'objet et la légitimité d'un visiteur et s'assurer que les visiteurs ne constituent pas une menace. Dans certaines circonstances, l'accès peut devoir être contrôlé de manière très stricte ; les visiteurs peuvent être activement dissuadés ou dirigés vers un bâtiment séparé, éloigné des installations principales de l'organisation. Dans tous les cas, il est utile de disposer d'un espace d'attente réservé aux visiteurs. Celui-ci doit être facilement visible par le personnel de sécurité et la réceptionniste.

Il doit être équipé de toilettes, mais les visiteurs en attente d'autorisation ne doivent pas pouvoir accéder librement au bâtiment.

Il existe différents niveaux de contrôle de sécurité. Par exemple, demander aux visiteurs de s'inscrire à leur arrivée et à leur départ n'est pas vraiment une mesure de sécurité en soi, car n'importe qui peut toujours entrer. Des procédures standard plus strictes pourraient consister à s'assurer que :

- tout le personnel porte un badge d'identification visible avec photo lorsqu'il se trouve dans les locaux ;
- tous les visiteurs présentent une pièce d'identité ;
- tous les visiteurs reçoivent un badge d'identification ou un laissez-passer, qui leur est retiré lorsqu'ils quittent les lieux ;
- aucun visiteur n'est autorisé à entrer sans l'autorisation explicite de la personne qu'il souhaite voir ou qui accepte de le recevoir ; et
- aucun visiteur n'est autorisé à entrer sans être accompagné d'un membre du personnel.

Les procédures plus strictes comprennent la vérification des sacs des visiteurs et des fouilles au corps manuelles ou électroniques (des gardes femmes et une formation spéciale sont généralement nécessaires à cet effet).

Dans les environnements à haut risque, toute personne inconnue, non autorisée ou incapable de fournir une pièce d'identité convaincante ne doit pas être admise. Les premières vérifications sommaires visant à déterminer si un visiteur pourrait représenter une menace doivent être effectuées à l'extérieur du périmètre, avant qu'il ne soit admis à l'intérieur du périmètre d'un bâtiment. Seuls les visiteurs qui ne semblent pas représenter de menace doivent être autorisés à entrer. La détermination de l'objet de la visite, la prise de contact avec le service d'accueil, l'enregistrement de la visite et la délivrance d'un badge visiteur peuvent alors être effectués dans un deuxième temps, à l'intérieur des locaux, ce qui permet de réduire au minimum le nombre de personnes attendant à l'entrée principale. En cas de doute, les gardes doivent être invités à contacter un supérieur hiérarchique.

En cas de rencontre avec une personne suspecte ou non autorisée, le personnel de sécurité ou les points focaux doivent être immédiatement alertés. Des protocoles peuvent être mis en place pour avertir le personnel rapidement et discrètement, par exemple à l'aide de radios ou de boutons d'alarme. Le personnel de sécurité peut envisager d'introduire des mots de code pour appeler à l'aide discrètement. Si la situation s'aggrave ou constitue une menace importante, un confinement peut s'avérer nécessaire pour sécuriser les locaux et protéger le personnel. Il est recommandé de présenter clairement au personnel les procédures de confinement, en détaillant les mesures à prendre, telles que la sécurisation des portes et le barricadage des points d'entrée.

Politique d'accès : questions à prendre en considération

- **Les véhicules des visiteurs doivent-ils être autorisés à entrer dans l'enceinte (le cas échéant) ?** Il peut être utile de réfléchir à l'endroit où les visiteurs doivent se garer. Par exemple, en cas d'alerte à la bombe, il est conseillé de s'assurer qu'aucun véhicule n'appartenant pas à l'organisation ne se trouve dans l'enceinte. Les organisations peuvent également envisager d'interdire le stationnement des visiteurs autour du bâtiment. Les gardes peuvent être chargés de fouiller les véhicules, mais il s'agit d'une tâche qui nécessite des compétences et une formation appropriée.
- **Quelle est la politique de l'organisation concernant les visiteurs accompagnés de gardes du corps ou portant des armes dans ses locaux ?** Les organisations peuvent choisir d'adopter une politique relative à la présence d'armes dans leurs locaux, en tenant compte du contexte et du type de visiteurs (par exemple, des policiers ou des représentants du gouvernement), et déterminer si les visiteurs accompagnés de leurs propres gardes du corps sont autorisés à les faire entrer dans les locaux. La responsabilité potentielle de l'organisation en cas d'attaque contre un visiteur dont les gardes du corps n'ont pas été autorisés à entrer doit être prise en compte. Tenir les réunions dans une annexe du bâtiment ou sous une véranda, où les gardes du corps peuvent rester à proximité, peut constituer un compromis pratique. Les gardes doivent être formés à la gestion de ce type de situation.
- **Comment gérer l'accès du personnel de service et des livraisons ?** L'accès du personnel de service doit être soigneusement étudié, notamment l'accès pour l'entretien, les réparations, l'équipement et les livraisons. Décider si le personnel de service doit être autorisé à pénétrer dans les locaux en l'absence du personnel habituel, et si les arrivées peuvent être planifiées et programmées à l'avance. Exiger une pièce d'identité du personnel de service pourrait renforcer la sécurité et, dans le cas des vendeurs ambulants, le personnel peut acheter des marchandises à l'extérieur de l'enceinte afin de limiter l'accès.

► Voir le chapitre 4.2 pour plus d'informations sur la protection armée.

Au-delà des mesures traditionnelles de contrôle d'accès telles que l'enregistrement des visiteurs, on observe une tendance croissante vers les méthodes

d'authentification biométrique, telles que la reconnaissance des empreintes digitales ou de l'iris. L'intégration de l'authentification biométrique dans les procédures de contrôle d'accès peut renforcer leur sécurité tout en conservant leur efficacité et leur commodité pour les visiteurs légitimes et les membres du personnel. Certaines organisations ont opté pour une authentification à deux facteurs (2FA) (par exemple, la biométrie et une carte) ou ont créé différents niveaux d'autorisation pour différentes installations ou différents services. Les organisations doivent tenir compte des risques de pannes de courant, ainsi que de la sensibilité des données biométriques collectées et des risques potentiels de violation des données. Un stockage ou un cryptage inadéquat des données biométriques pourrait entraîner une usurpation d'identité ou d'autres violations de la vie privée en cas de violation des données. Ces risques peuvent être gérés grâce à des mesures de sécurité appropriées de stockage des données, de cryptage et de sécurité des systèmes.

Appels téléphoniques menaçants et lettres de menaces

Les appels téléphoniques problématiques peuvent aller des canulars téléphoniques au harcèlement sexuel et aux alertes à la bombe. Lorsque ce risque existe, le personnel doit être formé à la manière d'y répondre. L'utilisation de la technologie d'identification de l'appelant ou de la localisation des appels peut aider à identifier l'origine des appels problématiques et faciliter les enquêtes. Les appels à caractère sexuel (harcèlement sexuel) adressés à des femmes peuvent parfois être évités en demandant à un collègue ou à un colocataire masculin de répondre au téléphone. Si l'appelant persiste, il peut être préférable de changer de numéro de téléphone. En règle générale, les employés ne doivent pas communiquer leur numéro de téléphone personnel et doivent uniquement indiquer leur numéro professionnel dans leur signature électronique et sur leurs cartes de visite.

En cas d'appels menaçants, les destinataires doivent essayer de rester calmes et polis, s'abstenir de communiquer des informations personnelles ou une information sensible, donner le moins d'informations possible à l'appelant, écouter attentivement afin de recueillir autant d'informations que possible pour aider à l'identification de l'appelant, noter tous les détails pertinents, y compris le nom et le numéro de téléphone, s'ils sont connus, et signaler immédiatement la menace. Si l'appel est une alerte à la bombe, la question clé sera de savoir quand et où la bombe explosera. À moins d'être certain que la menace n'est pas réelle, le bâtiment doit être immédiatement évacué. Si le bureau reçoit une lettre de menace, celle-ci doit être prise au sérieux et transmise rapidement aux cadres supérieurs, aux autorités et aux autres organisations de la zone, selon le cas.

Lettres ou colis suspects

Bien que cela ne constitue pas une menace courante pour les organisations humanitaires, il est possible qu'une lettre ou un colis soit délibérément contaminé par une substance chimique ou biologique toxique, ou qu'il contienne une matière

explosive. Les indices possibles sont des traces de poudre sur l'enveloppe, une odeur étrange et, dans le cas d'une bombe, un tic-tac ou des fils visibles. Le colis peut être anormalement lourd pour sa taille, l'adresse peut être mal orthographiée ou la lettre ou le colis peut être adressé à une personne qui ne travaille plus pour l'organisation. Il se peut que l'affranchissement soit insuffisant ou excessif, ce qui indique qu'il n'a pas été affranchi dans un bureau de poste.

Ces lettres ou colis doivent être laissés où ils se trouvent, la pièce doit être évacuée et le personnel de sécurité doit être alerté. Toute personne ayant manipulé l'objet doit être invitée à se laver immédiatement avec du savon, en particulier les mains. Il peut être nécessaire de faire détruire ou ouvrir la lettre ou le colis par du personnel de sécurité spécialement formé et équipé (la contamination par une substance toxique nécessite au minimum le port de gants de protection intégrale et éventuellement de masques de protection intégrale, car certaines substances peuvent pénétrer dans l'organisme par inhalation).

7.2.4 Sites de distribution

Un certain nombre de mesures peuvent contribuer à renforcer la sécurité du personnel et des populations cibles sur les sites de distribution.

- **Comprendre la population cible.** Il est utile de bien comprendre la population cible, notamment la manière dont elle et les personnes vivant à proximité peuvent percevoir la distribution, s'il existe des tensions potentielles entre les groupes et s'il y a un risque d'ingérence politique. Le personnel pourra ainsi repérer tout signe de détresse concernant les articles distribués et identifier les éléments qui pourraient avoir intérêt à manipuler le processus de distribution.
- **Gestion du périmètre et du site.** Il peut être utile d'établir un périmètre bien défini. Des clôtures ou des murs peuvent être appropriés, ou encore des barricades avec une surveillance supplémentaire.
- **Emplacement du site de distribution.** Il peut être judicieux de choisir un emplacement où la circulation, tant automobile que piétonne, n'est pas gênée, et de s'assurer que le site n'attire pas de passants indésirables ou ne provoque pas de perturbations.
- **Gestion des points d'entrée et de sortie.** Désigner un point d'entrée et un point de sortie. Une gestion efficace du flux de personnes à l'entrée permet de séparer rapidement les bénéficiaires légitimes de l'aide de ceux qui ne sont pas éligibles. Veiller à ce que le personnel soit en nombre suffisant pour prendre en charge les personnes difficiles. Les points de sortie doivent être gérés avec soin, afin de garantir que les bénéficiaires puissent quitter le site de manière sûre et ordonnée.
- **Contrôle et circulation des foules.** Il est important de faire circuler les gens. Le personnel ou les autorités peuvent surveiller la zone afin d'éviter que des foules, y compris les membres de la famille qui aident les bénéficiaires, ne se rassemblent et n'empêchent le départ des autres. Il convient de veiller à la sûreté et à la

protection des personnes qui quittent les lieux, en particulier les femmes et les jeunes enfants. Le fait de transporter de gros paquets, par exemple, peut rendre les bénéficiaires de l'aide plus vulnérables à d'éventuelles attaques, et le personnel pourrait envisager des moyens de rendre les articles distribués moins visibles.

- Pour plus de détails sur les risques liés à la distribution, voir le chapitre 7.6 sur les troubles civils.

Informations complémentaires

Recommandations

Davis, J. et al. (2020) 'Module 8, Security of facilities' in *Security to go: a risk management toolkit for humanitarian aid agencies* (en anglais, « Module 8, Sécurité des établissements dans La sécurité en pratique : boîte à outils de gestion de risque à l'attention des agences humanitaires »), 4e édition. GISF (<https://gisf.ngo/resource/security-to-go/>).

GISF (2024) 1. *Plans de sécurité*. Guide interfonctionnel sur la sécurité des ONG (<https://gisf.ngo/toolbox-pwa-fr/resource/1-plans-de-securite/>).

International CPTED Association (n.d.) L'Association Internationale de Prévention du crime par l'aménagement du milieu (www.cpted.net/).

Safer Edge (2014) *Office closure* (en anglais, « Fermeture de bureau »). European Interagency Security Forum (<https://gisf.ngo/resource/office-closure/>).

Source8 (2015) *Ouvrir un nouveau bureau: Manuel à l'attention des organisations non gouvernementales*. European Interagency Security Forum (<https://gisf.ngo/resource/office-opening/>).

7.3 Sécurité des fonds en espèces

Bien que l'adoption généralisée de la monnaie numérique ait globalement réduit les quantités d'espèces que les organisations doivent détenir et manipuler, dans de nombreux contextes et circonstances, il reste nécessaire de détenir, de transférer et d'effectuer des transactions en espèces. Ce chapitre traite de multiples aspects de la sécurité des espèces, du vol et du braquage aux risques liés aux transferts monétaires.

7.3.1 Risques

Si les risques liés aux espèces et leur gestion relèvent souvent de la responsabilité du personnel des finances et de la direction, les activités liées aux espèces comportent des risques de sécurité importants. Le retrait ou le transport de sommes importantes en espèces rend les travailleurs humanitaires vulnérables au vol et au braquage. Se déplacer avec des espèces, en particulier dans des zones reculées ou touchées par des conflits, augmente le risque d'être pris pour cible par des criminels ou des groupes armés. Les risques de sécurité liés aux transferts monétaires doivent également être pris en compte et traités, notamment les risques liés au transfert de fonds aux bénéficiaires de l'aide, à la fraude et à l'atteinte à la réputation.

7.3.2 Mesures d'atténuation des risques

Une première étape essentielle consiste à évaluer les risques liés aux flux d'espèces au sein de l'organisation, puis à concevoir et mettre en œuvre des mesures d'atténuation aux points présentant un risque élevé.

La section suivante met en évidence les mesures visant à traiter les risques associés aux activités impliquant des espèces. Idéalement, celles-ci devraient être décidées et mises en œuvre conjointement par le personnel chargé de la sécurité et celui chargé des finances.

Réduire l'utilisation d'espèces

Les organisations peuvent réduire leur utilisation d'espèces en effectuant leurs paiements par chèque, virement bancaire, cartes prépayées, cartes de crédit ou autres moyens de paiement électroniques. Aucun moyen de paiement n'est exempt de risque, et il est important d'établir des directives sur l'utilisation des cartes de crédit et de les contrôler régulièrement. Les organisations qui effectuent des transactions importantes doivent envisager de souscrire une assurance spécifique contre la perte ou le vol.

Risques liés aux transactions électroniques

Il existe plusieurs moyens de transférer de l'argent sans utiliser d'espèces. Les risques associés à ces mécanismes concernent davantage la sécurité financière, opérationnelle ou numérique, mais peuvent avoir des répercussions sur la sécurité du personnel, par exemple si un retard dans le transfert provoque des tensions avec les parties qui attendent le paiement. Les services de transfert d'argent numérique et les applications mobiles peuvent être vulnérables au piratage, aux attaques de phishing et à d'autres formes de fraude et de cybercrime. Les systèmes informels connus sous le nom de hawala se sont retrouvés dans une situation difficile après le 11 septembre, car on craignait que certaines transactions facilitent le transfert illégal de fonds vers des groupes interdits. La législation en matière de lutte antiterroriste et les pratiques bancaires visant à réduire les risques ont imposé des contraintes supplémentaires aux organisations qui tentent de transférer des sommes importantes, les obligeant dans certains cas à revenir à l'utilisation d'espèces.

Un risque spécifique lié aux paiements financiers électroniques est le ciblage des virements effectués par des donateurs à des organisations ou des paiements au sein d'organisations. Les criminels savent que des sommes très importantes sont transférées par les donateurs vers les organisations opérationnelles, ainsi qu'entre le siège social et les bureaux de programmes. Ils peuvent intercepter les échanges par e-mail, cloner les comptes des employés et donner de fausses instructions afin de détourner les paiements vers des comptes bancaires externes. Les modifications ou instructions de dernière minute concernant des virements bancaires importants peuvent également être le signe d'une activité frauduleuse.

- Voir le chapitre 6.2 pour d'autres mesures d'atténuation des risques de sécurité numérique.

Faire preuve de discrétion

Lorsque l'on s'occupe d'espèces, la discrétion est importante. Moins il y a de personnes au courant, moins le risque est élevé. Les communications susceptibles d'être interceptées peuvent être transformées en une forme de code. Si un retrait doit être effectué dans une banque, il convient de prendre les dispositions nécessaires à l'avance et en toute discrétion ; éviter d'effectuer des retraits à des heures ou à des jours réguliers (par exemple avant le versement des salaires mensuels) peut réduire le risque. Il est préférable de payer les fournisseurs en utilisant l'un des moyens de paiement autres que les espèces mentionnés ci-dessus, en particulier pour les montants importants. Si le personnel utilise

régulièrement le même hôtel ou le même fournisseur, les organisations peuvent envisager d'ouvrir un compte.

Dans certaines économies, et en cas d'hyperinflation, le volume et la quantité d'espèces peuvent poser un problème. Même des montants relativement modestes en devises étrangères peuvent se traduire par des liasses importantes de billets locaux. Lors du retrait d'espèces dans une banque, le personnel peut demander à ce que l'argent soit versé en grosses coupures et doit tenir compte des aspects pratiques liés au transport et au stockage.

Recommandations à l'intention du personnel sur les bonnes pratiques en matière de sécurité des fonds en espèces

- Faites tout votre possible pour limiter l'utilisation d'espèces.
- Veillez à fixer un plafond de crédit et de retrait d'espèces raisonnable.
- Vérifiez les relevés bancaires et examinez tout paiement non reconnu.
- Conservez une liste des numéros à appeler en cas de perte ou de vol de cartes bancaires.
- Bloquez ou annulez une carte bancaire dès qu'elle est perdue.
- Conservez les codes PIN en lieu sûr.
- Gardez vos cartes bancaires à portée de vue lorsque vous les présentez pour régler un achat.
- Ne résistez pas face à un voleur.

Limiter l'exposition

Il existe plusieurs moyens de réduire l'exposition aux risques de perte ou de vol. Les paiements justes à temps aux fournisseurs réduisent le temps pendant lequel les espèces sont conservées dans les bureaux. Une autre pratique courante consiste à fixer un plafond pour les montants en espèces pouvant être retirés, transférés ou conservés dans le coffre-fort de l'organisation. Cependant, la réduction du montant des transactions individuelles entraînera probablement une augmentation du nombre de transactions à effectuer, ce qui augmentera les coûts. Si les espèces sont plus exposées aux risques lorsqu'elles sont transportées physiquement, les organisations doivent envisager de transporter des montants plus importants moins fréquemment, en particulier si des moyens de transport plus sûrs sont disponibles périodiquement, tels que des vols en hélicoptère ou de grands convois. Les organisations peuvent également examiner les risques à différents points de la chaîne de transfert, de la banque au coffre-fort de l'organisation jusqu'au destinataire final, et représenter cette chaîne sous forme d'organigramme. Il sera peut-être possible de réduire le nombre de maillons de la chaîne, par exemple en demandant aux fournisseurs de se rendre au bureau pour recevoir leur paiement plutôt que de leur apporter des espèces.

Si les risques de cambriolage et de braquage sont élevés, il est conseillé de ne pas conserver tout l'argent au même endroit et d'en garder une certaine somme à portée de main, dans un endroit visible, afin de satisfaire et de distraire les voleurs. Une partie de l'argent doit être facilement accessible, le reste doit être mieux caché. Lorsqu'ils se déplacent, les membres du personnel doivent être encouragés à répartir les espèces en plusieurs endroits et entre les différents membres du personnel en déplacement. En période de forte tension, lorsqu'un retrait, une relocalisation ou une évacuation peuvent s'avérer nécessaires, les espèces peuvent être réparties entre les membres du personnel qui partent, d'une part pour répartir les risques et d'autre part pour garantir que le personnel dispose d'espèces à portée de main au cas où il serait séparé. Les organisations doivent vérifier que leur personnel est disposé à transporter d'importantes sommes en espèces sur lui dans des situations de forte tension ou lors de déplacements.

Dans les pays où une relocalisation ou une évacuation est fortement probable, les mouvements d'espèces doivent être organisés et planifiés à l'avance. Les besoins en espèces du personnel qui pourrait devoir rester sur place doivent être pris en compte et satisfaits.

Exemple de cas : Soudan

Au Soudan, une organisation a dû distribuer régulièrement des espèces à titre d'« aide d'urgence » pour permettre à ses employés de se rendre dans les bureaux locaux. Afin de réduire la visibilité et la vulnérabilité de ces espèces, une certaine somme en billets a été placée entre deux feuilles de papier (ou une seule feuille pliée), puis glissée dans une pochette en plastique spéciale et plastifiée. Des instructions écrites et une ligne pointillée ont été imprimées à l'avance sur le papier. Cela a permis d'obtenir un paquet soigné et protégé contenant de l'argent précompté. Cela a également facilité la comptabilité, car il n'était pas nécessaire de compter les espèces lorsqu'elles étaient distribuées et restituées, tant que la pochette était intacte.

Réduire la prévisibilité

La routine augmente les risques, c'est pourquoi les organisations doivent essayer d'éviter la prévisibilité dans les activités liées aux espèces. Parmi les risques courants prévisibles, on peut citer :

- La paie mensuelle.
- Les paiements spéciaux versés au personnel avant la relocalisation ou l'évacuation.
- L'arrivée du personnel à l'aéroport et les transferts vers l'hôtel/le bureau (les voleurs peuvent surveiller les heures d'arrivée de certains vols et cibler les véhicules sur la route principale menant à la ville).

- Les trajets effectués par le personnel entre le bureau et la banque, en particulier s'ils empruntent toujours le même itinéraire et à peu près à la même heure de la journée.
- Les trajets vers la banque impliquant plusieurs membres du personnel peuvent indiquer qu'une somme d'argent plus importante que la normale est sur le point d'être déposée ou retirée.

Des mesures de sécurité supplémentaires peuvent réduire la prévisibilité. Par exemple:

- Utiliser un véhicule banalisé, loué ou local, ou un itinéraire moins évident pour transporter le personnel de l'aéroport au bureau ou à l'hôtel.
- Modifier les périodes de paie et les dates de paiement, même si cela risque de ne pas plaire au personnel.
- Autoriser différents membres du personnel à se rendre à la banque, en modifiant les itinéraires et les horaires de déplacement.

Réduire la vulnérabilité

Les organisations peuvent mettre en place des mesures visant à réduire la vulnérabilité liée au transport d'espèces, notamment des directives relatives au transport d'espèces et des mesures de sécurité du site.

Afin de réduire la vulnérabilité lors du transport d'espèces par la route, il est recommandé d'impliquer au moins deux personnes et, de préférence, plusieurs véhicules. Il est préférable d'éviter toute prévisibilité, ce qui peut impliquer de varier le nombre de passagers et de véhicules utilisés. Dans les cas extrêmes, il est possible de faire appel à une escorte armée ou d'utiliser un véhicule blindé, même si cela risque d'attirer une attention indésirable. L'option la plus sûre pour retirer des espèces à un distributeur automatique de billets (DAB) est sans doute un distributeur situé dans une rue animée, où d'autres personnes font la queue pour faire de même. L'idéal est que le personnel retire l'argent pendant la journée et en compagnie d'un collègue afin de garder un œil sur les environs. Il est possible que le personnel soit observé lorsqu'il retire des espèces et qu'il soit suivi. Il doit donc éviter les rues calmes ou les quartiers plus douteux après s'être rendu à un DAB.

Au bureau, les organisations peuvent envisager d'installer des coffres-forts et de mettre en place des mesures de sécurité du site solides. Voici quelques considérations pour assurer la sécurité des coffres-forts:

- Fixer le coffre-fort au sol et le placer dans une pièce à l'arrière ou derrière un bureau afin qu'il soit invisible pour les visiteurs.
- Installer une serrure qui nécessite deux clés pour ouvrir et remettre les clés à deux personnes différentes, ou utiliser une serrure à clé et à combinaison.
- Être préparé au cas où des voleurs menaceraient le personnel de violence si le coffre-fort n'était pas ouvert à leur demande (par exemple, conseiller au personnel de remettre les clés ou la combinaison s'il est menacé).

- Si le détenteur d'une clé s'absente ou part en congé, s'assurer qu'un décompte précis de la caisse est effectué avec le nouveau détenteur de la clé, puis signé par les deux parties.

► Pour plus d'informations sur la sécurité du site, voir le chapitre 7.2.

Remarque sur l'usurpation d'identité

L'usurpation d'identité et la fraude financière, y compris la fraude à la carte bancaire, constituent des problèmes importants et croissants. Parmi les formes les plus courantes, on peut citer :

- Le vol physique de cartes et la fraude par chèque (impression de faux chèques ou vol de chèques).
- Le « dumpster diving » ou « fouille de poubelles » (vol de documents financiers dans les poubelles).
- La redirection de compte (remplissage frauduleux d'un formulaire de changement d'adresse).
- Le vol à l'arrachée d'un portefeuille ou d'un sac à main.
- La détention d'individus, y compris à leur domicile, pendant que des complices se rendent à un DAB à proximité avec leurs cartes de crédit et leurs codes PIN.

7.3.3 Transferts monétaires

De nombreuses organisations humanitaires ont adopté les transferts monétaires (TM) comme l'une de leurs principales modalités d'aide aux populations en situation de crise. Le mécanisme de transfert peut prendre différentes formes, telles que les virements électroniques ou les coupons, mais peut également impliquer la distribution d'espèces. Le mécanisme de distribution doit être adapté au contexte et tenir compte des contraintes pratiques et des risques de sécurité. Le recours aux banques et autres institutions financières permet de réduire les risques de sécurité liés aux transferts d'espèces.

En général, lors du transport et du stockage d'espèces dans le cadre d'activités de transferts monétaires, bon nombre des mesures d'atténuation énumérées précédemment s'appliquent. Une analyse des risques, des mesures d'atténuation et un suivi adéquats sont essentiels. Il est conseillé au personnel de procéder à une évaluation des risques programmatiques en tenant compte de tous les risques de sécurité pour les organisations, le personnel et les bénéficiaires de l'aide avant et pendant le transfert monétaire. Le personnel n'est pas le seul à courir des risques lorsqu'il manipule des espèces : il n'est pas rare que des groupes criminels ciblent et

volent les bénéficiaires de transferts monétaires. Les sites de distribution d'espèces sont également des lieux à haut risque et nécessiteront probablement des mesures de sécurité du site appropriées.

Il existe également des risques liés au stockage des données financières et des données relatives aux bénéficiaires. Certaines organisations utilisent des outils tiers de gestion des données pour stocker et gérer leurs données. Les risques pour la sécurité des données et les risques de réputation associés à l'utilisation de tels outils devront être évalués avant leur adoption.

Exemples d'atténuation des risques dans les transferts monétaires

En Afghanistan et en Somalie, des organisations ont utilisé avec succès des sociétés locales de transfert de fonds pour acheminer de l'argent vers des personnes vivant dans des zones reculées et peu sûres.

En Éthiopie, une organisation internationale a souscrit une assurance contre le risque de perte lors du transport d'espèces vers des projets situés dans des zones dépourvues de banques.

En Zambie, une organisation internationale a sous-traité la livraison dans des zones rurales reculées à un groupe bancaire et financier, qui a fait appel à des véhicules appartenant à une société de sécurité pour livrer les espèces, accompagnés par la police locale.

Le transfert d'espèces à grande échelle crée des risques institutionnels liés à la fraude, au détournement et à l'appropriation illicite. Il existe également des risques de non-conformité liés à la législation en matière de lutte antiterroriste et aux sanctions imposées aux donateurs dans les environnements à haut risque. Ces risques sont souvent considérés comme plus graves que s'ils concernaient l'aide en nature, et doivent être soigneusement pris en compte, anticipés, atténués et traités. Toute activité frauduleuse liée aux opérations d'une organisation humanitaire peut nuire gravement à sa réputation et avoir de graves conséquences (voir l'exemple ci-dessous).

Exemple de cas : Turquie

En 2015, une enquête menée par USAID a mis au jour une fraude impliquant plusieurs personnes, dont certaines travaillaient pour des ONG, dans le cadre de l'aide humanitaire transfrontalière fournie par la Turquie à la Syrie. L'enquête a révélé des cas de corruption majeurs dans le processus d'approvisionnement, notamment des pots-de-vin, des ententes illicites, des commissions occultes et des collusions entre le personnel logistique des ONG et des partenaires commerciaux corrompus. Au moins un membre du personnel d'une ONG internationale a fait l'objet de poursuites pénales et d'une procédure d'extradition, et les ONG concernées ont subi une grave atteinte à leur réputation auprès de leurs donateurs et du grand public. Le volume considérable et la rapidité des financements accordés aux ONG internationales en Turquie, qui étaient sous pression pour intensifier rapidement leurs opérations, ont contribué à l'insuffisance des contrôles financiers, des procédures de passation des marchés et des exigences en matière de vérification.

Source : Parker, B. (2018) 'US bans aid workers in Turkey-Syria scam' The New Humanitarian, 11 September (en anglais, « Les États-Unis interdisent les travailleurs humanitaires impliqués dans une escroquerie en Turquie et en Syrie » The New Humanitarian, 11 septembre) (www.thenewhumanitarian.org/news/2018/09/11/us-bans-aid-workers-turkey-syria-scam).

Informations complémentaires

Recommandations, outils et analyses

CICR (2021) *SAFE : Manuel de sécurité pour les humanitaires* (www.icrc.org/en/publication/4425-safe-manuel-de-securite-pour-les-humanitaires).

Cornish, L. (2017) 'New security concerns raised for RedRose digital payment systems' Devex, 28 November (en anglais, « Nouvelles préoccupations en matière de sécurité pour les systèmes de paiement numérique RedRose » Devex, 28 novembre) (www.devex.com/news/new-security-concerns-raised-for-redrose-digital-payment-systems-91619).

Mouvement international de la Croix-Rouge et du Croissant-Rouge (n.d.) « Modèle de matrice des risques liés aux TM ». Module 3, étape 1, sous-étape 4, boîte à outils des espèces en situations d'urgence (<https://cash-hub.org/guidance-and-tools/cash-in-emergencies-toolkit/all-toolkits/>).

Parker, B. (2018) 'US bans aid workers in Turkey-Syria scam' The New Humanitarian, 11 September (en anglais, « Les États-Unis interdisent les travailleurs humanitaires impliqués dans une escroquerie en Turquie et en Syrie » The New Humanitarian, 11 septembre) (www.thenewhumanitarian.org/news/2018/09/11/us-bans-aid-workers-turkey-syria-scam).

The CALP Network (n.d.) Ressources clés (www.calpnetwork.org/key-resources/).

7.4 Criminalité

Dans de nombreux contextes opérationnels, la criminalité est l'incident de sécurité le plus fréquent touchant le personnel humanitaire. Ce chapitre aborde l'éventail des menaces posées par les acteurs criminels, des délits courants et du harcèlement au crime organisé, en passant par les activités des gangs et le chevauchement avec les groupes armés non étatiques, et la manière dont les organisations humanitaires peuvent mieux comprendre et gérer les risques liés à la criminalité.

7.4.1 Types de criminalité et environnements criminels

La criminalité est universelle, et les organisations qui interviennent dans les crises humanitaires sont souvent confrontées à différents niveaux de criminalité. Si la plupart des attaques majeures visant les travailleurs humanitaires ont historiquement été perpétrées par des forces armées étatiques et des groupes armés non étatiques, dans de nombreux contextes, ce sont les acteurs criminels qui constituent la menace la plus importante. Une étude réalisée en 2015 a révélé que le taux d'homicides volontaires dans le monde dépassait celui des décès liés aux conflits.⁹⁹

Les activités criminelles peuvent être motivées par plusieurs facteurs, notamment les fortes inégalités, la concentration des désavantages et le chômage généralisé. Dans de nombreux contextes humanitaires, la criminalité augmente en raison de l'instabilité politique et de l'incapacité des gouvernements à faire respecter l'état de droit et à offrir des perspectives économiques intéressantes. Dans de nombreux contextes, la facilité d'accès aux armes peut contribuer à l'augmentation des crimes violents. La présence d'opérations d'aide humanitaire peut souvent attirer et favoriser la corruption et la criminalité. Outre les crimes opportunistes, les organisations humanitaires peuvent être la cible du crime organisé. Les groupes criminels profitent des changements dans l'environnement politique et économique pour étendre leurs activités illégales de recherche de revenus.

Les distinctions entre criminels, parties au conflit et autres acteurs politiques et économiques sont souvent très floues. Les groupes armés non étatiques et les autorités gouvernementales collaborent fréquemment avec les groupes criminels lorsque leurs intérêts convergent, et les mouvements rebelles se financent souvent par des activités illicites telles que le trafic de drogue. Toutefois, à des fins d'analyse et de gestion des risques, les organisations trouvent toujours utile de faire la distinction entre la criminalité à motivation économique et les risques de sécurité découlant des conflits armés, des « actes de terrorisme » et des troubles civils.

99 Secrétariat de la Déclaration de Genève (2015) *Global burden of armed violence 2015: every body counts* (en anglais, « Le fléau mondial de la violence armée en 2015: chaque corps compte »). Cambridge University Press (<https://doi.org/10.1017/CBO9781107707108>).

Voici quelques exemples de crimes à motivation économique que les organisations humanitaires doivent prendre en compte dans leur évaluation des risques et leurs stratégies d'atténuation :

- vol mineur ;
- cambriolage ;
- extorsion et corruption ;
- vol à la tire et vol à l'arraché ;
- agression ;
- braquage à main armée ;
- intimidation et extorsion ;
- détournement de voiture et vol de véhicule ; et
- enlèvement contre rançon, y compris les « enlèvements express », où les victimes sont retenues juste assez longtemps pour les forcer à retirer des fonds avec leur carte bancaire.

La plupart des crimes énumérés ci-dessus impliquent des actes de violence ou risquent de dégénérer en violence. Il est également important de garder à l'esprit que travailler dans un contexte de forte criminalité, où l'insécurité est omniprésente, peut avoir un impact considérable sur le niveau de stress et le bien-être général d'une personne. Cette situation se complique lorsque le personnel est originaire du pays et que les risques liés à l'environnement affectent également leur famille.

Les crimes « en col blanc », tels que le détournement de fonds et la fraude, sont également courants, mais moins directement liés au devoir de diligence et à la gestion des risques de sécurité physique (même s'ils peuvent avoir des répercussions pouvant entraîner des risques de sécurité) et relèvent généralement de la compétence des équipes financières, juridiques et de conformité d'une organisation.

► *Pour en savoir plus sur l'enlèvement, voir le chapitre 7.9.*

► *Pour plus de détails sur les risques dans la sphère numérique, voir le chapitre 6.2.*

La présence de groupes organisés cherchant à exercer un contrôle sur les zones locales et leurs habitants ajoute un niveau de risque supplémentaire. Le risque de harcèlement et d'extorsion peut être particulièrement difficile à atténuer, car les attaques sont persistantes plutôt qu'opportunistes, et les organisations peuvent se retrouver victimes de harcèlement, d'intimidation et d'extorsion répétés. La culture des gangs, les normes sociales et le désir d'obtenir un statut au sein du groupe créent souvent un environnement où la violence est attendue et récompensée. La menace qui pèse sur les acteurs humanitaires travaillant dans ces contextes nécessite une attention particulière et des mesures solides de gestion des risques de sécurité.

7.4.2 Considérations pratiques

Les bonnes pratiques en matière de gestion des risques de sécurité impliquent de comprendre le contexte et les risques de criminalité, puis de prendre des mesures pour atténuer ces risques et dissuader les délinquants potentiels. Ces mesures comprennent le renforcement de la protection physique des biens et de la sécurité du site générale afin de prévenir les vols et les effractions, ainsi que la formation du personnel sur les moyens de réduire l'exposition aux risques de criminalité. Certaines organisations ont investi dans une programmation de lutte contre la criminalité et la violence afin de réduire les risques pour l'ensemble de la communauté.

Compréhension du contexte

Tout comme pour l'insécurité liée aux conflits, des analyses contextuelles complètes et actualisées, des évaluations des risques et une cartographie des acteurs sont des outils essentiels pour gérer les risques liés à la criminalité.

Comprendre le contexte implique de déterminer si le risque provient d'une criminalité organisée, d'opportunité ou d'une combinaison des deux. La criminalité organisée est complexe et souvent liée à des intérêts politiques et économiques plus larges, contrairement à la criminalité d'opportunité, « courante » ou « de rue », qui est plus sporadique et conjoncturelle.

Les taux de criminalité sont généralement plus élevés dans les zones urbaines que dans les zones rurales, et les crimes violents ont tendance à se concentrer dans des zones spécifiques des villes, voire des quartiers.¹⁰⁰ De nombreux types de crimes violents et non violents présentent généralement un degré élevé de concentration spatiale et démographique. Étant donné que la violence urbaine engendre elle-même de plus en plus de crises humanitaires et que les actions humanitaires se multiplient dans les zones urbaines, l'analyse du contexte, la cartographie des acteurs clés et l'évaluation de base des groupes criminels (qui, quoi, où, quand et comment) devraient toutes faire partie de l'évaluation des risques.

La densité et la complexité des environnements urbains font que la dynamique de sécurité peut varier d'une petite zone à l'autre, même si celles-ci sont proches les unes des autres, ce qui nécessite des évaluations des risques plus détaillées que celles requises pour les zones rurales. Plusieurs organisations humanitaires en Amérique latine et dans les Caraïbes cartographient activement les gangs et les territoires qu'ils contrôlent, en faisant appel à des informateurs locaux pour maintenir les informations à jour. Les lignes peuvent changer tous les jours, voire se déplacer d'une rue à l'autre.

¹⁰⁰ Voir Muggah, R., Aguirre, K. et Chainey, S. (2017) 'Targeting "hot spots" could drastically reduce Latin America's murder rate' (en anglais, « Cibler les « points chauds » pourrait réduire considérablement le taux d'homicides en Amérique latine ») *Americas Quarterly* (<https://americasquarterly.org/article/targeting-hot-spots-could-drastically-reduce-latin-americas-murder-rate/>).

Les organisations ont tout intérêt à identifier des sources d'information fiables au sein de la communauté ou parmi d'autres acteurs locaux. Par exemple, les groupes criminels organisés peuvent transporter, livrer et distribuer des articles à des endroits précis et à des heures fixes. Avec l'aide des communautés locales, il est possible de savoir quand ces activités ont généralement lieu et ainsi d'éviter ces moments et ces lieux.

Les organisations doivent également évaluer l'impact de leur présence et de leur programmation sur les économies criminelles. Il ne suffit pas de supposer que, si elles n'interfèrent pas directement avec leurs intérêts, les acteurs criminels réagiront de la même manière. Dans les zones où le taux de criminalité violente est élevé, la « sensibilité à la criminalité » doit s'ajouter à la sensibilité aux conflits parmi les compétences et les approches d'une organisation.

► Voir le chapitre 4.1 pour plus de détails sur la manière de procéder aux analyses et aux évaluations.

Mesures d'atténuation des risques

Outre la réalisation d'une évaluation des risques et d'autres efforts visant à mieux comprendre le contexte, les organisations pourraient envisager certaines des mesures d'atténuation des risques pratiques présentées dans le tableau 22.

Tableau 22 Mesures pratiques visant à dissuader, prévenir et atténuer les risques criminels

Mesure	Description	Notes
Gestion des actifs et travail à distance	• Maintenir un inventaire à jour des actifs et mettre en œuvre des systèmes de suivi pour les articles de grande valeur. • Effectuer des audits réguliers. • Mettre en place des protocoles pour le travail à distance.	Le télétravail étant devenu plus courant, les organisations ont dû mettre en place des procédures régissant le transport et le stockage du matériel informatique et des autres équipements de travail. Des mesures simples, telles que ne pas transporter les ordinateurs dans des sacs prévus à cet effet, peuvent réduire considérablement les risques.

Mesure	Description	Notes
Signalement des incidents	• Veiller à ce que tous les incidents, même mineurs, soient signalés.	Des incidents criminels apparemment mineurs peuvent avoir de graves conséquences. Le vol d'un téléphone, d'un ordinateur ou d'un sac contenant des informations personnelles ou financières peut ouvrir la voie à des opportunités criminelles plus importantes. Le fait de signaler tous les cas de manière appropriée et de les analyser correctement peut faciliter la mise en place de mesures de réponse et de prévention pour l'avenir. Voir le chapitre 4.4 pour plus d'informations sur le signalement des incidents.
Mesures de sécurité physique, y compris le contrôle d'accès	• Prendre des mesures anti-braquage et anti-cambriolage dans tous les bureaux et établissements du projet, même ceux qui ne sont accessibles qu'au personnel de l'organisation. • Installer des mesures de sécurité physiques telles que des clôtures, des serrures, des alarmes et des caméras CCTV, selon les besoins. Effectuer des contrôles d'entretien réguliers. • Appliquer des mesures strictes de contrôle d'accès (par exemple, badges d'identification et registres des visiteurs) dans les bureaux, dans les entrepôts et sur les sites de distribution.	Pour plus de détails, voir le chapitre 7.2 sur la sécurité du site.

Mesure	Description	Notes
Procédures de gestion des espèces	- Mettre en place des procédures sécurisées de gestion des espèces, notamment en recourant aux services bancaires ou à des méthodes de transfert sécurisées lorsque cela est possible. - Réduire au minimum les transactions en espèces. - Éviter les routines liées aux paiements. - Préserver la confidentialité des informations.	<i>Pour plus de détails, voir le chapitre 7.3 sur la sécurité des fonds en espèces.</i>
Mesures de sûreté personnelle	Promouvoir les mesures de sûreté personnelle pour le personnel, telles que rester vigilant et conscient de son environnement, éviter les zones et les moments à haut risque, éviter les routines et les trajets prévisibles, garder ses effets personnels en sécurité, hors de vue et hors de portée, éviter d'afficher sa richesse et utiliser le système de binôme.	Toutes les recommandations doivent être adaptées au contexte, régulièrement mises à jour et communiquées au personnel. Par exemple, dans un contexte donné, il peut être conseillé au personnel de ne jamais être en possession d'espèces ou d'objets de valeur, alors que dans un autre contexte, il peut être plus risqué pour lui de ne pas avoir quelque chose à remettre à un agresseur.
Liaison avec les autorités	Maintenir un contact régulier avec les forces d'application de la loi locales et les autres autorités.	Partager les informations et solliciter leur aide si nécessaire et si cela est approprié. Il convient toutefois de noter que certaines autorités peuvent ne pas être des sources fiables d'informations et de protection dans des environnements où les acteurs étatiques et les criminels sont étroitement liés.
Mesures anticorruption	- Mettre en œuvre et appliquer des politiques anticorruption, notamment la vérification du personnel et des fournisseurs. - Mener des audits réguliers et des formations de sensibilisation.	–
Gestion des incidents	Être prêt à répondre à un incident, en apportant une aide immédiate aux personnes touchées ainsi que des soins à long terme.	<i>Voir le chapitre 4.4 pour plus de détails sur la réponse aux incidents.</i>

Mesure	Description	Notes
Bien-être du personnel	- Envisager et développer des structures et des interventions de prise en charge du personnel. - Apporter un soutien psychosocial après un incident, mais aussi plus régulièrement afin d'aider le personnel à gérer son stress.	Vivre dans des environnements où le taux de criminalité est élevé peut avoir des impacts stressants et des répercussions psychologiques négatives sur le personnel et sa famille, tout comme travailler dans des zones de conflit. Être victime d'un crime violent peut causer des traumatismes physiques et psychologiques durables. Voir le chapitre 5.4 sur le bien-être du personnel.
Mesures de sécurité numérique	- La criminalité est de plus en plus perpétrée en ligne, via les réseaux sociaux et d'autres moyens de communication numériques. - Mettre en œuvre des mesures de sécurité numérique, notamment des recommandations à l'intention du personnel sur la manière de se protéger en ligne.	Par exemple, en fonction des paramètres de confidentialité, les publications du personnel sur les réseaux sociaux peuvent être utilisées par des criminels pour identifier et cibler des victimes. Voir le chapitre 6.2 sur la sécurité numérique.

Harcèlement

Le risque de harcèlement par des acteurs criminels et autres constitue une menace importante pour les travailleurs humanitaires. Le harcèlement est un comportement abusif qui peut être physique ou verbal, et qui peut se produire en personne, par exemple aux points de contrôle ou lors de distributions, ou bien en ligne. La plupart des cas de harcèlement sont verbaux ; généralement, le harcèlement physique fait suite à un incident préalable de harcèlement verbal. Les raisons peuvent être diverses : il peut s'agir d'une tactique utilisée par des criminels pour faire pression sur le personnel afin qu'il se plie à leurs exigences, ou bien des membres de la communauté peuvent harceler le personnel en raison de la perception qu'ils ont du travail effectué par leur organisation. Les incidents doivent toujours être signalés, notamment parce qu'ils peuvent donner lieu à des menaces plus graves.

Plusieurs mesures peuvent contribuer à réduire le risque de harcèlement :

- Suivre l'opinion locale à l'égard de l'organisation et de son personnel, y compris sur les réseaux sociaux.

- Former le personnel à adopter un comportement qui n'attire pas une attention négative, par exemple en respectant et en s'adaptant aux coutumes locales, en discutant des activités et de la mission de l'organisation et en évitant les discussions sur la politique ou la culture locale.
- Veiller à ce que le personnel respecte les protocoles de sécurité, tels que les recommandations en matière de déplacements, éviter les foules importantes ou les environnements tendus, être en possession des documents appropriés, maintenir une présence en ligne sûre et signaler les incidents.
- Former le personnel à la conscience situationnelle, notamment à repérer les individus suspects et les situations susceptibles de dégénérer.
- Former le personnel à réagir face à différents types de harcèlement (par exemple, se retirer d'une situation et se rendre dans un endroit plus sûr, appeler à l'aide ou attirer l'attention).

À la suite d'un incident, les organisations peuvent discuter avec les parties prenantes concernées des raisons pour lesquelles le harcèlement a eu lieu et des moyens d'éviter que de tels incidents ne se reproduisent à l'avenir. Des mesures supplémentaires, telles que la suspension des activités ou des changements dans la répartition du personnel, peuvent être nécessaires. Le personnel touché peut également avoir besoin d'une prise en charge post-incident.

Au-delà des mesures de protection : la négociation

Tout comme pour les autres menaces pour la sécurité, les organisations doivent être conscientes des risques criminels dans les environnements où elles travaillent et comprendre comment leur propre présence et leur programmation peuvent interagir avec la dynamique criminelle et l'influencer. Si les organisations humanitaires ont développé des outils pour cartographier, sensibiliser et négocier avec les groupes armés et les détenteurs du pouvoir politique, elles adoptent rarement une approche aussi proactive avec les acteurs criminels.

Les organisations humanitaires ont tendance à éviter toute collaboration avec des groupes criminels en raison des risques juridiques, éthiques et réputationnels que cela pourrait entraîner, sans parler des risques de sécurité pour l'organisation qui deviendrait alors une entité connue d'un groupe susceptible de la prendre pour cible, elle ou son personnel. Entamer des négociations avec ces acteurs pourrait

être considéré comme de la complicité et entraîner des poursuites judiciaires. Il n'existe aucun cadre légal similaire aux Conventions de Genève qui fournisse une base et des directives fondées sur des principes permettant aux organisations de traiter avec les acteurs criminels comme elles le feraient avec les parties à un conflit. Il peut également être difficile d'identifier les personnes à contacter et celles qui ont le pouvoir de représenter le groupe.

Certaines organisations humanitaires ont réussi à négocier l'accès avec des acteurs criminels en s'inspirant des enseignements et des pratiques des groupes de développement communautaire qui œuvrent à réduire la violence au niveau local.

Les négociations avec les groupes criminels peuvent s'inspirer de celles menées avec les groupes armés non étatiques, dans le but d'atteindre des objectifs concrets tels que des garanties de sécurité pour certaines activités du programme ou l'accès à des lieux contrôlés par des groupes criminels. Comme pour les acteurs au conflit, le meilleur moyen d'y parvenir n'est souvent pas de faire appel à des principes humanitaires ou éthiques abstraits, mais d'identifier un intérêt du groupe criminel qui correspond aux objectifs humanitaires. Si les acteurs criminels sont originaires de la zone, ils peuvent avoir des enfants ou d'autres membres de leur famille et des liens sociaux avec la communauté qui pourraient bénéficier de la programmation d'aide. Ils peuvent également avoir intérêt à être considérés et traités comme l'autorité de contrôle.

Exemple de cas : Opérer en Haïti sous le contrôle des gangs

Une ONG internationale gérant des établissements de santé en Haïti a communiqué et négocié en permanence avec les chefs de gangs, les membres de la communauté, la police et d'autres autorités, soulignant l'importance de protéger les travailleurs et les établissements de santé afin qu'ils puissent soigner tout le monde, y compris les membres de gangs blessés. L'organisation a également conclu un accord confidentiel avec la police concernant l'accès à ses établissements.

Approches programmatiques de la gestion de risque lié à la criminalité

Outre les négociations directes, les organisations humanitaires se sont engagées dans des programmes d'intervention au niveau communautaire visant à réduire la criminalité et la violence. Par exemple, des organisations actives en Amérique latine et dans les Caraïbes ont mis en œuvre des projets axés sur la réduction de la criminalité et les alternatives pour les jeunes à risque.¹⁰¹ Ces approches nécessitent des analyses et des mesures de sensibilisation très localisées, voire rue par rue.

¹⁰¹ Voir, par exemple, Cure Violence Global, qui applique une méthodologie de santé publique pour lutter contre la violence : <https://cvg.org/about/>

Informations complémentaires

Recherche et analyse

CICR (2023) 'Organized Crime, IRR 923' (en anglais, « Crime organisé, CICR 923 »), juin (<https://international-review.icrc.org/reviews/irrc-no-923-organized-crime>).

GISF (2023) *Good practices, lessons learned, and the unique challenges affecting security risk management in urban humanitarian responses* (en anglais, « Bonnes pratiques, enseignements tirés et défis particuliers liés à la gestion des risques de sécurité dans les réponses humanitaires en milieu urbain ») (<https://gisf.ngo/resource/good-practices-lessons-learned-and-the-unique-challenges-affecting-security-risk-management-in-urban-humanitarian-responses/>).

Humanitarian Outcomes (2021) *Aid worker security report 2021. Crime risks and responses in humanitarian operations* (en anglais, « Rapport 2021 sur la sécurité des travailleurs humanitaires: risques liés à la criminalité et réponses apportées dans le cadre des opérations humanitaires ») (<https://humanitarianoutcomes.org/AWSR2021>).

Lucchi, E. (2013) *Humanitarian interventions in situations of urban violence* (en anglais, « Interventions humanitaires dans les situations de violence urbaine »). ALNAP (<https://alnapp.org/documents/4666/alnap-lessons-paper-urban-violence-1.pdf>).

Mohor, D. (2023) 'Gang violence in Latin America poses a challenge for the aid sector' (en anglais, « La violence des gangs en Amérique latine représente un défi pour le secteur humanitaire ») *The New Humanitarian*, 17 mai (www.thenewhumanitarian.org/analysis/2023/05/17/gang-violence-latin-america-challenge-aid-sector).

Muggah, R. (2017) 'A humanitarian response to Central America's fragile cities. The humanitarian consequences of violence in Central America' (en anglais, « Une réponse humanitaire aux villes fragiles d'Amérique centrale. Les conséquences humanitaires de la violence en Amérique centrale ») *Humanitarian Exchange* 69. Humanitarian Practice Network (HPN) (<https://odihpn.org/publication/humanitarian-response-central-americas-fragile-cities/>).

Muggah, R., Aguirre, K. et Chainey, S. (2017). 'Targeting "hot spots" could drastically reduce Latin America's murder rate' « Cibler les « points chauds » pourrait réduire considérablement le taux d'homicides en Amérique latine » *Americas Quarterly*, 9 mars (<https://americasquarterly.org/article/targeting-hot-spots-could-drastically-reduce-latin-americas-murder-rate/>).

Savage, K. et Muggah, R. (2012) *Urban violence and humanitarian action: Engaging the fragile city* (en anglais, « Violence urbaine et action humanitaire: s'engager dans la ville fragile »). ALNAP (<https://alnapp.org/help-library/resources/urban-violence-and-humanitarian-action-engaging-the-fragile-city/>).

Secrétariat de la Déclaration de Genève (2015) *Global burden of armed violence 2015: Every body counts* (en anglais, « Le fléau mondial de la violence armée en 2015: chaque corps compte »). Cambridge University Press (<https://doi.org/10.1017/CBO9781107707108>).

Ressources

Cure Violence Global (n.d.), « À propos de Cure Violence Global ». Page Web (<https://cvg.org/about/>).

Davis, J. et al. (2020) 'Module 2: Actor mapping and context analysis' in *Security to go: a risk management toolkit for humanitarian aid agencies* (en anglais, « Cartographie des acteurs et analyse du contexte dans La sécurité en pratique: boîte à outils de gestion de risque à l'attention des agences humanitaires »), 4e édition. GISF (www.gisf.ngo/resource/security-to-go/).

Igarapé Institute (n.d.a) *Humanitarian action in situations other than war* (en anglais ou en portugais, « Action humanitaire dans des situations autres que la guerre ») (HASOW) (<https://igarape.org.br/en/hasow/>).

Igarapé Institute (n.d.b) 'Homicide monitor' (en anglais, « Observatoire des homicides ») (<https://homicide.igarape.org.br/>).

7.5 Surveillance hostile

La surveillance hostile peut présenter un risque de sécurité important pour les travailleurs humanitaires et les populations vulnérables. Elle peut toutefois être négligée dans les efforts standard de gestion des risques de sécurité humaine, car il s'agit souvent d'un risque «invisible». S'appuyant sur l'expertise et l'expérience des défenseurs des droits humains et de la justice sociale, pour qui il s'agit d'une préoccupation constante, ce chapitre examine la surveillance hostile, ses implications pour le travail humanitaire et les réponses à y apporter, notamment les mesures de détection et de lutte contre la surveillance.

7.5.1 Comprendre la surveillance hostile

Alors que la «surveillance» implique un suivi systématique visant à recueillir des informations ou à exercer un contrôle, la «surveillance hostile» cible spécifiquement des personnes, des biens ou des propriétés dans le cadre d'une planification préalable à une attaque ou avec une intention malveillante. Il convient de noter que toutes les activités de surveillance ne sont pas secrètes: elles peuvent parfois être intentionnellement visibles (par exemple, à des fins d'intimidation).

Tableau 23 Distinction entre surveillance et surveillance hostile

Surveillance	Surveillance hostile
• Les activités de surveillance peuvent être menées par diverses entités, notamment des gouvernements et des sociétés privées, à des fins de sécurité, de collecte de renseignements ou de suivi. • La surveillance peut servir des objectifs légitimes tels que la sûreté publique ou l'application de la loi, mais elle peut également être utilisée à des fins malveillantes, en violation de la vie privée ou pour réprimer la dissidence. • On peut citer comme exemples la surveillance par les pouvoirs publics des communications, le suivi des réseaux sociaux et la surveillance des entreprises à des fins d'études de marché.	• La surveillance hostile est menée avec une intention hostile, menaçant directement la sûreté et sécurité des cibles. • Elle a pour but de recueillir des renseignements, d'identifier des vulnérabilités ou de planifier et d'exécuter des actions hostiles telles que le vol, l'espionnage ou des attaques physiques. • La traque, les activités de reconnaissance, l'utilisation de technologies de logiciels espions et la surveillance des mesures de sécurité afin d'identifier les faiblesses à exploiter sont des comportements typiques associés à la surveillance hostile.

La surveillance hostile en contexte humanitaire peut être exercée par divers acteurs, notamment des groupes armés non étatiques, des forces gouvernementales et des éléments criminels (voir l'encadré ci-dessous).

Acteurs susceptibles d'exercer une surveillance

- Les groupes armés non étatiques peuvent mener des opérations de surveillance hostiles afin de recueillir des renseignements, de surveiller les activités humanitaires et de cibler les travailleurs humanitaires.
- Dans les régions touchées par un conflit, les forces gouvernementales ou les agences de sécurité peuvent surveiller les organisations humanitaires afin de détecter toute infiltration éventuelle de groupes armés non étatiques au sein de la population locale.
- Des éléments criminels peuvent mener des activités de surveillance afin d'exploiter ou de perturber les opérations humanitaires dans un but lucratif ou pour servir leurs propres intérêts.

Les organisations doivent garder à l'esprit que les agences de renseignement nationales peuvent surveiller les acteurs humanitaires et que cette collecte d'informations peut influencer la manière dont les autres acteurs gouvernementaux nationaux perçoivent ces organisations et interagissent avec elles. Les régions en proie à des conflits armés ou à des crises humanitaires sont particulièrement exposées à ce type de surveillance.

7.5.2 Types de surveillance hostile

Cette section présente les types courants de surveillance hostile et les tactiques associées à chacun d'entre eux. Ces tactiques peuvent être utilisées individuellement ou combinées.

Surveillance physique

- **Surveillance dissimulée :** Des opérations de surveillances peuvent être menées par des individus ou des groupes afin d'observer et de suivre les déplacements de leurs cibles depuis une position dissimulée.
- **Filature :** Les acteurs hostiles peuvent prendre leurs cibles en filature, parfois à pied, afin de recueillir des informations sur leurs habitudes, leurs activités ou leurs vulnérabilités.

Surveillance technique

- **Écoute électronique :** Les acteurs hostiles peuvent utiliser des dispositifs d'écoute, des micros cachés ou des écoutes téléphoniques pour intercepter et surveiller les communications, y compris les conversations téléphoniques, les e-mails et les messages électroniques.

- **Surveillance vidéo :** Des caméras et des appareils d'enregistrement sont déployés pour surveiller les activités, les déplacements et les interactions des cibles dans divers lieux, tels que les espaces résidentiels, les lieux de travail ou les espaces publics.
- **Surveillance par GPS :** Des dispositifs de suivi par système de positionnement global (GPS) peuvent être installés discrètement sur des véhicules ou des effets personnels afin de suivre les déplacements des cibles et de recueillir des données de localisation.
- **Drones et satellites :** Les technologies avancées telles que les véhicules aériens sans pilote (drones) offrent des capacités de surveillance aérienne, permettant à des acteurs hostiles d'effectuer des missions de reconnaissance et de surveiller des activités à distance. Les satellites assurent une couverture de surveillance étendue, offrant des images à haute résolution et un suivi en temps réel de vastes zones géographiques.

Cybersurveillance

- **Piratage et logiciels malveillants :** Les acteurs hostiles peuvent utiliser des techniques de piratage, des logiciels malveillants/espions ou des attaques par hameçonnage pour obtenir un accès non autorisé aux appareils, réseaux ou comptes en ligne de leurs cibles, ce qui leur permet de surveiller leurs activités, de voler de l'information sensible et des contacts, ou de perturber leurs opérations.
- **Ingénierie sociale :** Les acteurs hostiles manipulent des individus ou des employés par la tromperie ou des tactiques psychologiques afin d'obtenir des informations ou d'accéder à des données sensibles, des mots de passe ou des systèmes.
- **Exploration de données et renseignement d'origine sources ouvertes :** Les acteurs hostiles peuvent collecter des informations à partir de sources accessibles au public, de plateformes de réseaux sociaux ou de bases de données en ligne afin de recueillir des renseignements sur leurs cibles, leurs affiliations ou leurs vulnérabilités.

► Voir le chapitre 6.2 sur les considérations relatives à la sécurité numérique.

Observation secrète

- **Déguisements et identités fictives :** Les acteurs hostiles peuvent adopter des déguisements ou créer de fausses identités pour se fondre dans leur environnement ou pour « interagir » avec leurs cibles de manière discrète, afin de mener une surveillance secrète sans éveiller les soupçons.
- **Espionnage et opérations d'infiltration :** Il s'agit d'infiltrer des organisations, des groupes ou des communautés cibles afin de recueillir des renseignements, d'établir des relations ou d'accéder à des zones ou à des informations d'accès restreint.

Exemple de cas : Yémen

Au Yémen, les travailleurs humanitaires ont fait l'objet d'une surveillance de la part des autorités locales et de groupes internationaux. Après les visites liées aux projets, les communautés cibles ont été approchées et interrogées sur l'organisation et son personnel. Cela affecte la façon dont les communautés cibles perçoivent l'organisation et peut nuire à l'image de celle-ci au niveau local.

7.5.3 Risques liés à la surveillance hostile

Les risques liés à la surveillance hostile dans le cadre de l'aide humanitaire vont au-delà des préoccupations immédiates en matière de sécurité. Fondamentalement, le risque dans ce contexte concerne l'incertitude qui entoure la sûreté et l'efficacité de l'acheminement de l'aide, englobant les menaces qui pèsent sur le personnel, les ressources et l'intégrité des opérations humanitaires. La surveillance hostile amplifie ces risques en introduisant un risque de compromission de la confidentialité, d'attaques ciblées et de perturbations opérationnelles.

Par exemple, l'interception de communications ou la compromission de systèmes de données peuvent exposer la population et les communautés locales à des représailles de la part d'acteurs hostiles. De même, les travailleurs humanitaires opérant dans des environnements où la surveillance hostile est répandue peuvent être exposés à des risques accrus de dommages physiques, d'enlèvements ou de harcèlement.

Le fait que les organisations humanitaires soient perçues comme des cibles légitimes pour la surveillance ou les attaques peut également dissuader les individus de demander de l'aide ou de coopérer avec les initiatives humanitaires, ce qui aggrave encore leur vulnérabilité et entrave leur accès aux services essentiels.

7.5.4 Comment répondre face à la surveillance hostile

Les acteurs humanitaires peuvent répondre efficacement aux tactiques de surveillance hostiles en étant vigilants et en mettant en place des mesures préventives. Pour ce faire, ils peuvent évaluer les risques liés à la surveillance, former leur personnel aux mesures préventives et mettre en œuvre des stratégies de détection et de lutte contre la surveillance. La détection de la surveillance implique une observation et une surveillance vigilantes de l'environnement immédiat afin d'identifier les menaces potentielles ou les activités suspectes avant qu'elles ne dégénèrent en atteintes à la sécurité. Les mesures anti-surveillance visent principalement à contrer et à dissuader les efforts de surveillance hostile.

Anti-surveillance et contre-surveillance

Il existe une distinction entre l'anti-surveillance et la contre-surveillance, cette dernière dépassant le cadre de la présente RBP et étant généralement utilisée par les militaires et les forces d'application de la loi ayant suivi une formation spécialisée et acquis des compétences particulières. La contre-surveillance est réactive et agressive, tandis que l'anti-surveillance est une mesure préventive. L'anti-surveillance repose sur des tactiques plus simples, telles que la modification des routines et des trajets, le déploiement de mesures de sécurité physique comme des caméras de surveillance et du personnel, et le renforcement des relations avec la communauté afin d'obtenir un soutien supplémentaire pour détecter et répondre à la surveillance. Plutôt que de s'appuyer sur des mesures de sécurité étendues ou la force, l'anti-surveillance peut être intégrée dans l'approche par acceptation d'une organisation, en mettant l'accent sur une interaction et une communication régulières avec les communautés locales.

Un premier point de départ peut être une conversation avec le personnel de sécurité ou des experts locaux/régionaux qui comprennent les menaces et les risques liés à la surveillance en fonction du lieu, du profil du personnel ou du programme. Cette étape peut être suivie d'une évaluation des risques complète. Une fois les risques liés à la surveillance identifiés, les organisations peuvent former leur personnel et mettre en place des mesures préventives.

► *Voir le chapitre 4.1 pour plus d'informations sur la manière de procéder à une évaluation des risques.*

Les défenseurs des droits humains et les militants utilisent fréquemment une combinaison des techniques anti-surveillance suivantes en fonction du contexte ; certaines d'entre elles peuvent également être utilisées par les organisations humanitaires pour détecter et contrecarrer la surveillance hostile.

Tableau 24 Exemple de techniques d'atténuation des risques

Technique	Détails
Identification de schémas	L'établissement de schémas de référence correspondant aux comportements et activités normaux au sein des locaux de l'organisation ou des sites du programme/projet permet de détecter les anomalies ou les écarts susceptibles d'indiquer des activités de surveillance.
Analyse des itinéraires	La variation régulière des trajets et des horaires des opérations du personnel humanitaire minimise la prévisibilité et réduit le risque d'être pris pour cible par la surveillance.
Observation du comportement	Former le personnel à observer et à signaler les comportements ou les individus suspects, tels que les personnes qui rôdent ou manifestent un intérêt inhabituel pour les activités de l'organisation, peut aider à détecter rapidement les menaces potentielles.
Contre-mesures techniques de surveillance	L'utilisation d'équipements de détection électroniques pour rechercher des dispositifs de surveillance cachés ou des signaux au sein des locaux de l'organisation permet d'identifier les tentatives de surveillance secrète.
Surveillance des communications	La surveillance des canaux de communication à la recherche d'activités inhabituelles ou non autorisées, telles que des tentatives d'accès non autorisées ou un trafic réseau inhabituel, peut aider à détecter les tentatives de surveillance électronique.
Hygiène de la communication numérique et protection des appareils	Éviter les réseaux Wi-Fi ouverts, utiliser des VPN et un gestionnaire de mots de passe, s'abstenir de partager des informations personnelles sensibles sur WhatsApp et d'autres plateformes de communication non sécurisées, vérifier les informations avant de les partager et rester vigilant face aux informations erronées.
Limitation des données	Prendre des mesures pour réduire la quantité de données que les individus ont sur leurs appareils et qui pourraient être utilisées à leur détriment en cas de violation, telles que les applications de rencontre, les profils sur les réseaux sociaux/en ligne et les coordonnées bancaires.
Sécurité opérationnelle	Mettre en œuvre des mesures de sécurité opérationnelle strictes, telles que la limitation de la diffusion de l'information sensible et l'application du principe du besoin de savoir.
Partenariats de collaboration	Établir des collaborations solides avec des experts en contre-surveillance ainsi qu'avec des organisations de justice sociale et de défense des droits humains, en tirant parti de leur expertise pour lutter contre le risque de surveillance hostile.

Des mesures d'atténuation peuvent être intégrées au plan de sécurité afin de faire face aux risques identifiés en matière de surveillance, et une formation peut être mise en place autour de ces mesures afin de permettre au personnel de contribuer activement aux efforts de détection de la surveillance. Le personnel concerné doit être sensibilisé et recevoir régulièrement une formation sur les menaces liées à la surveillance, les techniques de détection et les procédures de signalement. Il convient de noter que la sensibilisation à la surveillance hostile est généralement absente de la Formation «Sensibilisation en milieu hostile» (HEAT) standard ; il serait très utile d'y intégrer les principes fondamentaux de la sensibilisation à la surveillance.

La gestion du risque de surveillance hostile dans le domaine de l'aide humanitaire exige une approche multidimensionnelle qui englobe des stratégies de détection et d'anti-surveillance adaptées aux défis spécifiques du secteur. Pour faire face à une surveillance hostile, les acteurs humanitaires peuvent mettre en œuvre toute une série de stratégies, notamment l'identification de schémas, l'analyse des itinéraires, l'observation du comportement, les contre-mesures techniques de surveillance, la surveillance des communications et les mesures de sécurité opérationnelle. Promouvoir une culture de sensibilisation à la surveillance grâce à des sessions de formation régulières et à des actions de sensibilisation aide le personnel à contribuer activement aux efforts de détection de la surveillance. Des partenariats de collaboration avec des experts en contre-surveillance et des organisations de justice sociale/droits humains peuvent renforcer encore davantage l'efficacité des mesures anti-surveillance.

Informations complémentaires

Ressources sur la surveillance

Haggerty, K.D. et Gazso, A. (2005) 'Seeing beyond the ruins: surveillance as a response to terrorist threats' (en anglais, «Voir au-delà des ruines: la surveillance comme réponse aux menaces terroristes») *The Canadian Journal of Sociology* (<https://doi.org/10.2307/4146129>).

McCue, C. (2007) 'Surveillance detection – an overview' in *Data mining and predictive analysis* (en anglais, «Détection de la surveillance – aperçu général» dans *Exploration de données et analyse prédictive*) (www.sciencedirect.com/topics/computer-science/surveillance-detection).

7.6 Troubles civils

Les manifestations, les émeutes et autres rassemblements de masse ou perturbations, ainsi que la réponse des autorités à ces événements et les actes criminels ou d'extorsion qui en découlent, peuvent présenter un risque pour les personnes, les biens et les opérations humanitaires. Dans tout contexte opérationnel, mais en particulier dans les situations tendues et conflictuelles, des troubles civils peuvent éclater soudainement et dégénérer en violences et agressions. La violence peut être spontanée ou planifiée et provoquée. Les rassemblements pacifiques planifiés, tels que les événements politiques ou les manifestations, peuvent dégénérer de manière inattendue en troubles civils. De même, des tensions qui couvaient depuis longtemps peuvent soudainement dégénérer en violence à la suite d'un événement déclencheur. Les organisations humanitaires peuvent également être confrontées à des risques liés à des mouvements de foule incontrôlables, voire à des violences collectives, dans les lieux où se déroulent leurs programmes, tels que les sites de distribution et les camps de déplacés. Ce chapitre traite de certaines mesures d'atténuation possibles de ces risques, notamment la connaissance situationnelle, la préparation (procédures opérationnelles standards et plans d'urgence) ainsi que la formation et la sensibilisation aux mesures qui peuvent être prises.

7.6.1 Suivi et analyse de la situation

Bien qu'il soit difficile de les prévoir et de les suivre, il est important que les troubles civils et leurs différentes manifestations fassent partie intégrante de l'analyse des risques et des efforts de suivi réguliers.

- **Même s'il n'est pas possible de tout prévoir, il peut être utile d'identifier les déclencheurs potentiels.** Parmi les exemples, citons : les changements politiques et économiques, tels que la décision d'une puissance étrangère d'intervenir militairement ; une crise économique soudaine provoquée par les conditions du commerce international ; la décision d'un gouvernement de réduire les subventions sur des produits de première nécessité tels que la nourriture ou le carburant ; la décision de fermer un camp de réfugiés avant que les personnes ne soient prêtes à rentrer chez elles ; l'arrestation ou l'assassinat d'une personnalité importante ; la distribution d'aide humanitaire ; et les élections nationales/locales.
- **Une tension et une frustration croissantes peuvent souvent être détectées à l'avance.** Il est important de suivre de près les médias locaux et l'opinion publique et, si possible, cette tâche devrait être confiée à un membre du personnel ou à une unité spécifique. Cela pourrait inclure le suivi des actualités locales et des réseaux sociaux, le maintien du contact avec les communautés locales et les dirigeants, et l'évaluation du niveau d'acceptation.
- **L'analyse du contexte peut aider à prévoir les réponses possibles aux troubles civils.** Le contexte juridique et le déroulement des événements passés peuvent aider à prévoir la manière dont les autorités locales et d'autres acteurs peuvent réagir aux manifestations et autres rassemblements. Ces éléments peuvent être pris en compte dans les mesures de planification et de préparation.

Exemple de cas : Les réponses non violentes aux troubles civils peuvent néanmoins présenter un risque pour les opérations

La violence n'est pas le seul risque auquel sont confrontés les membres du personnel des organisations humanitaires en période de troubles civils. Un exemple de ce type s'est produit pendant la période électorale de 2018 en République démocratique du Congo, où les autorités ont coupé l'accès à Internet et aux services SMS dans tout le pays pendant 20 jours, ce qui a eu des répercussions sur les opérations humanitaires et la gestion des risques de sécurité.

Dans le cadre de leur suivi et de leur analyse, les organisations devraient se poser les questions suivantes.

- Y a-t-il eu des épisodes de troubles civils dans le passé ? Si oui, où ont-ils commencé et comment ont-ils évolué ? Y a-t-il un schéma qui pourrait se répéter ? Quelles ont été les principales causes ? Quel a été le niveau de violence ? Qui ou quoi était la cible de cette violence ?
- Quels facteurs peuvent déclencher des troubles civils ? Quelle forme pourrait prendre la violence ? Comment les autorités ont-elles réagi par le passé à des épisodes de troubles ?
- Qui sont les cibles du ressentiment local et quelle est la cause profonde de ces tensions ?
- L'organisation ou son personnel sont-ils exposés à un risque de troubles civils ? Comment atténuer les vulnérabilités ?
- Certains membres du personnel sont-ils plus exposés que d'autres, compte tenu de leur profil de risque individuel ?
- Certains projets ou types d'intervention sont-ils exposés à un risque, par exemple les projets jugés contraires à la culture ou à la religion locale, ou perçus comme soutenant l'une ou l'autre des parties belligérantes ?
- Comment les autorités réagissent-elles aux troubles civils aux niveaux national, local et communautaire ? Gaz lacrymogène ? Canon à eau ? Balles en caoutchouc ?
- Comment les autorités religieuses ou ethniques réagissent-elles aux troubles civils (droit et pratiques autochtones) ?

Parmi les questions à se poser concernant les activités et programmes propres à l'organisation, notons les suivantes :

- Quelles sont les attentes des habitants ?
- Attendent-ils quelque chose de l'organisation, par exemple une distribution ?
- L'organisation est-elle capable de gérer les attentes grâce à une communication claire avant toute activité programmatique ?

Exemple de cas : Un membre du personnel des Nations Unies tué lors d'une manifestation sans lien avec la situation en Afghanistan

Une organisation située à proximité de troubles civils peut être exposée à des risques de violence même si elle n'est pas la cible directe, comme le montre cet exemple impliquant l'ONU. En 2011, des manifestations ont eu lieu dans le nord de l'Afghanistan en réponse à l'incinération d'un Coran par un pasteur américain en Floride. La manifestation était prévue, mais la violence s'est propagée spontanément et de manière imprévisible. Lorsque les manifestants ont pénétré dans l'enceinte de l'ONU, les gardes ont ouvert le feu. Quatre gardes, trois membres du personnel de l'ONU et cinq manifestants ont été tués.

7.6.2 Planification et préparation

Les mesures de planification et de préparation peuvent comprendre les éléments suivants :

- **Procédures opérationnelles standards et plans d'urgence.** Les plans et procédures doivent couvrir tous les événements susceptibles de dégénérer en violences (manifestations prévues, rassemblements électoraux, événements sociaux et communautaires, distributions d'aide humanitaire et tout autre rassemblement de grande ampleur) ainsi que leurs conséquences (restrictions gouvernementales, vols, pillages et autres formes de violence). Chaque bureau devra probablement mettre en place ses propres procédures et protocoles de sécurité, notamment des plans d'urgence (plans d'hibernation, d'évacuation et de relocalisation) ; des listes de contacts à jour (accessibles à l'ensemble du personnel) ; des listes de contacts à jour pour les urgences médicales (hôpitaux et compagnies de transport aérien, par exemple) ; et des protocoles de sécurité de l'information (sauvegardes régulières des ordinateurs et fichiers/documents marqués à détruire et à emporter en cas d'évacuation, par exemple). Une fois les plans élaborés, le personnel doit être informé et formé aux procédures et aux attentes.

- **Prendre des mesures de protection.** Les mesures doivent se référer directement aux risques et menaces identifiés. Des pièces sécurisées peuvent être désignées et préparées dans chaque bâtiment, avec des kits d'hibernation, du matériel de communication, des trousseaux de premiers secours et des extincteurs. En cas de coupure de courant ou d'interruption des services de communication, des systèmes de secours pour l'alimentation électrique et les communications doivent être disponibles dans tous les bâtiments de l'organisation.

► Voir le chapitre 7.2 sur la sécurité du site.

- **Gestion des déplacements.** Si des troubles civils sont imminents, l'organisation peut envisager d'autres modalités de travail pour son personnel, telles que le travail à distance, la réduction des effectifs ou des restrictions de déplacement. Il convient également de déterminer quand et où des foules sont susceptibles de se rassembler et où elles se dirigeront (par quel itinéraire). Dans le cas d'un rassemblement politique, les itinéraires peuvent être clairement identifiés. Dans le cas d'une distribution, cela permettrait notamment de bien gérer les voies d'accès et de sortie des bénéficiaires de l'aide et du personnel, ainsi que de mettre en place des zones de réponse premiers secours.
- **Réponse de gestion de crise et d'incident.** L'organisation doit être prête à réagir rapidement en cas d'incident critique ou si des troubles civils déclenchent une réponse de gestion de crise organisationnelle.

► Voir le chapitre 4.4 pour plus d'informations sur la réponse aux incidents et la gestion de crise.

- **Formation sur les mesures clés que le personnel peut prendre pour assurer sa sécurité et celle de ses collègues.** Le personnel a bien sûr le droit de participer à des rassemblements et d'exercer ses droits en tant que citoyens, et les organisations peuvent dispenser une formation afin de garantir que, si ces événements deviennent dangereux, le personnel sache comment assurer sa sécurité. Cette formation peut porter sur la connaissance et la sensibilisation aux règles et procédures de sécurité, en particulier dans le cadre d'événements ou dans des lieux à haut risque, sur la manière de réagir face aux armes de contrôle des foules telles que les balles en caoutchouc, les matraques et les gaz lacrymogènes, et sur les conseils à suivre pour se mettre en sécurité et trouver un abri. Le personnel doit être conscient que sa sûreté prime sur les équipements, les locaux ou les magasins de l'organisation. Si possible, les équipements de valeur tels que les ordinateurs portables doivent être emportés et les équipements qui ne peuvent être emportés peuvent être mis hors service (par exemple, les véhicules). Les équipements sensibles qui ne peuvent être ni emportés ni mis hors service devront peut-être être détruits.
- **Visibilité.** Le personnel doit tenir compte de la visibilité de son organisation. Si une organisation est bien acceptée au niveau local et n'est pas directement visée, elle peut être protégée des foules si elle est clairement visible et identifiable. Cependant, si une organisation est la cible d'un mécontentement ou n'est pas bien connue localement, il serait préférable de retirer les logos des bureaux et des véhicules, et que le personnel fasse profil bas.

► Voir le chapitre 4.2 pour plus d'informations sur les mesures d'acceptation.

Recommandations en période d'élections

Connaître le contexte

Quel est le système politique et quel est le processus électoral? Qui sont les candidats et quel est leur programme politique? Quel est le calendrier électoral?

Connaître les différentes étapes de la période électorale et les risques associés

Les étapes peuvent souvent être divisées en plusieurs phases: pré-élections/campagne électorale, scrutin/vote, dépouillement des votes et proclamation des résultats, investiture du vainqueur et célébrations/manifestations qui l'accompagnent.

La durée de chacune de ces étapes peut varier d'un jour à plusieurs mois. Les risques associés à ces élections comprennent les incitations à la violence en ligne, les actes de violence ou les émeutes à proximité des bureaux de vote ou lors de rassemblements de masse, l'escalade et la perpétuation de violences ethniques ou sectaires, les affrontements entre groupes, les vols, le vandalisme et les attaques physiques contre des biens, ainsi que l'intimidation et le harcèlement d'individus, de groupes et d'organisations. Les autorités peuvent imposer des couvre-feux et des restrictions de circulation, restreindre l'accès aux médias, interrompre certains services (par exemple, Internet et l'électricité) et placer en détention le personnel des organisations. Il est notoire que des groupes politiques confisquent les actifs d'organisations à des fins électorales.

Mettre en œuvre des mesures d'atténuation

Les mesures d'atténuation peuvent comprendre:

- Des protocoles de gestion des déplacements, notamment les restrictions de circulation et les couvre-feux (en particulier autour des zones à haut risque et pendant certaines étapes de l'élection).
- Des recommandations à l'intention du personnel sur la manière de voter en toute sécurité (par exemple, ne pas se déplacer seul et rester vigilant).
- La sécurisation des bâtiments et des véhicules; la préparation du personnel à répondre aux incidents de vol, de harcèlement, d'intimidation et de détention, et l'augmentation du nombre de points de contrôle et de barrages routiers.

- L'adaptation des méthodes de travail pendant les périodes électorales (par exemple, le travail à distance).
- Des conseils au personnel sur la manière de se protéger dans un climat politique tendu (par exemple, éviter les discussions politiques (en personne et en ligne), ne pas porter de couleurs pouvant être associées à un parti politique et rester vigilant face aux groupes et aux discussions susceptibles de dégénérer en violences).

Le personnel peut être formé à la manière de communiquer avec les partis politiques et les autorités au cas où ceux-ci solliciteraient leur aide ou leurs services.

7.6.3 Au cours d'un épisode de troubles civils

Si des troubles civils éclatent avant que l'organisation ait eu le temps de prendre des mesures d'atténuation, ou si ces mesures échouent, il est impératif que le personnel suive la situation de près et soit prêt à prendre des mesures immédiates. Cela peut inclure les mesures suivantes :

- **Mettre en œuvre les plans d'urgence.** Par exemple, si des manifestants ou des émeutiers pénètrent dans un bâtiment, le personnel se réfugie immédiatement dans une pièce sécurisée.
- **Réévaluer les modes de transport et limiter les trajets, en particulier dans les zones à risque.** À titre d'exemple, il peut être plus sûr d'effectuer des trajets dans des véhicules locaux banalisés ou des taxis plutôt que dans de gros véhicules qui attirent l'attention.
- **Envisager de demander l'aide des autorités ou des forces de sécurité.** Les forces de sécurité seront probablement armées, ce qui devra être concilié avec la politique organisationnelle et le niveau de risque, en particulier si les acteurs de la sécurité sont impliqués dans le contrôle ou la dispersion des foules.
- **Veiller à ce que la communication entre les membres du personnel soit maintenue.**
- **Ouvrir éventuellement des voies de communication avec les leaders de la contestation.** Idéalement, toutes les négociations devraient être menées par du personnel ayant reçu une formation dans ce domaine.

Exemple de cas : Des organisations humanitaires attaquées lors de violences communautaires

En 2014, des bandes ont attaqué les bureaux et les résidences de plusieurs organisations humanitaires au Myanmar. Les attaques étaient alimentées par des tensions entre deux groupes religieux. Plusieurs bureaux et bâtiments ont été envahis, et le mobilier et les équipements ont été détruits. À la suite de cet incident, le personnel humanitaire a dû quitter ses bureaux, ce qui a perturbé les opérations. Cet incident montre à quel point les conflits peuvent rapidement dégénérer, créant des risques pour les organisations humanitaires présentes dans la zone. Un meilleur suivi du contexte local aurait permis d'identifier les risques potentiels avant l'incident, donnant ainsi aux organisations plus de temps pour préparer leur personnel et leurs installations.

7.6.4 Après un épisode de troubles civils

À la suite d'un incident, les organisations peuvent être amenées à :

- Réfléchir aux modalités de travail du personnel ; il peut être préférable pour lui de continuer à travailler à domicile et de faire profil bas jusqu'à ce que la situation se calme.
- Maintenir des mesures de sécurité renforcées jusqu'à ce que la situation se soit clairement apaisée et qu'il n'y ait plus de risque perceptible de nouvelle menace ou de représailles.
- Évaluer l'impact de l'événement sur le personnel concerné et lui apporter le soutien nécessaire – être prêt à aider les membres du personnel qui ont été relocalisés ou évacués.
- Réfléchir à la position de l'organisation en matière de relations publiques et aux messages qu'elle souhaite éventuellement diffuser ; il est utile d'évaluer en permanence l'opinion publique et les efforts de communication de l'organisation.
- Être prêt à faire face à une surveillance hostile à la suite d'un événement grave lié à l'organisation.
- Envisager de revoir le processus décisionnel et les actions de l'organisation ; tirer les enseignements des événements passés joue un rôle essentiel dans l'amélioration du système de gestion des risques de sûreté et sécurité d'une organisation et de son approche programmatique (par exemple, la manière dont les distributions sont menées).

Informations complémentaires

Ressources

International Foundation for Electoral Systems (IFES) (n.d.) ElectionGuide (en anglais) (www.electionguide.org/elections).

OSAC (2022) *Preparing for election violence (en anglais, « Se préparer à la violence électorale »)* (www.osac.gov/Content/Report/d7cd68ad-cee9-4386-b647-1e9f5c7745f6).

OSAC (2023) *Coups d'état: thinking through your organization's response (en anglais, « Coups d'état : réfléchir à la réponse de votre organisation »)* (www.osac.gov/Content/Report/cf60640f-7cob-4410-ae6f-228341955588).

Overseas Security Advisory Council (OSAC) (2019) *Surviving a protest (en anglais, « Survivre à une manifestation »)* (www.osac.gov/Content/Report/ob882e6f-co5f-4d1c-9601-15f4ad6883fc).

7.7 Violence sexuelle

La violence sexuelle est l'un des incidents les plus graves auxquels peuvent être confrontés les travailleurs humanitaires et peut avoir des conséquences à vie pour la personne survivante. Les organisations humanitaires ont un devoir de diligence de protection de leur personnel contre les menaces de cette nature, qu'elles proviennent de l'intérieur ou de l'extérieur de l'organisation. Bien que le rôle joué par le personnel de sécurité dans la gestion de ce type d'incident varie selon les organisations et doit probablement être géré en collaboration avec d'autres collègues (en particulier les RH et d'autres spécialistes), la gestion des risques de sécurité peut jouer un rôle important dans la prévention, la préparation et la réponse aux incidents. Ce chapitre présente les définitions et les mesures clés que les professionnels de la sécurité doivent prendre en considération, notamment la manière d'adopter une approche centrée sur la personne survivante lorsqu'ils interviennent dans ce type d'incident.

7.7.1 Définitions et champ d'application

La violence sexuelle désigne tout acte à caractère sexuel ou toute tentative d'obtenir un acte sexuel, non désiré ou imposé. La violence sexuelle peut être perpétrée par toute personne à l'encontre d'une autre (quelle que soit leur relation) en recourant à la force physique, à la coercition ou à des menaces. La violence sexuelle comprend les situations dans lesquelles les auteurs exploitent un environnement coercitif ou l'incapacité d'une personne à donner son consentement éclairé.¹⁰²

La frontière entre harcèlement sexuel et coercition ou agression peut parfois être difficile à établir, mais il est important de comprendre que ces incidents coexistent souvent et peuvent être considérés comme s'inscrivant dans un continuum allant d'actes mineurs (par exemple, des commentaires à caractère sexuel) à des actes graves (par exemple, le viol).¹⁰³ Voir la figure 12.

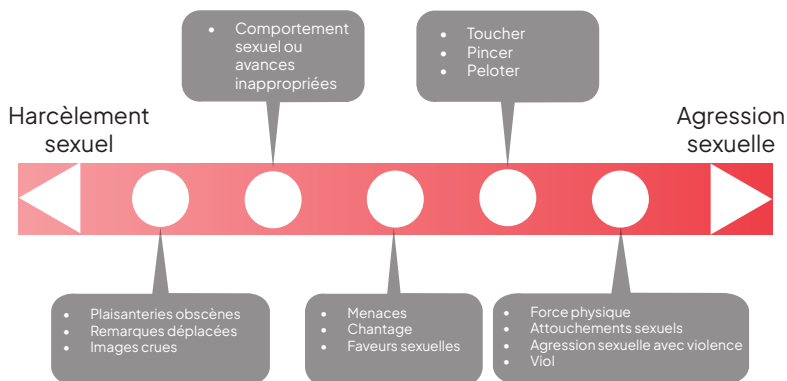
Dans le contexte du secteur humanitaire, la violence sexuelle peut prendre de nombreuses formes, par exemple :

- le ciblage individuel, y compris l'administration de drogues pour neutraliser la cible ;
- l'exploitation et abus sexuels, lorsque les travailleurs humanitaires sont contraints par des personnes en position de pouvoir (y compris d'autres travailleurs humanitaires) ; et
- la violence sexuelle comme arme de guerre ou d'intimidation, lorsque les travailleurs humanitaires sont pris pour cible par des acteurs armés.

¹⁰² European Interagency Security Forum (2019) *Gérer la violence sexuelle à l'encontre du personnel humanitaire : prévention, préparation, réponse et suivi* (<https://gisf.ngo/resource/managing-sexual-violence-against-aid-workers/>), pages 12 et 13.

¹⁰³ L'European Interagency Security Forum (2019) fournit une liste complète des formes de violence sexuelle et de leurs définitions.

Figure 12 Exemples dans le continuum



Source : European Interagency Security Forum (2019) *Gérer la violence sexuelle à l'encontre du personnel humanitaire : prévention, préparation, réponse et suivi* (<https://gisf.ngo/resource/managing-sexual-violence-against-aid-workers/>).

Note sur la violence fondée sur le genre

La violence fondée sur le genre est un « terme générique désignant tout acte préjudiciable commis contre la volonté d'une personne et fondé sur des différences (de genre) socialement attribuées aux hommes et aux femmes ». ⁱ Elle englobe diverses formes de violence, y compris, mais sans s'y limiter, la violence sexuelle. Ce chapitre traite spécifiquement des incidents à caractère sexuel, du harcèlement à l'agression, en raison de leur nature extrême et du rôle que jouent les professionnels de la sécurité dans l'atténuation de ces risques. Toutes les formes de violence fondée sur le genre doivent être prises en considération et traitées au sein d'une organisation, car elles peuvent être des précurseurs ou accompagner la violence sexuelle.

ⁱ Comité permanent interorganisations (IASC) (2015) *Directives pour l'intégration d'interventions ciblant la violence basée sur le genre dans l'action humanitaire* (<https://gbvguidelines.org/en/gbv-guidelines/>).

Travailler dans des environnements violents où l'état de droit est faible peut augmenter le risque de formes particulièrement traumatisantes de violence sexuelle. Le personnel peut également être victime de violence sexuelle dans le cadre domestique, et les organisations doivent discuter en interne de la manière et des circonstances dans lesquelles elles peuvent répondre à ce type d'événements afin d'assurer le bien-être du membre du personnel concerné.

Contrairement à d'autres incidents critiques dans le secteur humanitaire, la gestion de risque lié à la violence sexuelle reste entravée par la stigmatisation et les idées fausses sur ce qu'elle est et pourquoi elle se produit (par exemple, qu'elle ne touche que les femmes, que la plupart des auteurs sont des inconnus, qu'elle est consensuelle s'il n'y a pas eu de résistance physique, qu'elle est toujours extrêmement violente et que les personnes survivantes la signalent immédiatement après les faits). Il est impératif que le personnel chargé de gérer les incidents de cette nature soit formé et puisse bénéficier du soutien d'experts.

Termes et domaines de travail connexes

Les termes et domaines de travail suivants présentent des similitudes et méritent d'être définis plus clairement.

La protection contre l'exploitation et les abus sexuels (PEAS) est un domaine d'intervention qui vise à protéger les populations touchées contre l'exploitation et les abus sexuels dans le cadre des opérations de réponse humanitaire. Pour plus d'informations, voir : <https://psea.interagencystandingcommittee.org/>

La sauvegarde englobe les efforts visant à protéger toute personne (y compris le personnel, les bénévoles et les bénéficiaires de l'aide) contre toute forme de préjudice, d'abus et d'exploitation. Pour en savoir plus, voir : <https://safeguardingsupporthub.org/>

Sur le plan conceptuel, la violence sexuelle à l'encontre des travailleurs humanitaires et la PEAS relèvent de la sauvegarde, bien que les définitions et la manière dont ces domaines d'activité interagissent dans la pratique puissent varier d'une organisation à l'autre. L'important est que ces domaines d'activité collaborent et se soutiennent mutuellement lorsque cela est approprié.

7.7.2 Considérations relatives aux risques

Les considérations relatives aux risques liés à la violence sexuelle peuvent être regroupées en quatre domaines :

- les considérations relatives aux risques individuels ;
- le profil des auteurs ;
- les facteurs de risque organisationnels ; et
- les facteurs de risque externes.

Les stratégies d'atténuation des risques doivent viser à traiter ces quatre domaines. Le personnel de sécurité peut veiller à ce que les procédures accordent la priorité non seulement à la gestion du comportement du personnel, mais aussi à la dissuasion des auteurs potentiels et à la prise en compte d'autres facteurs de risque. Par exemple, les organisations peuvent se concentrer sur la formation du personnel à la réduction de leur exposition au risque, tout en mettant en place des mesures visant à dissuader les auteurs, en s'attaquant aux conditions organisationnelles et externes qui contribuent à la violence sexuelle (lorsque cela est possible) et en atténuant les risques dans ces environnements.

Considérations relatives aux risques individuels

Si certains profils sont particulièrement exposés au risque de violence sexuelle, celle-ci peut toucher n'importe qui, et les mesures de préparation et de réponse doivent en tenir compte. L'identité intersectionnelle d'une personne peut influencer sur sa vulnérabilité à la violence sexuelle, notamment son genre, sa race, son orientation sexuelle, son handicap, ainsi que son pouvoir relatif et ses choix. Les travailleurs humanitaires nationaux sont particulièrement à risque, surtout dans les environnements violents ou les sociétés patriarcales. Ces membres du personnel bénéficient également souvent de moins de garanties que leurs homologues internationaux, par exemple en matière d'accompagnement lors de leurs trajets domicile-travail.¹⁰⁴ Une enquête menée pour le compte de l'ONU a révélé que les « non-salariés » (tels que les consultants, les stagiaires et les bénévoles) sont également particulièrement vulnérables et moins enclins à signaler les incidents.¹⁰⁵

Le sous-signallement des incidents de violence sexuelle est omniprésent pour diverses raisons, notamment la stigmatisation sociale, l'absence de canaux de signalement sûrs et les environnements juridiques et culturels restrictifs. Ces obstacles au signalement touchent aussi bien les hommes que les femmes, et dans de nombreux contextes où les organisations humanitaires interviennent, ils peuvent être particulièrement difficiles à surmonter pour les personnes qui s'identifient comme LGBTQI+.

¹⁰⁴ Stoddard, A., Harvey, P., Czwarno, M. et Breckenridge, M. (2019) *Aid Worker Security Report 2019* (en anglais, « Rapport 2019 sur la sécurité des travailleurs humanitaires »). *Speakable* (en anglais, « Verbaliser »): *Addressing sexual violence and gender-based risk in humanitarian aid* (lutter contre la violence sexuelle et les risques liés au genre dans l'aide humanitaire). Humanitarian Outcomes (<https://humanitarianoutcomes.org/AWSDR2019>).

¹⁰⁵ Cronin, E.A. et Afifi, A. (2018) *Review of whistle-blower policies and practices in United Nations system organizations* (en anglais, « Examen des politiques et pratiques en matière de dénonciation dans les organisations du système des Nations Unies »). Corps Commun d'inspection, ONU (<https://digitallibrary.un.org/record/1643065?ln=en&v=pdf>).

► Pour plus d'informations sur les risques liés à l'identité, voir le chapitre 1.2.

Profil des auteurs

Les auteurs peuvent être externes ou internes à l'organisation, par exemple des membres du personnel, des sous-traitants et des personnes appartenant aux forces armées, à des groupes armés non étatiques et à des communautés locales. Si les auteurs sont plus souvent des hommes, d'autres genres peuvent également être auteurs ou complices.

Les auteurs peuvent être motivés par des facteurs totalement indépendants des caractéristiques personnelles ou du comportement de leur cible, tels que des circonstances personnelles, notamment les antécédents familiaux, la personnalité et le comportement (par exemple, la toxicomanie), un environnement organisationnel permissif et des pairs sexuellement agressifs. Les auteurs de ces actes s'appuient souvent sur des occasions et des alliés pour commettre leurs agressions, ainsi que sur des facteurs environnementaux, culturels et sociétaux, notamment les déséquilibres de pouvoir, les justifications culturelles ou sociétales, le sentiment d'avoir des droits et un climat d'impunité.

Dans les cas de violence sexuelle plus grave, les auteurs peuvent s'en prendre à leurs cibles par la coercition, l'incapacité (par exemple, en utilisant des drogues ou de l'alcool) ou la force (en utilisant des armes ou la force physique). Les auteurs ont souvent besoin :

- de moyens : le pouvoir, le soutien et les ressources nécessaires pour commettre leur infraction ;
- d'un accès : un accès psychologique ou physique à leur cible ;
- de connaissances : la connaissance de la vulnérabilité ou de la sensibilité de leur cible ;
- de capacités : leurs capacités à commettre leur infraction ;
- d'une motivation : la volonté de commettre leur infraction ; et
- d'une opportunité : des circonstances ou des moments propices à la commission de leur infraction.

Facteurs de risque organisationnels

En raison de la gêne suscitée par les discussions sur la violence sexuelle et les dynamiques de genre au sein des organisations, ce type de risque n'est pas encore suffisamment abordé dans les organisations humanitaires. Le manque d'attention directe et explicite accordée à cette question peut exacerber le risque en contribuant à créer des cultures organisationnelles permissives. La prévention des incidents graves peut dépendre de la rapidité avec laquelle on répond aux incidents mineurs. Tolérer des cas mineurs de violence sexuelle ou d'autres formes de ciblage, telles que le harcèlement, les intimidations et les blagues indécentes, peut encourager des formes plus graves de violence, y compris la violence sexuelle (ce phénomène est parfois décrit comme une pyramide de la violence¹⁰⁶). Les auteurs profitent d'environnements permissifs et peuvent être influencés par leurs pairs agressifs. Une organisation doit veiller à ce qu'aucun environnement dans lequel

106 Pour un exemple de pyramide de la violence, voir European Interagency Security Forum (2019).

son personnel travaille ne soit un lieu où l'hostilité, sexuelle ou non, soit la norme. Les événements mineurs doivent être pris au sérieux, car ils peuvent être les signes avant-coureurs d'incidents plus graves.

La culture organisationnelle, notamment l'inclusion, joue un rôle important dans la décision de signaler et de traiter les incidents de violence sexuelle. Dans la communauté humanitaire, les cultures organisationnelles peuvent souvent valoriser la ténacité et les attitudes machistes (en particulier dans des contextes patriarcaux), ce qui peut dissuader davantage le signalement. Il est conseillé aux organisations d'avoir des directives claires sur ce qu'est une infraction à signaler, car cela peut aider le personnel à comprendre quand un comportement n'est pas acceptable et à se sentir habilité à agir.

Tout le personnel doit être formé et se sentir capable de lutter contre les attitudes qui peuvent favoriser la violence sexuelle, par exemple en décourageant les propos indécents. Les managers et les points focaux jouent un rôle particulièrement important dans le fait que le personnel se sente libre de faire part de ses préoccupations. Grâce aux efforts de communication et de sensibilisation, le personnel de sécurité peut également faire évoluer la culture organisationnelle.

Lorsque la culture dans un contexte opérationnel est plus permissive à l'égard de la violence sexuelle, il est particulièrement important que les dirigeants des organisations communiquent et démontrent par leurs actions que ce qui peut être accepté en dehors du bureau ne sera pas toléré par la culture organisationnelle en son sein.

Enquêtes sur le climat ou consultations ciblées

Les consultations auprès du personnel peuvent aider les organisations à mieux comprendre leur culture organisationnelle et à déterminer si les attitudes et les actions au sein de l'organisation sont révélatrices d'un environnement propice à la violence sexuelle. Elles peuvent prendre la forme d'« enquêtes sur le climat », parfois menées par une entité externe, qui se concentrent sur les perceptions des comportements acceptables au sein de l'organisation. Des consultations plus ciblées posent des questions spécifiques concernant le harcèlement, l'intimidation et les préoccupations de groupes particuliers de personnel, par exemple les employées ou les personnes qui s'identifient comme LGBTQI+.

Facteurs de risque externes

Les analyses contextuelles peuvent aider à identifier les facteurs externes qui influent sur le risque de violence sexuelle, par exemple :

- Des niveaux élevés d'agression sexuelle dans l'environnement général.
- Un État défaillant ou fragile ou toute autre forme d'effondrement de l'ordre public.
- Une impunité généralisée, y compris un système de justice pénale qui tolère la violence sexuelle ou en favorise les auteurs.
- Un conflit actif ou une zone militarisée.
- Une société conservatrice ou patriarcale.
- Des déséquilibres de pouvoir, par exemple entre les hommes et les femmes ou entre les groupes ethniques.

Ces facteurs de risque environnementaux favorisent la violence sexuelle à l'encontre des populations locales et, par extension, à l'encontre des personnes travaillant pour les organisations humanitaires. Les sites présentant un risque plus élevé peuvent inclure les zones où opèrent des groupes armés, les prisons et les centres de détention, les hôtels et les logements du personnel, ainsi que les postes-frontières et les points de contrôle. Il peut y avoir des moments où le risque est accru, par exemple après la tombée de la nuit, lors d'événements très fréquentés et lorsque des acteurs armés entrent ou sortent d'un lieu. Les assaillants peuvent commettre des agressions sexuelles sur les résidents lors des raids dans les complexes. La violence sexuelle peut également se produire lorsque le personnel humanitaire est détenu ou retenu en captivité.

7.7.3 Atténuation des risques : prévention et préparation

De nombreuses mesures d'atténuation des risques de violence sexuelle se concentrent sur la réglementation du comportement du personnel. Si la vulnérabilité d'un individu à la violence sexuelle dépend en partie de l'interaction entre son identité intersectionnelle (qui est la personne), son comportement, sa localisation, son rôle et son organisation (sa vulnérabilité intersectionnelle), il arrive parfois qu'une personne ne puisse rien faire pour atténuer le risque inhérent d'être prise pour cible. Comme pour toute autre menace, des mesures doivent être prises aux niveaux individuel et organisationnel afin de réduire les risques.

Ce qui suit est un bref aperçu de mesures d'atténuation des risques. Pour des recommandations plus détaillées, consulter le guide du GISF (anciennement European Interagency Security Forum) *Gérer la violence sexuelle à l'encontre du personnel humanitaire*.¹⁰⁷

Gouvernance

Des politiques, des systèmes et des mécanismes doivent être mis en place pour prévenir les incidents de violence sexuelle touchant le personnel, s'y préparer et y

¹⁰⁷ European Interagency Security Forum (2019).

répondre. Ces mesures peuvent inclure une politique de tolérance zéro à l'égard de la violence sexuelle et un code de conduite organisationnel qui fait explicitement référence à toutes les formes d'inconduite sexuelle. Ces instruments organisationnels doivent être transparents et appliqués de manière cohérente, et inclure des recommandations sur leur mise en œuvre pratique.

Les bonnes pratiques organisationnelles incluent l'élaboration de déclarations de politique claires sur ce que les personnes survivantes peuvent attendre de l'organisation à la suite d'un incident. Une organisation internationale a constaté que le fait de s'assurer que chaque incident d'agression sexuelle et de harcèlement sexuel grave était signalé à l'équipe de direction exécutive contribuait considérablement à la redevabilité.

Rôles et responsabilités

La manière dont le personnel de sécurité est impliqué dans la gestion des risques de violence sexuelle varie selon l'organisation. Le personnel de sécurité doit idéalement être équipé pour : identifier les facteurs de risque ; mettre en œuvre des mesures d'atténuation des risques respectueuses et inclusives ; communiquer de manière appropriée sur les menaces ; faire face aux comportements inappropriés ; reconnaître les signes d'un environnement hostile ; agir en tant que témoins actifs (voir l'encadré ci-dessous) ; et élaborer des plans d'urgence centrés sur la personne survivante qui donnent la priorité à la sûreté, à la confidentialité, au respect et à la non-discrimination.

Témoin actif

Alors qu'un simple spectateur peut être témoin d'une situation sans intervenir, un témoin actif, appelé «upstander» au sein de l'ONU, reconnaît les situations préjudiciables ou injustes et intervient pour soutenir les personnes touchées et prévenir tout préjudice supplémentaire. Ces témoins actifs sont dotés des connaissances et de la confiance nécessaires pour agir, que ce soit en intervenant directement, en cherchant de l'aide ou en apportant leur soutien aux personnes touchées, tout en assurant leur propre sécurité et celle des autres.

Au sein de l'ONU, une «approche upstander» à un événement implique les étapes suivantes :

- remarquer l'événement ;
- interpréter la situation ;
- prendre ses responsabilités ;
- décider d'aider ; et
- intervenir.

Le personnel des ressources humaines joue souvent un rôle central dans l'élaboration des politiques et des pratiques relatives à la violence sexuelle, notamment en élaborant et en diffusant le code de conduite, en créant des politiques en matière de devoir de diligence envers les personnes survivantes et le personnel, en guidant les processus de réponse confidentiels et en menant des enquêtes internes. Ils effectuent également des vérifications d'antécédents destinées à prévenir le recrutement de prédateurs sexuels et met en place des procédures disciplinaires.

Un certain nombre de rôles peuvent être plus directement impliqués dans la gestion des risques de violence sexuelle et le soutien aux personnes survivantes.

- **Premier intervenant.** Le premier point de contact pour une personne survivante de la violence sexuelle, chargé d'assurer sa sûreté immédiate, de lui apporter un soutien émotionnel, de l'aider à préserver les preuves et de faciliter l'accès à des soins médicaux. Il peut s'agir d'un membre du personnel formé ou d'un collègue de confiance. Étant donné que tous les membres du personnel peuvent être des premiers intervenants, il est de bonne pratique de s'assurer qu'ils ont accès à des recommandations sur les premiers secours psychologiques.
- **Accompagnant de la survivante.** Un accompagnant de la survivante agit comme le principal point de contact entre la personne survivante et l'organisation. Cette personne doit avoir reçu une formation et des recommandations pour offrir un soutien émotionnel, maintenir la confidentialité et aider la personne survivante à s'orienter dans les protocoles de réponse de l'organisation. Il est recommandé aux organisations de laisser les personnes survivantes choisir leur accompagnant.
- **Point focal sauvegarde/médiateur.** Certaines organisations ont mis en place un point focal sauvegarde ou un médiateur afin d'offrir au personnel un moyen confidentiel de signaler leurs préoccupations. Il est utile d'avoir des points focaux masculins et féminins.
- **Enquêteurs internes.** Les personnes chargées de mener une enquête interne sur des allégations de violence sexuelle doivent être totalement indépendantes de la personne survivante, de l'auteur présumé et de leurs hiérarchies respectives.

Intégration, briefings et formation

Tous les membres du personnel, où qu'ils se trouvent, sont exposés au risque de violence sexuelle car ce risque existe dans tous les pays et peut même être perpétré en ligne. Les organisations doivent veiller à ce que tous les membres du personnel, quels que soient leur rôle ou leur lieu de travail, soient informés de la nature et des formes de violence sexuelle auxquelles ils peuvent être confrontés dans le cadre de leur travail. Ils doivent être informés des menaces en ligne, du risque que représentent les drogues du viol et du fait que les auteurs peuvent être des personnes qu'ils connaissent, voire des collègues. Le personnel peut également être sensibilisé aux facteurs contextuels et autres qui peuvent rendre certains profils plus vulnérables que d'autres. Cela permet au personnel de :

- comprendre ce que l'organisation a mis en place pour réduire le risque ;
- comprendre les procédures et règles qu'il doit suivre ;
- utiliser ces informations pour identifier leur propre profil de risque personnel (qui peut être unique en raison de leur identité intersectionnelle); et
- obtenir des conseils auprès des points focaux et travailler avec leur organisation pour réduire les risques.

► Voir le chapitre 1.2 sur les risques liés à l'identité.

Les briefings d'intégration et d'orientation du personnel couvrent les politiques, les mécanismes de signalement et de redevabilité en relation avec la violence sexuelle. Afin de respecter les normes culturelles, l'organisation peut choisir d'organiser des briefings et des formations réservés aux hommes ou aux femmes. En tenant compte des attitudes locales, l'organisation peut adapter son approche afin d'encourager des discussions ouvertes sur des questions sensibles.

La formation à la sécurité permet de fournir des informations importantes sur les risques de violence sexuelle, notamment sur la manière dont le personnel peut réduire ces risques et répondre en cas d'incident. Cela peut inclure des recommandations sur la conduite culturellement appropriée, quand et comment signaler les incidents ou préoccupations, comment se déplacer (par exemple dans des groupes plus importants), comment établir des limites personnelles et quels endroits, heures et groupes éviter. Tout le personnel bénéficie d'une formation sur les risques locaux et les stratégies de prévention, sur leurs rôles et responsabilités spécifiques en matière de réponse à la violence sexuelle, et sur l'importance de protéger la confidentialité lorsque des incidents sont signalés. Il peut être judicieux de fournir des recommandations sur la collecte et la préservation des preuves au cas où la personne survivante déciderait de porter plainte.

L'intégration et la formation sont l'occasion de promouvoir une culture organisationnelle positive, dans laquelle l'organisation fait clairement savoir que toute forme de violence est inacceptable et que personne ne doit jamais être blâmé s'il est la cible de violence sexuelle.

Certaines organisations forment leur personnel à l'intervention des témoins, qui peut être une stratégie efficace pour prévenir la violence sexuelle. La formation peut inclure des éléments interactifs tels que des jeux de rôle et des discussions adaptés au contexte spécifique.¹⁰⁸

Évaluations des risques inclusives et plans de sécurité

Une évaluation des risques inclusive doit identifier les lieux, les moments et les situations à haut risque, tout en tenant compte de facteurs tels que l'âge, le sexe, la nationalité, la race, l'orientation sexuelle, le handicap, l'aspect physique et le

¹⁰⁸ Pour plus de recommandations, voir European Interagency Security Forum (2019), Outil 2, intervention des témoins (p.100).

comportement, qui influent sur la vulnérabilité individuelle. Une évaluation des risques complète doit intégrer les facteurs de risque individuels, organisationnels et externes. Cette évaluation doit porter à la fois sur les menaces externes et internes, en reconnaissant que les auteurs peuvent être des employés, et comprendre les profils des auteurs potentiels.

L'analyse des risques peut s'appuyer sur diverses sources, notamment les systèmes de signalement interne, les consultations confidentielles auprès du personnel et de la communauté locale, ainsi que les informations fournies par les points focaux d'autres organisations humanitaires ou de défense des droits humains. La discrétion et la sensibilité aux normes culturelles et sociales peuvent être nécessaires lors de la collecte d'informations.

Les directives et les procédures opérationnelles standards relatives à la réponse à la violence sexuelle doivent être claires et facilement accessibles au personnel. Elles doivent éviter soigneusement toute formulation suggérant que la victime est « en partie responsable » et accorder une attention égale à la compréhension et à la dissuasion des auteurs potentiels.

Les plans d'urgence organisationnels (tels que l'évacuation ou la relocalisation du personnel affecté) doivent également tenir compte des risques de violence sexuelle et des moyens de soutien disponibles à court et à long terme. Il peut être utile de discuter avec le personnel de divers horizons culturels des mesures de prévention, des protocoles et du soutien qu'ils jugent les plus appropriés. Ces consultations garantissent que l'organisation réagit efficacement dans chaque contexte et ne cause pas davantage de préjudice.

Stratégies d'atténuation basées sur l'identité

Dans certaines circonstances, les procédures de sécurité peuvent différer pour certains groupes du personnel si l'évaluation des risques indique que leur profil personnel les expose à un risque plus élevé de violence sexuelle. Les questions clés suivantes peuvent être prises en considération pour éviter toute discrimination injustifiée.

- L'évaluation des risques tient-elle compte de ses caractéristiques personnelles et indique-t-elle clairement les risques différenciés selon les profils du personnel (ce qui implique de prendre en considération toutes les caractéristiques d'identité et leur intersectionnalité, notamment le sexe, l'orientation sexuelle, l'ethnicité et les handicaps visibles et invisibles) ?
- Les personnes concernées ont-elles été informées de leur risque accru (en reconnaissant qu'elles peuvent déjà en être conscientes) et ont-elles eu l'occasion de discuter des mesures d'atténuation des risques ?

- Des formes moins extrêmes d'atténuation des risques pourraient-elles être mises en œuvre? Une interdiction générale ou le retrait d'un groupe d'employés est une stratégie courante d'atténuation des risques, mais d'autres mesures peuvent être plus acceptables et mieux adaptées aux circonstances. Des consultations avec le personnel concerné peuvent aider à trouver d'autres options de gestion des risques de sécurité.

► Voir le chapitre 1.2 - *Approche de sécurité centrée sur la personne pour une analyse plus détaillée sur les risques différenciés.*

Intégrer les risques de violence sexuelle dans les procédures de sécurité

Les procédures de sécurité doivent tenir compte de tout risque accru de violence sexuelle.

- **Sécurité du site.** Les hôtels et les logements utilisés par le personnel doivent offrir une protection maximale contre les intrus. Dans certains cas, l'évaluation des risques peut mettre en évidence la nécessité de loger le personnel particulièrement à risque, comme les femmes, avec des collègues ou dans des zones jugées plus sûres.
- **Sécurité des déplacements.** Le personnel doit être informé des procédures de déplacement appropriées et de la manière de se protéger et de protéger les autres contre le risque de violence sexuelle pendant les déplacements. Les membres du personnel considérés comme exposés à un risque élevé (international ou national) peuvent être accompagnés de leur domicile à leur lieu de travail dans un véhicule de l'organisation. Le personnel à risque peut se déplacer en groupe ou accompagné d'autres personnes, pendant et en dehors des heures de travail. Dans un environnement particulièrement risqué, le personnel à risque ne devrait pas être laissé seul, même pour de courtes périodes.
- **Sécurité de l'information.** Les coordonnées personnelles des membres du personnel ne doivent pas être affichées à l'extérieur de leur domicile ni figurer dans l'annuaire téléphonique. Des mesures de sécurité doivent être mises en place pour protéger le personnel contre toute révélation indésirable concernant son identité et ses déplacements, tant en ligne que hors ligne.

- *Pour en savoir plus sur les mesures de sécurité du site, voir le chapitre 7.2.*
- *Pour davantage de recommandations sur la sécurité des déplacements, voir le chapitre 7.1.*
- *Pour en savoir plus sur la sécurité de l'information et des communications, voir le chapitre 6.1.*

Plan d'urgence

Prestataires de services

Créer un réseau de prestataires de services compétents, notamment des professionnels des soins médicaux et psychologiques, dans tous les contextes opérationnels, peut garantir un soutien rapide aux personnes survivantes de la violence sexuelle (qui devrait idéalement être apporté dans les 24 heures suivant l'incident). Ce réseau doit faire l'objet d'une évaluation approfondie afin de déterminer sa réactivité et ses capacités. Il convient également d'évaluer l'attitude envers les personnes survivantes afin de s'assurer qu'elle ne cause pas davantage de préjudice en rejetant la responsabilité sur la victime ou en tenant des propos inappropriés.

Tout le personnel doit avoir accès à des soins médicaux d'urgence, notamment à la contraception d'urgence, à des kits de prophylaxie post-exposition au VIH et à d'autres médicaments visant à réduire le risque de transmission de maladies. Dans les zones reculées, les kits de prophylaxie post-exposition au VIH peuvent être stockés par l'ONU, le CICR et/ou des ONG médicales. Si les kits de prophylaxie post-exposition au VIH et autres médicaments sur prescription ne sont pas immédiatement disponibles auprès des établissements médicaux ou d'autres organismes de la zone, les organisations peuvent s'assurer qu'ils sont disponibles dans leurs locaux et peuvent être administrés sous surveillance médicale (car les effets secondaires doivent être surveillés), ou que la personne survivante peut être immédiatement transportée vers un endroit où ils sont disponibles. Les organisations doivent pré-identifier des lieux sûrs pour les examens médicaux et les soins, et mettre en place des procédures d'orientation. Si la personne survivante choisit de ne pas signaler l'incident, elle a la possibilité de se rendre dans une clinique privée connue et de confiance.

Les organisations soumises à des restrictions particulières (par exemple, contre la contraception) devraient en informer leur personnel de manière plus générale.

- *Voir le chapitre 5.4 pour plus d'informations sur le bien-être du personnel.*
- *Voir le chapitre 5.5 pour plus d'informations sur les considérations médicales et de santé.*

Logistique

Les dispositions logistiques comprennent un moyen de transport fiable pour la personne survivante et l'accompagnant, ainsi que des dispositions pour la relocalisation ou le rapatriement confidentiels des personnes survivantes, si nécessaire.

Assurances

Avec le consentement de la personne survivante et lorsque des polices d'assurance ont été souscrites, il est essentiel d'informer rapidement l'assureur de l'incident afin de garantir que la personne survivante puisse avoir accès à un soutien médical et psychologique. Le délai de notification peut varier en fonction des accords existants avec le ou les assureurs, et les organisations doivent connaître les informations minimales requises par les assureurs pour mettre en place un soutien. Des protocoles doivent être établis pour garantir la confidentialité.

Il est également utile de conclure des accords clairs avec les assureurs concernant les types spécifiques de couverture disponibles pour les incidents de violence sexuelle. Cela implique notamment de bien comprendre l'étendue des soins médicaux, du counseling psychologique et des autres formes de soutien psychosocial, ainsi que toute aide juridique éventuelle. Veiller à ce que ces domaines soient explicitement couverts par la police d'assurance peut éviter des retards et des complications lorsqu'un incident se produit.

► Voir le chapitre 5.4 pour plus d'informations sur l'assurance.

Considérations juridiques

Les organisations doivent être prêtes à conseiller les personnes survivantes sur les options qui s'offrent à elles, notamment sur les implications d'un signalement aux autorités locales et sur les définitions juridiques de la violence sexuelle dans ce contexte. Il convient d'établir des relations avec des professionnels juridiques locaux de confiance qui peuvent apporter une aide immédiate en cas de besoin. Pour plus d'informations sur les considérations juridiques, voir la section 7.7.4 ci-dessous.¹⁰⁹

Signalement et lancement d'alertes

Des mécanismes solides et confidentiels de signalement et de lancement d'alertes facilitent non seulement la réponse aux incidents, mais peuvent également dissuader les auteurs potentiels. Le personnel responsable doit veiller à ce que ces mécanismes soient confidentiels et accessibles à tous les membres du personnel, indépendamment de leur position et de leur langue. Le personnel doit être encouragé à signaler même les incidents mineurs. Les canaux de signalement de la violence sexuelle peuvent être distincts des mécanismes de signalement des autres incidents de sécurité en raison de la nécessité d'une confidentialité supplémentaire. Le nombre de signalements non officiels d'incidents de violence sexuelle (par exemple via les

¹⁰⁹ Pour des recommandations plus détaillées, voir European Interagency Security Forum (2019), Outil 3, questionnaire sur l'environnement juridique (p.102).

services médicaux, les services de counseling et les enquêtes) peut être considérablement plus élevé que le nombre d'incidents signalés par les canaux officiels.

Il est recommandé aux organisations de proposer à leur personnel plusieurs canaux de signalement confidentiels, y compris la possibilité de signaler des préoccupations de manière anonyme, formelle et informelle. Les employés d'un bureau peuvent hésiter à s'exprimer si tous les rapports sont transmis à un seul cadre supérieur, qui peut être l'auteur des faits ou un complice de celui-ci. Pour parer à ce risque, une ONG internationale a fait appel à un prestataire de services tiers spécialisé dans l'éthique et la conformité afin d'héberger un site web dédié aux lanceurs d'alerte, sur lequel il est possible de signaler des problèmes d'éthique ou des inconduites impliquant le personnel de l'organisation.

Les points focaux sauvegarde/médiateurs désignés peuvent aider les membres du personnel qui ont besoin de plus d'informations, qui ne savent pas si un incident est suffisamment grave pour justifier une plainte officielle ou qui craignent les répercussions d'un signalement.

Enfin, les organisations doivent faire preuve de transparence quant à la suite donnée à un signalement, notamment en ce qui concerne les enquêtes et les mesures disciplinaires qui peuvent être prises et la manière dont la personne ayant fait le signalement peut être impliquée dans le processus. Les personnes ayant fait le signalement doivent recevoir régulièrement des informations sur la suite donnée à leur signalement. Des protocoles de partage d'informations strictement nécessaires peuvent être suivis, limitant ainsi l'accès à ces informations à un nombre minimal de personnes. Il peut également être judicieux de conserver un registre sécurisé de toutes les communications et décisions relatives à la réponse.

Exemple de cas : Défaillances dans la protection d'un lanceur d'alerte

En 2009, une travailleuse humanitaire bénévole a été assassinée au Bénin après avoir signalé à son directeur de pays que l'un des sous-traitants de l'agence abusait sexuellement des membres de la communauté locale. L'enquête sur cet incident a révélé que des failles dans la confidentialité avaient pu permettre de révéler l'identité de la lanceuse d'alerte à l'auteur présumé des faits, qui avait des relations personnelles au sein de l'organisation. Cette affaire met en évidence de nombreuses lacunes, notamment l'absence de mécanismes de signalement sûrs et confidentiels, de procédures d'enquête rigoureuses et de mesures de sécurité pour protéger les lanceurs d'alerte.

Source: Peace Corps Office of Inspector General (n.d.). *Ressources: Kate Puzey, Volunteer Protection Act of 2011 (en anglais, «Loi de 2011 sur la protection des bénévoles»)* (www.peacecorps.org/resources/resources-kate-puzey-volunteer-protection-act-2011).

Lorsqu'ils enregistrent des comptes rendus d'incident dans le système de gestion des informations sur les incidents de l'organisation, les personnels de sécurité devront réfléchir à la manière de garantir la confidentialité lorsque les noms et d'autres détails doivent être saisis dans des champs obligatoires. Certaines organisations conservent ces types de comptes rendus d'incident séparément pour des raisons de confidentialité. Les signalements sont nécessaires à la gestion des risques de sécurité et à l'analyse des risques, mais ils doivent être mis en balance avec la sûreté, le bien-être psychologique et le droit à la vie privée de la personne survivante.

Recrutement, enquêtes et mesures disciplinaires

Une sélection rigoureuse des candidats à l'emploi, comprenant une vérification approfondie de leurs antécédents et de leurs références dans plusieurs pays, peut empêcher les auteurs connus de violence sexuelle de passer d'une organisation humanitaire à une autre. Au cours des dernières années, plusieurs initiatives de sauvegarde ont été mises en place pour aider les organisations dans ce domaine.¹¹⁰

Les organisations doivent disposer d'une procédure officielle pour enquêter sur les signalements de violence sexuelle, avec des mesures adaptées si l'auteur présumé est employé par l'organisation. Les allégations à l'encontre de membres du personnel doivent faire l'objet d'une enquête interne et, le cas échéant, de mesures disciplinaires. Si la personne survivante souhaite engager des poursuites judiciaires, les autorités peuvent être saisies. Les auteurs, leurs complices et ceux qui leur ont permis d'agir doivent être tenus pour redevables par l'organisation. Afin de dissuader toute nouvelle infraction, le non-respect de la politique et des enquêtes doit entraîner des mesures disciplinaires.

7.7.4 Réponse

Il est essentiel de répondre rapidement aux incidents de violence sexuelle afin d'assurer la sûreté et le bien-être des personnes touchées. La réponse d'une organisation dépendra de diverses circonstances, notamment le moment où l'incident s'est produit, les souhaits de la personne survivante, la gravité de l'incident et les risques pour les autres. Voici quelques points généraux à garder à l'esprit au moment de répondre :

- Les personnes survivantes de la violence sexuelle peuvent signaler les incidents immédiatement, quelques jours, semaines, mois ou années après les faits. Les facteurs qui influencent le moment où un incident est signalé comprennent la sûreté, la culture et l'impact psychologique et émotionnel de l'événement sur la personne survivante. Les organisations doivent traiter tous les signalements comme une priorité, quelle que soit la date à laquelle l'incident a eu lieu.
- Les organisations doivent être prêtes à informer les personnes survivantes de toute considération culturelle et juridique pertinente. Dans certaines régions, le signalement d'actes de violence sexuelle peut entraîner des préjudices supplémentaires pour la personne survivante en raison des lois locales et des pratiques culturelles.

¹¹⁰ Par exemple, the Misconduct Disclosure Scheme (en anglais, le schéma de la révélation des inconduites »): <https://misconduct-disclosure-scheme.org/>

- Les risques de retraumatisation, d'automutilation et de suicide sont très élevés. Il est impératif que les intervenants soient formés pour apporter un soutien adéquat et préserver la confidentialité.

Les bonnes pratiques soulignent la nécessité de veiller à ce que les réponses aux incidents de violence sexuelle soient guidées par une prise en charge centrée sur la personne survivante, qui respectent autant que possible ses souhaits, du moment que ceux-ci ne mettent pas en danger sa sécurité, celle de ses collègues ou celle de l'organisation. Une approche centrée sur la personne survivante tient compte de ses besoins et de ses préférences, et vise à la protéger contre la stigmatisation, la discrimination, les représailles ou d'autres conséquences préjudiciables. Cette approche vise à créer un environnement favorable dans lequel les droits, la sûreté et la confidentialité de la personne survivante sont respectés et prioritaires, et dans lequel la personne survivante est traitée avec dignité et respect. Elle vise à soutenir le rétablissement de la personne survivante en lui permettant de choisir le soutien et la prise en charge dont elle a besoin, de prendre des décisions à propos du signalement facultatif et de décider si elle souhaite participer à une enquête et, le cas échéant, de quelle manière. Cette approche se distingue de celle dirigée par la personne survivante, qui laisse à cette dernière tout le pouvoir décisionnel, même si ses décisions peuvent l'exposer, elle ou d'autres personnes, à un risque de préjudice.

- *Pour plus de détails sur l'approche centrée sur la personne survivante, voir le chapitre 5.4 sur le bien-être du personnel.*

Communiquer avec la personne survivante

Comme pour tous les événements traumatisants, la manière dont les individus et l'organisation interagissent avec un la personne survivante joue un rôle important dans la guérison et le rétablissement. Le soutien psychologique et émotionnel peut venir des collègues et des amis, via des réseaux de soutien par les pairs et d'interactions empreintes de compassion. Toute communication avec la personne survivante doit viser à :

- la faire se sentir en sécurité ;
- lui donner le sentiment de contrôler la situation ;
- lui donner le sentiment d'être crue et écoutée ; et
- lui donner le sentiment que l'organisation prend l'incident au sérieux.

La communication ne doit pas :

- sous-entendre que la personne survivante est responsable ou la juger de quelque manière que ce soit ;

- minimiser ce qu'elle a vécu ;
- lui imposer une compagnie ou un autre type de soutien ;
- lui dire comment elle doit agir ou se sentir, ou normaliser sa réponse ; ou
- lui mettre la pression pour qu'elle prenne des décisions ou agisse.

Réponse initiale

Lorsqu'une personne est victime de violence sexuelle, en particulier d'un incident grave, le timing est essentiel. Il est souvent utile de hiérarchiser les réponses dans un calendrier de réponse identifiant les besoins immédiats, à court terme et à long terme. Il est également important de reconnaître que chaque expérience est différente. Certaines personnes peuvent avoir besoin d'un soutien médical et psychosocial immédiat, tandis que d'autres peuvent demander un soutien plus tard. Il n'y a pas de « bonne » voie à suivre. Cependant, en ce qui concerne certains aspects de la réponse, tels que les soins médicaux et le signalement, le timing peut jouer un rôle plus important.¹¹¹

En fonction de la gravité, la structure de gestion des incidents de l'organisation peut devoir être activée, y compris les fonctions de soutien aux familles et à la communication. Le premier intervenant, les points focaux responsables ou l'équipe de gestion de l'incident (pour les incidents graves) superviseront généralement tout ou partie des activités de réponse initiale décrites ci-dessous. En raison de leur nature sensible, de nombreuses organisations peuvent mettre en place une équipe de réponse aux incidents distincte chargée de traiter les cas de violence sexuelle.

► Voir le chapitre 4.4 pour plus de détails sur la gestion des incidents critiques.

- **Sûreté et sécurité.** La priorité absolue est d'assurer la sûreté immédiate de la personne survivante et des autres personnes à risque, tout en préservant la confidentialité afin de protéger la personne survivante.
- **Soins médicaux.** Des soins médicaux d'urgence, notamment le traitement des blessures, des infections et la prévention des grossesses, doivent être prodigués dès que possible avec le consentement de la personne survivante. Les personnes survivantes d'agression sexuelle peuvent avoir besoin d'une contraception d'urgence, d'un traitement prophylactique contre les infections sexuellement transmissibles, d'une prophylaxie post-exposition au VIH et de médicaments pour d'autres maladies telles que l'hépatite B. Tous ces traitements doivent être administrés dès que possible après l'incident.
- **Soins psychosociaux.** Un accès immédiat à un soutien psychosocial approprié doit être proposé.

111 L'European Interagency Security Forum (2019) présente un cadre de réponse détaillé décrivant les mesures clés que le personnel responsable peut prendre à différents moments.

- **Identifier l'accompagnant de la survivante.** Les organisations peuvent demander à la personne survivante qui elle souhaiterait comme accompagnant, ou lui proposer l'aide d'un accompagnant de la survivante formé par l'organisation.
- **Liaison avec la famille.** Avec le consentement de la personne survivante, sa famille peut être informée par l'intermédiaire d'une personne de contact désignée, dans le respect de directives strictes de confidentialité.
- **Lieu.** Les personnes survivantes peuvent avoir besoin d'être hébergées dans un lieu sûr et confidentiel, à proximité de personnes pouvant leur apporter un soutien, et d'être relocalisées ou évacuées si nécessaire.
- **Compte rendu d'incident.** L'incident doit être signalé par les voies appropriées, tout en sauvegardant la sûreté et la confidentialité de la personne survivante.
- **Soutien et recommandations.** L'organisation doit clairement indiquer qu'elle croit le récit de la personne survivante et donner des recommandations claires sur les étapes suivantes, en assurant une communication et un soutien continus tout au long du processus.¹¹²

À plus long terme, un soutien administratif et logistique supplémentaire peut être nécessaire, comme l'organisation d'une aide financière pour la personne survivante et le personnel de soutien, l'organisation d'un transport privé pour les personnes impliquées dans le processus de réponse, la suspension des tâches professionnelles du personnel concerné, la définition d'une stratégie de communication à l'intention des collègues au sujet de l'absence de la personne survivante et la mise en place de suivis réguliers afin de répondre aux besoins et préoccupations des personnes survivantes. Les assureurs peuvent également devoir être informés, avec le consentement de la personne survivante.

Il peut être nécessaire d'offrir un soutien à d'autres membres du personnel, tels que les témoins et l'équipe au sens large. Soutenir les personnes survivantes de la violence sexuelle est stressant et exigeant. Les personnes qui s'en chargent peuvent bénéficier d'un soutien émotionnel et psychosocial, notamment en prenant des pauses ou en s'éloignant temporairement.

112 Pour des conseils plus détaillés à l'attention des premiers intervenants, voir European Interagency Security Forum (2019) *Outil 5, directives à l'attention des accompagnants des survivantes* (p.111).

Risques de violence sexuelle en ligne

Les formes de violence sexuelle en ligne constituent une préoccupation croissante pour les organisations humanitaires. Bien que tout le monde puisse être pris pour cible, les femmes et les personnes LGBTQI+ sont touchées de manière disproportionnée, ce qui nécessite des mesures de prévention et de réponse adaptées. Les risques comprennent le harcèlement, la traque et la cybertraque, l'extorsion de faveurs sexuelles et le partage non consenti d'images intimes.

- Voir le chapitre 6.2 pour plus de détails sur les risques numériques et les mesures d'atténuation.

Considérations relatives à la réponse

Les points focaux ou l'équipe de gestion de l'incident peuvent être amenés à aborder certaines des considérations plus complexes en matière de réponse qui sont abordées dans la section suivante.

Confidentialité et communications

Les organisations doivent gérer de manière proactive la communication en cas d'incident grave de violence sexuelle en établissant des protocoles internes et externes clairs, en tenant compte des implications du partage d'informations à propos de l'incident et de l'auteur, et en garantissant la confidentialité et la sûreté de la personne survivante. Parallèlement, les organisations doivent respecter le droit de la personne survivante à s'exprimer si elle le souhaite et lui fournir des conseils et un soutien, notamment en lui donnant accès à des points focaux formés qui peuvent l'aider à gérer les risques et les conséquences potentiels d'une révélation publique.

Si l'incident est rendu public, une gestion des médias peut s'avérer nécessaire.

- Voir le chapitre 4.4 pour plus de détails sur la gestion des médias.

Signalement à la police et procédures judiciaires

Les organisations doivent s'assurer qu'elles ont une compréhension approfondie du cadre juridique dans lequel elles opèrent, en particulier en ce qui concerne les incidents de violence sexuelle, et qu'elles ont accès à des avocats locaux pour leur fournir des conseils et un soutien en cas d'incident.¹¹³

L'organisation peut assister la personne survivante dans toutes les procédures judiciaires et juridiques qu'elle choisit d'engager. Cela comprend l'accompagnement de la personne survivante pour signaler l'incident à la police, le soutien si un interrogatoire par la police est nécessaire, et la garantie de sa sûreté et de son bien-être pendant toute la procédure de collecte de preuves. La collecte de preuves

¹¹³ Pour des recommandations plus détaillées, voir European Interagency Security Forum (2019) *Outil 3, questionnaire sur l'environnement juridique* (p.102).

n'engage pas la personne survivante à intenter une action en justice, mais lui permet de conserver cette option pour l'avenir. Le simple fait de signaler un incident à la police peut être une expérience traumatisante, même dans les meilleures circonstances.

Les organisations peuvent également avoir besoin de trouver une représentation juridique appropriée pour la personne survivante. Le conseiller juridique de l'organisation peut aider à préciser les procédures et les délais de signalement, car l'obtention de documents officiels peut s'avérer cruciale si la personne survivante décide par la suite de porter plainte ou de poursuivre son traitement. La décision de poursuivre en justice appartient à la personne survivante, qui doit se sentir soutenue et habilitée à faire un choix éclairé.

Plus généralement, les organisations doivent comprendre les exigences légales en matière de signalement des incidents de violence sexuelle à la police dans le pays, y compris toute obligation de signalement, les implications pour la personne survivante et l'auteur présumé, et s'ils doivent rester dans le pays après le signalement. Certains ressortissants étrangers pourraient choisir de ne pas signaler les incidents à la police si cela les obligeait à rester dans le pays jusqu'à la fin du procès (qui pourrait prendre plusieurs années). Dans certains pays, les personnes survivantes peuvent être accusées d'adultère ou de fornication si elles ne peuvent pas prouver qu'elles ont été agressées. Cela peut entraîner des sanctions pour la personne survivante plutôt que pour l'auteur des faits. Les organisations doivent également tenir compte de l'impact des poursuites légales sur les auteurs présumés, en particulier s'il s'agit de membres du personnel.

Si des poursuites judiciaires sont engagées, elles auront généralement lieu dans le pays où l'incident s'est produit et peuvent nécessiter la collecte de preuves médicales. Le risque d'un nouveau traumatisme est immense dans ces circonstances, et il est conseillé à l'organisation de se préparer à aider les personnes survivantes à naviguer en toute sécurité dans ces procédures, par exemple en identifiant à l'avance des établissements médicaux de confiance et en se renseignant sur les attentes locales en matière de collecte de preuves médico-légales. Certains établissements médicaux qui traitent des personnes survivantes peuvent également signaler automatiquement les cas à la police.

Dans certains cas, l'accent peut être mis moins sur la question de savoir si l'incident a eu lieu que sur celle de savoir s'il était consensuel, ce qui peut poser différents défis.

Exemple de cas : Une deuxième expérience traumatisante

Il n'est pas rare qu'une personne survivante subisse un second traumatisme en raison d'un traitement insensible de la part de la police. Dans un cas, une femme membre du personnel humanitaire international a fait l'objet d'une agression sexuelle alors qu'elle travaillait à l'étranger. Immédiatement après l'incident, personne dans l'organisation ne savait quoi faire. Le lendemain, elle a été envoyée seule à son ambassade pour signaler l'incident.

L'ambassade l'a envoyée à la police locale accompagnée de l'agent de sécurité de l'ambassade, un ressortissant national. Une fois au poste de police, quatre policiers armés l'ont interrogée, lui posant des questions détaillées sur l'incident. Lorsqu'elle a hésité dans ses réponses, ils l'ont accusée de mentir. Pendant l'interrogatoire, d'autres policiers ont fait des allées et venues par curiosité. Les policiers chargés de l'interrogatoire ont insisté pour qu'elle leur montre ses blessures avant de la laisser quitter le poste. Ils ont ensuite insisté pour qu'elle les emmène sur le lieu de l'incident afin de reconstituer les faits, ce qu'ils ont qualifié d'essentiel pour l'enquête. Aucune véritable enquête n'a jamais été menée. L'agresseur n'a jamais été arrêté, et la personne survivante a appris plus tard qu'il était très rare dans ce pays que quelqu'un soit jugé ou condamné pour agression sexuelle. Son expérience au poste de police a en fait constitué une seconde agression.

Une personne bien informée et de confiance devrait toujours accompagner la personne survivante au poste de police afin de s'assurer qu'elle ne soit pas intimidée ou victime d'autres abus, que les entretiens se déroulent dans une langue que la personne survivante comprend et qu'elle reçoive les documents et l'aide appropriés. L'accompagnant doit être prêt à intervenir si les droits et la dignité de la personne survivante ne sont pas respectés. Il est important que cette personne assume le rôle de représentant de l'organisation et ne soit pas perçue comme agissant à titre individuel.

Lorsque l'auteur présumé est un membre du personnel

Lorsque l'auteur présumé d'un incident de violence sexuelle est un membre du personnel, les organisations peuvent être amenées à prendre une série de mesures immédiates et mûrement réfléchies, notamment la sauvegarde de la personne survivante et des autres personnes susceptibles de subir un préjudice supplémentaire, ainsi que la protection de l'auteur présumé. Les auteurs présumés

peuvent continuer à représenter un risque de sécurité pour la personne survivante et d'autres membres du personnel, y compris ceux chargés d'enquêter sur les allégations.

Si les allégations sont graves, l'organisation peut décider de suspendre l'auteur présumé ou de le mettre en congé administratif (tout en préservant la confidentialité quant à la raison de son absence). Si l'auteur présumé représente un risque ou est lui-même en danger en raison des allégations, il peut être nécessaire de le relocaliser dans un lieu sûr et de l'accompagner pendant son séjour. Il est généralement conseillé d'empêcher tout contact entre la personne survivante et l'auteur présumé, en particulier dans les cas graves, bien qu'il convienne de tenir compte des préférences de la personne survivante en matière de contact.

Il est important que des enquêteurs formés et indépendants mènent le processus (avec le soutien des services concernés, tels que les RH et la sécurité) afin d'éviter tout nouveau traumatisme ou préjudice supplémentaire.¹¹⁴ Une enquête mal menée peut être extrêmement préjudiciable à la personne survivante, à l'auteur présumé et aux autres personnes touchées par l'incident. Ne pas donner suite à une allégation peut avoir des conséquences tout aussi préjudiciables.

7.7.5 Actions post-incident

Assistance postérieure

Le personnel touché peut avoir besoin d'une assistance postérieure à long terme après un incident de violence sexuelle. Les organisations doivent mettre en place un cadre de soutien tout en évitant de submerger les personnes survivantes par des décisions à prendre. Il est impératif que la politique d'une organisation définisse clairement l'étendue, le coût et la durée du soutien qu'elle peut réellement offrir aux personnes survivantes, en veillant à ce qu'elles ne soient pas induites en erreur quant à la disponibilité d'une aide indéfinie.

Les personnes survivantes peuvent avoir besoin d'un soutien médical continu, notamment de bilans de santé réguliers et de traitements pour tout problème de santé physique. Les personnes survivantes peuvent avoir besoin d'un soutien psychosocial à long terme pour faire face au traumatisme, à l'anxiété, à la dépression et à d'autres problèmes de santé mentale pouvant survenir après un incident. Ce soutien doit être adapté aux besoins de chaque individu et fourni par des professionnels formés et expérimentés dans la prise en charge des traumatismes.

Un plan complet de soutien à long terme pour personne survivante peut être élaboré en tenant compte des préférences et des besoins de la personne survivante. Il peut inclure des évaluations et des thérapies médicales et psychologiques, un soutien logistique pour l'assistance postérieure, une évaluation des options professionnelles,

114 Pour connaître le processus détaillé d'une enquête interne, y compris les étapes clés, voir European Interagency Security Forum (2019).

un plan de réintégration professionnelle et une transition vers des services de soutien à long terme (tels que les services nationaux), ainsi qu'un calendrier de communication et de vérification. La durée des procédures judiciaires doit être prise en compte dans le plan de soutien. Le plan de soutien doit être flexible afin de s'adapter aux besoins changeants de la personne survivante au fil du temps. Un traumatisme peut se manifester plusieurs mois, voire plusieurs années après un incident, et il peut être difficile d'anticiper quand et comment les déclencheurs apparaîtront. Idéalement, les personnes survivantes devraient avoir un accès facile et direct aux ressources et aux soins psychosociaux, même si elles ont besoin d'aide plusieurs mois après l'incident ou après la fin de leur emploi. Il est important de garder à l'esprit que les facteurs culturels peuvent influencer considérablement la réponse d'une personne. Lorsqu'elles apportent leur soutien, les organisations doivent rester ouvertes et sensibles aux différentes voies de rétablissement et aux préférences des personnes survivantes.

► Voir le chapitre 5.4 pour plus d'informations sur le bien-être du personnel.

Examen post-incident

Enfin, les organisations devraient mener des examens post-incident approfondis, tout en préservant une confidentialité stricte afin de protéger le personnel concerné, afin d'évaluer la gestion des incidents graves de violence sexuelle et d'identifier les domaines à améliorer.

► Voir le chapitre 4.4 sur la réponse aux incidents et la gestion de crise pour davantage de recommandations sur les examens post-incident.

Informations complémentaires

Recommandations

Centre de ressources et de support (n.d.) *Together, we can build a safer sector* (en anglais, « Ensemble, nous pouvons bâtir un secteur plus sûr ») (<https://safeguardingsupporthub.org/>).

Comité permanent interorganisations (IASC) (2023) *Définition et principes d'une approche centrée sur les victimes/survivantes, tels qu'établis par le Comité Permanent Interorganisations* (<https://interagencystandingcommittee.org/iasc-champion-protection-sexual-exploitation-and-abuse-and-sexual-harassment/iasc-definition-principles-victim-survivor-centered-approach>).

Comité permanent interorganisations (IASC) (n.d.) *Protection from sexual exploitation and abuse* (en anglais, « Protection contre l'exploitation et les abus sexuels ») (<https://psea.interagencystandingcommittee.org/>).

European Interagency Security Forum (2018) *Gérer la sécurité des travailleurs humanitaires aux profils diversifiés* (<https://gisf.ngo/resource/managing-the-security-of-aid-workers-with-diverse-profiles/>).

European Interagency Security Forum (2019) *Gérer la violence sexuelle à l'encontre du personnel humanitaire : prévention, préparation, réponse et suivi* (<https://gisfprod.wpengine.com/resource/managing-sexual-violence-against-aid-workers/>).

European Interagency Security Forum et InterAction (2014) *NGO Safety and Security Training Project: how to create effective security training for NGOs* (en anglais, «Projet de formation en sûreté et sécurité des ONG: comment créer une formation en sécurité efficace pour les ONG») (<https://reliefweb.int/report/world/ngo-safety-and-security-training-project-how-create-effective-security-training-ngos>).

GISF (2022) *Gérer la violence sexuelle à l'encontre du personnel humanitaire [Formation]*. DisasterReady (<https://ready.csod.com/ui/lms-learning-details/app/course/581feec5-4ce2-493a-9266-90ed6099bc48>).

Karaman, S. (n.d.) *Online harassment of politically-active women: an overview* («Harcèlement en ligne des femmes engagées politiquement: aperçu général»). XYZ, Tactical Technology Collective Project (<https://xyz.informationactivism.org/en/online-harassment-of-politically-active-women-overview/>).

PEN America (n.d.) *Pratiques exemplaires pour les employeurs. Manuel de défense contre le cyberharcèlement*. (<https://onlineharassmentfieldmanual.pen.org/best-practices-for-employers/>).

Persaud, C. (2012) *Genre et sécurité: orientations pour l'intégration du genre à la gestion des risques de sécurité*. European Interagency Security Forum (<https://gisf.ngo/resource/gender-and-security/>).

Steering Committee for Humanitarian Response (n.d.) 'Misconduct disclosure scheme' (en anglais, «le schéma de la révélation des inconduites») (<https://misconduct-disclosure-scheme.org/>).

Recherche et analyse

Cronin, E.A. et Afifi, A. (2018) *Review of whistle-blower policies and practices in United Nations system organizations* (en anglais, «Examen des politiques et pratiques en matière de dénonciation dans les organisations du système des Nations Unies»). Corps Commun d'inspection, ONU (<https://digitallibrary.un.org/record/1643065?ln=en&v=pdf>).

Deloitte (2019) *Safe space survey report* (en anglais, «Rapport d'enquête sur les espaces sûrs») (https://viraltopiczone.wordpress.com/wp-content/uploads/2019/01/d3bcc-un_safe_space_survey_report_15_january_2019_final.pdf).

Humanitarian Women's Network (HWN) (2016) *Full survey results* (en anglais, «Résultats complets de l'enquête»)

(https://interagencystandingcommittee.org/sites/default/files/migrated/2016-11/hwn_full_survey_results_may_2016.pdf).

Mazurana, D. et Donnelly, P. (2017) *STOP the sexual assault against humanitarian and development aid workers* (en anglais, «STOPPER les agressions sexuelles contre le personnel humanitaire et de développement»). Feinstein International Center, Tufts University (<https://fic.tufts.edu/publication-item/stop-sexual-assault-against-aid-workers/>).

Nobert, M. (2017) *Humanitarian experiences with sexual violence: compilation of two years of Report the Abuse data collection* (en anglais, «Expériences des humanitaires avec la violence sexuelle : compilation de deux années de collecte de données pour Report the Abuse»). Report the Abuse (<https://reliefweb.int/report/world/humanitarian-experiences-sexual-violence-compilation-two-years-report-abuse-data>).

Peace Corps Office of Inspector General (n.d.) *Ressources: Kate Puzey, Volunteer Protection Act of 2011* (en anglais, «Loi de 2011 sur la protection des bénévoles») (www.peacecorps.org/resources/resources-kate-puzey-volunteer-protection-act-2011).

Stoddard, A., Harvey, P., Czwarno, M. et Breckenridge, M. (2019) *Aid Worker Security Report 2019* (en anglais, «Rapport 2019 sur la sécurité des travailleurs humanitaires»). *Speakable: addressing sexual violence and gender-based risk in humanitarian aid* (en anglais, «Verbaliser : lutter contre la violence sexuelle et les risques liés au genre dans l'aide humanitaire»). Humanitarian Outcomes (<https://humanitarianoutcomes.org/AWSDR2019>).

7.8 Détention et arrestation

La gestion efficace des incidents de détention et d'arrestation nécessite une planification et des investissements dans les capacités locales, ainsi que des protocoles de réponse bien établis. Les situations de détention et d'arrestation nécessitent généralement la mise en œuvre d'un plan de réponse aux incidents (décrit au chapitre 4.4.). Dans tous les scénarios évoqués ici, la priorité est la libération rapide et en toute sécurité du membre du personnel. Pour y parvenir, l'organisation doit adopter une approche de réponse éclairée, qui inclura probablement la mobilisation du soutien des parties prenantes locales.

7.8.1 Définitions

Il est important de faire la distinction entre détention et arrestation, tant pour le signalement que pour une réponse efficace.

La détention désigne la rétention d'une personne contre son gré par un individu ou un groupe (par exemple, des groupes communautaires, des autorités locales, des milices ou des groupes militaires). Bien qu'il n'y ait aucune intention de nuire au détenu, il n'existe aucune condition claire pour sa libération. La détention peut être fréquente dans le cadre des activités humanitaires ; les détentions de courte et de longue durée sont courantes. Les motifs invoqués pour justifier la détention peuvent inclure des documents d'identité ou administratifs incorrects, tandis que les causes sous-jacentes peuvent aller du mécontentement quant à la qualité ou à l'emplacement du programme, à une erreur d'identité du personnel humanitaire ou de l'organisation, à des soupçons et à des informations erronées, jusqu'à la simple recherche de pots-de-vin. Il peut également y avoir une frustration liée au fait que les autorités ne collaborent pas avec un groupe particulier ou ne le font pas de manière satisfaisante ; le personnel humanitaire peut souvent être considéré comme un moyen de pression.

L'arrestation désigne la détention officielle par une autorité officielle (généralement la police, mais aussi l'armée) ou les autorités présumées. L'arrestation diffère du type plus général de détention mentionné ci-dessus par l'intervention d'autorités officielles invoquant leurs pouvoirs légaux. La situation peut être plus difficile et dangereuse lorsque les autorités gouvernementales procèdent à une arrestation illégale (c'est-à-dire sans mandat d'arrêt en bonne et due forme) ou lorsque la personne arrêtée « disparaît ». Les autorités peuvent alors nier que l'arrestation a eu lieu et refuser de révéler le lieu où se trouve la personne arrêtée.

7.8.2 Risques

Le risque de détention et d'arrestation augmente dans les contextes où l'on dépend substantiellement de l'aide humanitaire, où il existe un sentiment négatif à l'égard d'une organisation humanitaire ou du travail humanitaire en général et où des incitations politiques ou financières entrent en jeu. Ces types d'incidents comportent des risques secondaires qui doivent également être pris en compte :

- Risques pour la santé, la sûreté et le bien-être du personnel détenu/arrêté, en particulier s'il est victime de violences, souffre de troubles médicaux ou a subi des traumatismes dans le passé. Le fait d'être détenu contre son gré peut exacerber des problèmes de santé mentale existants. Il se peut également que le personnel n'ait pas accès à des soins médicaux, aux libertés fondamentales, à la vie privée, à des interprètes, à un avocat ou à d'autres formes de soutien.
- Perturbation des activités, en particulier si des membres clés du personnel sont retenus pendant une période prolongée. Une stratégie courante consiste à retirer et suspendre la programmation pendant que la libération est organisée.
- Risques pour la réputation de l'organisation et ses relations avec les communautés locales, les donateurs et les partenaires. Cela pourrait compromettre les capacités de l'organisation à fonctionner.
- Risques que le personnel soit détenu dans des installations inappropriées, en particulier s'il présente des vulnérabilités particulières.
- Risques encourus par les collègues chargés d'aider ou de rendre visite au personnel détenu/arrêté. Ces personnes s'exposent à des risques d'intimidation et de représailles, ainsi qu'au stress lié à leur rôle.

Les organisations humanitaires peuvent planifier et se préparer à ce type d'incidents, en particulier dans les contextes où le risque est élevé, et disposer de mécanismes de réponse bien établis.

7.8.3 Planification, préparation et atténuation des risques

Une planification et une préparation efficaces sont essentielles pour atténuer les risques d'arrestation et de détention du personnel humanitaire. Il convient de noter qu'il n'est évidemment pas possible d'empêcher une arrestation qui suit une procédure légale. Si une arrestation qui ne respecte pas la procédure légale peut être contestée, il est peu probable qu'elle puisse être évitée.

Dans le cadre de leur planification et de leur préparation, les organisations devraient idéalement élaborer des plans d'urgence détaillés et à plusieurs niveaux afin de protéger leur personnel et d'assurer la continuité de leurs activités, tant en ce qui concerne les risques de détention que d'arrestation.

Analyse du contexte, analyse des risques et plan d'urgence

- **Les risques de détention et d'arrestation sont intégrés dans la gestion des risques de sécurité.** Les évaluations des risques et le plan d'urgence tiennent compte du risque de détention et d'arrestation. Les plans d'urgence comprennent les procédures d'évacuation et d'extraction. Les analyses du contexte comprennent un aperçu des environnements politiques, juridiques et de sécurité dans les zones d'opération.
- **La cartographie des acteurs** peut faciliter l'accès, la négociation et les efforts visant à développer des relations avec les communautés locales, les autorités et les autres parties prenantes, ce qui peut contribuer à accélérer la réponse en cas d'arrestation ou de détention.

Préparation juridique

- **Compréhension du contexte juridique et politique de l'environnement opérationnel.** Le personnel doit être informé de la hiérarchie des forces de sécurité nationales ou des autres autorités de facto dans la zone d'opération de l'organisation. Cela peut inclure les structures claniques et communautaires, ainsi que la connaissance des procédures juridiques régissant les arrestations dans le pays.
- **Briefing juridique.** Le personnel doit être informé des lois locales, de ses droits et des procédures à suivre en cas de détention ou d'arrestation. Les organisations doivent indiquer clairement le type de soutien qui peut être apporté au personnel détenu ou arrêté, y compris le soutien après la libération et à l'intention des membres de la famille.
- **Aide juridique.** Il est conseillé d'établir des contacts avec des professionnels du droit locaux et des organisations internationales d'aide juridique qui peuvent fournir une assistance immédiate.
- **Suivi régulier.** Le personnel responsable peut examiner et rendre compte des tendances en matière de détention et d'arrestation dans le contexte opérationnel, ainsi que des acteurs impliqués.

Formation et sensibilisation

- **Tenir à jour les plans de réponse locaux.** Des protocoles clairs doivent être mis en place et le personnel doit connaître les procédures à suivre pour signaler et répondre aux incidents liés de détention et d'arrestation, savoir quelles parties prenantes informer et connaître les rôles et responsabilités au sein de l'organisation. Les plans doivent inclure des protocoles de communication et des procédures d'escalade, ainsi que des mesures visant à assurer la continuité des opérations en cas de détention ou d'arrestation de membres clés du personnel.
- **Formation à la sécurité.** Orientation et formation doivent être dispensées au personnel sur les mesures de sécurité personnelle, la conscience situationnelle, la prévention des risques et les protocoles à suivre lors des interactions avec les autorités.

- **Exercices de simulation.** Des exercices de simulation réguliers permettent au personnel de s'entraîner aux procédures de réponse en cas de détention.
- **Documentation.** Le personnel doit être au courant de la documentation qu'il doit avoir sur lui et des autres mesures à respecter pour pouvoir accéder aux zones d'opération et s'y déplacer en toute sécurité.

Plaidoyer et réseautage

- **Rôles et responsabilités en matière de communication.** Le personnel humanitaire doit être en mesure d'expliquer son rôle et la mission de son organisation en termes simples et clairs. Cela peut nécessiter une pratique régulière.
- **Engagement des parties prenantes.** Le personnel doit collaborer avec les autorités locales, les dirigeants communautaires et les autres parties prenantes afin d'établir des relations et de réduire le risque d'incident.
- **Plaidoyer international.** Les organisations peuvent travailler ensemble et par voie diplomatique pour plaider en faveur de la protection des travailleurs humanitaires.

Bien-être du personnel

- **Des protocoles de bien-être du personnel** (y compris le soutien en santé mentale et le counseling) peuvent être mis en place pour le personnel avant, pendant et après un incident.

► Voir le chapitre 5.4 sur le bien-être du personnel.

Liaison avec la famille

- **Travailler avec les familles** est essentiel pour répondre efficacement aux situations à moyen et long terme. Les proches peuvent être chargés de nourrir et de veiller à la santé de leur membre de famille détenu/arrêté. Ils devront probablement aussi gérer le paiement de la caution et des amendes. Envisager d'établir des protocoles pour soutenir et communiquer avec les familles du personnel détenu/arrêté, précisant notamment le type d'aide financière ou juridique qui peut être fourni et dans quelles conditions.

Suivi et évaluation

- **Examens et rapports réguliers.** Les organisations peuvent procéder à des examens et à des mises à jour réguliers des évaluations des risques, des plans d'urgence et des programmes de formation. Ceci permet d'identifier les progrès réalisés et sert d'alerte précoce pour les risques futurs.
- **Analyse d'incident.** Les entretiens et les évaluations des incidents d'arrestation ou de détention peuvent aider à tirer des enseignements et à améliorer les réponses futures.

Certains membres du personnel peuvent être détenus ou arrêtés pour des raisons sans rapport avec leur travail ou celui de l'organisation humanitaire. Parmi les facteurs susceptibles de jouer un rôle, citons les affiliations sociales ou culturelles, la dynamique du pouvoir et les activités politiques ou criminelles. Les organisations humanitaires doivent avoir une politique claire concernant le niveau de soutien qu'elles apporteront en cas d'arrestation ou de détention sans rapport avec le travail. Si la détention ou l'arrestation est due à des circonstances politiques, les organisations humanitaires peuvent craindre d'être perçues comme s'ingérant dans la politique locale. Cela ne devrait toutefois pas constituer un obstacle automatique à la prise de responsabilité envers le personnel se trouvant dans cette situation et à la mise en œuvre de tous les efforts nécessaires pour assurer son retour en toute sécurité.

7.8.4 Répondre à un incident

Lorsque des membres du personnel sont portés disparus, le premier défi consiste à déterminer la nature exacte de la situation et à la signaler. Cela peut prendre des heures, des jours, voire des semaines. Les informations de base doivent être établies et communiquées dans un compte rendu d'incident qui est ensuite transmis au personnel concerné.

Une bonne pratique consiste à déterminer clairement qui a été ou devrait être informé, et qui est déjà au courant de l'incident à l'extérieur de l'organisation, y compris si la police, les forces de sécurité ou les autorités sont au courant, ont été ou seront informées ; si la presse ou des tiers sont au courant de l'incident ; et si les proches ont été informés. La gestion de l'information peut être difficile, mais elle doit être soigneusement étudiée et traitée par le personnel chargé de la réponse. Il convient également d'envisager de suivre la presse, les réseaux sociaux et autres médias, qu'ils soient locaux, nationaux, régionaux ou internationaux.

Les organisations doivent tenir compte de la confidentialité et du respect de la vie privée dans le cadre du signalement ou du partage d'informations. Lorsque la situation perdure, une organisation peut décider d'intensifier sa réponse et de lancer une campagne de plaidoyer publique afin d'obtenir la libération d'un membre du personnel ou d'attirer l'attention sur sa situation. Dans l'idéal, cela devrait être fait avec l'accord du membre du personnel concerné.

Les procédures de réponse aux incidents sont abordées plus en détail au chapitre 4.4. Vous trouverez ci-dessous quelques considérations plus détaillées.

En cas de détention ou d'arrestation

En cas de détention, une approche musclée risque d'être contre-productive et d'accroître l'antagonisme envers le membre du personnel et l'organisation. La détention peut avoir pour but de contraindre l'organisation ou une autre entité à prêter attention et à engager un dialogue sérieux, auquel cas le fait de répondre à cette attente peut suffire à mettre fin à l'incident.

Dans certains cas, il peut être possible pour le détenu de négocier sa propre libération, et les organisations devraient former leur personnel en conséquence. Il est souvent important, dans un premier temps, de mettre l'accent sur leur travail humanitaire et sur le caractère neutre, impartial et indépendant de leur organisation et de ses activités. Certains membres du personnel des organisations ont sur eux des aide-mémoire ou d'autres documents expliquant le rôle de leur organisation. Il est également utile d'avoir sur soi les coordonnées des personnes à contacter en cas d'urgence en cas de détention.

Si un membre du personnel est arrêté et que l'on ignore où il se trouve, la première priorité est de déterminer où il est et sous quelle autorité. Cela peut impliquer de se rendre auprès des autorités locales compétentes, d'informer l'ambassade (dans le cas d'un ressortissant étranger) et d'utiliser les réseaux locaux pour recueillir des informations. Il est important de garder à l'esprit qu'un membre du personnel peut être arrêté pour des raisons légitimes et devoir rendre compte de ses actes. Dans tous les cas, les organisations peuvent envisager de faire appel à un bon avocat local qui connaît les langues et le système locaux, qui a l'expérience de ce type de situation et qui dispose de relations utiles.

Lorsqu'elles savent avec certitude qui a arrêté ou placé en détention le membre du personnel et le lieu où il se trouve, les organisations doivent veiller à ce que ses droits soient protégés. Les organisations doivent envisager de plaider auprès des autorités locales en faveur d'un traitement équitable et humain du personnel concerné, notamment l'accès aux soins médicaux, à un avocat et à une procédure régulière. Cela peut se faire après une évaluation et des discussions avec les parties prenantes, car l'attention d'une organisation internationale peut exacerber la situation. Des mesures supplémentaires pourraient être envisagées si ces demandes ne sont pas satisfaites. Tout mauvais traitement ou violation des droits doit être documenté, et la redevabilité doit être engagée si nécessaire (en gardant à l'esprit que cela peut faire plus de mal que de bien).

Les arrestations peuvent être effectuées sans qu'aucune accusation officielle ne soit portée. Dans ce cas, l'organisation peut demander qu'une accusation soit formulée dans un délai déterminé. L'accusation peut viser la personne (par exemple, elle est accusée d'être impliquée dans un crime) ou l'organisation (par exemple, une accusation d'espionnage sous couvert d'une mission humanitaire). Dans tous les cas, la priorité absolue est d'œuvrer pour la libération rapide et en toute sécurité du

membre du personnel. Dans la plupart des cas, ce n'est qu'une fois qu'un membre du personnel a été innocenté de toute accusation injustifiée qu'il convient de s'efforcer de rétablir la réputation de la personne ou de l'organisation.

Dans le cadre d'un plan d'urgence plus large, l'organisation peut avoir besoin de discuter du soutien administratif et financier qui sera apporté au membre du personnel concerné et à sa famille. Dans quelles circonstances une aide juridique serait-elle fournie ou une caution versée ? Par quels moyens et qui en serait responsable ? De nombreuses organisations disposent d'une assurance qui couvre certaines de ces éventualités. Il peut être nécessaire de déterminer si la couverture est applicable et s'étend à l'ensemble du personnel ou uniquement à certaines personnes clés. Cette question peut être examinée au niveau de la politique générale dans le cadre d'une approche plus large de la gestion des risques.

► Voir le chapitre 5.4 pour plus d'informations sur l'assurance.

Les organisations peuvent souhaiter apporter un soutien supplémentaire aux personnes chargées de rendre visite au personnel détenu/arrêté et d'assurer la liaison avec les autorités, car cette tâche peut s'avérer difficile et avoir de nombreuses répercussions sur le membre du personnel concerné (par exemple, sur sa santé mentale, ainsi que sur ses relations avec les autorités ou les groupes locaux). Ce rôle ne doit pas être attribué au hasard à une personne en fonction de sa proximité avec le contexte. Il est également essentiel d'assurer la liaison avec la famille du membre du personnel et de s'occuper de celle-ci en cas d'arrestation ou de détention. Idéalement, elle devrait être informée des mesures prises ; les organisations devraient s'efforcer de maintenir une ligne de communication directe et régulière, rester informées des mesures que la famille a l'intention de prendre ou a prises, et l'avertir si ce qu'elle prévoit de faire est susceptible de perturber, de compliquer ou d'aller à l'encontre de la réponse prévue par l'organisation.

► Voir le chapitre 4.4 pour plus d'informations sur la liaison avec la famille.

Il est probable que le soutien de la communauté locale et des parties prenantes jouera un rôle déterminant dans la libération d'un membre du personnel détenu/arrêté. Il peut être utile de cartographier les dynamiques claniques et sociales et d'identifier des interlocuteurs pour faciliter les demandes de renseignements et les requêtes. Les organisations qui ne sont pas implantées localement peuvent trouver utile les informations fournies par les acteurs locaux pour suivre l'état du personnel affecté et transmettre des messages informels.

Considérations post-incident

Les membres du personnel libérés et les personnes étroitement impliquées dans l'incident, telles que les membres de la famille ou l'équipe de gestion de l'incident, peuvent avoir besoin d'un soutien supplémentaire après un incident. Ce soutien peut inclure un congé, une assistance médicale et un accompagnement psychologique.

- Voir le chapitre 5.4 pour plus d'informations sur la prise en charge post-incident du personnel.

Il peut être utile de discuter avec les autorités compétentes, les parties prenantes et les dirigeants communautaires des raisons qui ont motivé la détention ou l'arrestation, et des mesures à prendre pour éviter qu'un incident similaire ne se reproduise à l'avenir.

De nombreuses organisations organisent une session officielle de débriefing factuel ou un examen a posteriori.

- Voir le chapitre 4.4 pour plus d'informations sur les examens a posteriori.

Informations complémentaires

Recommandations et ressources

Buth, P. (2010) *Crisis management of critical incidents* (en anglais, «Gestion de crise des incidents critiques»). European Interagency Security Forum (www.gisf.ngo/resource/crisis-management-of-critical-incidents).

Davidson, S. (2013a) *La famille avant tout: soutien et liaison en situation de crise*. European Interagency Security Forum (www.gisf.ngo/resource/family-first/).

Davidson, S. (2013b) *Gérer le message: gestion de la communication et des médias en cas de crise de sécurité*. European Interagency Security Forum (www.gisf.ngo/resource/managing-the-message).

Hostage International (n.d.) *Best practice in family support* (en anglais, «Pratiques exemplaires en matière de soutien aux familles») (<https://hostageinternational.org/resource/best-practice-in-family-support/>).

Hostage US (n.d.) *Hostage US guides* (en anglais, «Guides de Hostage US») (<https://hostageus.org/resources/hostage-us-guides>).

7.9 Enlèvement, enlèvement contre rançon et situation d'otages

Les incidents d'enlèvement, y compris les enlèvements contre rançon et les situations d'otages, peuvent avoir des répercussions physiques et émotionnelles durables. La prévention, la préparation et la réponse à un enlèvement nécessitent un investissement et une planification de la part de l'organisation. Ce chapitre traite des bonnes pratiques en matière de gestion des risques d'enlèvement. Il comprend des conseils sur les enlèvements express et virtuels, qui sont devenus plus fréquents ces dernières années, et aborde les répercussions à long terme et d'autres problèmes persistants liés aux enlèvements.

7.9.1 Définitions

Un enlèvement désigne toute capture illégale et forcée d'une personne. L'enlèvement contre rançon désigne un enlèvement dont le but explicite est d'obtenir quelque chose en échange de la libération de la personne enlevée. Le plus souvent, les auteurs exigent une rançon, mais ils peuvent également demander des concessions politiques. Dans certains cas, ce qui semble être une cause politique peut en réalité être un acte d'extorsion.

Le terme «prise d'otage» désigne une situation dans laquelle le lieu où se trouve la personne enlevée est connu et où sa libération dépend de la satisfaction de certaines exigences. Dans une situation de siège, les auteurs et leurs otages ont été localisés et encerclés par les forces de sécurité, et les auteurs menacent de tuer les otages s'ils ne leur fournissent pas un moyen de s'échapper.

Types d'enlèvements contre rançon

- **Enlèvement contre rançon** - lorsque le motif principal est un gain financier ou politique. Les auteurs d'un enlèvement exigent une rançon à la famille ou aux associés de la personne enlevée en échange de sa libération. Les auteurs d'un enlèvement peuvent également exiger la libération de prisonniers, des changements politiques ou la publicité pour leur cause.
- **Enlèvement express** - la victime est détenue pendant une courte période, généralement moins de 24 heures, et contrainte de verser rapidement une rançon (par exemple en retirant de l'argent à un DAB). Les enlèvements express sont généralement opportunistes et ne nécessitent pas beaucoup de préparation.

- **Enlèvement contre rançon virtuel** - lorsque des criminels tentent de contraindre leurs victimes à payer une rançon en prétendant à tort avoir kidnappé une personne de leur entourage. Les tactiques consistent notamment à maintenir la victime au téléphone afin de l'empêcher de s'assurer que la personne est bien en sûreté ou de vérifier l'authenticité des enregistrements audio ou vidéo de la victime présumée. Ces dernières années, ce type d'enlèvement contre rançon a été facilité par les nouvelles technologies, notamment l'IA.
- **Le « Tiger kidnapping » ou enlèvement contre rançon furtif** - enlèvement de personnes connues de la victime, qui est ensuite contrainte de participer à un crime, tel que pénétrer dans un lieu sécurisé pour voler de l'argent, afin d'assurer leur libération en toute sécurité.

7.9.2 Planification, préparation et formation

Pour faire face à la menace d'enlèvement, les organisations doivent évaluer qui est le plus à risque et adapter leurs mesures d'atténuation des risques et de préparation au contexte. Une formation régulière, des exercices de simulation, des ressources appropriées, un apprentissage continu et une capacité d'adaptation sont essentiels tant pour la prévention que pour la réponse. Des exemples d'actions sont présentés ci-dessous.

Au niveau du siège

- Établir et maintenir à jour des politiques et des protocoles de sécurité traitant spécifiquement des risques d'enlèvement, et veiller à ce que tous les membres du personnel connaissent ces politiques et reçoivent une orientation à ce sujet.
 - Créer une structure organisationnelle de gestion des crises, avec une sélection et une formation appropriées du personnel.
- *Pour en savoir plus sur la structure de gestion de crise, voir le chapitre 4.4.*
- Établir des liens à l'échelle locale et internationale afin de garantir l'expertise nécessaire pour assurer un soutien efficace à la gestion des incidents, au moment où cela s'avère nécessaire. Par exemple, discuter de l'aide gouvernementale à laquelle on peut s'attendre en cas d'enlèvement d'un membre du personnel ou identifier des experts externes qualifiés pour la gestion de crise et le soutien post-crise aux personnes enlevées et à leurs familles.¹¹⁵
 - Tenir à jour les dossiers du personnel, notamment les coordonnées des proches et les éventuels problèmes médicaux. Envisager de demander à tous les membres du personnel de documenter les questions relatives à la « preuve de vie » (voir ci-dessous pour plus d'informations à ce sujet).

¹¹⁵ Il existe plusieurs organisations de réponses spécialisées qui apportent leur soutien aux organisations et aux familles tout au long d'événements liés à un enlèvement, dont nombreuses sont associées à des polices d'assurance spéciales. Certains gouvernements disposent d'équipes spécialisées chargées de l'application de la loi qui interviennent lorsqu'un de leurs ressortissants est victime d'un enlèvement.

- Être clair à propos des responsabilités et des obligations envers le personnel et leurs familles en cas d'enlèvement, y compris lorsque le personnel est détaché.
- Informer pleinement le personnel du risque d'enlèvement avant de l'affecter dans des zones à haut risque.
- Préparer des modèles ou des directives pour les déclarations aux médias et les communiqués de presse en cas d'enlèvement.
- Former le personnel aux stratégies d'atténuation des risques d'enlèvement et aux techniques de survie en cas d'enlèvement.
- Veiller à ce que des polices d'assurance soient en place, notamment une assurance médicale et une assurance couvrant les risques spéciaux ou les enlèvements et demandes de rançon.

Au niveau du bureau opérationnel

- Veiller à ce qu'une structure organisationnelle de gestion de crise dotée de personnel et formée soit mise en place.
- Veiller à ce que le personnel soit informé de la politique de l'organisation en matière d'enlèvements et de rançons et soit prêt à réagir en cas d'enlèvement (y compris aux appels des auteurs d'un enlèvement).
- Élaborer des plans d'urgence spécifiques aux enlèvements, les réviser et les mettre à jour régulièrement, ainsi que les procédures opérationnelles standards.
- Mettre en place et maintenir des canaux de communication efficaces et fiables pour signaler les incidents et partager les notifications pendant la gestion d'un incident critique.
- Établir et maintenir le contact avec les ambassades concernées (si les personnes enlevées sont des ressortissants étrangers) et d'autres acteurs diplomatiques, tels que l'ONU, en coordination avec l'équipe de gestion de crise de pays.
- Savoir qui contacter au sein du gouvernement en cas d'enlèvement et, s'il existe des équipes spécialisées, prendre le temps de comprendre leur mode de fonctionnement et leur manière d'intervenir.
- Se tenir informé de la structure de commandement des forces de sécurité nationale et des autres acteurs armés pertinents dans la zone d'opération de l'organisation.
- Comprendre la politique gouvernementale en matière de contact avec les auteurs ; entamer des négociations directes avec les auteurs peut avoir de graves conséquences.
- Veiller à ce que des dossiers clairs soient conservés et à ce que la confidentialité soit préservée. Ces dossiers doivent être marqués comme « confidentiels » et le personnel doit s'attendre à ce qu'ils puissent être demandés à un moment donné dans le cadre d'une enquête.
- Être prêt à apporter un soutien psychosocial au personnel touché et à sa famille, et à prendre en charge les problèmes liés aux traumatismes et au stress.

- Voir le chapitre 5.4 pour plus de détails sur la prise en charge du personnel après un incident critique.

Assurance enlèvement, rançon et extorsion

L'assurance enlèvement, rançon et extorsion est spécialement conçue pour protéger les particuliers et les organisations contre les pertes financières et les responsabilités associées.

Bien que les conditions et la couverture varient selon les polices et les assureurs, l'assurance enlèvement et rançon peut offrir :

- Des « services de prévention », tels que des informations et des recommandations spécifiques à chaque pays.
- La mise à disposition de consultants en intervention de crise qui peuvent offrir un soutien à la négociation et des conseils stratégiques.
- La couverture des frais liés aux poursuites judiciaires, aux relations publiques, au repos et à la réadaptation, aux soins médicaux et psychiatriques, à l'indemnisation des accidents corporels, à la perte de revenus et à toute autre responsabilité juridique connexe. Elle peut également couvrir le remboursement de la rançon si cela n'est pas illégal dans la juridiction concernée (par exemple, si les auteurs sont des groupes ou des individus sous sanctions).

L'assurance enlèvement, rançon et extorsion comprend généralement une clause de confidentialité, seuls les cadres supérieurs étant informés des détails de la police. Il est important que les organisations puissent discuter du plan d'assurance avec leur personnel sans compromettre cette confidentialité. Les organisations peuvent rédiger une déclaration et désigner un porte-parole en cas de demande de renseignements.

Certains plans d'assurance permettent de déduire 10 % de la prime annuelle pour la préparation et la formation.

- Voir le chapitre 5.4 pour plus de détails sur l'assurance.

7.9.3 Mesures de réduction des risques

Voici quelques exemples de mesures visant à réduire les risques d'enlèvement.

- **Connaissance du contexte.** Recueillir des informations sur le contexte de sécurité et les risques d'enlèvement, par exemple en suivant les informations en matière de sécurité, en assistant à des briefings sur la sécurité spécifiques au contexte et en comprenant les mesures adoptées par d'autres organisations opérant dans la même zone.
- **Communication et acceptation.** Discuter du rôle et du travail de l'organisation avec les acteurs concernés tout en garantissant la qualité et l'acceptation du programme.
- **Éviter la prévisibilité.** Varier les routines et les horaires de trajet, y compris pour les déplacements domicile-travail et en dehors du travail.
- **Réduire la visibilité.** Réduire au minimum la visibilité en évaluant l'image de marque, par exemple les logos sur les véhicules, en étant conscient des comportements susceptibles d'attirer l'attention, en utilisant des moyens de transport fiables plutôt que des véhicules identifiables pour certains déplacements, en opérant en équipes plus petites et en limitant la présence sur les réseaux sociaux.
- **Respecter les procédures opérationnelles.** Utilisation de canaux de communication sécurisés pour l'information sensible, mise en place et respect de mesures de gestion de risque lié aux déplacements et mise à jour des plans d'urgence pour faire face aux situations imprévues.
- **Éliminer les vulnérabilités potentielles.** Restriction temporaire de l'accès aux zones à haut risque, demande au personnel de travailler à distance et envisager la suspension des programmes sont autant de stratégies à envisager lorsqu'il existe des preuves suggérant un risque accru. Certaines organisations estiment utile que leur personnel se déplace avec des appareils professionnels temporaires «propres», tels que des téléphones et des ordinateurs portables, afin d'éviter toute utilisation abusive des données stockées. Une mesure plus radicale consiste à retirer le personnel le plus à risque.
- **Sécurité du site.** Mettre en place des contrôles d'accès et des procédures d'identification stricts dans les résidences, les bureaux et les sites de projets. Bien que les enlèvements se produisent souvent pendant les déplacements, il reste essentiel de maintenir la sécurité des sites.

► Voir le chapitre 7.2 - Sécurité du site.

- **Sensibilisation accrue et anti-surveillance.** Être vigilant (collectivement et individuellement) vis-à-vis de tout signe de surveillance et de comportement inhabituel. Un enlèvement nécessite généralement une certaine planification, et les auteurs peuvent surveiller le domicile, le bureau et les déplacements de leur cible pendant un certain temps avant de passer à l'action. Il est recommandé de suivre régulièrement des formations sur les protocoles de signalement et les pratiques anti-surveillance.

► Voir le chapitre 7.5 pour plus d'informations sur la surveillance hostile.

- **Utilisation de la technologie.** Les équipements de suivi numériques peuvent être portés sur soi ou installés dans des véhicules, ce qui permet d'envoyer des alertes numériques et de suivre les trajets. Les équipements de suivi numériques doivent être utilisés avec prudence et évalués en termes de risques de sécurité.
- **Soutien et protection au niveau local.** Établir et entretenir de bonnes relations avec les dirigeants communautaires et les autorités locales peut aider à obtenir des conseils sur les mesures de sécurité à prendre et les risques potentiels d'enlèvement. Dans certains contextes, cela peut également offrir une certaine protection. Cependant, les dynamiques de pouvoir peuvent évoluer rapidement, et il convient d'y réfléchir attentivement avant ou au moment de solliciter un tel soutien.
- **Protection armée.** Le recours à des gardes armés ou à des gardes du corps peut avoir un effet dissuasif sur les auteurs potentiels d'actes criminels dans les résidences, les bureaux et pendant les déplacements. Cependant, le recours à une protection armée peut également accroître la visibilité et augmenter les risques tant pour le personnel armé que pour les employés. Cela doit être soigneusement évalué à la lumière des politiques, des principes, de l'image et des mesures d'acceptation de l'organisation. Il est également essentiel de tenir compte des sanctions et de la législation de lutte antiterroriste lors du recours à une protection armée.

► Voir le chapitre 4.2 pour une analyse plus détaillée sur la protection armée.

- **Politique publique de « non-paiement de rançon » ou autres concessions substantielles.** Adopter une position claire sur les rançons dans les documents de politique et les communications publiques peut faire du personnel une cible moins attrayante. En réalité, des sommes d'argent sont parfois versées, par les familles, les entreprises privées, les gouvernements et les organisations humanitaires. Une stratégie de « non-paiement » est difficile à maintenir sans une préparation soutenue à tous les niveaux d'une organisation et sans un niveau élevé de contacts et de liens avec la communauté et un large éventail de parties prenantes.

Atténuer les risques d'enlèvement contre rançon express et virtuel

Les enlèvements express sont généralement motivés par l'argent, et les auteurs d'un enlèvement n'ont pas l'intention de s'en prendre physiquement à leurs cibles. Certaines des mesures suivantes peuvent contribuer à atténuer les risques :

- Réaliser des évaluations des risques (zones à haut risque, cibles potentielles, impact).
- Former le personnel à la conscience situationnelle, à la manière d'éviter de devenir une cible (conseils sur l'utilisation des DAB) et à réagir de manière appropriée pour être libéré en toute sécurité (se conformer aux demandes).

- Ne transporter que des objets de valeur limitée (minimale) et des cartes bancaires avec des soldes faibles ou des limites de retrait journalières.

Les enlèvements contre rançon virtuels sont conçus pour extorquer rapidement de l'argent. Les mesures d'atténuation comprennent :

- Former le personnel à l'existence des « deep fakes » ou hypertrucages générés par l'IA et à la manière d'identifier les signes indiquant qu'il s'agit d'un enlèvement contre rançon virtuel (par exemple, les auteurs tentent de maintenir la cible en ligne, empêchent tout contact ou communication avec la victime présumée et réduisent rapidement le montant de la rançon demandée).
- Former le personnel à réagir calmement : raccrocher, contacter la victime présumée ou demander des détails que seule celle-ci pourrait connaître.
- Veiller à ce que le personnel sache qu'il ne doit pas accepter de payer une rançon, en particulier en personne, car cela pourrait l'exposer à un risque supplémentaire.

7.9.4 Répondre à un incident

Considérations générales relatives à la réponse

Lorsqu'un enlèvement se produit, l'organisation active généralement sa structure de gestion de crise. Les grandes organisations disposent parfois d'une équipe de gestion de crise au siège social, soutenue par une équipe de gestion de l'incident au bureau opérationnel ou sur le site de l'incident. Les organisations internationales peuvent également disposer d'une équipe de gestion de crise régionale. Ces équipes sont généralement soutenues par des collègues spécialisés dans divers domaines, souvent liés à la sécurité, à la santé, à l'informatique et à la communication. L'organisation désigne généralement un communicateur chargé de transmettre les messages aux auteurs et de recevoir leurs réponses. (Ce rôle n'est pas le même que celui d'un négociateur, et cette personne n'agira pas en tant que décideur ou membre officiel d'une équipe de réponse.) Les équipes de réponse travaillent souvent avec d'autres organisations, telles que les forces d'application de la loi, les agences gouvernementales, les médias et les compagnies d'assurance.

L'une des principales responsabilités de l'équipe de gestion de crise consiste à élaborer et à mettre en œuvre une stratégie de réponse aux incidents adaptée à la situation et ajustée en fonction de l'évolution des circonstances. Cette stratégie,

élaborée avec l'aide d'experts tels que des conseillers juridiques, permet de garantir le respect des cadres juridiques applicables et guide l'approche de l'organisation en matière de réponse, notamment les négociations avec les auteurs, la gestion des parties prenantes et la communication. Les stratégies à l'égard des auteurs, des proches, des autorités, des médias et d'autres organisations devront être régulièrement revues par l'équipe de gestion de crise.

► *Voir le chapitre 4.4 pour plus d'informations sur les bonnes pratiques en matière de réponse aux incidents critiques et de mise en place d'une structure de gestion de crise.*

Les mesures à prendre lors des premières phases d'un enlèvement présumé peuvent inclure :

- Établir les faits et préparer un compte rendu d'incident.
- Assurer la sûreté des autres membres du personnel, éventuellement en limitant leurs déplacements ou en les transférant vers un endroit plus sûr.
- Envisager la suspension des programmes.
- Informer les autres bureaux et la direction.
- Informer les membres de la famille et les préparer à un éventuel contact avec les auteurs.
- Alerter les compagnies d'assurance.
- Consulter des experts externes compétents, conformément au plan de gestion de crise.
- Gérer les communications et les informations, notamment en mettant en place un registre pour consigner les événements, les discussions, les décisions, les responsabilités et les mesures prises dans tous les bureaux concernés.
- Identifier le communicateur désigné.
- Suivre les informations relatives à l'incident dans les médias.
- S'assurer de la disponibilité des fonds nécessaires pour couvrir les coûts initiaux, ce qui peut nécessiter l'obtention de fonds auprès du siège social.

Au cours des premières phases d'un enlèvement, le personnel de réponse devra souvent être déchargé de ses autres tâches et disposer d'un espace de travail et d'installations dédiés. Les membres de l'équipe auront besoin de repos et de soutien réguliers, et si la crise se prolonge, une transition en douceur vers des remplaçants sera nécessaire.

Experts externes

Dans certains cas, un spécialiste des situations d'enlèvement, externe à l'organisation et pouvant être détaché par le gouvernement du pays hôte ou du pays d'origine, la compagnie d'assurance ou une société de sécurité privée, peut rejoindre l'équipe de gestion de crise. Son rôle consiste à conseiller et à soutenir, et non à prendre des décisions. Les experts en gestion des enlèvements peuvent proposer leurs services volontairement ou être recommandés. Leur connaissance du contexte local et régional, leur compréhension des aspects juridiques, ainsi que leurs compétences, leurs réseaux et leur expérience peuvent s'avérer inestimables.

Bien que les conseillers externes ne gèrent généralement pas les incidents et ne participent pas aux négociations directes avec les auteurs, ils peuvent apporter une valeur ajoutée considérable en tant que conseillers et coachs auprès du personnel, notamment les équipes chargées de la réponse et des relations avec les médias. Ils peuvent offrir un point de vue objectif, aider à anticiper les scénarios possibles, contribuer à garantir l'état de préparation de la réponse et évaluer son efficacité. Il convient de veiller à ce qu'aucun conflit d'intérêts ne survienne. Par exemple, dans le cas d'un expert recommandé ou nommé par le gouvernement, il peut y avoir un décalage en termes de politiques, d'objectifs et d'approches.

Lorsque des membres du personnel de plusieurs organisations sont enlevés ensemble, la collaboration entre les différentes parties concernées est essentielle pour garantir une approche cohérente. Il est conseillé de mettre en place des équipes de gestion de crise conjointes au niveau opérationnel et au niveau du siège. Bien que chaque organisation souhaite être impliquée, les membres de l'équipe doivent être choisis pour leurs compétences et leur aptitude à gérer les incidents, plutôt que comme représentants de leurs organisations respectives. Des experts externes peuvent être sollicités afin de garantir l'objectivité et la pertinence des efforts.

Même lorsqu'un incident n'affecte qu'une seule organisation, il peut avoir des répercussions sur la sécurité d'autres organisations situées dans la même zone. La sécurité relève donc d'une responsabilité collective. Le paiement d'une rançon ou la manière dont une organisation interagit avec les autorités a également des conséquences plus larges en matière de sécurité. Si l'organisation dont un membre du personnel a été enlevé est responsable du choix de l'approche qu'elle souhaite adopter, il peut néanmoins être prudent d'écouter les conseils d'autres personnes

ayant de l'expérience dans ce domaine, en particulier si elles ont déjà vécu des situations similaires.

Lorsque le lieu où se trouve la personne enlevée est inconnu

Un enlèvement est particulièrement délicat lorsque le lieu où se trouve la personne enlevée et son état sont inconnus, et s'il est impossible de contacter les auteurs. L'organisation visée peut chercher à médiatiser l'incident, mais comme pour toute intervention médiatique, cela peut être contre-productif si cela attire inutilement l'attention sur la personne enlevée et augmente sa valeur aux yeux des auteurs de l'enlèvement. Cette approche peut également s'avérer efficace si elle permet de signaler aux autorités que le sort de la personne concernée est largement connu et que son enlèvement prolongé nuirait gravement à l'image des autorités et à leur capacité à établir ou à maintenir l'état de droit. Les organisations de défense des droits humains et d'autres organisations de plaidoyer sont généralement plus aptes à créer ce type de médiatisation que les organisations humanitaires, et il peut être possible de coopérer avec elles. Dans d'autres cas, il n'y a pas grand-chose à faire, si ce n'est diffuser des informations et des photos de la personne enlevée et essayer de trouver quelqu'un qui puisse fournir une piste ou un contact.

Gérer les relations avec la famille

- **Contact immédiat et liaison avec la famille.** Il est essentiel d'informer rapidement la famille de la personne enlevée, de préférence en personne et, dans l'idéal, avant qu'elle n'apprenne l'incident par les médias ou par des tiers. Une visite en personne est recommandée. Il est conseillé de mettre en place des fonctions dédiées à la liaison avec la famille. Les personnes chargées de la liaison avec les familles, qu'elles soient personnel interne ou personnel de spécialistes¹¹⁶, peuvent contribuer à instaurer et à maintenir la confiance. Elles doivent posséder de solides compétences interpersonnelles et être capables de communiquer dans la langue de la famille. Certains gouvernements disposent également d'agents de liaison familiale, qui devraient compléter plutôt que remplacer l'engagement organisationnel.

Dans certains cas, les familles, en particulier celles qui sont issues du contexte local, peuvent préférer gérer elles-mêmes les enlèvements en s'appuyant sur leurs connaissances et leurs réseaux locaux, surtout si les enlèvements sont motivés par

116 Si une organisation ne dispose pas d'un agent de liaison avec les familles dédié ou formé, des dispositions préalables peuvent être prises avec des organisations spécialisées telles que Hostage International : www.hostageinternational.org

des rivalités sociales ou politiques locales. Cependant, dans les cas criminels ou politiques, elles ne sont pas nécessairement mieux équipées que l'organisation. Il arrive parfois que des membres du personnel soient enlevés pour des raisons sans rapport avec leur travail, et certaines organisations peuvent choisir de ne pas intervenir à moins d'être directement impliquées. Dans ces circonstances, il est important que la famille et l'organisation comprennent et s'accordent sur la stratégie de réponse à adopter et sur les domaines dans lesquels un soutien mutuel peut être envisagé.

- **Développer une approche claire.** Il est essentiel de maintenir une communication transparente avec la famille pour instaurer un climat de confiance. Un manque de confiance peut conduire la famille à agir de manière indépendante, par exemple en s'adressant aux médias, en se rendant sur le lieu de l'enlèvement ou en tentant de mener ses propres négociations. La famille sera également plus disposée que l'organisation à payer une rançon et pourrait commencer à vendre des biens pour réunir l'argent nécessaire. Même si les familles ont leur propre droit d'initiative, les organisations doivent les informer des conséquences et des risques potentiels de telles actions. Le paiement d'une rançon ne garantit pas la libération et peut entraîner d'autres demandes.
- **Gérer la révélation d'informations.** Le partage d'informations avec les membres de la famille et d'autres personnes doit être soigneusement mis en balance avec la nécessité de gérer efficacement l'incident.

► Voir le chapitre 4.4 pour plus d'informations sur la liaison avec la famille.

Liaison avec les autorités

Il est conseillé d'informer immédiatement les autorités (services et institutions gouvernementaux compétents) à propos d'un enlèvement. Cela inclut les autorités du pays où l'enlèvement a eu lieu, ainsi que le gouvernement du pays de la personne enlevée (cela peut concerner plusieurs autorités si celle-ci possède plusieurs nationalités). Même si l'enlèvement a lieu dans une zone non contrôlée par le gouvernement, celui-ci doit tout de même être informé.

L'équipe de gestion de crise devra décider d'une ligne de conduite et de la manière de tirer parti des relations avec toutes les autorités compétentes. Les autorités auront accès à des informations et à des renseignements, à des réseaux et à des services qui ne sont peut-être pas à la disposition de l'organisation et seront donc peut-être les mieux placées pour appuyer une libération. C'est particulièrement le cas des autorités du pays où l'enlèvement a eu lieu. En même temps, les autorités peuvent avoir des objectifs qui ne servent pas directement les intérêts et le bien-être de la personne enlevée. Elles peuvent également se méfier de la capacité d'une organisation humanitaire à gérer correctement l'enlèvement, ou vouloir empêcher l'organisation d'entamer un dialogue avec les auteurs de l'enlèvement, qu'elles considèrent comme des «terroristes» ou des rebelles (dans certains pays,

tout contact avec ces derniers peut être illégal). Si les autorités souhaitent régler rapidement l'incident, elles pourraient être enclines à recourir à la force plutôt qu'à la négociation, ou à les utiliser conjointement.

Les aspects pratiques et les principes à convenir et à confirmer avec les autorités compétentes peuvent être les suivants:

- La sécurité, la sûreté et le bien-être de la personne enlevée doivent être la préoccupation principale.
- La stratégie globale de réponse.
- La stratégie médiatique (notamment la confidentialité).
- Une approche commune envers la famille – la collaboration avec les agents de liaison familiale de tout organisme gouvernemental est bénéfique.
- Le choix d'un communicateur (voir ci-dessous).

Certaines organisations ont intégré un membre de leur personnel dans une équipe gouvernementale chargée de la gestion de la réponse. Dans le cadre d'un tel arrangement, il est important que le représentant de l'organisation comprenne la position de l'organisation et les limites de la relation.

Recommandations pour le premier contact avec les autorités locales

- Discuter et convenir au sein des différentes équipes de réponse de la ligne à suivre.
- Préparer un texte pour informer les autorités des faits.
- Contacter un interlocuteur officiel, qui devrait déjà être connu.
- Mettre tout en œuvre pour garantir que la sécurité de la personne enlevée soit la priorité absolue.
- Anticiper le fait qu'une fois informées, les autorités pourraient contacter les médias et communiquer avec eux.
- Établir une procédure de contact pour les futurs briefings.

► Voir le chapitre 4.4 pour plus d'informations sur la liaison avec les autorités en cas de crise.

Gérer les communications

Une gestion efficace de la communication lors d'un enlèvement nécessite une planification stratégique, le maintien de la confidentialité et une coordination avec les parties prenantes internes et externes afin d'assurer la sûreté et le bien-être de la personne enlevée et de sa famille.

Le partage d'informations détaillées en dehors de l'organisation doit être déterminé avec soin et ne doit avoir lieu que dans le cadre d'un plan délibéré visant à faciliter la libération. Le partage d'informations sur la base du « besoin de savoir » est considéré comme une bonne pratique.

Il est conseillé à l'équipe de gestion de crise de décider des communications avec les parties prenantes internes et externes, avec le soutien d'une équipe de communication de crise. L'équipe de communication de crise serait chargée de gérer les relations avec les médias, notamment en élaborant et en mettant en œuvre des stratégies de communication, en suivant les médias et en désignant un porte-parole. Elle peut également contribuer à protéger la vie privée de la personne enlevée et de sa famille en gérant les réseaux sociaux. Il peut être judicieux de fermer les comptes sur les réseaux sociaux afin d'empêcher les auteurs d'y accéder.

Il est utile de rédiger des messages clairs et concis pour gérer la couverture médiatique. Un message central peut souligner que l'organisation tient les auteurs des faits responsables de la sûreté et du bien-être du membre du personnel, et que tout ce qui peut être fait est en train d'être fait. Étant donné que différents médias (internationaux et nationaux) peuvent présenter l'histoire de manière différente, il est essentiel que les responsables médias des différents bureaux se consultent avant de publier toute déclaration de l'organisation.

Pour gérer les demandes des médias et l'intérêt du public, l'organisation peut publier des mises à jour sur son site web. Cela permet de réduire les demandes par téléphone et d'assurer la cohérence des messages. Les organisations doivent partir du principe que les auteurs suivent l'actualité, ce qui rend imprudente toute tentative de communication ou de négociation via les médias publics. Les messages diffusés par les médias peuvent facilement être déformés, ce qui compromet les efforts sincères de communication et de négociation. Il est important de dialoguer avec les rédacteurs et les journalistes afin d'encourager la collaboration.

Si la famille souhaite lancer un appel public, celui-ci doit être constructif et géré avec prudence. Le public cible n'est généralement pas les auteurs des faits, mais les autorités chargées de la sécurité, avec des messages rédigés de manière à garantir la poursuite des efforts pour résoudre la situation.

Exemple de cas : Contrôler la rumeur

Au cours de la phase finale des négociations pour la libération du personnel humanitaire enlevé en Somalie, contrôler les rumeurs est devenu un véritable défi. Alors que la situation était encore tendue, une autre organisation humanitaire a annoncé de manière inattendue que les otages avaient été libérés et avaient quitté le pays la veille à bord d'un avion. Cette rumeur s'est immédiatement répandue au sein de la communauté humanitaire et a été reprise par les médias locaux. Il a fallu deux heures de recherche effrénée à l'organisation concernée par cet enlèvement contre rançon pour découvrir d'où venait cette annonce et publier un rectificatif.

La médiatisation peut être bénéfique si les auteurs sont sensibles à leur réputation, mais c'est rarement le cas des groupes qui recourent aux enlèvements pour attirer l'attention. Dans de tels cas, les auteurs peuvent eux-mêmes faire appel aux médias, transformant ainsi la situation en un spectacle dangereux où la mort de la personne enlevée peut être utilisée pour créer un dénouement dramatique. Pour contrer cela, il faut persuader les médias de ne pas contribuer à dramatiser la situation.

Lorsque les personnes enlevées ont la possibilité d'accéder aux médias, leur envoyer des messages de soutien par ces canaux peut contribuer à leur remonter le moral.

Une communication interne efficace, par exemple au moyen de briefings ou de publications sur l'intranet, peut aider le personnel à se sentir impliqué et informé, ce qui soutient et renforce les efforts officiels de réponse. Parfois, le personnel met en place des fonds d'appel volontaires pour soutenir la famille de la personne enlevée.

► *Pour en savoir plus sur la communication et la gestion de crise, voir le chapitre 4.4.*

Rançon

En principe, aucune rançon ne devrait jamais être versée, car cela augmente le risque général de récurrence ou d'imitation d'incidents ciblant la même organisation ou d'autres organisations dans la zone. La réalité est que, dans de nombreux cas, une rançon est versée ou des concessions sont faites, même si les organisations peuvent le nier.

Lorsque le paiement d'une rançon est une stratégie potentielle viable, une analyse juridique et politique approfondie doit être menée au préalable afin d'identifier les conséquences et les risques juridiques ou financiers potentiels (dans toutes les juridictions concernées : le pays où l'incident s'est produit, le pays d'origine de

l'organisation et le pays d'origine de la personne enlevée). Cela dit, des considérations politiques peuvent influencer la décision d'un gouvernement d'appliquer ou non cette législation. Les organisations doivent également savoir que, même si elles ont souscrit une assurance couvrant le paiement des rançons, celles-ci ne sont remboursées qu'après coup. Elles doivent donc s'assurer de disposer des fonds nécessaires pour effectuer le paiement en premier lieu.

7.9.5 Négociations et communications

Communiquer et négocier avec les auteurs

Les revendications formulées par les auteurs constitueront un élément crucial des négociations, tout comme la question de savoir qui, dans la pratique, peut ou doit y répondre. Les objectifs et les revendications des auteurs peuvent évoluer. Il existe de nombreux exemples de situations où les revendications politiques ont disparu, ne laissant place qu'à une demande d'argent. L'inverse peut également se produire : un groupe criminel peut « revendre » une personne enlevée à un groupe à motivation politique si aucune rançon n'est versée. Si les auteurs demandent des concessions politiques aux autorités, cela échappera au contrôle de l'organisation.

Recommandations pour le premier contact avec les auteurs

- Veiller à ce qu'un communicateur soit briefé et dispose d'un script pour la prise de contact ; celui-ci devra être rédigé dans les langues appropriées.
- Toujours enregistrer la conversation. Cela peut nécessiter un équipement distinct (par exemple, un smartphone).
- Adopter une attitude coopérative.
- Demander à parler à la personne enlevée.
- Insister pour obtenir la preuve que la personne enlevée est en vie.
- Expliquer les responsabilités limitées du communicateur (voir ci-dessous).
- Fixer un délai de réponse.
- Établir une procédure pour les rappels (par exemple, numéro de téléphone, mot de passe).
- Une fois le contact établi, préparer un script révisé pour les interactions suivantes.

Les bonnes pratiques en matière de communication avec les auteurs comprennent les éléments suivants.

- Enregistrer et consigner tous les détails et scripts relatifs aux appels avec les auteurs. Ceux-ci doivent rester confidentiels.
- Évaluer les motivations des auteurs et déterminer si leur comportement suit un schéma cohérent dans le temps. Sont-ils agressifs et menaçants, rationnels et factuels, ou très émotifs? Quel ton et quel style de communication seraient les plus efficaces pour désamorcer la situation et établir une relation?
- Demander une preuve d'identité et de détention afin de confirmer que la personne enlevée est toujours en vie et n'a pas été transférée à un autre groupe. Si un enregistrement audio ou vidéo peut être utile, il ne constitue pas une preuve de vie définitive, en particulier compte tenu de l'utilisation croissante de l'IA (qui permet de reproduire des voix et des vidéos). L'organisation doit demander à la famille ou à un ami proche de fournir un détail spécifique et intime, quelque chose que les auteurs sont peu susceptibles de connaître. Les questions de preuve de vie peuvent également être utilisées si elles figurent dans le dossier. Si aucune preuve crédible d'identité et de vie n'est fournie, les organisations doivent envisager de mettre fin aux négociations.

Preuve de vie

Il est essentiel d'établir la preuve qu'une personne enlevée est toujours en vie, et les organisations devraient envisager d'exiger des questions relatives à la preuve de vie dans le cadre des informations sur les proches. Il convient de veiller à la manière dont ces informations sont stockées et transmises. Dès que possible, des questions supplémentaires de preuve de vie doivent être obtenues auprès de la famille afin de permettre à l'organisation de continuer à vérifier cela au fur et à mesure que l'incident évolue. Ces questions doivent être uniques et faciles à répondre pour la personne enlevée.

- Mentionner le nom de la personne enlevée chaque fois que possible afin de l'humaniser aux yeux de l'auteur et d'encourager un traitement équitable, notamment en indiquant ses besoins particuliers, par exemple le port de lunettes ou la prise de médicaments. Il peut être utile de signaler d'autres préoccupations, telles que l'état émotionnel de la famille et des enfants, et d'étudier la possibilité d'organiser un échange de messages.

- Souligner que le communicateur n'a aucune autorité décisionnelle et doit consulter d'autres personnes. Cela laisse le temps de réfléchir et donne à l'organisation une certaine marge de manœuvre. En même temps, rien ne doit laisser entendre qu'un tiers (les autorités ou un expert en réponse de crise, par exemple) conseille l'organisation. Il faut se préparer au cas où les auteurs exigeraient de parler au décideur plutôt qu'au communicateur.
- Réaffirmer la politique de non-paiement de rançon afin de montrer que l'organisation reste cohérente et que le temps qui passe n'affaiblit pas sa détermination.
- Convenir des délais et des méthodes de communication, en prévoyant des solutions de secours en cas de problèmes tels qu'une mauvaise couverture mobile ou une interruption du réseau. Cela implique notamment de convenir d'un mot de passe avec les auteurs afin de confirmer leur identité et de s'assurer que l'organisation ne communique pas avec des imposteurs.
- Maintenir la communication. Les organisations ne doivent pas rompre le contact avec les auteurs, sauf s'il est certain que la personne avec laquelle elles communiquent n'est pas le véritable auteur ou que la personne enlevée n'est plus en vie. Les auteurs doivent savoir que l'organisation tient à maintenir la communication.
- Refuser de se rendre à un endroit précis pour une rencontre. Si la pression est très forte, l'organisation doit exiger des garanties détaillées en matière de sûreté. Il y a un risque que d'autres enlèvements aient lieu.

À un moment donné, le responsable de la communication de l'organisation peut s'adresser directement au membre du personnel enlevé, et il est important d'être clair sur le type d'informations et de messages à transmettre. Le communicateur doit éviter de fournir à la personne enlevée des informations dont les auteurs ne doivent pas avoir connaissance, mais la rassurer en lui affirmant que tout est mis en œuvre pour obtenir sa libération. Souvent, les personnes enlevées s'inquiètent de la façon dont leur famille fait face à la situation, et le communicateur peut essayer d'apaiser cette inquiétude.

Le rôle du communicateur

L'appellation « communicateur » est délibérément distincte de celle de « négociateur », car l'équipe de gestion de crise doit garder le contrôle de toutes les négociations. La désignation d'un communicateur dans les phases initiales peut également servir à créer un délai permettant de mener des consultations et des analyses internes et externes avant de répondre aux demandes des auteurs, et renforce la position du communicateur selon laquelle il n'est pas en mesure de prendre des décisions. Ces personnes doivent être bien préparées et soutenues, car elles communiquent directement avec les auteurs. Elles relèvent généralement directement de la haute autorité décisionnelle de l'équipe de gestion de crise.

Comme les enlèvements peuvent durer longtemps, il peut être nécessaire de faire appel à plusieurs communicateurs.

Le communicateur doit être capable de gérer efficacement des niveaux élevés de stress tout en respectant une stratégie de négociation. Ce rôle peut être assumé par une personne de l'organisation ou par un expert externe. Idéalement, le communicateur serait un ressortissant national parlant couramment la langue et le dialecte des auteurs, comprenant la culture et ayant une solide connaissance des dynamiques locales et des interactions sociales. Il doit être fiable et capable de travailler sous une pression extrême, disponible 24 heures sur 24, 7 jours sur 7, et prêt à suivre les instructions de l'équipe de gestion de crise. Le communicateur doit être bien formé, idéalement au moyen d'exercices de simulation, car il est susceptible d'être confronté à des demandes et à des pressions inattendues de la part des auteurs.

Les communicateurs ne font pas partie de l'équipe de gestion de crise et ne participent pas aux réunions régulières de cette dernière. Ceci afin d'éviter qu'ils en sachent trop et divulguent accidentellement des informations importantes aux auteurs. Si les auteurs exigent de parler à quelqu'un d'autre que le communicateur désigné, l'organisation doit veiller à ce que le communicateur désigné écoute discrètement la conversation.

Les communicateurs peuvent également provenir de l'extérieur de l'organisation. Un intermédiaire peut se présenter au sein de la communauté, ou être recherché par l'organisation, proposé ou contacté par les autorités, voire présenté par les auteurs. Il n'est pas rare que des personnes respectées et influentes au niveau local s'impliquent dans la résolution d'un enlèvement. Les anciens ont par exemple joué un rôle influent en Somalie et en Afghanistan.

Dans une situation où le degré d'acceptation est élevé et où la communauté conserve une certaine influence sur les auteurs, une personne de confiance issue de la communauté locale peut être en mesure d'obtenir la libération de la personne enlevée. Il convient toutefois de préciser qu'elle ne peut prendre d'engagement au nom de l'organisation sans son consentement préalable. Face à des criminels bien organisés et plus autonomes par rapport à la communauté, les dirigeants traditionnels peuvent s'avérer inefficaces. La question de la confiance est cruciale. Au nom de qui l'intermédiaire agit-il ? A-t-il des liens avec les auteurs ? Qui contrôle les négociations ? La question d'une rémunération se posera également. Les organisations peuvent envisager de rembourser certaines dépenses opérationnelles aux intermédiaires locaux, par exemple pour couvrir les frais de déplacement, de logement, d'alimentation et de communication. Une telle rémunération peut toutefois ne pas être appropriée si l'organisation traite avec une personne qui, selon les normes locales, est déjà considérée comme relativement aisée.

Les autorités peuvent également désigner un négociateur officiel. La première étape du négociateur consistera probablement à instaurer un climat propice au dialogue. Dans un premier temps, l'accent sera probablement mis sur des questions mineures sur lesquelles un accord peut être trouvé. Cela permettra d'établir une base pour discuter des questions plus difficiles. Si les autorités désignent le négociateur, il existe un risque que des considérations autres que la sûreté et la libération de la personne enlevée entrent en jeu. Une autre solution consiste à demander à une entité non gouvernementale prestigieuse de proposer un envoyé pour tenter de négocier la libération.

Obtenir la libération par la force

Il n'est pas rare que les forces de sécurité tentent de localiser la personne enlevée et tentent de la secourir ou créent un état de siège pour forcer les auteurs à se rendre. Il s'agit d'une stratégie très risquée pour la personne enlevée. Une libération forcée peut mal tourner pour plusieurs raisons, avec des conséquences potentiellement fatales.

Du point de vue de l'organisation, deux éléments sont particulièrement importants.

- Les personnes qui mènent l'action ont-elles un commandement général clair ? Si ce n'est pas le cas, des actions non coordonnées pourraient mettre en danger la vie de la personne enlevée.
- Les troupes disposent-elles d'une description claire de la personne enlevée afin de pouvoir la différencier des auteurs, et ont-elles reçu des instructions claires leur enjoignant de ne tirer que sur ceux qui tirent sur elles ? La personne enlevée peut porter le même type de vêtements que les auteurs et être blessée pendant la confusion causée par un siège.

En réalité, les capacités de la famille ou de l'organisation à influencer les plans et les actions des forces de sécurité peut être limitée. Les autorités réagiront comme elles le jugent opportun, et toute mesure prise par une autorité sera probablement tenue secrète pour des raisons de sécurité opérationnelle.

Répondre à des situations de siège soudaines

Certaines situations de siège peuvent se produire soudainement et échapper largement au contrôle de l'organisation. On peut citer comme exemple le siège de l'hôtel Radisson Blu au Mali en 2015, où des travailleurs humanitaires figuraient parmi les otages. Bien que les forces armées soient chargées de mener la réponse dans ces situations, les organisations peuvent chercher à :

- Déterminer rapidement si des membres du personnel ont été touchés par l'incident.

- Mettre en œuvre des mesures pour protéger le personnel restant, par exemple en le transférant hors de la zone.
- Mobiliser des équipes de gestion de crise pour assurer la liaison avec la famille, gérer les relations avec les médias et coordonner les efforts avec les autorités.
- Se préparer à apporter un soutien au personnel en difficulté, notamment en matière de soins médicaux et psychologiques, de paiement des assurances et de rapatriement.
- Procéder à un examen a posteriori afin de déterminer l'efficacité des mesures de sécurité prises avant l'incident et de la réponse de l'organisation, et communiquer les conclusions au personnel concerné.

7.9.6 Gérer les conséquences

Un enlèvement peut se terminer par la libération ou la mort de la personne enlevée ou, dans certains cas, rester indéfiniment sans issue. Les organisations humanitaires doivent être préparées à gérer toute une série de scénarios possibles.

Libération

Le retour des personnes libérées doit être correctement organisé et géré. Au moment de leur libération, les personnes survivantes devraient être accueillies par quelqu'un qu'elles connaissent, par exemple un collègue proche. Une collègue féminine serait préférable lorsque la personne enlevée est également une femme. Il faudra en priorité répondre à ses besoins physiques immédiats et veiller à son confort.

Si plusieurs membres du personnel de différentes organisations avaient été enlevés, la situation pourrait ne pas être résolue pour toutes les parties prenantes. Si tel est le cas, il convient d'être extrêmement prudent dans les déclarations publiques jusqu'à ce que l'incident soit résolu pour toutes les parties.

Les considérations relatives aux bonnes pratiques comprennent :

- Répondre aux besoins de la personne survivante et des membres de sa famille, tant dans l'immédiat qu'à plus long terme.
- Informer et assurer le suivi auprès des parties prenantes concernées, telles que les médias, d'autres organisations et autorités, et gérer leurs interactions avec la personne survivante et son accès à celle-ci.
- Débriefing la personne survivante lorsqu'elle est prête.
- Assurer le suivi auprès des personnes et des groupes qui ont soutenu la réponse.

- Apporter un soutien, par exemple sous forme de congés, aux membres de l'équipe de réponse.
- Désactiver la structure de gestion de crise, notamment en classant les dossiers et les documents, et en rédigeant un compte rendu d'incident final qui pourra être partagé avec les parties prenantes internes et externes.

Les enlèvements peuvent être des expériences traumatisantes. Les personnes survivantes peuvent avoir besoin d'une aide à long terme et d'un soutien professionnel, en particulier pendant les phases initiales. L'organisation devrait prendre toutes les mesures possibles pour réduire le fardeau qui pèse sur les personnes survivantes et leur permettre de se rétablir.

Il est recommandé d'associer les personnes survivantes aux décisions qui les concernent directement, en suivant une approche centrée sur elles, mais de le faire progressivement et conformément aux avis médicaux et aux souhaits de chacune.

► *Pour plus de détails, voir le chapitre 5.4 sur le bien-être du personnel.*

Résolution infructueuse

Une résolution infructueuse peut impliquer la confirmation du décès avec récupération du corps, la notification du décès sans récupération du corps, ou le fait que l'affaire reste non résolue (par exemple, si aucune preuve de vie n'est obtenue ou si les auteurs ne donnent pas de nouvelles).

Il est conseillé aux organisations d'être prêtes à fournir un soutien à long terme à la famille et aux autres membres du personnel touchés par l'incident.

► *Pour plus de détails sur le contenu de ce soutien, voir le chapitre 5.4 sur le bien-être du personnel.*

Si un corps est retrouvé, une autopsie et une enquête seront probablement nécessaires, soit dans le pays où l'incident s'est produit, soit ailleurs. Une enquête officielle du médecin légiste (ou enquête judiciaire) peut également être menée dans le pays d'origine de la personne enlevée. Les organisations doivent être prêtes à coopérer avec les autorités et à partager les preuves.

La famille peut également remettre en question la manière dont l'organisation a géré l'incident, ouvrir une enquête et intenter une action en justice contre elle. Dans ce cas, les registres tenus par l'organisation au fur et à mesure que l'incident s'est déroulé constitueront une source importante de preuves.

Si les choses tournent mal lors d'un enlèvement géré par les autorités, l'organisation peut demander une enquête sur la manière dont l'opération a été menée et sur la question de savoir si ce qui a mal tourné aurait pu être évité.

Examens a posteriori

Les examens a posteriori se concentrent sur ce qui s'est passé et pourquoi : les décisions prises, les raisons pour lesquelles elles ont été prises et leurs résultats. Un examen a posteriori peut inclure des éléments de redevabilité, mais ne doit pas être un exercice visant à attribuer des responsabilités. L'examen devrait viser à déterminer les mesures qui peuvent être prises pour éviter que des incidents similaires ne se reproduisent à l'avenir et la manière de les gérer s'ils se produisent.

Il est important qu'une organisation fasse preuve de transparence quant à ses conclusions, en particulier auprès du personnel concerné par l'incident. L'examen peut être diffusé dans le cadre d'une session où les principales parties prenantes, y compris la personne survivante, sont invitées à partager les enseignements tirés. L'absence de partage d'informations en toute transparence avec le personnel concerné par le Norwegian Refugee Council a été identifiée comme une lacune lors du procès qui a suivi l'enlèvement de membres du personnel à Dadaab, au Kenya, en 2012.

► Pour plus de détails sur les examens a posteriori, voir le chapitre 4.4.

Informations complémentaires

Recommandations et ressources

Buth, P. (2010) *Crisis management of critical incidents* (en anglais, «Gestion de crise des incidents critiques»). European Interagency Security Forum (www.gisf.ngo/resource/crisis-management-of-critical-incidents).

Clamp, D. (2022) *Ten years on: learning from the Steve Dennis case* (en anglais, «Dix ans plus tard : enseignements tirés de l'affaire Steve Dennis»). GISF (www.gisf.ngo/blogs/ten-years-on-learning-from-the-steve-dennis-case/).

Davidson, S. (2013) *Gérer le message. Gestion de la communication et des médias en cas de crise de sécurité*. European Interagency Security Forum (www.gisf.ngo/resource/managing-the-message).

European Interagency Security Forum (2017) *Abduction and kidnap risk management guide* en anglais, «Guide de la gestion de risque en cas d'enlèvement et d'enlèvement contre rançon») (www.gisf.ngo/resource/abduction-and-kidnap-risk-management-guide/).

Hostage International (n.d.a) *Comment pouvons-nous vous aider* (www.hostageinternational.org/how-we-can-help/).

Hostage US (2022) *A life after captivity* (en anglais, «Une vie après la captivité. Reintegration guide (Guide de réintégration)») (www.gisf.ngo/resource/a-life-after-captivity/).

Hostage US (n.d.) *Hostage US guides* (en anglais, «Guides de Hostage US») (<https://hostageus.org/resources/hostage-us-guides>).

Merkelbach, M. et Kemp, E. (2016) *Duty of care : a review of the Dennis v Norwegian Refugee Council ruling and its implications* (en anglais, «Devoir de diligence : examen de l'arrêt Dennis contre Norwegian Refugee Council et de ses implications»). European Interagency Security Forum (www.gisf.ngo/resource/review-of-the-dennis-v-norwegian-refugee-council-ruling/).

7.10 Menaces liées au combat et vestiges de guerre

Ce chapitre examine les menaces découlant des conflits armés majeurs ou des «actes terroristes», notamment les bombardements, les tirs de missiles et d'obus, les tirs croisés et les tirs de snipers, les engins explosifs improvisés (EEI) et les armes chimiques, biologiques, radiologiques et nucléaires (CBRN). Il aborde également les tactiques de siège et les dangers liés aux «vestiges de guerre» tels que les mines terrestres et les munitions non explosées. Ce chapitre présente des mesures d'atténuation que les organisations peuvent envisager, mais dans les environnements extrêmes impliquant des combats importants, les recommandations de bonnes pratiques contenues dans cet ouvrage ne seront pas suffisantes et ne peuvent remplacer une consultation directe avec des experts.

7.10.1 Questions et considérations fondamentales

Les premières questions à examiner dans les zones de combat actif sont de savoir si l'organisation est disposée et capable d'opérer dans ces conditions, et si les avantages d'une telle opération (c'est-à-dire la criticité des programmes) l'emportent sur les risques résiduels. Existe-t-il des besoins importants en matière d'assistance et/ou de protection, et des possibilités d'y répondre, qui justifient la présence de l'organisation? Combien de personnes et quel type de personnel seront nécessaires pour remplir efficacement cette fonction? Quels moyens supplémentaires, notamment en matière de formation, d'équipement, de compétences spécialisées et d'assurance, seront nécessaires pour respecter le devoir de diligence?

La réalité est que, dans la plupart des zones de combat actif, la présence humanitaire, en particulier celle des organisations internationales, sera bien moins importante que dans les zones de conflit de faible intensité ou dans les zones sans conflit. Comme d'autres civils, les travailleurs humanitaires risquent de subir la violence collatérale (et d'être directement pris pour cible par des acteurs armés), ce pour quoi les efforts de gestion des risques de sécurité ne peuvent pas faire grand-chose au-delà de l'évitement des lieux à haut risque et de l'adoption de protocoles de mise à l'abri. Pour la plupart des organisations, les coûts et les capacités nécessaires pour atténuer les risques encourus par le personnel dans les conflits armés majeurs actifs sont prohibitifs, et celles qui choisissent d'intervenir programment souvent leurs activités dans des zones plus sûres et se concentrent sur les populations déplacées et les besoins adjacents.

Pour les organisations opérant dans des zones de combat, le risque ne se limite pas toujours à la violence collatérale. Il existe de nombreux exemples d'attaques ciblant directement les acteurs humanitaires et les opérations humanitaires, perpétrées tant

par des armées nationales que par des groupes armés non étatiques. Les organisations qui sont disposées à atténuer les risques de violence collatérale fixent généralement leurs limites là où il existe un risque élevé d'être directement pris pour cible et où les efforts visant à obtenir l'acceptation et un accès négocié sont insuffisants pour atténuer ces risques. Dans ces circonstances, ce sont souvent des groupes informels locaux bénévoles et des particuliers, qui ont encore moins de capacités à se protéger, qui sont les premiers à apporter une aide.¹¹⁷ Cela soulève une autre question fondamentale : si une organisation soutient ces efforts ponctuels au moyen de subventions ou d'autres moyens, dans quelle mesure contribue-t-elle à atténuer les risques de ses partenaires ?

Enfin, même si seule une petite partie des organisations humanitaires choisissent d'intervenir dans les zones à haut risque les plus extrêmes, la coordination et la communication dans ces contextes sont plus vitales que jamais. Dans ces contextes, les organisations devraient s'efforcer de rechercher, soutenir et participer aux efforts d'action collective sur la déconfliction, l'accès humanitaire et le plaidoyer pour la protection et le passage sûr de l'aide.

7.10.2 Mesures d'atténuation générales pour les zones de combat

Les organisations qui ont l'intention d'opérer dans des zones de combat actif, où elles peuvent être confrontées à la violence directe ou collatérale résultant de frappes aériennes et/ou de l'utilisation de munitions lourdes (bombardements, tirs d'artillerie, mines terrestres ou grenades, par exemple), devraient inclure les considérations générales suivantes dans leur planification de la gestion des risques de sécurité.

Évaluations des risques et mesures d'atténuation

Les menaces liées au combat doivent être soigneusement prises en compte dans les évaluations des risques. L'avis d'un spécialiste peut être nécessaire pour identifier et mettre en œuvre des mesures d'atténuation (des exemples sont donnés ci-dessous). Les structures de gestion de crise et les plans d'urgence actualisés sont particulièrement importants dans les zones de conflit actif. Les organisations ont tout intérêt à mettre en place un système permettant de suivre les niveaux de sécurité et d'adapter les mesures de gestion des risques de sécurité lors du passage d'une situation de non-conflit à une situation de conflit (ou inversement), qui peut être progressif ou soudain.¹¹⁸ Plus le risque est élevé, plus le devoir de diligence de l'organisation est important. Cela signifie que le personnel le plus à risque doit être identifié et bénéficier du niveau de soutien le plus élevé en matière de gestion des risques de sécurité. Les organisations devraient également réfléchir à la manière de soutenir les partenaires qui pourraient mettre en œuvre les programmes en leur nom dans ces contextes.

► Voir le chapitre 3,5 sur les partenariats.

117 Voir GISF et Humanitarian Outcomes (2024) *State of practice: the evolution of security risk management in the humanitarian space* (en anglais, «État des lieux: l'évolution de la gestion des risques de sécurité dans le domaine humanitaire») (https://humanitarianoutcomes.org/security_risk_mgmt_humanitarian_space_2024).

118 Pour une analyse plus approfondie, voir GISF et Humanitarian Outcomes (2024).

Choix de l'emplacement

L'emplacement du personnel et des actifs est généralement la première considération et doit être éclairé par l'évaluation des risques et l'analyse du contexte. Les bureaux, entrepôts et résidences doivent être situés loin des cibles militaires évidentes ou probables, telles que les aéroports, les casernes, les dépôts de carburant, les bâtiments officiels ou les points stratégiques tels que les carrefours, les gares ferroviaires, les centrales électriques et les bâtiments de radio et de télévision. Si l'organisation travaille dans une zone susceptible d'être la cible de tirs, ses installations doivent être déplacées aussi loin que les exigences opérationnelles le permettent. Un premier et un deuxième emplacement de repli peuvent être identifiés à l'avance au cas où la violence s'intensifierait dans la zone cible ou s'étendrait à d'autres zones.

Recrutement et dotation en personnel

Idéalement, le personnel humanitaire travaillant dans des zones touchées par les combats, en particulier ceux qui ont des responsabilités en matière de sécurité, aura à la fois une expérience préalable dans des environnements comparables et une formation spécialisée dans les domaines pertinents de la gestion des risques de sécurité. Il devra également faire preuve de discernement, de capacités à travailler sous pression et de résilience mentale. Le recrutement, qui a toujours été un défi pour le secteur humanitaire, l'est encore plus dans les opérations menées en situation de conflit armé. Ces contextes requièrent des investissements accrus, tant dans la gestion des risques de sécurité que dans le bien-être du personnel en général, notamment en matière d'indemnités de repos et de récupération (R&R) et de soutien en santé mentale. Afin de réduire la stigmatisation et d'encourager davantage de membres du personnel à y avoir recours, les services de santé mentale peuvent être proposés à tous les membres du personnel sur une base facultative, plutôt que sur demande.

► Voir le chapitre 5.4 pour plus d'informations sur le bien-être du personnel.

Formation

Il est recommandé de veiller à ce que le personnel soit formé aux procédures opérationnelles standards et aux mesures à prendre en cas d'incident grave ou d'escalade de la violence. La formation du personnel en vue de son déploiement dans des zones de combat actif doit inclure la connaissance de la situation, les premiers secours, l'utilisation de l'équipement de protection individuelle (EPI) et d'autres équipements pertinents, les procédures d'évacuation et de mise à l'abri, les mesures à prendre en cas de tirs et de stress, ainsi que les premiers secours psychologiques.

► Voir le chapitre 5.2 pour plus d'informations sur la formation.

► Voir le chapitre 5.5 pour plus d'informations sur les premiers secours.

Déconfliction

Les efforts de déconfliction – tels que le Système de notification humanitaire pour la déconfliction (HNS4D) – fournissent des informations sur les mouvements et les emplacements statiques d'une organisation aux acteurs militaires afin d'éviter les frappes accidentelles et les dommages collatéraux.

Il peut arriver qu'un ou plusieurs acteurs armés ne participent pas à la déconfliction ou utilisent les informations à des fins malveillantes. Si l'organisation sait que les combattants agissent de mauvaise foi et pourraient cibler les humanitaires, une approche discrète des lieux et des déplacements (y compris une sécurité de l'information solide) peut être conseillée.

Dans les cas où l'organisation estime plus sûr d'avoir une visibilité élevée et d'informer les acteurs militaires de sa présence, des mesures de déconfliction supplémentaires pourraient inclure la peinture du logo en couleurs vives sur les toits et les murs des bâtiments de l'organisation, le marquage des véhicules, l'utilisation de plaques d'immatriculation spéciales ou l'utilisation de matériaux thermo-réfléchissants visibles par les drones, les armes antichars et autres systèmes d'armes qui utilisent des caméras thermiques. Le drapeau d'une organisation peut ne pas être visible de loin ou par temps sans vent. Il ne faut pas partir du principe que tous les acteurs de menaces potentielles connaissent le nom et le logo d'une organisation humanitaire, ni même l'objectif de cette organisation.

► Voir le chapitre 2.1 pour plus d'informations sur la déconfliction.

Protection physique des sites

Atténuer les risques liés aux combats actifs dans les installations organisationnelles (bureaux, résidences et sites de travail) peut être coûteux et nécessiter des conseils et un soutien spécialisés. Les menaces peuvent inclure des frappes directes ou des dommages collatéraux causés par des bombardements, des missiles ou des tirs d'artillerie, des attaques à la grenade depuis l'extérieur du périmètre, des raids armés et des explosifs embarqués dans des véhicules. Dans les zones de combat, les installations nécessiteront généralement une protection physique ou une fortification, et devront peut-être être situées à proximité de sites d'abri appropriés.

Mesures de fortification

Les blessures causées par une explosion peuvent être causées par une fragmentation primaire (morceaux du corps ou de la coque de l'arme explosive) ou par une fragmentation secondaire (débris de l'environnement environnant propulsés par l'onde de choc, comme les éclats de vitres). Malgré leur nom, les murs anti-explosion sont conçus pour arrêter les éclats d'obus et les balles, et non nécessairement l'onde de choc d'une bombe. Ils peuvent être faits de béton, d'acier, de sacs de sable, de barils de pétrole ou de boîtes remplies de terre, et sont utilisés pour protéger les portes et les fenêtres d'un bâtiment ainsi que la voie d'accès à un abri.

Des salles tampons situées le long des côtés d'un bâtiment peuvent offrir une protection contre les explosions. Les blessures causées par le verre peuvent être réduites en appliquant un film de rétention de fragmentations, également appelé film anti-bris ou «film anti-éclats», à l'intérieur des fenêtres. Il convient de noter que le film de rétention de fragmentations appliqué sur une fenêtre à double vitrage est largement inefficace, de même que lorsqu'il est appliqué à l'extérieur d'une fenêtre. Le film de rétention de fragmentations n'arrête pas non plus les éclats d'obus ou les balles. Bien que le film de rétention de fragmentations soit conçu pour maintenir le verre en place, il n'est pas destiné à le maintenir dans son cadre. Lors d'une forte explosion, toute la vitre peut être projetée dans la pièce. S'éloigner des fenêtres et les laisser ouvertes pour éviter la pression intérieure sont deux mesures d'atténuation simples. Sécuriser ou retirer les objets susceptibles de devenir des projectiles dangereux, tels que les poubelles et les pots de fleurs, peut également contribuer à réduire les risques. Bien que la remise en état des bâtiments pour résister aux ondes de choc puisse être coûteuse et prendre du temps, le renforcement des zones clés comme les halls d'entrée, où une explosion est plus probable, peut être une mesure pratique.

Certaines caractéristiques du bâtiment peuvent offrir une protection supplémentaire, même si aucun bâtiment ne répondra probablement à toutes les exigences. Idéalement, les bâtiments ne devraient pas être directement reliés à des zones hors du contrôle de l'organisation, comme les voies publiques. Les entrées principales ne doivent pas être en ligne de mire directe depuis un espace hors du contrôle de l'organisation, et les bureaux doivent être séparés des entrepôts ou des garages avec accès aux véhicules et avoir leur propre périmètre de sécurité. Un périmètre extérieur clairement défini avec des points d'accès réduits peut sécuriser davantage la zone intérieure du site. Il est préférable d'éviter les garages souterrains, qui présentent des risques importants en cas d'explosion d'une voiture piégée, mais s'ils sont utilisés, leur accès doit être limité au personnel. Les barrières d'accès peuvent offrir une protection supplémentaire. Les zones de stationnement et de dépose des visiteurs doivent être situées à l'extérieur du périmètre extérieur.

Mesures pour le périmètre

Les mesures de contrôle de la vitesse le long des voies d'accès menant aux points d'entrée peuvent contribuer à empêcher les véhicules d'accélérer et de percuter le bâtiment. Ces mesures peuvent inclure l'utilisation d'équipements spécialisés ou, à défaut, de barils remplis de gravier ou de grands chaudrons en béton contenant des fleurs ou des arbustes, solidement enchaînés les uns aux autres. Si le périmètre extérieur est proche du bâtiment, des mesures supplémentaires peuvent être prises, telles que des blocs de béton ou des caissons, afin de minimiser l'impact d'une explosion.

Plus une explosion se produit loin d'un bâtiment, moins elle a d'impact. Bien qu'une distance de 30 mètres entre le bâtiment et une éventuelle explosion soit souhaitable,

cela n'est souvent pas réalisable. Il est conseillé de séparer les entrées réservées au personnel et aux visiteurs, ainsi que les zones de stationnement. Les véhicules du personnel, même à l'intérieur des périmètres sécurisés, doivent être contrôlés au cas où un véhicule aurait été secrètement chargé d'explosifs destinés à être déclenchés à distance, ou qu'un kamikaze se serait emparé du véhicule. Les véhicules et les visiteurs autorisés à entrer dans le bâtiment par le périmètre extérieur doivent être fouillés.

Il est recommandé de laisser un espace libre d'au moins 10 mètres entre le périmètre extérieur et le périmètre intérieur. Des couloirs de circulation à l'intérieur de cet espace peuvent être désignés pour contrôler le trafic, tout mouvement non autorisé en dehors de ces couloirs entraînant une réponse immédiate du personnel de sécurité. À l'intérieur du bâtiment, les espaces accessibles aux visiteurs doivent idéalement rester séparés des zones réservées au personnel. Des mesures de contrôle des visiteurs (et éventuellement du personnel) à l'entrée, y compris la fouille des sacs, sont recommandées. L'entrée ou le hall d'accueil doit idéalement être suffisamment spacieux afin d'accueillir les contrôles sans être directement relié aux autres parties du bâtiment, au cas où une explosion se produirait dans cette zone. Les biens importants, tels que les systèmes informatiques centraux, doivent être situés plus profondément dans les zones réglementées du bâtiment et ne doivent pas être facilement identifiables.

Mesures de mise à l'abri

Bien que la fortification physique puisse réduire les dégâts causés par les quasi-accidents, tels que les effets des explosions et des éclats d'obus, elle est moins efficace contre les coups directs : aucun abri, pas même un bunker en béton, ne peut offrir une protection totale contre toutes les armes. La meilleure protection réside souvent dans une action immédiate, comme se mettre à l'abri ou, en l'absence d'alerte préalable, se jeter au sol pour réduire l'exposition aux éclats. Les abris souterrains, tels que les sous-sols ou les parkings, constituent généralement les options les plus sûres, les salles renforcées situées au rez-de-chaussée étant la meilleure alternative. Les abris doivent être suffisamment grands afin d'accueillir toutes les personnes présentes dans le bâtiment, ainsi que l'équipement essentiel, et suffisamment proches pour être atteints rapidement. Les organisations devraient fixer un délai pour atteindre l'abri, d'environ une ou deux minutes. Le personnel qui ne peut pas se rendre dans un abri dans ce délai depuis son lieu de travail habituel devra trouver un abri plus proche. Si les autorités ont identifié ou construit des abris publics, le personnel doit savoir où ils se trouvent.

Les tranchées et les trous peuvent offrir une protection contre les obus de mortier et les tirs d'avions ou d'hélicoptères volant à basse altitude. Elles doivent être profondes (2 mètres), étroites et suffisamment larges pour accueillir jusqu'à quatre personnes. Une bonne construction est une petite tranchée en forme de L, avec deux points d'entrée et de sortie. Le dessus peut être protégé à l'aide de rondins et de deux

couches de sacs de sable. Ces installations nécessitent également un entretien : la pluie peut provoquer l'effondrement des entrées et inonder la tranchée. Le personnel doit prendre garde aux serpents et autres animaux dangereux qui peuvent faire leur nid dans les tranchées ou les trous.

► *Pour plus d'informations sur les bonnes pratiques générales en matière de sécurité du site, voir le chapitre 7.2.*

Équipement de protection individuelle

L'EPI est souvent requis dans les zones de combat actif, mais il faut garder à l'esprit que l'équipement de protection n'est pas une solution en soi, mais plutôt un élément de plan de sécurité.

Le choix de l'EPI dépend des menaces spécifiques à la zone, en équilibrant la protection avec la mobilité et le confort. Bien que les équipements de niveaux supérieurs offrent une meilleure protection, ils ont aussi tendance à être plus lourds et plus restrictifs, et une formation initiale est nécessaire pour les utilisateurs. Des efforts doivent être faits pour garantir que l'EPI fourni soit bien ajusté et puisse être porté par tout le personnel nécessaire. Parfois, l'EPI disponible n'est pas conçu pour les femmes et n'est pas disponible dans toutes les tailles. Les couvre-gilets et les couvre-casques doivent permettre d'identifier l'organisation humanitaire afin de distinguer les membres du personnel humanitaire des combattants. Dans la plupart des cas, les EPI ne doivent pas être portés sans cette marque de visibilité (à moins que l'organisation ne soit une cible particulière), afin d'éviter que ceux qui les portent ne soient pris pour des acteurs militaires.

Il existe différents types de protection balistique (gilets pare-balles) offrant différents niveaux de protection. Les niveaux de protection sont généralement classés selon les normes de l'Institut national américain de la justice (NIJ).¹¹⁹ Dans la norme NIJ 0101.06, il existe cinq niveaux de protection, allant de IIA (le plus bas) à IV (le plus élevé). Les gilets les plus couramment utilisés par les travailleurs humanitaires opérant dans des zones de combat sont les gilets pare-balles souples de niveau IIIA selon la norme du NIJ, qui protègent contre la plupart des balles d'armes de poing, ou les porte-plaques de niveau III avec inserts rigides (plaques frontales et latérales), qui peuvent protéger contre les balles d'armes d'assaut. Les casques balistiques (niveau III) protègent contre les blessures à la tête causées par les balles et les éclats.

Les véhicules blindés peuvent offrir une bonne protection contre certaines menaces liées au combat. Les véhicules blindés civils sont construits avec des matériaux renforcés tels que l'acier trempé, les fibres synthétiques et le verre pare-balles épais. Les composants spécifiques utilisés dépendent du niveau de protection souhaité. Ils peuvent offrir une protection contre les agressions et les attaques, les balles et les tirs. À moins d'être spécialement conçus pour résister aux mines, ils n'offrent pas une protection adéquate contre les ondes de choc et les éclats d'une mine

¹¹⁹ Voir <https://nij.ojp.gov/library/publications/understanding-nij-010106-armor-protection-levels>

antichar ou d'une bombe artisanale sophistiquée placée en bordure de route. Les véhicules blindés sont beaucoup plus lourds que les véhicules normaux et très coûteux. Compte tenu du poids supplémentaire et de la distance de freinage plus longue qui en résulte, les conducteurs doivent suivre une formation spéciale. Il peut être difficile pour les non-spécialistes de distinguer un véhicule blindé d'un véhicule standard. Cependant, lorsqu'il est connu qu'une organisation utilise des véhicules blindés, cela peut influencer la façon dont elle est perçue par la population locale et les acteurs armés ; leur utilisation doit être conforme aux approches de sécurité de l'organisation dans le contexte en question.

► Voir le chapitre 4.2 pour plus d'informations sur les approches de sécurité.

Formation à la conduite défensive pour les manœuvres d'évitement

Des cours sont proposés pour former les conducteurs à la manière de réagir si un véhicule est pris sous le feu ennemi. La décision d'accélérer ou de s'arrêter dépendra de la provenance des tirs et de la cible visée. En général, l'intérieur du véhicule offre une meilleure protection que l'extérieur, et la meilleure option consiste généralement à quitter les lieux en restant le plus bas possible, mais chaque situation est différente.

Si le personnel est pris dans un tir croisé alors qu'il se trouve à l'extérieur à pied, il doit immédiatement se mettre à l'abri derrière un objet solide, rester baissé et se mettre en sûreté en s'accroupissant en cas de tirs d'armes légères. S'il est pris dans un bombardement d'artillerie, il doit se coucher au sol et rester à plat ventre.

7.10.3 Armes et tactiques de combat

Les armes utilisées dans les conflits majeurs varient considérablement en termes d'ampleur, de gravité et de létalité, et le risque d'exposition à une ou plusieurs d'entre elles dans une zone d'opération peut dépasser le seuil de risque acceptable pour de nombreuses organisations humanitaires. Les sections suivantes de ce chapitre décrivent chacune d'entre elles plus en détail, ainsi que les mesures d'atténuation possibles. En général, pour les organisations travaillant dans des zones de conflit actif, certains domaines importants à prendre en considération et dans lesquels investir comprennent :

- les capacités de sensibilisation et d'alerte précoce ;
- l'accès immédiat à un abri ou à un refuge approprié ;
- les plans d'évacuation et les protocoles de mise à l'abri ;
- la disponibilité des EPI ; et
- les formations et exercices spécifiques aux menaces, y compris la formation aux premiers secours en cas de traumatisme.

Le tableau 25 présente les catégories et les caractéristiques des armes de combat typiques utilisées dans les conflits majeurs.

Tableau 25 Aperçu des armes de combat

Arme	Description
Bombardement aérien	Bombes larguées depuis des avions en vol (frappes aériennes). Comprend les bombes traditionnelles larguées depuis les airs et les bombes planantes modernes, qui peuvent parcourir jusqu'à 60 km pour atteindre leur cible.
Missiles/roquettes	Arme explosive autopropulsée pouvant être guidée vers une cible précise (missile guidé) ou simplement dirigée selon une trajectoire donnée (roquette).
Drones (UAV)	Véhicules aériens sans pilote pouvant transporter des charges explosives. Également utilisés à des fins de surveillance et de ciblage.
Projectiles/mortiers (bombardements)	Tir d'obus d'artillerie sur une haute trajectoire en arc afin d'atteindre des cibles éloignées. Parfois décrits comme des projectiles d'artillerie ou des mortiers.
Lance-grenades propulsé par roquette (RPG)	Grenades antichars tirées à l'épaule, capables de détruire des véhicules blindés et des positions fortifiées à courte distance.
Engins explosifs improvisés (EEI)	Une arme explosive qui peut être placée à un endroit, transportée/portée ou livrée par un véhicule. Peut être déclenchée à distance ou par contact.
Armes légères	Armes à feu portatives, par exemple fusils et armes de poing.
Mines	Engins explosifs dissimulés conçus pour exploser en présence, à proximité ou au contact d'une personne ou d'un véhicule.
Munitions non explosées (UXO)	Bombes, obus, grenades ou autres munitions qui ont été tirés, largués ou lancés, mais qui n'ont pas explosé.
Phosphore blanc	Substance toxique utilisée pour créer des écrans de fumée, pouvant être propulsée par des obus d'artillerie, des roquettes et des grenades.
Armes chimiques, biologiques, radiologiques et nucléaires (CBRN)	Bombes et autres armes ou tactiques utilisant des substances biologiques ou chimiques, des radiations ou des explosions nucléaires pour causer la mort et/ou un danger de toxicité.

Bombardements depuis des plateformes aériennes

Lorsque l'on fait face à la menace de violences collatérales résultant de frappes aériennes, il est important de garder à l'esprit que les zones à haut risque sont celles situées à proximité de cibles de grande valeur, dont la destruction présenterait un avantage militaire. Les cibles habituelles des frappes aériennes comprennent les installations militaires, les aérodromes, les centrales électriques, les tours de communication, les ponts, les carrefours routiers stratégiques, les réseaux

de transport et même, de plus en plus, les hôpitaux. Les armes utilisées pour les bombardements aériens comprennent les missiles et les drones.

Les missiles varient en termes de portée, de précision et de vitesse, ce qui peut avoir une incidence sur l'efficacité des systèmes d'alerte et le temps disponible pour se mettre à l'abri. Les missiles sont équipés de systèmes de guidage internes qui leur permettent d'être dirigés ou guidés vers une cible spécifique après leur lancement.

- Les missiles balistiques voyagent à des vitesses hypersoniques pendant la majeure partie de leur vol, les missiles balistiques intercontinentaux (ICBM) atteignant leurs cibles en environ 30 minutes. Leur précision s'est considérablement améliorée, certains systèmes modernes atteignant une précision de l'ordre de quelques dizaines de mètres. Ils peuvent transporter des charges très lourdes, souvent mesurées en milliers de kilogrammes, ce qui leur confère une immense capacité destructrice.
- Les missiles de croisière volent généralement plus bas et plus lentement, avec des temps d'approche mesurés en heures pour les missions à longue portée. Bien que leurs ogives soient généralement plus petites que celles des missiles balistiques, les missiles de croisière modernes peuvent transporter des charges utiles de plusieurs centaines de kilogrammes.
- Les missiles balistiques lancés depuis les airs, comme le Kinzhal russe, peuvent atteindre des vitesses hypersoniques similaires à celles des missiles balistiques, ce qui leur permet d'atteindre leur cible en peu de temps, mais peuvent également manœuvrer en vol. Ils transportent généralement des charges utiles plus importantes que les missiles de croisière, mais plus petites que les missiles balistiques traditionnels.

Les drones, ou UAV, constituent une alternative peu coûteuse aux missiles et aux bombes larguées depuis les airs. Le drone de type «kamikaze» Shahed 136 transporte une charge utile de 40 kg et peut parcourir jusqu'à 2 400 km à une vitesse d'environ 100 km/h. Il est conçu pour une mission aller simple, s'écrasant sur sa cible et fonctionnant efficacement comme un missile bon marché. Les drones de renseignement ou de collecte d'informations (ou drones de surveillance) sont des drones relativement petits, guidés, qui peuvent ou non transporter des charges explosives. Certains drones de surveillance peuvent être utilisés pour coordonner des attaques de missiles balistiques. La présence de tels drones peut servir d'indicateur d'alerte.

Le ciblage direct des acteurs humanitaires, bien que possible, est moins probable que le risque de dommages collatéraux. Les armes utilisées auront des temps d'approche différents et certaines seront plus faciles à intercepter que d'autres. L'Ukraine a développé en 2022 un système national de notification par application mobile afin de diffuser des alertes aériennes accompagnées d'informations sur le type d'arme

utilisé. Des protocoles organisationnels peuvent être mis en place pour demander au personnel de se réfugier dans des abris souterrains ou dans des pièces intérieures, en fonction du type d'attaque.

Tirs d'artillerie/bombardements depuis des plateformes terrestres

Les tirs provenant de plateformes terrestres ciblent généralement les positions (bunkers, tranchées, etc.) et les mouvements des forces adverses. Ils sont souvent utilisés pour perturber les lignes d'approvisionnement, les dépôts et les centres logistiques. On distingue généralement les tirs aléatoires ou de saturation, les tirs prédictifs et les tirs observés.

- Les tirs aléatoires ou de saturation sont très imprécis. Ils peuvent résulter du type d'arme utilisé, comme les lance-roquettes multiples, qui saturent une zone d'obus, ou d'une tactique délibérée, comme un barrage d'artillerie ou ce qu'on appelle un bombardement intensif.
- Les tirs prédictifs sont moins aléatoires. Le ciblage s'appuie sur des calculs cartographiques, sans possibilité d'ajustement par rapport à une cible spécifique.
- Les tirs d'artillerie ou les attaques aériennes observés signifient que des drones ou des observateurs humains au sol surveillent l'endroit où les obus, les roquettes ou les bombes tombent, et transmettent des instructions pour guider l'équipe chargée du tir. Ce type de tir peut être très précis et permet de suivre ou de changer de cible.

Les armes antichars et les RPG sont des armes d'épaule qui tirent des roquettes équipées d'ogives explosives. Elles sont couramment utilisées contre les véhicules blindés, les fortifications et le personnel ennemi se trouvant dans leur ligne de mire directe. Elles sont portatives, polyvalentes et faciles à utiliser. La meilleure façon de s'en protéger est de rester hors de leur portée, qui est de 200 à 500 mètres. Si l'on se trouve dans leur rayon d'action, minimiser le temps passé dans les espaces ouverts et éviter les déplacements prévisibles peut réduire le risque d'être pris pour cible. Les véhicules blindés et les abris fortifiés peuvent constituer des mesures d'atténuation essentielles.

Tirs croisés et tirs de sniper

Les tirs croisés constituent un risque à proximité de toute arme légère ou de tout tir d'artillerie. Bien que la plupart des tirs d'armes légères ne soient généralement efficaces que jusqu'à 300 mètres, certaines mitrailleuses ont une portée effective de plus de 1 800 mètres et les balles peuvent parcourir jusqu'à 6 kilomètres. Les tirs de sniper sont ciblés, et certains fusils de précision peuvent atteindre une cible à longue distance (plus d'un kilomètre).

La meilleure défense contre les tirs croisés et les snipers consiste à réduire l'exposition en gardant le personnel hors de portée (ce qui n'est possible que lorsque les lignes de front sont relativement stables) et loin des zones où des tirs

d'armes légères ont lieu ou où des snipers opèrent. En cas de tir croisé soudain, lorsque le personnel n'est pas ciblé, il doit se mettre immédiatement à terre et essayer de se déplacer vers un endroit plus sûr. À l'intérieur, il doit rester à l'écart des fenêtres et des portes et essayer de se placer entre au moins deux murs et les balles. Cette précaution permettra également d'augmenter la protection contre les ricochets.

Ces précautions s'appliquent également en cas de «tirs de célébration», comme ceux qui peuvent avoir lieu lors de fêtes ou de manifestations, où les blessures et les décès causés par des balles perdues constituent un risque grave.

Prévention et réponse face à un tireur actif

Les incidents impliquant un tireur actif constituent une menace grave dans certains contextes, pouvant entraîner des pertes humaines massives et avoir un impact psychologique important sur les personnes survivantes. Les organisations humanitaires ne sont pas à l'abri de telles menaces, qui peuvent survenir sans avertissement ou presque. L'atténuation des risques nécessite généralement plusieurs niveaux de sécurité, chacun étant conçu pour ralentir ou bloquer l'accès du tireur aux bâtiments ou aux complexes. Le niveau de sécurité le plus interne est généralement une pièce renforcée.

Comprendre les indicateurs de violence potentielle, mettre en œuvre des mesures d'atténuation et disposer d'un plan de réponse bien rodé peut réduire considérablement les risques associés aux fusillades. La formation peut inclure des recommandations sur la stratégie «fuir, se cacher, prévenir».

- **Fuir.** S'il existe une voie d'évacuation sûre, essayer de quitter la zone. Encouragez les autres à partir avec vous, mais ne laissez pas leur indécision vous ralentir. Laissez vos effets personnels derrière vous et gardez vos mains bien visibles à l'intention des personnes armées.
- **Se cacher.** Si l'évacuation n'est pas possible, trouver un endroit où se cacher. Cet endroit doit être hors de vue du tireur, offrir une protection si des coups de feu sont tirés dans votre direction et, si possible, ne pas restreindre les options de sortie. Verrouillez et/ou barricadez les portes, éteignez les lumières et mettez les téléphones en mode silencieux. Si un événement impliquant un tir actif est probable, la construction d'une pièce sécurisée renforcée doit être envisagée.
- **Prévenir.** Une fois en sécurité, contacter les services d'urgence (ou d'autres contacts d'urgence selon le protocole de l'organisation) et de leur fournir autant d'informations que possible. Cela comprend l'emplacement du tireur, une description du tireur et de ses armes, ainsi que le nombre de personnes présentes sur les lieux.

Mines, engins explosifs improvisés et munitions non explosées

Mines

Les groupes armés posent des mines pour défendre leurs positions, perturber les mouvements de l'ennemi, lui interdire l'accès à certains itinéraires et/ou le canaliser sur un itinéraire déterminé. Elles peuvent également être placées autour de cibles potentielles telles que les pylônes électriques (tours de transmission), les usines d'eau et d'électricité et les jonctions ferroviaires, afin de les protéger contre le sabotage et les attaques. Les mines sont utilisées dans des zones civiles et agricoles afin de semer la peur et de provoquer des déplacements de population. Une fois posées, les mines peuvent être déplacées sur une distance considérable par des inondations ou des glissements de terrain.

Il existe généralement deux catégories : les mines antichars et les mines antipersonnel.

- **Les mines antichars** sont de grande taille et ont une puissance explosive considérable. Elles nécessitent généralement un poids important ou un mouvement pour être activées, mais cela peut ne pas être le cas si elles sont anciennes et instables, et elles peuvent causer la destruction presque totale d'un véhicule non blindé (y compris la plupart des véhicules blindés civils, qui ne sont protégés que contre les armes légères).
- **Les mines antipersonnel** sont plus petites. Certaines sont conçues pour causer des blessures en arrachant une main ou un pied. D'autres peuvent causer des dommages beaucoup plus graves, voire mortels. Les dispositifs à fragmentation directe sont conçus pour disperser des fragments sphériques afin de tuer ou de blesser jusqu'à 500 mètres dans une direction donnée.

Exemple de cas : minage répété

En 1995, un véhicule d'une ONG a roulé sur une mine antichar sur une route en Afrique centrale. L'explosion a tué deux passagers et en a blessé trois autres. Pendant la nuit, de nouvelles mines antipersonnel ont été posées autour de l'épave. Le lendemain, une femme du voisinage qui était venue voir ce qui s'était passé à marché sur l'une d'elles et a perdu une jambe.

La sensibilisation du personnel aux dangers des mines est un élément essentiel de la gestion des risques de sécurité dans les zones où des mines sont activement utilisées ou subsistent à la suite de conflits antérieurs. Cela implique notamment :

- De rester vigilant et de savoir à quoi s'attendre.
- Identification, marquage et signalement des mines et des munitions non explosées.
- Techniques d'évitement.
- Que faire lorsque l'on se trouve dans une zone minée, en véhicule ou à pied.
- Réponse d'urgence (en cas d'explosion et de blessures).

Des organisations humanitaires internationales spécialisées dans le déminage, telles que HALO Trust et Mines Advisory Group, proposent des formations et des informations. Dans le pays même, les principales sources d'informations générales et spécifiques à certaines localités sont les suivantes :

- L'organisation nationale de lutte antimines ou les autorités locales et les forces de sécurité.
- Les organisations de déminage et un centre central de lutte antimines de l'ONU.
- Les observateurs militaires ou les forces de maintien de la paix de l'ONU.
- Les hôpitaux et les dispensaires qui prennent en charge les victimes des mines.
- La population locale.

La connaissance du terrain est particulièrement importante. Lorsqu'elles s'aventurent dans une nouvelle zone où des combats sont en cours ou ont eu lieu par le passé, les organisations peuvent se renseigner sur l'histoire des combats dans la zone, sur les accidents survenus (des véhicules, des personnes ou des animaux ont-ils été touchés par des mines, et si oui, quand et où ?), sur les endroits où se rendent les populations locales et ceux qu'elles évitent, sur les routes ou les sections de routes utilisées et dans quelle mesure, ainsi que sur l'utilisation de ces routes (les populations locales marchent-elles, utilisent-elles des vélos ou des véhicules ?). Les mines antichars n'ont peut-être pas explosé et restent un danger.

Les populations locales créent souvent leurs propres signalisations pour marquer les champs de mines, mais celles-ci peuvent être difficiles à identifier pour les étrangers et peuvent être ambiguës ou peu claires. La signalisation peut se résumer à un petit tas de cailloux ou à deux branches croisées au début d'un chemin. On peut demander aux populations locales quelle signalisation elles utilisent et si elles ont un système commun. Si chacun fait à sa manière, il n'y a pas de signalisation commune. Les opérations de déminage marquent les champs identifiés de différentes manières selon les pays, mais la signalisation est généralement assez claire. La couleur rouge est normalement utilisée pour le marquage. Il est important de garder à l'esprit que la signalisation peut être tombée ou être masquée.

Engins explosifs improvisés

Les engins explosifs improvisés (EEI) peuvent être utilisés pour cibler des véhicules, des sites ou du personnel militaires, ainsi que des civils. Ils sont également couramment utilisés pour empêcher l'accès à certaines zones ou à certains itinéraires. Ils peuvent être déclenchés à distance, à retardement ou par la victime elle-même. Les dispositifs généralement déclenchés par la victime, par exemple en marchant sur une plaque de pression ou en tirant sur un fil, nécessitent des restrictions de déplacement prudentes. Les dispositifs à retardement visent généralement un type d'activité particulier ou sont retardés afin de permettre à l'auteur de s'échapper. Les dispositifs de détonation télécommandés ou à commande peuvent être plus précis. Souvent, les EEI sont posés par une force qui se replie afin de compliquer la réoccupation d'une zone. Lorsqu'ils sont utilisés comme pièges, ils sont dissimulés ou camouflés : une porte ou une fenêtre d'une maison peut être piégée, tout comme un puits, un cadavre ou un objet d'usage courant d'apparence anodine, tel qu'un jouet. Une tactique courante consiste à frapper une cible, puis à frapper le même endroit peu après afin de viser les secouristes et les passants qui viennent aider les blessés. Il est important de comprendre comment les EEI sont utilisés afin que l'organisation puisse adapter ses procédures opérationnelles standards en conséquence.

Munitions non explosées

Les munitions non explosées désignent les munitions qui devaient exploser à l'impact, mais qui n'ont pas fonctionné. Les obus d'artillerie et de mortier, et même les munitions pour armes légères, peuvent rester explosifs et devenir de plus en plus instables avec le temps. Les bombes et les obus peuvent s'être enfoncés profondément dans le sol, représentant un danger permanent, par exemple pour les agriculteurs et les constructeurs. Les véhicules et bâtiments militaires ou militarisés détruits ou abandonnés utilisés par des groupes armés peuvent contenir des munitions non explosées, ainsi que des combustibles volatils et des résidus chimiques. Les munitions non explosées peuvent représenter une menace bien plus grande que les mines terrestres, car leur dispersion peut être plus aléatoire et imprévisible, et parce que les munitions elles-mêmes sont susceptibles d'être instables. Les armes à sous-munitions lancées par des obus d'artillerie ou depuis un avion présentent un risque particulier. En plein vol, les conteneurs se brisent et dispersent une multitude de bombes qui peuvent saturer toute une zone.

Recommandations essentielles à l'intention du personnel – mines et munitions non explosées

Lorsqu'il s'agit de mines et de munitions non explosées, les conseils à donner au personnel sont les suivants : ne pas toucher, ne pas s'approcher, marquer si possible, signaler.

Les munitions non explosées sont généralement visibles, bien qu'elles puissent être partiellement ou même totalement enfouies. Elles doivent être considérées comme instables et il ne faut pas y toucher. Le personnel doit marquer leur emplacement et en informer les autorités.

Tout objet suffisamment grand peut être improvisé/piégé pour transporter des explosifs. L'objet piégé est généralement visible, mais pas l'explosif qui y est relié. Tout ce qui se trouve dans une zone non sécurisée peut potentiellement être piégé. Le personnel présent dans la zone ne doit donc pas pénétrer dans des bâtiments vides ou des ruines, ni ramasser quoi que ce soit, ni ouvrir des volets ou des portes.

Les mines ne sont généralement pas visibles. Dans une zone où des mines ont été utilisées, le personnel ne doit pas emprunter de route dont le déminage n'a pas été confirmé. Si une mine est repérée, son emplacement doit être marqué et les autorités informées.

Les personnes non formées ne doivent jamais manipuler des mines ou des munitions non explosées. Une formation «Sensibilisation en milieu hostile» (HEAT) standard ne peut être considérée comme une formation adéquate.

Menaces chimiques, biologiques, radiologiques et nucléaires

À ce jour, les organisations humanitaires ont peu d'expérience directe des menaces chimiques, biologiques, radiologiques et nucléaires (CBRN). En réalité, aucune organisation humanitaire n'est actuellement équipée pour protéger son personnel, et encore moins les civils locaux, en cas d'événement CBRN catastrophique. La plupart des organisations qui ont pris la décision d'opérer dans des zones de conflit majeur ont estimé que la probabilité d'un incident était suffisamment faible pour accepter le risque. Cependant, le risque n'est jamais absent dans un contexte de conflit majeur, il est donc important de l'évaluer, d'en discuter et d'envisager des mesures d'atténuation.

Des armes chimiques ont été utilisées à plusieurs reprises pendant la guerre civile syrienne (à partir de 2012) et en Ukraine (à partir de 2022), où le risque supplémentaire d'accidents nucléaires délibérés ou accidentels a souvent été discuté parmi les organisations humanitaires opérant dans ces pays. Les risques peuvent être les suivants :

- Accidents industriels, tels qu'un incendie ou une explosion dans une usine chimique ou un entrepôt, un accident dans une centrale nucléaire ou une fuite dans une installation de confinement biologique. De tels incidents peuvent entraîner le rejet de substances toxiques dans l'environnement, ce qui présente des risques immédiats et à long terme pour la santé de la population et des intervenants.
- Accidents lors du transport d'agents CBRN à des fins industrielles ou militaires.
- Les dangers naturels tels que les tremblements de terre ou les tsunamis peuvent endommager les installations industrielles ou les entrepôts militaires, entraînant potentiellement la libération de matières CBRN.

- Dommages collatéraux causés aux installations industrielles, aux hôpitaux (services de radiologie) ou aux installations de recherche, de fabrication et militaires à la suite d'un conflit.
- Attaques directes menées par des forces armées utilisant des agents chimiques ou biologiques afin de causer des pertes massives, ou par d'autres groupes utilisant des matières CBRN pour fabriquer des armes telles que des «bombes sales» (dispositifs de dispersion radioactive).

Les individus peuvent être exposés aux dangers CBRN de différentes manières, notamment par inhalation, par contact physique (entre personnes ou avec des objets) et par consommation d'aliments ou d'eau contaminés.

Aux fins de l'atténuation des risques, les questions clés à prendre en considération sont notamment les suivantes: qui sont les membres du personnel les plus à risque (par exemple, le personnel médical)? Existe-t-il des procédures opérationnelles standards élaborées par des experts qui pourraient être adoptées (par exemple, concernant l'utilisation et la nature des EPI)? Quels plans d'urgence peuvent être mis en place (par exemple, retrait, évacuation et aide médicale d'urgence)? Une formation spécialisée est-elle recommandée pour les membres du personnel les plus à risque, par exemple sur la manière de réduire l'exposition en cas de suspicion de contamination? Toute mesure de gestion des risques de sécurité doit être prise en connaissance de cause par des spécialistes.

Phosphore blanc

Le phosphore blanc est utilisé dans les zones de combat pour créer un écran de fumée. Il forme très rapidement un nuage qui non seulement empêche toute vision, mais brouille également les rayons infrarouges, perturbant ainsi les systèmes optiques infrarouges et les systèmes de guidage des armes, tels que ceux utilisés par les missiles antichars. Il peut être dispersé à l'aide de petites grenades fumigènes, de canons de chars, de mortiers ou d'autres pièces d'artillerie. Lors de l'explosion, des particules incandescentes sont projetées vers l'extérieur, suivies de près par des volutes de fumée blanche qui se fondent ensuite en un nuage très blanc.

Bien que son utilisation déclarée ne soit pas celle d'une «arme chimique», le phosphore blanc n'en reste pas moins un produit chimique toxique qui, lorsqu'il est utilisé dans des zones peuplées, a des effets nocifs sur les personnes. Les particules incandescentes adhèrent à la peau et peuvent provoquer de graves brûlures. Les particules continuent à brûler jusqu'à ce qu'elles soient complètement consumées ou qu'elles soient privées d'oxygène. De plus, le phosphore peut être absorbé par l'organisme à travers les zones brûlées et causer des lésions au foie, aux reins et au cœur, voire une défaillance organique. Les particules de phosphore peuvent également être ingérées par voie orale. L'inhalation de la fumée est dangereuse et irrite les yeux, le nez et les voies respiratoires, mais ne présente pas le même danger mortel que les brûlures et l'ingestion.

Informations complémentaires

Recherche générale

GISF et Humanitarian Outcomes (2024) *State of practice: the evolution of security risk management in the humanitarian space* (en anglais, «État des lieux: l'évolution de la gestion des risques de sécurité dans le domaine humanitaire») (https://humanitarianoutcomes.org/security_risk_mgmt_humanitarian_space_2024).

Atténuation des risques de conflit armé

CICR (2006) *Staying alive: safety and security guidelines for humanitarian volunteers in conflict areas* (en anglais, «Rester en vie: directives de sécurité pour les volontaires humanitaires dans les zones de conflit») (<https://reliefweb.int/report/world/staying-alive-safety-and-security-guidelines-humanitarian-volunteers-conflict-areas>).

CICR (2021) *Manuel de sécurité pour les humanitaires* (www.icrc.org/en/publication/4425-safe-manuel-de-securite-pour-les-humanitaires).

Torelli, C. (2024) *Explosive violence monitor 2023* (en anglais, «Observatoire de la violence explosive 2023»). Action on Armed Violence (<https://aoav.org.uk/2024/explosive-violence-monitor-2023/>).

Wilson, O. (2017) *Counter-terrorism: IED, bomb, and active shooter procedures* (en anglais, «Lutte antiterroriste: procédures EEL, bombe et tireur actif»). Risks Incorporated (<https://gisf.ngo/resource/risks-counter-terrorism-procedures/>).

Menaces chimiques, biologiques, radiologiques et nucléaires

CICR (2014) *Chemical, biological, radiological and nuclear response: introductory guidance* (en anglais, «Réponse aux incidents chimiques, biologiques, radiologiques et nucléaires: guide d'introduction.»). À des fins de formation uniquement (www.icrc.org/en/doc/assets/files/publications/icrc-002-4175.pdf).

IFRC (2023) *Risques chimiques, biologiques, radiologiques et nucléaires (CBRN)* (<https://epidemics.ifrc.org/manager/disaster/chemical-biological-radiological-and-nuclear-cbrn-hazards>).

Initiative des Centres d'excellence d'atténuation des risques CBRN de l'UE (n.d.) *Atténuation des risques chimiques, biologiques, radiologiques et nucléaires* (https://cbrn-risk-mitigation.network.europa.eu/index_en).

ONU (2019) «Politique sur les Menaces et Attaques Chimiques, Biologiques, Radioactives et Nucléaires» *Gestion de la sécurité*, Section Q, Chapitre 4 (<https://policy.un.org/en/security/specific-security-considerations/chemical-biological-radiological-and-nuclear-threats-and>).

Roper, R. et Goodzey, C. (2005) 'Extreme emergencies: humanitarian assistance to civilian populations following chemical, biological, radiological, nuclear and explosive incidents – a sourcebook' (en anglais, «Situations d'urgence extrême: aide humanitaire aux populations civiles à la suite d'incidents chimiques, biologiques, radiologiques, nucléaires et explosifs – recueil de ressources») *Journal of Homeland Security and Emergency Management* 2(2) (<https://doi.org/10.2202/1547-7355.1146>).

Mines et munitions non explosées

Service de l'action anti-mines des Nations Unies (UNMAS) (2015) *Landmines, explosive remnants of war and IED safety handbook* (en anglais, «Manuel de sécurité sur les mines terrestres, les restes explosifs de guerre et les engins explosifs improvisés») (www.unmas.org/en/landmines-erw-and-ied-safety-handbook).

UNMAS (2023) *Marking explosive ordnance hazards* (en anglais, «Marquage des dangers liés aux engins explosifs»). IMAS 08.40 troisième édition (www.mineactionstandards.org/standards/08-40/#::~:~:text=The%20marking%20of%20explosive%20ordnance,unintentional%20entry%20into%20hazardous%20areas).

Équipement de protection individuelle

National Institute of Justice (2024) *Understanding NIJ 0101.06 armor protection levels* (en anglais, «Comprendre les niveaux de protection des gilets pare-balles NIJ 0101.06») (<https://nij.ojp.gov/library/publications/understanding-nij-010106-armor-protection-levels>).

Postface

La gestion des risques de sécurité humanitaire a considérablement progressé au cours des deux dernières décennies, passant d'une approche largement réactive à une approche proactive davantage alignée sur les objectifs stratégiques et opérationnels des organisations humanitaires. Ces progrès ont permis à l'action humanitaire de se poursuivre dans des environnements de plus en plus dangereux, grâce à un personnel mieux formé, à des systèmes de sécurité plus sophistiqués, à une meilleure coordination interagences et à une attention croissante accordée aux profils de risque personnels et au bien-être du personnel. Malgré cela, des lacunes notables subsistent.

Il existe toujours des disparités considérables entre les organisations en termes de ressources, les organisations locales manquant encore souvent des fonds, des outils et des formations nécessaires pour gérer les risques au même niveau que leurs homologues internationales. L'accès sécurisé aux zones de conflit, en particulier celles impliquant des acteurs étatiques importants, reste limité. De plus, les risques de sécurité numérique, la fragmentation croissante des environnements de conflit et les défis posés par le changement climatique ont ajouté des niveaux supplémentaires de complexité aux opérations humanitaires, que la plupart des systèmes existants de gestion des risques de sécurité ne sont pas encore en mesure de traiter efficacement.

À l'avenir, le secteur devra veiller à ce que les travailleurs humanitaires et les organisations locales ne soient pas laissés pour compte dans le développement des pratiques de sécurité. Des partenariats équitables, un transfert de connaissances bidirectionnel et un financement direct accru peuvent y contribuer. L'IA et les outils numériques améliorent la détection des menaces, l'évaluation des risques et la coordination, mais ils introduisent également de nouveaux défis, risques et menaces. Les futurs systèmes de gestion des risques de sécurité devront intégrer efficacement ces technologies tout en restant vigilants face aux risques.

Une approche de sécurité centrée sur la personne doit être plus largement adoptée, en reconnaissant les divers profils de risque des travailleurs humanitaires, leurs forces et leurs vulnérabilités, et en adaptant les pratiques de gestion des risques de sécurité aux besoins individuels. La gestion des risques de sécurité doit également devenir plus prospective, adaptative et agile afin de s'adapter au rythme des changements dans les menaces mondiales et de répondre efficacement aux nouveaux risques dès leur apparition. Bien que cette Revue des bonnes pratiques (RBP) présente un éventail large et détaillé de pratiques et d'outils pour la gestion des risques de sécurité, ceux-ci doivent être adaptés aux besoins et aux capacités des organisations et de leur personnel. Le système doit être au service des personnes, et non l'inverse.

Enfin, la recrudescence de la violence à l'encontre des travailleurs humanitaires, en particulier de la part d'acteurs étatiques, souligne la nécessité d'une redevabilité accrue. Les résolutions du Conseil de sécurité de l'ONU soulignent ce point, et une collaboration accrue entre les équipes de sécurité et celles du plaidoyer au sein des organisations peut soutenir les efforts visant à renforcer les mesures de redevabilité afin de mieux protéger les acteurs humanitaires.

Adelicia Fairbanks

Rédactrice en chef

