eisf

Communications Technology and Humanitarian Delivery

Challenges and Opportunities for Security Risk Management

European Interagency Security Forum (EISF)

European Interagency Security Forum (EISF)

EISF is an independent network of Security Focal Points who currently represent 66 Europe-based humanitarian NGOs operating internationally. EISF is committed to improving the security of relief operations and staff. It aims to increase safe access by humanitarian agencies to people affected by emergencies. Key to its work is the development of research and tools which promote awareness, preparedness and good practice.

EISF was created to establish a more prominent role for security risk management in international humanitarian operations. It facilitates exchange between member organisations and other bodies such as the UN, institutional donors, academic and research institutions, the private sector, and a broad range of international NGOs. EISF's vision is to become a global reference point for applied practice and collective knowledge, and key to its work is the development of practical research for security risk management in the humanitarian sector.

EISF is an independent entity currently funded by the US Office of Foreign Disaster Assistance (OFDA), the Swiss Agency for Development and Cooperation (SDC), the Department for International Development (DFID) and member contributions.

www.eisf.eu

Editors

Raquel Vazquez Llorente and Imogen Wall.

The editors welcome comments and further submissions for future publications or the web-based project. If you are interested in contributing, please email eisf-research@eisf.eu. Imogen Wall can be contacted at imogenwall@hotmail.com.

Acknowledgments

The editors would like to thank Lisa Reilly, EISF Coordinator, for her input and advice, and especially for her comments on the initial drafts. We would also like to extend our gratitude to Tess Dury, for her research support at the initial stages of the project, Brian Shorten for sharing his expertise with us, and Crofton Black for his early guidance and, as always, his continuous support.

Suggested citation

Vazquez Llorente R. and Wall, I. (eds.) (2014) *Communications technology and humanitarian delivery: challenges and opportunities for security risk management*. European Interagency Security Forum (EISF).

Cover photo: Mary Kiperus, community health worker, uses a mobile phone for reporting to the local nurse. Leparua village, Isiolo County, Kenya. February, 2014. © Christian Aid/Elizabeth Dalziel.

Disclaimer

Contents

Foreword

Hugo Slim

When I was working for an NGO in northern Ethiopia in 1985, amazingly we had a telephone. It was a very old one with a handle that you turned very fast to be put through to the local operator. His name was Alex, and he had only one eye but good ears. His job was to connect phone calls and then listen to them and report their content to security officials. Alex did this with good humour but often he would cough and sniff while we were talking, and I had to ask him to be quiet because the line was bad enough without his mucousy interruptions.

How things have changed! In this important new contribution to humanitarian policy and practice, seventeen specialist contributors analyse the many different ways that communications technology is used in and around humanitarian operations today. Each one of them writes with significant field experience and sophisticated knowledge of communications technology.

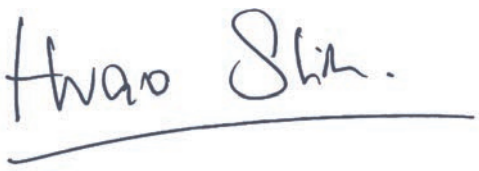
Computer software, mobile phones, smart phones and tablets are all making a huge impact on the delivery of humanitarian assistance and protection. People affected by conflict and disaster are also communicating their situation directly to humanitarian agencies and the wider world on Facebook, in tweets and in Skype broadcasts. In many ways, new communications technology is changing the relationship between humanitarian agencies and the people they are trying to help. Much of this is real progress, and several of these applications are discussed in expert fashion in the articles that follow.

Communications technology, however, is not only used within humanitarian agencies but also against them. Several articles in this publication examine how agency IT systems are deliberately targeted and infiltrated by security services, or how modern communications can compromise agencies. They explain how today's profound reliance on communications technology can be a source of vulnerability as well as innovation. It can put protected populations and agency staff at risk of attack and arrest. Communications technology can also be a powerful weapon: warring parties in a conflict or political groups now routinely use technology to spread e-rumour or propaganda against humanitarians, to issue threats, or to coordinate violence.

All this means that today's humanitarian agencies are required to operate across two spaces: physical space and virtual space. In each of these spaces there is a distinct emergency needing to be managed. One is a situation dominated by physical needs, relief commodities and bodily human suffering. The other is a realm of words and images, ideological contest and reputation management. The struggle for humanitarian acceptance is now fought as much in virtual space as in physical space.

The editors and contributors of this volume are to be congratulated on a practical text that pushes forwards our knowledge and understanding of the virtual space that now surrounds humanitarian operations, and which can have such a physical impact upon them. I encourage you to read it. The articles that follow have certainly brought me up to speed.

Even if this publication describes the daily work environment that you live and breathe, it will help to focus your mind on some very strategic aspects of the technology in your working day. So, please stop tweeting, texting and skyping for an hour and give it a good read.



Hugo Slim
Senior Research Fellow, Oxford Institute for Ethics, Law and Armed Conflict (ELAC), University of Oxford

Dr Hugo Slim specialises in humanitarian ethics, the protection of civilians, conflict resolution, and business ethics. From 1983-1994 he worked as a frontline humanitarian worker for Save the Children UK and the United Nations in Morocco, Sudan and Ethiopia, the Palestinian Territories and Bangladesh. In 1994 he was appointed Reader in International Humanitarianism at Oxford Brookes University where he co-founded an award winning Masters programme for international humanitarian workers. From 2003-2007 he was Chief Scholar at the Centre for Humanitarian Dialogue in Geneva, leading policy work on civilian protection and political mediation. He is on the Board of the Catholic Agency for Overseas Development (CAFOD).

Introduction

Raquel Vazquez Llorente / Imogen Wall

On 20 June 2013, the militant Somali group Al Shabaab attacked the UNDP compound in Mogadishu. Seven militants attacked the gate with a truck bomb, then forced their way inside the compound. A total of 12 people died, along with the seven militants. Such attacks, sadly, are not new in Mogadishu. But this event was characterised by a new and alarming theme: Al Shabaab live-tweeted the entire attack. Their updates, which became the first sources of information for media and the public, spread misinformation about the attack (they claimed to have control of the whole compound), accused the UN of spreading poverty and dependency, and concluded with a direct personal threat to the UN Resident Representative with a tweet showing a picture of the bombed office and the caption, 'So, Nicholas Kay, still planning on moving to Mogadishu?'[1] Nor was this the first time Al Shabaab had live tweeted a security incident: during a previous event involving an NGO in which two staff members were killed, the militants had claimed responsibility for the attack – which was actually an incident involving a disgruntled former employee – and shared personal details of the two victims.

Such incidents are a vivid illustration of the threat communications technology is starting to pose for humanitarian organisations. Modern digital platforms allow information to move fast, help disinformation to spread, and undermine the capacity of aid organisations to control security incidents. They have created new platforms for making threats, and new ways in which aid agencies' information can be accessed and stolen – it is not known how Al Shabaab accessed information about staff members in the latter incident. From a security perspective, such examples are the tip of a large and complex technological iceberg which is creating threats that are both profoundly serious and unlike those aid agencies have faced before.

There is no question that communications technology is transforming the way humanitarians do business in ways that are only beginning to be understood. It is changing the operating environment: from wars that are fought online as well as off, to the new ways in which those affected by conflict access, share and interpret information, and the use of formats such as SMS to intimidate. A number of publications in recent years have raised the alarm: from OCHA's Humanitarianism in the Network Age paper to the IFRC World Disasters Report of 2013 which focuses on technology and the future of humanitarian intervention. To date, however, few efforts have been made to understand the specific nature of the security threats created by the digital revolution, and the implications for security risk management. In the last decade, humanitarian organisations have been investing in more proactive acceptance strategies, but often forgetting to look at the impact that digital interactions have in the security of staff when we replace the traditional 'tea in the market' by Skype meetings with beneficiaries.

Nor have there been many efforts to understand the ways in which communications technology is creating new opportunities for humanitarian agencies to respond to emergencies and the impact that new programmes have on how we manage security. From the benefits of SMS and mobile phones in aid agency communications to the use of online mapping platforms like Ushahidi to improve the collection and analysis of security data, technology is also creating new ways that security information can be sourced, organised, shared and acted on. It is revolutionising remote management, creating new ways to build relationships and trust with affected populations, and opening up new possibilities in sourcing intelligence and understanding operating environments.

1 Lynch, C. (2013). Somali Militants Live-Tweet Their Deadly Attack on U.N. Compound. *Foreign Policy*. 19 June. Available from: http://blog.foreignpolicy.com/posts/2013/06/19/somali_militants_live_tweet_their_deadly_attack_on_un_compound. (Accessed 1 Sept. 2014).

The articles contained in this publication are dispatches from a new frontline in humanitarian action: the digital frontier. All are written by those observing, experiencing and attempting to respond to the challenges created by the digital revolution and the very real threats it is creating for humanitarian operations, and exploring the potential of new tools to create a safer, more responsive operational environment for aid workers.

Section 1 – Understanding the Operational Environment focuses on the ways in which communications technology is changing the places in which we work, particularly conflict environments. For this section we selected five articles that provide an overview of the 'cyber-space' in which humanitarians operate (Gilman), analyse the particular threats aid agencies are exposed to (Byrne, a), and explore how technology is changing personal interactions in conflict environments (Ayala). The latter addresses the concept of 'homophily' – the tendency to associate with people who are similar – and links up with the other two pieces that give a personal account of how intimidation messages spread via SMS can impact the work of field staff (Grayman and Anderson), and look at how online dangerous speech can materialise in violence on the ground (Sambuli and Awori).

Section 2 – Communications Technology and its Impact on Humanitarian Programmes looks at first hand experiences in the use of communications technology at field level for humanitarian programming. From the role of acceptance when implementing technology-based programmes in high-risk contexts (Porcaro and Walker), to Medair's experience in handling the security implications of rapid data collection during an emergency response in Lebanon (Kaiser and Fielding), this section presents some of the opportunities and challenges communications technology brings for managing security risks. A case study on mobile money systems for distribution of food items by World Vision (Tafere *et al.*) also offers an insight into how communications technology is changing the way humanitarian assistance is delivered.

Section 3 – Using Communications Technology For Security Risk Management provides practical tools that can help mitigate security risks, both digital and physical. Far from providing exhaustive measures or a checklist, this section offers a variety of case studies: it assesses the security advantages of SMS over traditional handheld radios as an organisational communication system, particularly with regard to working with national staff (Mayo), and presents the experience of Action Contre la Faim-Spain in using the Ushahidi platform as a tool for recording and analysing security incidents in real time, and the positive impact this has had on the organisation's security management (de Palacios). The final paper in this publication (Byrne, b) outlines some recommendations and actions for consideration by security focal points.

Themes that emerged from the project

The objective of this paper is to begin this important conversation, one that we can no longer ignore. Surveillance, hacking and sophisticated use of communications by warring parties to organise their work and to shape perceptions of conflict through propaganda, are all daily realities of aid agencies working on conflicts such as those in Syria or Iraq. Nor does this threat come only from parties to conflict: advanced hacking technology is now available to criminals. The more humanitarians use digital tools to collect and store information (from the personal details of staff to the contact details of displaced people, to the financial data of affected communities supported through digital cash transfer, for example), the more open we are to serious security breaches with devastating consequences not only for our staff and organisations, but also for those whom we serve.

The speed with which technology is developing and changing humanitarian programmes means that organisations are simply not keeping up from a security risk management perspective. This is true both for understanding the risks involved in the tools we are adopting for programming – for instance, use of tablets for needs assessments – and the tools we use for security risk management, such as tracking devices. This is partly a product of a disconnect between headquarters and field programmes, where security focal points do not have the technological skills, and IT staff in the headquarters lack field experience and are not aware of the risks humanitarians face on the ground. At present, most organisations see security and technology as entirely separate aspects of their operational structures. Clearly, this needs to change.

Technological change is also creating new pressures on humanitarians. In environments where insurgents such as Al Shabaab threaten aid agency staff publicly on Twitter, and displaced people post pleas for help on aid agencies' Facebook pages, how do we need

to rethink acceptance strategies and reputation management? When email and Skype mean that everyone in an organisation expects up-to-the-minute information just for them, how do we mitigate the pressures and stress on staff that can lead to increased vulnerability to security risks?

It is clear that this is just the beginning: hard as it can be to believe sometimes, the digital revolution is still in its infancy, and humanitarians generally and security managers particularly are already behind the curve. But if we are to do our job of protecting our staff, our reputations, and most importantly the people we seek to help, we have no choice but to catch up with the digital revolution. It is EISF's hope that this publication can help ignite discussions about how we as a sector adapt to this new world: what research is needed, what tools must be tested, and how we can better share our experiences and lessons learned. Clearly, the way ahead is not lacking challenges from a security risk management perspective, but it is also full of opportunities. EISF looks forward to the conversations to come.

Section 1

Understanding the Operational Environment

This section looks at how communications technology is changing the environments in which humanitarians work, particularly high-risk contexts. All these articles were selected because together, they raise questions that should be considered when assessing the context in which humanitarian organisations operate.

From a security risk management perspective, context analysis should question how communications technology is changing social dynamics in high-risk environments, as well as how organisations (and others, including hostile actors) gather and distribute information. Are humanitarian organisations being targeted for the data they hold, and how? Which information do we trust and how do we react to an overload of unverified information? If security managers keep referring back to the same sources, are we too suffering from homophily as a sector, and what are the risks this implies? Should our actor mapping also include digital actors, and how do we do this?

Cyber-Warfare and Humanitarian Space

Daniel Gilman

Introduction[2]

Recent publications, notably 'Humanitarianism in the Network Age' from the United Nations Office for the Coordination of Humanitarian Affairs and the 2013 Red Cross World Disaster Report on 'Technology and the Future of Humanitarian Action', have outlined the changing environments for humanitarian work and the potential to use advanced communication systems, 'big data' analytics and other information and communication technologies (ICTs) to transform the way humanitarian action occurs (see Section 2 – Communications Technology and its Impact on Humanitarian Programmes, pp. 32-44). These ideas, from online volunteers providing remote information management support through platforms like the Digital Humanitarian Network,[3] the increased use of biometrics in refugee camps,[4] or real-time tracking systems for cold-chain vaccines, are increasingly a reality.[5]

While offering the potential to improve the efficiency of a response to a crisis, these systems also create new vulnerabilities and ethical and legal challenges, particularly around how to respect and manage privacy. At the same time, many of the same techniques and systems are being increasingly used and co-opted by parties to conflicts, leading to an increase in 'cyber-warfare', politically motivated hacking to conduct sabotage and gather intelligence.[6] While originally cyber-warfare was largely the province of technologically sophisticated countries, like the United States and China, the spread of cheap and easy-to-use technology has fundamentally changed the dynamic in recent conflicts (see Byrne, a. p. 13).

Surveillance and cyberwarfare capacities are now found in many authoritarian regimes, particularly those that also host an international humanitarian presence, notably Ethiopia[7] and Sudan.[8] In addition, recent conflicts have seen the increasing 'para-militarisation' of cyber-warfare, with 'private citizens forming into on-line militia groups to perform cyber-attacks against political opponents'.[9] Evidence from the recent conflicts in Libya,[10] Syria[11] and elsewhere suggests that many of these groups are often linked to governments, but in ways that provide deniability and limit accountability. In some cases, these groups may share overlapping membership with armed groups, wielding guns one day and a laptop the next.[12]

This changing nature of cyber-warfare, particularly as seen in the ongoing conflict in Syria, poses some specific challenges for humanitarians and may largely shape the type of technology and programming that can be effectively used in conflict settings. They also pose a unique challenge to the concept of humanitarian space, understood as the idea that humanitarians can avoid being targeted by belligerents due to their adherence to neutrality and other humanitarian principles.

Increasing vulnerability of humanitarian organisations

The rapid spread of advanced ICTs in humanitarian response has made humanitarian organisations a potential target for different types of cyber-attacks. Humanitarian organisations increasingly store, or are given privileged access to, large quantities of data

2 The views expressed in this publication are those of the author alone, and do not reflect the position of the United Nations. Material for this report was drawn in part from the forthcoming OCHA publication 'Humanitarianism in the Age of Cyberwarfare'. The author would also like to thank John Scott-Railton of Citizen Lab for his expertise and support, without which this paper would not have been possible.
3 See http://digitalhumanitarians.com. [Accessed 1 Sept. 2014].
4 See Kanere. (2013). Classified Fingerprinting. 30 Nov. Available from: http://kanere.org/2013/11/30/classified-fingerprinting; UNHCR. (2012). Modern technology helps meet the needs of refugees in South Sudan. 27 Dec. Available from: http://www.unhcr.org/50dc5a309.html; UNHCR. (2014). UNHCR pilots new biometrics system in Malawi refugee camp. 22 Jan. Available from: http://www.unhcr.ie/news/irish-story/unhcr-pilots-new-biometrics-system-in-malawi-refugee-camp. [All accessed 1 Sept. 2014].
5 UNICEF. (2013). Searching for creative solutions in humanitarian action. 21 Oct. Available from: http://www.unicef.org/emergencies/index_70706.html. [Accessed 1 Sept. 2014].
6 See http://en.wikipedia.org/wiki/Cyberwarfare. [Accessed 1 Sept. 2014].
7 Marczak, B. *et al.* (2014). Hacking Team and the Targeting of Ethiopian Journalists. *Citizen Lab.* 12 Feb. Available from: https://citizenlab.org/2014/02/hacking-team-targeting-ethiopian-journalists. [Accessed 1 Sept. 2014].
8 Marczak, B. *et al.* (2014). Mapping Hacking Team's "Untraceable" Spyware. *Citizen Lab.* 17 Feb. Available from: https://citizenlab.org/2014/02/mapping-hacking-teams-untraceable-spyware. [Accessed 1 Sept. 2014].
9 Ottis, R. (2010). From Pitch Forks to Laptops: Volunteers in Cyber Conflicts. In Czosseck, C. and Podins, K. (eds). *Conference on Cyber Conflict Proceedings 2010.* Tallinn: CCD COE Publications. pp. 97-109. Available from: http://www.ccdcoe.org/publications/2010proceedings/Ottis%20-%20From%20Pitchforks%20to%20Laptops%20Volunteers%20in%20Cyber%20Conflicts.pdf. [Accessed 1 Sept. 2014].
10 Scott-Railton, J. (2013). Revolutionary Risks: Cyber Technology and Threats in the 2011 Libyan Revolution. *CIWAG Case Study Series.* Newport, RI: US Naval War College. Available from: https://www.usnwc.edu/getattachment/01e787b8-ee4c-4efb-8c5a-fe02aa2781ba/Scott-Railton-final-for-website.pdf. [Accessed 1 Sept. 2014].
11 Marczak, W. R., Scott-Railton, J., Marquis-Boire, M. and Paxson, V. When Governments Hack Opponents: A Look at Actors and Technology. *Citizen Lab.* (Unreleased draft).
12 Scott-Railton, J. (2014). Presentation at the 2014 Working Group on Emergency Telecommunications. Available from: http://wget2014.wordpress.com/tag/the-citizen-lab. [Accessed 1 Sept. 2014].

and communications, including phone numbers (for SMS applications), financial information (for cash transfers), fingerprints, iris scans, information on staff and local partners and other information. Humanitarians are also using more two-way communication systems, particularly with SMS and web-based tools like Twitter, to share early-warning and program information and collect feedback. Much of this information is potentially valuable – both commercially and to military or political actors. Humanitarian organisations, many of which have limited ICT expertise to begin with, are often lagging in developing appropriate security protocols. Nor do most organisations conduct privacy impact assessments or use other tools to evaluate the potential risks posed by the data they collect (see Kaiser and Fielding, p. 38).

Beyond criminal activity or fraud, there are a range of motivations to target humanitarian actors: political attacks against the organisations themselves (and what they are perceived to represent, i.e. 'western interests'); to facilitate attacks on communities or ethnic groups who are receiving aid; or to gain access to partner organisations that have provided information or access to networks. While nuisance attacks and vandalism, such as the Syrian Electronic Army vandalism of Human Rights Watch's website,[13] get a larger share of the press due to their public nature, the greatest risk is around data-theft, manipulation and monitoring. The most common attacks use malware like Remote Access Terminals (RAT), which targets are tricked into installing. These can provide almost total access to the target's computer – accessing data, turning on the webcam and microphone, logging keystrokes to identify passwords, manipulating files, etc. (See Byrne, a. pp. 13-16).

Beyond data-theft and surveillance, there are also other emerging areas of risk. One is social cyber-attacks – where people use social media or other communication systems to spread malicious rumours or incite panic. In Assam, India, in 2011, false social media messages, including doctored photos of violence from other situations, were used to convince people that riots and violence were happening in their neighbourhoods, leading to a mass exodus.[14] Humanitarian communications systems, which are presumably highly trusted for their neutrality and relay messages related to disaster and violence, are obvious targets. Hypothetically, a system could be hijacked to send out a warning of an impending attack or disaster, causing displacement without the direct use of force; or military groups could use false notifications of aid disbursements to gather civilians in one place for a terror attack.

Another emerging risk area is attacks on infrastructure systems and devices controlled by computers – the 'internet of things'. Objects with internet connections are recognised as being particularly vulnerable to cyber-attack due to the difficulty in upgrading software and a lack of attention to vulnerabilities until recently.[15] This could pose some unique problems for humanitarian systems. For example, 'smart boxes' that track temperature and location to maintain cold-chain vaccines could be prone to manipulation – resulting in ineffective vaccines being unknowingly delivered. Autonomous unmanned vehicles or delivery systems,[16] life towers that produce flood alerts, or smart toilets[17] that control sterilisation functions are all innovations that are being developed that could be prone to cyber-attacks with potentially serious consequences.

The paramilitarisation of cyber-warfare: the case of Syria

Humanitarian organisations are thus clearly vulnerable to cyber-attacks, and there are benefits for armed groups to consider targeting them explicitly. The role of the Syrian Electronic Army and other groups in the Syria conflict is illustrative of the nature of the way these groups are developing in contemporary warfare.

First, while the hijacking of Twitter accounts and other public advocacy attacks have garnered much of the attention, there is well-documented evidence of systematic attacks on the Syrian opposition and civil society, as well as NGOs. While the tools that are being used are not particularly sophisticated or expensive (the DarkComet RAT that was widely used in Syria to target opposition groups was available for free[18]), a common theme among the attacks has been 'sophisticated social engineering that is grounded in an awareness of the needs, interests, and weaknesses of the opposition.'[19] So, for example, malware has been embedded in tools to protect

13 Fisher, M. (2013). Syria's Pro-Assad Hackers Infiltrate Human Rights Watch Web Site and Twitter Feed. *The Washington Post*. 17 March. Available from: http://www.washingtonpost.com/blogs/worldviews/wp/2013/03/17/syrias-pro-assad-hackers-infiltrate-human-rights-watch-web-site-and-twitter-feed. [Accessed 1 Sept. 2014].
14 Goolsby, R. (Undated). On cybersecurity, crowdsourcing, and social cyber-attack. *Policy Memo Series*. 1. Washington, DC: The Wilson Center. Available from: http://www.wilsoncenter.org/sites/default/files/127219170-On-Cybersecurity-Crowdsourcing-Cyber-Attack-Commons-Lab-Policy-Memo-Series-Vol-1.pdf. [Accessed 1 Sept. 2014].
15 Eisen, M. (2014). The Internet of Things Is Wildly Insecure – And Often Unpatchable. *WIRED*. 4 Jan. Available from: http://www.wired.com/2014/01/theres-no-good-way-to-patch-the-internet-of-things-and-thats-a-huge-problem. [Accessed 1 Sept. 2014].
16 See http://www.matternet.us. [Accessed 1 Sept. 2014].
17 UNESCO. (2014). Smart eSOS toilet for emergencies. 8 July. Available from: http://www.unesco-ihe.org/news/smart-esos-toilet-emergencies. [Accessed 1 Sept. 2014].
18 McMillan, R. (2012). How the Boy Next Door Accidentally Built a Syrian Spy Tool. *WIRED*. 11 July. Available from: http://www.wired.com/2012/07/dark-comet-syrian-spy-tool. [Accessed 1 Sept. 2014].
19 Scott-Railton, J. and Marquis-Boire. M. (2013). A Call to Harm: New Malware Attacks Target the Syrian Opposition. *Citizen Lab*. 21 June. Available from: https://citizenlab.org/2013/06/a-call-to-harm. [Accessed 1 Sept. 2014].

privacy such as Skype encryption or proxy tools, preying precisely on anxieties around cyber-security. Other attacks have included distributing malware through existing social networks, such as hijacking the Facebook page of the 'Revolution Youth Coalition on the Syrian Coast' and posting a malicious link disguised as an investigation of the death of a well-known opposition commander. In other cases, material is designed to be of interest to NGOs or other activists who have connection to opposition groups, such as an NGO administrator receiving an email purporting to contain video evidence of the Syrian military abuses that contained embedded malware. The attacks often come from trusted sources or target private accounts, suggesting 'some degree of prior penetration of the opposition – either through computer network intrusion or other intelligence gathering activities.'[20]

Establishing what direct harm has been caused by these attacks is difficult, but there is circumstantial evidence linking arrests and disappearances to security breaches. Individuals have reported that they were confronted with material from their computers during interrogations, and detainees' accounts are known to have begun seeding malware shortly after their arrests by government forces.[21] All of this suggests that the Syrian cyber-groups are coordinating with military and security services, rather than as *ad hoc* or opportunistic attackers. Like paramilitaries in other conflicts, they have not shown particular respect for international humanitarian law, or for the neutrality of humanitarian actors. For example, there are reliable reports of people communicating with humanitarian organisations over Skype being tortured to give up their passwords, with their accounts then used to transmit malware to NGO staff and their contact networks[22] (see Byrne, a. p.15).

This matters for the way that humanitarians think of these attacks, and how to use information systems. *Ad hoc* attacks or vandalism by 'lone-wolf' hackers may be unavoidable, but will generally pose only limited risk, as these actors are unlikely to be able to act on the information obtained. Systematic targeting of humanitarian information systems and the people who use them by groups linked to military and security actors pose a direct challenge to humanitarian space, however. In particular, given that remote sensing and advanced information networks have been proposed as a way to mitigate access concerns due to increasing attacks on aid workers, the spread of paramilitary cyber-groups should be a worrying development.

The limits of a cyber-security risk management: acceptance in humanitarian cyber-space

Recent surveys and discussions with practitioners suggest that humanitarian organisations have a long way to go to ensure a sufficient level of technical security against cyber-attacks. Most staff are not aware of the nature of the threats faced by field operations, or of basic data security practices, such as how to identify malware attacks (see Byrne, a. pp. 13-16; and Byrne, b. pp. 56-58). There is relatively little use of more sophisticated encryption or security tools; and few if any organisations are working with cyber-security experts to conduct stress tests or monitor for breaches. Precautions like these will probably be a minimum requirement for humanitarians to function in cyber-insecure environments in the near future.

Of course, just as with the use of physical security protection – armoured cars, flak jackets or security guards – the use of a heavily securitised approach can have a negative impact on the acceptance of humanitarian workers, and reduce information sharing and transparency. In the future, humanitarian organisations will need to conduct cyber-security risk assessments to test the basic security of information systems being set up, and also to ensure that there is awareness of the type of threat from cyber-groups. Critically, the level of physical security and cyber-security may not be identical. So a conflict may be relatively secure for humanitarian workers physically, but information systems may be extremely vulnerable (see Byrne, a. pp. 12-16).

If the information coming out of Syria is any model, however, there will be fundamental limits to what technical investments in cyber-security can accomplish. This is because the sophistication in the attacks derives largely from 'social engineering', manipulating people into giving access to their computers, rather than circumventing encryption or other safeguards. Promoting awareness of the nature of threats and regular monitoring of systems can mitigate the risks, as can shifting more work offline or into closed systems. These approaches have obvious limitations, however.

20 *Ibid.*
21 Marczak *et al.* When Governments Hack Opponents. See n. 11 above.
22 Scott-Railton, J. (2014). Digital Security and Wired Humanitarians: Three Trends that Should Scare You. Presentation at the 2014 Working Group on Emergency Telecommunications. Available from: http://wget2014.wordpress.com/tag/the-citizen-lab. [Accessed 1 Sept. 2014].

Instead, it may be more useful to focus less on the nature of the attacks, and more on that of the attackers. With more organised entities, particularly those linked to armed groups, it may be possible to engage in the equivalent of access negotiations to get commitments not to target humanitarian information systems. More broadly, the concept of 'humanitarian cyber-space' could be promoted through negotiations with these groups, online communities, and enlisting local 'white hat' hackers or other online activists. This would require more outreach in local languages, to message boards and online communities, and a more nuanced understanding of dynamics both locally and within the wider diaspora community that may be involved. Of course this would still require regular security assessments to ensure that agreements were being respected, and the difficulty of attributing attacks will make enforcement difficult. Nonetheless, promoting the idea of the neutrality and sanctity of humanitarian information systems may be as effective as any of the other approaches available.

There is also a need for further advocacy on when cyber-attacks on humanitarian organisations constitute a violation of international humanitarian law (IHL). The International Committee of the Red Cross (ICRC) has recognised that cyber-warfare techniques are subject to IHL[23] and Rule 86 of the 'Tallinn Manual on the International Law Applicable to Cyber Warfare', a non-binding study, is that 'cyber operations shall not be designed or conducted to interfere unduly with impartial efforts to provide humanitarian assistance'.[24] Other customary international humanitarian law recognises that objects used for humanitarian relief operations need to be protected from destruction, misappropriation or looting.[25] A case can therefore be made that cyber-attacks on humanitarian information systems, even if only for data-theft, would constitute a violation of IHL as they undermine the ability of humanitarian organisations to deliver impartial assistance. A clearer agreement on what activities constitute a violation of IHL could provide some leverage on governments and non-State actors who might otherwise consider these types of attacks as acceptable, particularly since it is so hard to prove attribution to any specific incident. On this basis, humanitarian organisations should also insist that governments or other belligerents take steps to ensure the cyber-security of activities happening in their area of control.

Conclusions

Humanitarian organisations face a fundamental challenge when considering how to adapt to 21st century conflicts. On the one hand, using the most advanced information systems will allow them to better assess needs, target aid and increase the efficiency of delivery. But the more comprehensive these systems become, the more tempting they become as targets for military and criminal actors. More investments in better cyber-security training, technology and standards are clearly needed to ensure a basic level of robustness in the face of these threats (see Byrne, b. pp. 56-58). However, a highly securitised approach to information systems will be expensive and limit information sharing.

In any case, even the best-designed system will likely be vulnerable to persistent attacks by organised groups, particularly those with strong local networks able to use social engineering or direct coercion. To the extent that cyber-groups are organised or linked to formal armed groups, it is worth considering how humanitarians can engage with them and ensure that the concept of humanitarian space and the neutrality of humanitarian actors is extended to information systems. At the same time, there is an emerging need for more thinking and advocacy to clearly define what constitutes a violation of international humanitarian law in regards to cyber-attacks.

Mitigation and advocacy will only go so far, however. In the end, humanitarian organisations operating in cyber-insecure environments will need to weigh the benefits of setting up certain kinds of information systems, against the possibility that they will be abused or co-opted by parties to the conflict.

23 Furthermore, cyber-warfare does not have to produce permanent, physical destruction to be considered an 'attack'. See ICRC. (2011). *International Humanitarian Law and the challenges of contemporary armed conflicts.* pp. 36-38. Available from: http://www.icrc.org/eng/assets/files/red-cross-crescent-movement/31st-international-conference/31-int-conference-ihl-challenges-report-11-5-1-2-en.pdf. [Accessed 1 Sept. 2014]. See also ICRC. (2013). What limits does the law of war impose on cyber-attacks? 28 June. Available from: http://www.icrc.org/eng/resources/documents/faq/130628-cyber-warfare-q-and-a-eng.htm. [Accessed 1 Sept. 2014].
24 Schmitt, M. N. (ed.). (2013). *Tallinn Manual on the International Law Applicable to Cyber Warfare.* New York, NY: Cambridge University Press.
25 ICRC. (Undated). Customary IHL. Rule 32. Humanitarian Relief Objects. Available from: http://www.icrc.org/customary-ihl/eng/docs/v1_rul_rule32. [Accessed 1 Sept. 2014].

Trends in Intelligence Gathering by Governments

Rory Byrne

Introduction[26]

Advances in digital communication offer many advantages for organisations that seek to do good, such as speed and increased productivity, but also create many new risks such as intercepted communications and systems failure. Humanitarian aid agencies are not immune to either of these effects. While physical security threats and mitigation measures often differ between the human rights and humanitarian sectors, especially with regard to the implementation of security strategies such as acceptance, deterrence and protection, there is a possibility for digital security lessons to be shared – particularly as the humanitarian sector is rapidly increasing its use of technology.

With such a complex topic and such limited space, this article aims to give the non-technical reader an introduction to trends in digital intelligence gathering by governments – though the arguments put forward in this paper equally apply to the use of surveillance and intelligence gathering by non-state actors and private entities.

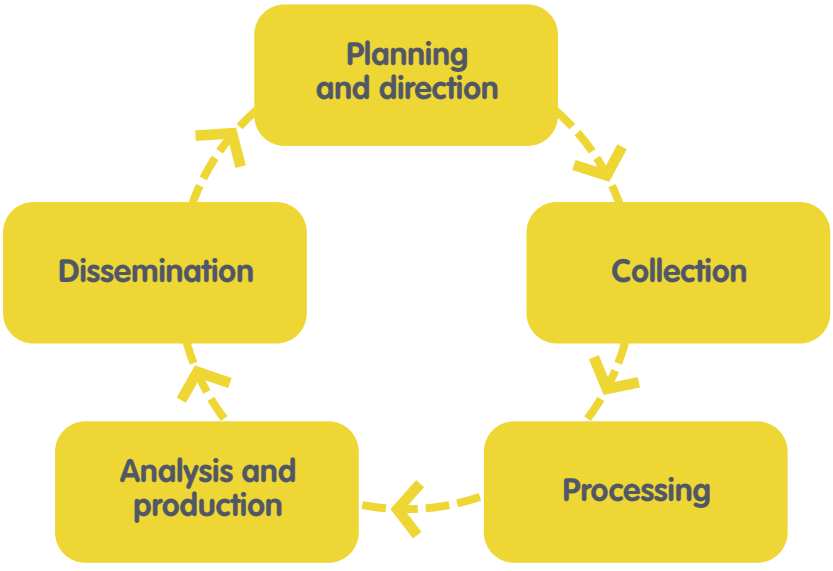
The intelligence cycle

To understand recent trends in digital intelligence gathering by governments, we will utilise the framework of a widely recognised standard to explain how information is gathered and used, overtly and covertly: the 'Intelligence Cycle'.

Planning and direction

Intelligence gathering activities at the governmental level generally begin with requirements set by policy-makers. While it can be argued that some governments, particularly repressive ones, were slow to recognise the threat from – and possible information gathering capabilities of – digital intelligence, developments since the Arab Spring indicate that government planning and direction for digital intelligence is now a common occurrence (see Gilman, pp. 8-10).

Efforts appear to be particularly concentrated around contentious issues such as the emergence of separatists; national groups seeking a change in the balance of power; and/or ad hoc protest movements,



26 The author wishes to thank Eric S. Johnson, Holly Kilroy and a number of anonymous people who graciously agreed to review the article before submission. Any errors or omissions are the author's only.

spurred on by social media and the wisdom of crowds. Security is tightened during critical time periods such as the scheduling/postponing of elections, visits of foreign dignitaries and trade delegations, or civil unrest in a neighbouring regime. The demise of a leader or the fall of a government can lead to a loss of civil liberties – with humanitarian agencies and human rights groups often considered threats that need to be monitored using advanced intelligence gathering methods. Such capabilities are not limited to the larger industrialised powers. Smaller countries such as Belarus, Sudan, Swaziland, Syria, U.A.E. and Vietnam have all been exposed by whistle-blowers and mainstream media as conducting digital intelligence efforts, often thanks, in part, to technical expertise and equipment they receive from governments and corporations.[27]

The increasing prevalence of 'hackers for hire' and the willingness of telecommunications companies to sell communications interception and cyber penetration tools to anyone – regardless of intent – has widely increased the availability of tools, methods and training that can be used not only to attack civilians and non-combatants but also to deliberately and intentionally disrupt the free flow of information by controlling and censoring the internet. Efforts to regulate the export of classified and highly sensitive technologies, by the United Kingdom, the European Union and the United States have been limited due to a range of factors: financial self-interest, dual-use arguments and the desire to 'backdoor' such products for intelligence gathering on the part of the very same countries advocating (publicly) for/against the sale of said products in the first place.

It appears that some organisations are singled out because of the human rights activities they carry out as part of their mandate (e.g. exposing secret prisons), while others are subject to increased scrutiny because of the value of the information they gather (e.g. medical records) (see Gilman, pp. 8-9). For example, Médecins du Monde, together with Amnesty International, UNICEF and WHO, have been targeted by both the Chinese Government[28] and the UK Government Communications Headquarters GCHQ).[29]

Collection

Collection is defined as 'the gathering of raw information based on requirements'.[30] It is the area most commonly focused on in media and other forums, both because of the mystery of 'spying' methods and tools, and because this stage is often the most vulnerable to being revealed, since evidence can often be collected using detection and forensic processes. The focus is often on covert communications intelligence (COMINT); although open source intelligence (OSINT), based on information freely available online, is said to make up the vast majority of final intelligence reports. This is because the raw material is relatively easy to obtain (voluntarily given), highly accurate (based on first person accounts), and rapidly growing in volume and magnitude (connecting the dots has never been easier).

Ironically, the very same tools and techniques associated with open source intelligence gathering represent an important resource for NGOs to help improve their own physical and digital security mitigation measures (see Byrne, b. pp. 56-58).

Background

The first widely publicised incidence of digital intelligence collection against human rights groups was in 2008 (though it is now considered that the alleged abuse(s) may have been ongoing for up to a decade before this) and were linked to Chinese government attacks on Tibetan organisations. This used a method called 'spear-phishing,' a process which involved Chinese intelligence operatives sending fake emails that often appeared to be from internal co-workers (a process known as 'social engineering') and tricked users into opening seemingly innocent documents – which then installed 'trojans' capable of recording all user activity and sending the illegally/illicitly garnered information back to external servers. By targeting the weakest, most vulnerable links – human beings – Chinese intelligence was then able to commandeer an organisation's internal network and establish a long-term capability to monitor all of their public and private communications (known as 'Advanced Persistent Threat').[31] This method continues to be one of the most simple, yet effective, ways of gathering digital intelligence.

27 For an ongoing collection of examples and excellent forensic reports about tools used against activists, see Citizen Lab at the Munk School of Global Affairs, University of Toronto, https://citizenlab.org.
28 Sterling, B. (2012). Amnesty International infested with Chinese Ghost RAT. *WIRED*. 20 May. Available from: http://www.wired.com/2012/05/amnesty-international-infested-with-chinese-ghost-rat. [Accessed 1 Sept. 2014].
29 Taylor, M. and Hopkins, N. (2013). Amnesty to take legal action against UK security services. *The Guardian*. 9 Dec. Available from: http://www.theguardian.com/world/2013/dec/09/amnesty-international-legal-action-uk-security-services. [Accessed 1 Sept. 2014].
30 FBI. Intelligence Cycle. Available from: http://www.fbi.gov/about-us/intelligence/intelligence-cycle. [Accessed 1 Sept. 2014].
31 Kaiman, J. (2013). Hack Tibet. *Foreign Policy*. 4 Dec. Available from: http://www.foreignpolicy.com/articles/2013/12/04/hack_tibet_china_cyberwar. [Accessed 1 Sept. 2014].

Waterholes

A similar vulnerability has been created through the increasing use of a technique referred to as website 'waterholes'. This type of attack works by identifying a website that intelligence targets are known to frequent (for example, a trusted NGO forum) and hacking the website in order to implant malicious pieces of code. When people visit the site with insufficient security (such as poorly maintained or outdated browsers and operating systems) the code can inject 'trojans' onto the user's machine.

Certificates

Another unsettling trend involves the manipulation of the basis upon which much of the security used online (called Secure Socket Layer) to protect web browsers, email, and important transactions depend. These protocols rely on 'digital certificates' (https:// as opposed to http://). The ability to issue false certificates and/or compromise a trusted source (a 'Certificate Authority') has allowed governments, and/or their agents, to impersonate/intercept the day-to-day activities of average citizens.[32] Most users think they have a secure connection to a wide variety of sites and tools – such as Gmail, Yahoo Mail, Facebook, Twitter, WhatsApp, etc.– when in fact, they often do not, as the connection may have been compromised and their data exposed at a number of points along the way (such as at their Internet Service Provider or their Wifi access point).

Mobile phones

Similarly, the technology used to intercept and locate mobile and satellite phones has become cheap and is readily available as COTS (commercial, off-the-shelf) hardware and software – and is suspected of contributing to the death of some journalists in Syria.[33] Phones can serve as tracking devices (even with location services turned off) with similar degrees of accuracy and unbeknownst to most subscribers, and can even be turned on with the microphone activated to allow remote eavesdropping while in off-mode unless the battery is removed. Practically all phone networks have the ability to intercept user calls. For platforms that offer some extra layers of security (such as Blackberry Enterprise Services), a recent trend has been for governments to threaten to or actually block the use and/or sale of such devices and services until the company provides them with a method of intercepting the encrypted data – for example in India and the UAE.

Even when governments cannot intercept the actual content of messages being sent via email and texting, phones generate a significant amount of 'meta-data' – such as location, servers used, sites connected to, time of day, etc.– which means governments already have a strong idea of with whom, where and how you are communicating, even if they don't know exactly what it is being said. Likewise, data generated through social media sites have become a huge reservoir for content-rich intelligence collected by governments and criminal elements because of 'liking and tagging', all done voluntarily.

Phones also pose a security management problem to organisations that want to reduce their exposure to a myriad of risks that stem from the proliferation of hand-held devices, the amount of data being stored, poor security precautions, frequent losses, and the evolution towards cheaper devices (in particular, Chinese-made products found in emerging markets). Recent examples have discovered that some newly purchased phones contain 'backdoors' – such as pre-installed software or hardware which can be used to gain access and control of the device, without the consent of the owner. Discovery of such threats is difficult, if not impossible for most organisations, though the problem can be reduced by sourcing from reputable manufacturers and monitoring phone activity and data usage. This vulnerability is compounded by the growing trend of employees buying and using their own phones, laptops and tablets for work purposes (instead of being issued them by their technical departments). At a minimum, organisations seeking to mitigate such threats should institute effective 'bring-your-own-device' strategies, which install security software onto personal phones to allow organisations to provide a base level of security for the work related information stored on the device (see Byrne, b. pp. 56-58).

Physical access

Collection efforts are not limited to remote digital efforts. Physical access to devices allows unscrupulous operators to take advantage of *ad hoc* situations to gather intelligence data. For example, installing hardware devices such as key-loggers into

32 For example, in Iran. BBC. (2011). Fake DigiNotar web certificate risk to Iranians. 5 Sept. Available from: http://www.bbc.co.uk/news/technology-14789763. [Accessed 1 Sept. 2014].
33 Rayner, G. and Spencer, R. (2012). Syria: Sunday Times journalist Marie Colvin killed in 'targeted attack' by Syrian forces. *The Telegraph*. 22 Feb. Available from: http://www.telegraph.co.uk/news/worldnews/middleeast/syria/9098175/Syria-Sunday-Times-journalist-Marie-Colvin-killed-in-targeted-attack-by-Syrian-forces.html. [Accessed 1 Sept. 2014].

computers or placing covert tracking devices on vehicles. A recent development, seen in many countries, has been the use of covert, and in some instances, overt actions deliberately designed to break into NGO offices and homes, with hardware being taken or destroyed. Many such examples have emerged from places as varied as Belarus,[34] Egypt,[35] Israel,[36] Russia,[37] Vietnam[38] and Zimbabwe.[39] Similarly, persons of interest have found themselves forcibly separated from their devices at checkpoints such as airports, police stations and hotels – where border patrol and law enforcement officers use the opportunity to search, copy, and retrieve information stored on devices. Another recent trend has been for governments (such as Turkey, Uganda, Kenya, UAE) to introduce laws that make digital intelligence gathering easier; for example, requiring that identification must be produced before purchasing a SIM card or instituting laws that force the disclosure of encryption keys. In some countries such as Syria[40] and Sudan,[41] human rights activists have been tortured until they reveal their passwords to social media, email accounts and computers (see Gilman, p. 10).

Processing

With the explosion of digital artefacts created as a result of the continued expansion of the internet, the increased ability of intelligence agencies to process and store large volumes of data indefinitely has been a troubling development. Helped by the decrease in cost of physical storage devices and the increase in sophisticated data-mining software, processing 'big data' (huge sets of data collected and sorted through advanced analysis techniques) has become not only easier, but routine – in fact, the ability to decrypt, recover (even after deletion), translate, tag and measure intelligence for reliability and relevance has increased the ability of analysts to deal with large volumes of data. As such, a trend has emerged in many countries where governments are attempting to 'collect it all'.[42]

Increased processing capability has led to a wider provision – beyond the need to know – of access to intelligence information. For example, in many countries, digital intelligence is no longer restricted to strategic intelligence organisations. Instead, it is now being made available to local law enforcement with the result that this may have changed the nature of interactions between such citizen-based groups and governmental authorities. With digital intelligence becoming increasingly cheap in comparison to large human intelligence (HUMINT) sources and/or physical surveillance operations, a potential exists that lower priority targets like humanitarian NGOs – who are already targeted because they can expose governments – will be subject to increased surveillance and monitoring (see Gilman, pp. 8-10).

Analysis and production

Recent advances in technology have enabled analysts to make use of a wide range of disparate sources. Data collection and processing can be integrated with sophisticated social network analysis tools, which in turn allow junior-level analysts – or any other low level criminal – to compile a fairly intricate picture of the people, locations and organisations a person and/or network interacts with on a daily basis.

Dissemination

How governments have disseminated and used digital intelligence for tactical purposes has not been without repercussions. Particularly prevalent has been the use of disruption instead of direct attacks on individuals and organisations – the theory being that direct attacks create more attention, while disruption can often produce, if not the same result, outcomes that are more manageable. An example would be the use of spurious legal cases to harass and intimidate. Tactically, this often includes the theft of laptops, the confiscation of servers and/or the burning of offices.

Concerned by the lack of predictability associated with open access, many governments have undertaken efforts to block or censor websites and communications devices, temporarily or permanently – for example China, Egypt, Syria and Turkey. During times of unrest, it is not uncommon for governments to try to shut down internet pipelines (as Sudan did in September 2013), thus limiting the free-flow of information. Organisations must prepare for such

34 Human Rights Watch. (2011). *World Report 2011: Belarus*. Available from: http://www.hrw.org/world-report-2011/belarus. [Accessed 1 Sept. 2014].
35 Australian Associated Press. (2013). Egypt NGO says office raided by police. 19 Dec. Available from: http://www.sbs.com.au/news/article/2013/12/19/egypt-ngo-says-office-raided-police. [Accessed 1 Sept. 2014].
36 Ma'an News Agency. (2012). Israeli forces raid NGO offices in Ramallah. 11 Dec. Available from: http://www.maannews.net/eng/ViewDetails.aspx?ID=546800. [Accessed 1 Sept. 2014].
37 Weiland, S. (2013). A Threat to Relations: Germany Irate over Russian NGO Raids. *Der Spiegel*. 26 March. Available from: http://www.spiegel.de/international/europe/russian-authorities-raid-german-foundations-and-ngos-a-890969.html. [Accessed 1 Sept. 2014].
38 BBC. (2012). Vietnamese bloggers deny charges, third in leniency bid. 16 April. Available from: http://www.bbc.co.uk/news/world-asia-17727373. [Accessed 1 Sept. 2014].
39 Karimakwenda, T. (2012). Civil Society Coalitions issue response to police crackdown. *SW Radio Africa*. 8 Nov. Available from: http://www.swradioafrica.com/2012/11/08/civil-society-coalitions-issue-response-to-police-crackdown. [Accessed 1 Sept. 2014].
40 Blomfield, A. (2011). Syria 'tortures activists to access their Facebook pages'. *The Telegraph*. 9 May. Available from: http://www.telegraph.co.uk/news/worldnews/middleeast/syria/8503797/Syria-tortures-activists-to-access-their-Facebook-pages.html. [Accessed 1 Sept. 2014].
41 Author's confidential security debriefing with Sudanese human rights defender subject to the practice.
42 Nakashima, E. and Warrick, J. (2013). For NSA chief, terrorist threat drives passion to 'collect it all'. *The Washington Post*. 14 July. Available from: http://www.washingtonpost.com/world/national-security/for-nsa-chief-terrorist-threat-drives-passion-to-collect-it-all/2013/07/14/3d26ef80-ea49-11e2-a301-ea5a8116d211_story.html. [Accessed 1 Sept. 2014].

eventualities by creating strategies for resilience such as switching to alternative communication channels that can help bypass censorship – for example, Virtual Private Networks (VPNs), Tor (a free software developed for providing increased anonymity and circumvention of restrictions) and the usage of satellite broadband (see Byrne, b. pp. 56-58).

Both democratic and non-democratic governments are using social media to spread propaganda, while also using these technologies to disrupt the activities of groups they perceive to be hostile to them. They accomplish this by spreading discord and false information within and among groups. Examples include collecting data on upcoming events and arresting people during meetings, or publishing propaganda aimed at the groups which creates conflicts and reduces their organisational effectiveness.

Finally, digital intelligence is often disseminated and used for launching human intelligence operations – for example, personal information about web browsing, email and social media activity can be used for manipulation, blackmail and recruiting agents within organisations. Such 'insider threats' continue to play a key role in the intelligence-gathering arsenal deployed by governments. Even more importantly, these techniques are increasingly used not only at local or national offices but are directed towards international headquarters. This author's experience has uncovered that insider threats – like disgruntled employees or paid cover sources like cleaners or security guards – are becoming a common intelligence tactic used against human rights NGOs by governments. Recruitment and management strategies should aim to reduce underlying threat models that undermine trust and create conditions that lead to the evolution of insider threats.

The Dichotomy of Technology in Conflict

Beauty and the Beast

Anahi Ayala

Introduction

In the field of Information and Communication Technology for Development there is often a debate rooted in the dichotomy between the highly enthusiastic view of technology, as an enabler of information exchange that bypasses traditional gatekeepers such as broadcasting media and governmental agencies; and the highly pessimistic view, that focuses on the dangers of technology such as technical gaps, the digital divide and privacy and security threats.

The truth is somewhere in between. Particularly in conflict situations, the reality is much more complicated. On the one hand, technology, and mobile technology in particular, allows for immediate and broad early warning systems to be created in places where real-time communication would previously have been almost impossible (see Porcaro and Walker, pp. 33-36; see also Mayo, pp. 46-50). On the other hand, the way information moves in those contexts can affect the deepening of already existing divisions and the further polarisation of opposing views, where technology enables both an immediacy and increase in volume of material feeding specific viewpoints. One of the most important ways in which these phenomena play out in humanitarian environments today is in the ways in which affected communities use and experience technology, particularly in conflict environments (see Grayman and Anderson, pp. 22-26; see also Sambuli and Awori, pp. 27-31). This article explores the polarising effect of communications systems that are becoming increasingly 'closed'.

From a security management perspective, this same dichotomy is even more accentuated. On one side technology is allowing a broader and larger reach for monitoring security and conversations happening on the ground that can give us real-time insights on risks (see Sambuli and Awori, pp. 27-31); on the other side technology is posing new risks for humanitarian organisations and creating new systems that bypass the usual communication streams and are therefore hidden. The ability to predict violence and provide real-time support in case of violent incidents is strictly related to both our ability to use technology to monitor the situation on the ground, and also to understand how others may be using it to organise violent actions or to create tension.

The link between violence, conflict and technology, especially its use by affected communities and parties to conflict, is only beginning to be understood and the available evidence is in some ways contradictory. In a study that looked at the correlation between the availability of mobile technology and violence, Shapiro and Weidmann (2012)[43] found that in the case of Iraq, the location of cell phone towers is inversely associated with violence: i.e. that areas of greater access to telecommunications experienced less violence. Using district level data and a difference-in-difference design (a research method for estimating causal effects), the authors find that the expansion of the cell phone network in Iraq is associated with decreases in successful violent attacks by insurgent forces. Shapiro and Weidmann (2013) state that this is due to the extensive use of cell phone surveillance by U.S. and Iraqi anti-insurgent forces as well as successful whistle-blower programs. Similarly, in the African context, Livingston (2011)[44] argues that while cell phones might empower violent groups and produce more violence, there is a potential for a reduction in violence if improved monitoring is done by international peacekeeping or governmental forces. Such efforts have been rare so far, however.

43 Shapiro, J. N. and Weidmann, N. B. (2013). *Is the phone mightier than the sword? Cell phones and insurgent violence in Iraq.* Department of Politics and Woodrow Wilson School, Princeton University. Available from: https://webspace.princeton.edu/users/esocweb/ESOC%20website%20publications/SW_CellphonesIraq.pdf. (Accessed 1 Sept. 2014).
44 Livingston, S. (2011). Africa's Evolving Infosystems: A Pathway to Security and Stability. *Africa Center for Strategic Studies.* Research Paper No. 2.

Alternatively, Pierskalla and Hollenbac (2013)[45] provide evidence to show that cell phone technology can increase the ability of violent groups to overcome collective action problems in Africa. In particular, they state that cell phones lead to a boost in the capacity of groups to communicate and monitor in-group behaviour, thus increasing cooperation. They offer some insights suggesting that the exploration of potential interactions with country or group-level variables can further illuminate the effects of communication technology on violence.

Pierskalla and Hollenbac conclude that enlarging the communication network of violent groups as well as increasing the rate of communication by group members should raise in-group trust between individual participants. The possibility for fast and easy communication boosts the propensity for and rate of information sharing within groups, creating a shared awareness among group members. This system can also be applied to ethnic groups, religious groups or specific sectors of the population. As Shirky (2008, 51) writes, collective action is critically dependent on group cohesion.[46] The expansion of within-group communication is likely to foster shared beliefs and awareness of groups, thus providing one channel of easing collective action. The higher rate of communication between individual group members also makes the transmission of messages and instructions from group leaders through the decentralised network more likely and efficient. Furthermore, the increase in two-way communication vastly raises opportunities for monitoring each other's behaviour (see Sambuli and Awori, p. 29).

Homophily or the closed network effect: a study from the Central African Republic

An example of this phenomenon is currently playing out in the Central African Republic. The Central African Republic has a mobile coverage of 30% and an Internet penetration of 0.1%. Internews is an international non-profit media organisation whose mission is to empower local media worldwide to give people the news and information they need, the ability to connect, and the means to make their voices heard. In the Central African Republic, where Internews has been working since 2010, the organisation works mainly with radio stations – as radio is without any doubt the most widespread medium of communication in the country, and in certain cases, the most trusted.

Even now, when more than 50% of the radio stations have been looted or destroyed, radio remains the only means to broadly reach the local population. But while technology use in the Central African Republic is not yet widespread, certain technology is available and at low cost. A fake Blackberry on the black market costs 15,000 CF (almost 32 USD). Other phones, either with or without Internet capability, cost around 12,000 CF (or 24 USD). Those phones have two things in common: a camera to take pictures and video, and Bluetooth.

In 2014 a new phenomenon emerged in the country: young people were taking video of massacres and killings with their phones to share with friends and peers. Especially in the capital of Bangui, youth began gathering in groups to share videos and pictures of the violence happening in their areas by using Bluetooth, or sometimes by exchanging memory cards. This information flow is a completely closed and untapped one, where access is gained through a shared view of the conflict or geographical and ethnic commonalities. In other words, access to the circle of information comes from having already been a part of it.

This system is typical of the phenomenon of 'homophily', as discussed by Ethan Zuckerman in his closing remarks at the 2014 PeaceTech conference in Boston [47] and increasingly a hallmark of modern conflicts. The homophily principle states[48] that people's personal networks are homogeneous with regard to many socio-demographic, behavioural, and intrapersonal characteristics. Therefore homophily limits people's social worlds in a way that has powerful implications for the information they receive, the attitudes they form, and the interactions they experience. Within this same context, ties between non-similar individuals also dissolve at a higher rate, which sets the stage for the formation of niches (localised positions) within social space. Use of social media and other closed systems for sharing information mean that digital social networks frequently become ways to reinforce views, limit exposure to alternative narratives and thus reduce dialogue and mutual understanding between groups in conflict.

The consequence is that conversations enabled through homophilic systems are more and more polarised towards one unique vision, the vision of the people forming the network. Within the network, the likelihood of a divergent opinion or conversation that

45 Pierskalla, J. H. and Hollenbach, F. M. (2013). Technology and Collective Action: The Effect of Cell Phone Coverage on Political Violence in Africa. *American Political Science Review*. 107. pp. 207-224. Available from: http://polisci.duke.edu/uploads/media_items/technology-collectiveactioncellphoneviolence.original.pdf. [Accessed 1 Sept. 2014].
46 Shirky, C. (2008) *Here Comes Everybody: The Power of Organizing Without Organizations*. Penguin Press.
47 Video at https://www.youtube.com/watch?v=Mj_SKNQX654. [Accessed 1 Sept. 2014].
48 McPherson, M., Smith-Lovin, L. and Cook, J. M. (2001). Birds of a Feather: Homophily in Social Networks. *Annual Review of Sociology*. 27 (1). pp. 415-444.

presents opposing or different opinions is minimised. The information received in those networks is likely to be aimed at enforcing and supporting a singular point of view, and less likely to be surprising or challenging. Common ground between sides in a conflict is therefore reduced.

This is exactly the situation we observe now in the Central African Republic, where Bluetooth is being used to create a closed information system that can function without Internet and still diffuse information that appeals to people sharing the same 'values' – which may be positive or negative. The use of this system is potentially having huge effects on the behaviours of the local population including acting as an incentive to violence, and is also a possible cause of displacement (see Gilman, p.9; see Grayman and Anderson, pp. 22-26; see also Sambuli and Awori, pp. 27-31). Owing to the lack of vetted and reliable information in the country, the local population makes decisions about its actions based on rumours, fears and word of mouth. The use of mobile phones to spread information that is not only unverified, but can also be manipulated *ad hoc* (for example, showing an old video of a destroyed village and stating that it was just destroyed the day before, therefore increasing the fear and feeling of a continuous attack being perpetrated against one group or another) can further increase the use of non-vetted and non-verified information to make important decisions, like fleeing from a certain area or looking for weapons to prepare for a potential attack.

Digital networks and security management: understanding information flows or controlling them?

The Central African Republic is not the only example of such systems. In 2014 in Kenya, during the armed attack carried out by Al Shabaab fighters at the popular Westgate mall, several messages were circulated via the WhatsApp smart phone application. One of the messages said,

> An intel guy, who is communicating with a military consultant, who is inside Westgate as we speak says that the terrorists are in Barclays Premier with some hostages and shielded by the bullet proof glass. Other hostages are tied to the pillars in the basement with explosives. Suicide bombers have been dispatched to other four unknown locations. Also confirmed that Samantha Lethwaite is the leader.

Another message was also sent over mobile phones,

> Guys, if you know anyone near that area please tell them to move as far as possible! Apparently all of the third and fourth floor are laced with explosives and those guys may blow anytime. Hear there are over a 100 people dead in Nakumatt maybe all or some of the hostages. They are in Nakumatt basement. All hostages surrounded by bombs. So if anyone tries to do anything they will blow it. So they are planning on how to go about it. Message from Special Squad.

Of course none of this information ended up being true or was ever confirmed by the local authorities. However, those messages helped in spreading panic and rumours and fostered an environment of fear and suspicion within the local population. Anecdotal evidence shows that people indeed left their houses and some even the country for fear of possible other attacks or for fear that the Westgate mall might explode. More research is necessary to determine whether any of those actions were indeed caused by the spread of this information over mobile phones (see Grayman and Anderson, pp. 22-26; see also Sambuli and Awori, pp. 27-31).

The messages spread over the WhatsApp application in Kenya have several characteristics in common:

1. The explicit request not to spread the information via social media. This made it impossible to correct, deny or confirm any of the rumours.[49]
2. All messages claim to come from an inside source from the official security apparatus.
3. They were all spread using a closed and existing network, WhatsApp, which is based on personal phone numbers. This means that the messages where spread quickly between people that trusted and knew each other well.

These closed systems, like the one used in CAR, spread quickly and work efficiently because they offer many advantages:

1. They are closed systems and rely on peer to peer trust – I trust you and therefore I trust what you are telling me – which allows for the primary source to become irrelevant to the reliability of the information, because the trust is transferred to others.

49 The capacity of Twitter to generate corrections to rumours was analysed in detail by the London School of Economics following the London riots in 2011. This research found that the power of Twitter users to correct false information was equal to their power to spread it: most rumours were identified as false and corrected within 2-3 hours. See Richards, J. and Lewis, P. (2011). How Twitter was used to spread – and knock down – rumours during the riots. *The Guardian*. 7 Dec. Available from: http://www.theguardian.com/uk/2011/dec/07/how-twitter-spread-rumours-riots. [Accessed 1 Sept. 2014].

2. They allow for the information to spread fast because it is free and relies on homophily; both the Bluetooth and the WhatsApp systems are relatively cheap if not totally free.
3. They prevent any sort of cross-verification from happening. Only people that are inclined to trust the information will receive it and they only share it with others that have their same values, so the likelihood of someone within the system to doubt the information declines considerably.

What these two examples highlight is that technology is not only democratising information but is also sequestering it, confining it into small areas that external actors cannot reach easily, and thereby enabling the creation of more closed systems, rather than open ones. Those systems are based on the existence of confirmation bias, a cognitive stance that favours information that confirms previously existing beliefs.

One of the main differences between the system developed in CAR and the one used in Kenya stems from distinction in the technology used. Systems like WhatsApp, as well as BBM, Twitter and Facebook private conversations, can be monitored by the authorities because they rely on a controlled and accessible infrastructure – the mobile and internet network. Collaborative efforts between authorities and mobile providers have already happened in several cases, such as the London Riots of 2011.[50] On the other hand, systems like Bluetooth are much more difficult to tap into and to monitor because the only way to see what is being exchanged is to have access physically to the phone or to be close enough to the exchange point to tap into it.

The evidence available to date, however, suggests that the approach of controlling or even blocking instant messaging systems has not generated particularly positive effects. Anecdotal evidence on the ground highlights that when a system is not available anymore, people find an alternative to exchange information anyway. No study so far has been able to prove that there are possible beneficial effects deriving from blocking the use of certain technologies. In addition to this, concerns need to be raised in terms of the implications that those types of measures, including surveillance, have when it comes to the right to privacy and to free speech.

There is also a value in being able to understand and see those conversations, and in engaging with the people who take part in them. From a programming and peacebuilding perspective, one of the main possibilities is the opportunity to break the homophily system by inserting voices in the conversation that can bring different and also opposing opinions. From a security perspective there is also a value, albeit an indirect one. As described above, the veracity of the information shared through such networks is often beside the point: therefore, accessing networks of this type is not likely to provide reliable warning of attacks or planned violence *per se*. However, developing ways to track information moving in closed communication systems could provide important insights into the perceptions of conflict and the framework through which parties to conflict interpret events and view those involved (see Grayman and Anderson, pp. 22-26; see also Sambuli and Awori, pp. 27-31).

One very interesting example of a completely different strategy that leveraged homophily and learnt from violent actors for the creation of a peace-keeping and early warning system is a small project implemented in Kenya during the 2013 elections. Sisi Ni Amani,[51] a local organisation, used mobile phones and SMS as a way to intervene in the decision-making processes that led to violence by studying the triggering factors of violence in different contexts. Sisi Ni Amani was able to use existing networks on the ground to develop a strategy that was based on groups' ethnic and demographic affinities. The messages developed and sent by SMS to people identified as vulnerable to violent behaviour were developed and designed by their peers, and therefore built on their common values and confirmation bias.

More applied research in this field is needed. Most of all, however, there is a need to move beyond the above-mentioned dichotomy: technology, along with other tools, can and will be used in positive and negative ways by affected populations. Preventing or blocking the use of certain technologies will not really address the issue. A much deeper understanding of the dynamics of information in conflict and how internal communication flows can be used to increase exposure to 'the other' and opposing views, rather than increase polarisation, is critically needed.

50 Jamieson, D. (2011). London Riots Co-ordinated with BlackBerry Messenger. *TechWeek Europe*. 8 Aug. Available from: http://www.techweekeurope.co.uk/news/london-looting-co-ordinated-with-blackberry-messenger-36303. [Accessed 1 Sept. 2014]. Halliday, J. (2011). London riots: BlackBerry to help police probe Messenger looting 'role'. *The Guardian*. 8 Aug. Available from: http://www.theguardian.com/uk/2011/aug/08/london-riots-blackberry-messenger-looting. [Accessed 1 Sept. 2014].
51 http://www.sisiniamani.org. [Accessed 1 Sept. 2014].

Network analysis, which analyses the relationships and interdependency between interacting units (such as individuals) and is widely used in epidemiology, social anthropology and organisational behaviour, has been used to examine and interpret the dynamics of wars for many years.[52] It has also more recently been applied to understanding how the internet functions, and the same approach – looking at how social networks connect and unite social groups – can be applied to offline systems such as mobile. Moody (2005)[53] suggests that a comprehensive social network analysis can help in identifying the magnitude of social multiplier effects, for example.

We also need to start learning from the use of technology by violent actors. Studying and understanding how already existing systems work can help us understand what they rely on, and leverage this information to create positive counter-systems, much like what Sisi Ni Amani did in Kenya. There is a requirement to look carefully at what is happening on the ground from a more sociological point of view, rather than a security one: in humanitarian emergencies local staff are also affected population, and can offer humanitarian organisations a window into the dynamics and tools used by the local population to communicate.

From a security perspective, it is easy to dismiss the kind of information that moves through closed networks: much of it is clearly (deliberately or accidentally) untrue, or (deliberately or accidentally) misrepresentative of ground realities. Yet the available evidence to date suggests that dismissing this information would be wrong. Such information can be extremely useful in predicting humanitarian problems, such as displacement (in response to rumours or threats), identifying misperceptions (deliberate or accidental) regarding the actions of international agencies, and in understanding the drivers of conflict. Accessing and triangulating this information, however, remains a key challenge.

52 See the work of Emile M. Hafner-Burton, Alexander Montgomery and others.
53 Moody, J. (2005). Fighting a Hydra: A Note on the Network Embeddedness of the War on Terror. *Structure and Dynamics*. 1 (2). Available from: http://escholarship.org/uc/item/7x3881bs. [Accessed 1 Sept. 2014].

Conjuring Zones of Insecurity

Post-Conflict Election Campaigning by Text Message in Aceh, Indonesia

Jesse Hession Grayman / Bobby Anderson

Introduction

Information Communications Technology (ICT)'s systematic penetration into the developing world has fundamentally changed the way people at the margins communicate with one another. The spread of cheap mobile devices has spawned a wave of development initiatives falling under the umbrella of Information Communications Technology for Development (ICT4D). These initiatives are said to be 'creating new venues for people's participation and giving new voice to those who have historically been marginalized.'[54] Mobile devices now allow hitherto excluded communities to access banking services in Kenya,[55] report corruption in India,[56] improve health services in Peru[57] and Rwanda,[58] raise educational levels in South Africa[59] and Tanzania,[60] and monitor elections and report electoral violence in Kenya,[61] Nigeria[62] and Indonesia.[63] Estonia even allows citizens to vote through mobile devices.[64] Mobile devices also powered the 'Arab Spring' on the ground in Egypt, Libya and Tunisia.

These examples may or may not, in the clichéd benchmark of development, prove 'sustainable' over time, but they do represent concrete examples of ICT4D's transformational possibilities. We would insert an important caveat that ICT tools bear the moralities of their wielders. In this collection, Sambuli and Awori (pp. 27-31) discuss how mobile and digital technologies may have played a catalysing role in the Kenyan 2007/08 post-election violence, and how the Umati project was created to track and counter such use in 2013.

In Afghanistan the night-letter phenomenon of the early occupation has moved from physical letters to text messages (SMS, Short Message Service) across cell phone networks. ISIS in Iraq and Syria embraced mobile technologies more than the nascent democrats in any preceding Arab Spring. Where we work in Indonesia, mobile technologies have been widely embraced in politics and elections, especially among gangster, police, military, and militia groups, to intimidate and manipulate outcomes. A differentiated spectrum of ICT is deployed across the archipelago: in Jakarta, youth gangs taunt one another and arrange fights and ambushes via Twitter.[65] In Maluku, e-rumour-mongering in the ethno-religious fracture zones of urban Ambon leads to arson, assaults and murders.[66] In Aceh, threats via SMS were readily adopted to extort from contractors in the post-tsunami reconstruction boom, but the use of SMS in that province has had more widespread impact through the cultivation of pervasive and ephemeral environments of insecurity that arrive with every election cycle. Most frustrating is that while these SMSs add to a feeling of insecurity that can penetrate uninvolved households, there is little concrete action that can be taken against them (see Ayala, pp. 19-21; see also Sambuli and Awori, pp. 27-31).

The quarter-century conflict between the Government of Indonesia and the Free Aceh Movement (known by their Indonesian acronym GAM, from Gerakan Aceh Merdeka) was distinguished by sporadic separatist violence and brutal counter-insurgency operations.

54 UNDP. (2012). Mobile Technologies and Empowerment: Enhancing human development through participation and innovation. Available from: https://www.undpegov.org/mgov-primer.html. [Accessed 1 Sept. 2014].
55 Karugu, W. N. and Mwendwa, T. (2007). Vodafone and Safaricom Kenya: Extending the Range and Reliability of Financial Services to the Poor in Rural Kenya. UNDP. Available from: http://growinginclusivemarkets.org/media/cases/Kenya_MPESA_2008.pdf. [Accessed 1 Sept. 2014].
56 http://ipaidabribe.com. [Accessed 1 Sept. 2014].
57 http://healthmarketinnovations.org/program/nacer. [Accessed 1 Sept. 2014].
58 UN. (Undated). Tracnet, Rwanda: Fighting Pandemics through Information Technology. Available from: http://www.un.org/esa/sustdev/publications/africa_casestudies/tracnet.pdf. [Accessed 1 Sept. 2014].
59 http://www.comminit.com/africa/content/dr-math. [Accessed 1 Sept. 2014].
60 Trucano, M. (2009). Checking in with BridgeIT in Tanzania: Using mobile phones to support teachers. World Bank. 25 Sept. Available from: http://blogs.worldbank.org/edutech/checking-in-with-bridgeit-in-tanzania. [Accessed 1 Sept. 2014].
61 http://www.ushahidi.com. [Accessed 1 Sept. 2014].
62 http://www.reclaimnaija.net/
63 http://www.kawalpemilu.org. [Accessed 1 Sept. 2014].
64 ICT Statistics Newslog. (2011). Estonians Vote in Parliamentary Election by Mobile Phone. 7 March. Available from: http://www.itu.int/ITU-D/ict/newslog/Estonians+Vote+In+Parliamentary+Election+By+Mobile+Phone.aspx. [Accessed 1 Sept. 2014].
65 Anderson, B. and Snyder, J. (2013). Coming of Age in the Urban Kampung: Gang Demographics and Territories in Select Jakarta Neighborhoods – Preliminary Findings. A paper presented at the European Association for South East Asian Studies Conference, Lisbon, Portugal, 2-5 July 2013. Available from: https://www.academia.edu/3849904/Coming_of_Age_in_the_Urban_Kampung_Gang_Demographics_and_Territories_in_Select_Jakarta_Neighborhoods-_Preliminary_Findings. [Accessed 1 Sept. 2014].
66 Spyer, P. (2002). Fire without smoke and other phantoms of Ambon's violence: Media effects, agency, and the work of imagination. *Indonesia*. 74. pp. 21-36. Available from: http://cip.cornell.edu/DPubS?service=UI&version=1.0&verb=Display&handle=seap.indo/1106939683. [Accessed 1 Sept. 2014].

The conflict ended in August 2005, when the Helsinki peace agreement was signed, catalysed in part by the promise of enough lucrative spoils for all former adversaries in Aceh's post-tsunami reconstruction economy. By mid-2008, former GAM separatists were preparing to contest seats in Aceh's provincial and district assemblies for the first time with their newly formed local political party, Partai Aceh (PA). The allowance for Aceh to field local parties in the April 2009 legislative elections was the first of its kind in Indonesia, and a benchmark achievement for GAM in the peace agreement.

Polarising the electorate

In mid-2008, while one of us (JHG) conducted ethnographic field research and the other (BA) implemented reintegration and stabilisation projects for post-conflict recovery in Aceh, we noticed that interviewees and other local partners in our work would routinely take out their cell phones to show us the frequently anonymous, political text messages they had received to illustrate ongoing tensions among conflict-era adversaries. One of the most memorable text messages was written in traditional Acehnese verse and sent anonymously to the cell phones of a select group of ex-GAM rebels who were not on the best of terms with their former comrades now campaigning for Partai Aceh:

> A YOUNG CHILD GATHERS RATTAN IN THE MOUNTAINS OF MEUREUDU / FIND THE BEST TO MAKE A BASKET / NOW IT IS ALMOST ELECTION SEASON / IT IS TIME TO CHOOSE A THRONE FOR THE KING / HEAD OVER THERE TO GAM'S PARTY / HAVE NO DOUBTS MY BROTHER / WHOEVER DOES NOT CHOOSE THE DESCENDANTS OF ACEHNESE KINGS / JUST MOVE TO JAVA / NO NEED TO STAY ANYMORE IN ACEH / JUST GET THE FUCK OUT OF HERE[67]

Recipients of this poetic intimidation were all GAM ex-combatants who surrendered before the peace agreement and underwent formal reeducation sponsored by the Indonesian military (Tentara Nasional Indonesia or TNI); the larger GAM conglomerate thus considers them traitors. During the final years of the conflict, these reformed ex-rebels operated as any of the other anti-separatist militia groups in Aceh with TNI backing, and in the early post-conflict era were seen as potential spoilers of the peace process. Not to be outdone, they expressed their disappointment with GAM's leaders by widely distributing an SMS of their own:

> IN THE YEAR 2000 WE RAN AWAY, FEARFUL OF POLICE AND SOLDIER'S WEAPONS. IN THE YEAR 2004 THE TSUNAMI CAME, ALLAH'S JUDGMENT THAT BROUGHT ENORMOUS WATER. IN THE YEAR 2006 THERE WAS NO MORE FIGHTING. IN THE YEAR 2007 WE INAUGURATED NEW KINGS. IN THE YEAR 2008 THEY FOUGHT AMONGST THEMSELVES. THE LEADERS OF THE LAND FORGOT TO COMPENSATE THEIR PEOPLE'S SERVICE. NOBODY CARES ABOUT THE VICTIMS OF SHOOTINGS, NOR DOES ANYBODY CARE ABOUT THE WIDOWS. THE ARISTOCRATS AND DISTRICT LEADERS ARE BUSY WITH THEIR TOYOTA LUXURY VANS. IN THE YEAR 2009 WE CHOOSE THE PEOPLE'S REPRESENTATIVES, AND AGAIN THEY BRING US PROMISES ON A HEAVENLY WIND. THOSE PROMISED A CAR WILL GET A BICYCLE. THOSE PROMISED A COFFEE WILL GET POISONED. CONGRATULATIONS TO THE LEADERS OF THIS LAND!

This exchange evokes the simmering tensions between ex-combatants, with implied threats from the first SMS and disappointment expressed by the second (a disappointment that has taken root across Aceh since those elections). Meanwhile, TNI fixated on the possibility of a resurgent separatist threat if PA won the elections. One officer at a base in East Aceh sent the following SMS to village heads in neighbouring sub-districts:

> BE CAREFUL, GAM HAS BEGUN LISTING YOUR CONSTITUENTS AS MEMBERS OF THEIR POLITICAL PARTY BY FILLING IN BLANK GAM PARTY FORMS. GAM'S METHODS ARE NOT SO DIFFERENT FROM THOSE USED BY THE PKI [THE INDONESIAN COMMUNIST PARTY] IN THE PAST. DO NOT BE SEDUCED BY GAM'S DECEPTION; IT COULD BE A TRAP, BUT IF PEOPLE WANT TO THEN FEEL FREE TO FILL IN THE FORMS COMPLETELY. SHARE THIS SMS WIDELY WITH YOUR FAMILY, NEIGHBOURS, FRIENDS, ETC., SO THAT PEOPLE IN THE COMMUNITY ARE NOT DECEIVED, AND BECOME VICTIMS LIKE THOSE CAUGHT UP IN THE PKI'S SEPTEMBER 30TH MOVEMENT REBELLION IN 1965.

67 The translations here and below are by JHG. The final verse in this message uses an unspeakably rude metaphor in Acehnese that our colleagues in Aceh insisted has no equivalent English meaning. The translation conveys the threat to leave Aceh with an equally offensive English expression.

The village head who showed it to us could not tell if the officer who sent it composed it himself or if he was simply forwarding it from another source. The message is a thinly veiled threat suggesting that the fate of PA members may resemble the fate of communists in 1965 who were massacred in the hundreds of thousands across Indonesia, including Aceh. Messages linking the fate of those who support GAM to those who were in the PKI were common in Aceh at the time, and were not limited to elections; in some reintegration programs that targeted ex-GAM in Aceh's highlands, local TNI circulated SMS messages stating that the GAM who signed up for such programs were also signing their names to 'death lists.' Anti-separatist militias in the highlands also sent out messages with similar themes.

Messages like these do not typically appear in the mass media or in analyst reports about post-conflict politics in Aceh, and yet our data and experience show that this global technology was routinely deployed to spread rumours and threats, campaign promises and political slander, poetry and invective, all across the province, often in rich Acehnese and Indonesian vernaculars. SMS technology may be the most cost-effective election campaign tool because it penetrates remote communities without requiring travel, and reaches voters and adversaries much more reliably and cheaply than telephone, radio, or television broadcasts (see Ayala, pp. 17-18). The medium also allows for anonymity; senders can terrorise individuals and communities from a distance. And they frustratingly provide little to act against. Most of these ephemeral documents transmitted across cell phone networks easily escape the archives that bear only partial historic witness to what was a momentous and occasionally tumultuous transition to peace.

Intimidation across phone networks during the 2009 elections

During the March 2009 Aceh legislative elections, one of us (JHG) worked as an election observer with an international NGO. As pairs of observers moved from one town to the next, our contact information travelled through election stakeholder networks, and we soon found it difficult to accommodate, much less sort out and make sense of, the barrage of data that people sent us via SMS, frequently from unknown sources. A few examples recall the atmosphere of fear that voters, candidates, officials, and other election stakeholders conveyed to us:

> YOU CAN SEND OUR BROTHER TO JAIL, BUT I WILL SEND YOU, COMMISSIONER, TO THE GATES OF HELL. GO AHEAD, ENJOY YOUR LIFE WITH YOUR WIFE AND CHILDREN, ONLY A FEW MORE MOMENTS REMAIN. [SENT TO THE HEAD OF THE BENER MERIAH DISTRICT ELECTION COMMISSION, FORWARDED TO US.]

> SIR, DO NOT RETURN SO FREQUENTLY TO YOUR HOME. WHEN YOU RETURN HOME, YOU'LL BE SHOT DEAD IMMEDIATELY. THIS IS VALID INFORMATION. WE HAVE THE WEAPONS NEAR SIMPANG MAMPLAM. [MESSAGE SENT TO A LOCAL PARTY CANDIDATE, FORWARDED TO US].

> ON TUESDAY NIGHT AT AROUND 1:30AM, SIX OFFICERS FROM THE TNI BASE ARRIVED ON THREE MOTORBIKES, CARRYING THREE FIREARMS. THEN THEY TOLD US 'DO NOT VOTE FOR ACEH. IF YOU VOTE FOR ACEH IT MEANS YOU'RE INVITING WAR WITH US.'

> THE TAMIANG POLICE CHIEF AND HIS MEN HAVE SURROUNDED THE HOME OF THE DISTRICT HEAD OF PARTAI ACEH, AND WE DON'T KNOW WHY. THE INTIMIDATION HERE IS SEVERE. PLEASE INVESTIGATE AND RESPOND.

> GOOD EVENING, WE ARE VERY FEARFUL OF THE TNI AND THE POLICE WHO HAVE BEEN ROAMING ABOUT. AT NIGHT, THEY ARE EVERYWHERE LIKE OWLS, BUT IN THE DAYTIME THEY DO NOT APPEAR. WE ASK THAT YOU WILL PUBLICISE THIS INFORMATION IN THE INTERNATIONAL NEWS, THAT THE PEOPLE OF ACEH ARE AFRAID OF THE TNI AND THE POLICE. PLEASE DO NOT SHARE MY PHONE NUMBER WITH ANYONE. THANK YOU.

These messages are anecdotal examples of overlapping individual and group communication strategies that were finding their way into the majority of mobile phones in Aceh. The volume of election-related SMS is not quantifiable, but our experience indicates that it was overwhelming. Intimidations by text message generally had their intended effect as they circulated in a setting of pre-election violence including arson, bombs, and targeted murders. Text messages reporting these violent acts (and threatening more to come) produced a sense of immediacy and proximity, amplifying and personalising among ordinary voters the effects of what were mostly isolated and parochial clashes between distant adversaries.[68] Rival candidates took to sleeping at different houses each night. They, and ordinary citizens, also ensured they were off the road before nightfall.

Intimidation by SMS: a winning campaign strategy?

Just five days before the election, in the early evening on 4 April, JHG was meeting with a local NGO at a popular restaurant in the city of Langsa, and it was there that the atmospherics of terror turned into concrete reality when his interviewee received an urgent SMS:

> TEUNGKU LEUBE, THE FORMER REGIONAL [GAM] COMMANDER OF ARAMIAH LANGSA [JUST WEST OF LANGSA IN EAST ACEH] AND CURRENT HEAD OF THE PA SUB-DISTRICT OFFICE THERE, AGE 41, HAS BEEN SHOT DEAD BY UNKNOWN ASSAILANTS AT AROUND 7:20PM. HIS BODY HAS BEEN BROUGHT TO THE LANGSA PUBLIC HOSPITAL.

Moments later, similar messages arrived on JHG's phone as well, with PA officials requesting the election observers bear witness. Five minutes later JHG arrived at the hospital, where a large crowd already stood outside the emergency room. This was the sixth murder of a PA activist since February 2009.

Despite these terrors visited upon PA activists, on election day PA easily won nearly half the votes province-wide, allowing them to dominate the provincial assembly. For their part, during the campaign PA had directed plenty of their own threats and intimidation, mostly toward the other five local political parties, ensuring only PA took part in organised local politics. In Aceh's subsequent 2013 gubernatorial and 2014 legislative elections, PA managed to unseat the enormously popular incumbent governor by creating an environment of pervasive threat not unlike what they had experienced in 2009. The number of violent incidents in the months immediately preceding the 2013 election correlated with the shift in public support to PA's ticket.[69] These former separatists threatened to return the province to war if they lost, and on that hopeful platform, they won. In the run-up to Aceh's 9 April 2014 legislative elections, the Commission for Missing Persons and Victims of Violence (Kontras) counted 48 cases of election-related violence from January to March, including murder. In both elections, SMS threats served as force multipliers for numerous targeted killings and bombings: intimations in their arrival on an uncounted and unsolicited number of mobile phones that no one was safe from such outcomes.

Conclusions

Mobile technologies have been as thoroughly embraced by ex-insurgent thugs, religious extremists, and other 'uncivil' societal forces as they have by Kenyan housewives, Tanzanian cattle traders and Indonesian electoral quick-count monitors. A decade ago in Indonesian Papua, when select military units wished to clear Jayapura's evening streets, they would circulate rumours of vampires killing children in major towns. These actors learned that SMS cheaply and efficiently cultivate and expand zones of insecurity; the last decade has shown the nefarious embrace of this seemingly innocuous tool.

One counter-response from peace activists includes the development of 'early warning, early response' methodologies with ICT elements, often using the same mobile technologies first employed by spoilers in pursuit of more violent ends. International Crisis Group has reported on a loosely organised group, the 'peace provocateurs,' that responded to re-emergent sectarian violence in Ambon, where partisans have long relied upon media technologies to amplify the atmospherics of insecurity. The peace provocateurs now respond with the same tools, bringing their mobile phones to trouble spots to check rumours, then send back information and photos to a point

68 On immediacy and proximity, see: Grayman, J. H. (2014). Rapid response: Email, immediacy, and medical humanitarianism in Aceh, Indonesia. *Social Science & Medicine*. In press. http://dx.doi.org/10.1016/j.socscimed.2014.04.024. [Accessed 1 Sept. 2014].
69 Anderson, B. (2013). Gangster, ideologue, martyr: The posthumous reinvention of Teungku Badruddin and the nature of the Free Aceh Movement. *Conflict, Security & Development*. 13 (1), p. 53.

person who broadcasts updates to journalists and the wider public via SMS.[70] This strategy, however, is a reactive solution, a stop-gap measure always one step behind potential spoilers.

Our experiences with these proliferating mobile technologies throughout the past decade in Aceh and elsewhere in Indonesia have led us to consider their security implications for aid and development projects. Text messages are now the first medium of choice in threatening and extorting not just stakeholders in local elections, but also aid projects and staff involved in the broad milieu of conflict recovery efforts.

The phenomenon of SMS-driven threats and rumours does not generally interfere with the sharing of genuine security information amongst security planners. As disseminators of rumour or threat, they are as common in deteriorating environments as confetti (a better comparison may be the chaff that disrupts flight radar), and reacting to them all is neither necessary nor possible: JHG's experience shows that they can contain relevant information, which is to be noted, but not responded to unless particularly rich in plausible detail. The overall security environment influenced how affected people made personal security decisions: political and ex-insurgent notables changed their travel and accommodation patterns in response to this, not driving on the same routes frequently, even relocating temporarily to safer and less-known locations, sometimes away from their families, or ensuring a security presence in their homes. Threatening SMSs generally served as symptoms of the environment, rather than anything actionable in themselves.

The vast majority of threatening SMSs that BA received while he managed dozens of stabilisation and reintegration projects in Aceh did not escalate beyond his phone and ended with the delete button. Only on three occasions in 3.5 years did SMS threats eventually lead to actual violence. Ease of delivery and the ability to change numbers suggests that these threats should not be taken as seriously as traditional ones (see Sambuli and Awori, pp. 27-31). But security managers should establish protocols for this medium: logging messages and numbers used, with particular attention to any personal information directed at individuals. Non-specific threats that contain no intimate information (such as addresses or license plate numbers or names of children or spouses, for example) should be treated as anecdotal measurements of the increasing volatility of a security environment, and it is that environment that security managers will react to, rather than the SMS. SMSs containing specific information, however, need to be reacted to, as do SMSs arriving on, for example, an individual's private number which they do not disseminate widely (implying the threat's origin is more intimately close to the individual).

Over-reaction to non-specific threats weakens project credibility in post-conflict contexts precisely because such threats are to be expected in the course of such work. Numerous NGOs in Aceh actually used the threat environment to declare *force majeure* on projects that were failing long before they received any SMS threats. The urge to respond to such SMSs also needs to be resisted, because generally a response indicates that the threat has made an impact, and exposes the respondent to more threats, and more manipulation.

In conclusion, SMS threats do not generally constitute threats in themselves. Their anonymity and ease of use allow them to take on the appearance of threats, but they generally only act as the connective tissue for a larger body of more obvious threats that persons and organisations can act against. With certain exceptions, they serve as indicators for insecurity, rather than the insecurity itself.

70 International Crisis Group. (2012). Indonesia: Cautious Calm in Ambon. *Asia Briefing*. 133. 13 Feb. p. 2. Available from: http://www.crisisgroup.org/en/regions/asia/south-east-asia/indonesia/b133-indonesia-cautious-calm-in-ambon.aspx. (Accessed 1 Sept. 2014). See also ICG's Asia Briefing 128, which first reports on the formation of the peace provocateurs.

Monitoring Online Dangerous Speech in Kenya

Insights from the Umati Project

Nanjira Sambuli / Kagonya Awori

Introduction

The Umati[71] project emerged out of concern that mobile and digital technologies may have played a catalysing role in the Kenyan 2007/08 post-election violence, and that the online dissemination of potentially harmful speech was inadequately monitored. In the build up to the 2007 Kenyan elections, avenues of propagating dangerous speech were generally limited to broadcast media transmissions, print media, SMS and email. Anecdotal evidence suggested that online spaces such as forums and blogs were also used to plan and incite violence on the ground. However, at that time, no system existed to track such data. Incendiary remarks by politicians and notable public figures such as musicians (through lyrics) have been noted to incite violence in Kenya's historical past, specifically around election periods, with a culmination noted during the 2007 election period and its aftermath. Efforts to monitor hate speech have been in place through undertakings by Kenyan civil society as well as police authorities. However, the migration of inflammatory speech to online media remained neither monitored nor analysed.

Since the submarine fibre optic cables landed on Kenyan shores in 2009, Internet penetration has been on a steep increase.[72] Greater access to affordable Internet, especially through the use of smart and feature phones,[73] has seen increased use of social media in the country. Such platforms offer new spaces for people to express their opinions, especially during times of heightened anxiety such as election periods. With over 2 million active[74] Kenyan Facebook users as of April 2013[75] (an estimated 19.2% of the country's online population), and over 2.48 million geo-located tweets generated in Kenya in the 4th quarter of 2011,[76] it can be deduced that social media is heavily used by Kenyans, and will continue to grow in popularity.

New media have diversified the audiences that engage in online communication. As these online spaces are a new medium for disseminating inflammatory speech, their influence on the actions of the audience warrants assessment. A possible result is the creation of a vicious cycle as audiences convene around hateful content, converse in self-selected groups and form new ideas or support their original biases with the hateful beliefs of others (see Ayala, pp. 17-21). However, there is a prospect of virtuous cycle creation, as new media spaces can also act as alternative information sources that neutralise the negative impacts of online and offline inflammatory speech. An example of this is noted in the findings section below.

Initially, the Umati project sought to better understand the use of dangerous speech in the Kenyan online space by monitoring particular blogs, forums, online newspapers, Facebook and Twitter. Online content monitored includes tweets, public status updates and comments, posts and blog entries. Umati was launched in October 2012, six months before the Kenya general elections (March 4, 2013) and exists in two distinct phases.

Phase I (September 2012 to May 2013) established the following initial goals:

- To monitor and understand the type of online speech most harmful to Kenyan society.
- To forward calls for help to Uchaguzi, a technology-based system that enabled citizens to report and keep an eye on election-related events on the ground.[77]

71 Umati is Kiswahili for 'crowd'.
72 Communications Commission of Kenya. (2013). *Quarterly Sector Statistics Report: First Quarter of The Financial Year 2013/14 (Jul-Sept 2013).* Available from: http://ca.go.ke/images/downloads/STATISTICS/Sector%20Statistics%20Report%20Q1%202013-14.pdf. (Accessed 2 Sept. 2014).
73 *Ibid.*
74 Number of people active on Facebook over a 30-day period.
75 Social Bakers Statistics. (2013). Available from: http://www.socialbakers.com/. (Accessed 12 April 2013).
76 Portland Communications. (2012). New Research Reveals How Africa Tweets. 1 Feb. Available from: http://www.portland-communications.com/2012/02/new-research-reveals-how-africa-tweets. (Accessed 2 Sept. 2014).
77 Uchaguzi was an election-specific deployment by Ushahidi and other stakeholders that saw collaboration between citizens, election observers, humanitarian response agencies, civil society, community-based organisations, law enforcement agencies and digital humanitarians to monitor elections.

- To define a process for online dangerous speech tracking that could be replicated in other countries.
- To further civic education on dangerous speech, and sensitise the Kenyan public in order that they are more responsible in their communication and interactions with people from different backgrounds.

Phase II (July 2013 to January 2016) further aims:

- To refine the Umati methodologies developed in Phase I and where applicable, increase scalability of the project through automation.
- To test the Umati methodology in other countries in order to improve and increase its global/contextual applicability.
- To explore non-punitive, citizen-centred approaches for reducing dangerous speech online.

Umati methodology for identifying dangerous speech

Umati uses Susan Benesch's definition of dangerous speech, that is, speech that has the potential to catalyse collective violence.[78] Benesch's 'Dangerous Speech Framework' offers the following key variables for identifying dangerous speech:[79] the speaker and his/her influence over a given audience – a political, cultural or religious leader or another individual with a significant following tends to have more influence over a crowd; a vulnerable audience subject to incitement by the influential speaker; the content of the speech that may be taken as inflammatory to the audience and be understood as a call to violence; the social and historical context of the speech – for instance, previous clashes or competition between two groups can make them more prone to incitement; and the medium of disseminating the speech, including the language in which it was expressed.

Umati built on the Benesch framework to form a practical identification method. Specifically, the project found that the following three components of the framework were the most relevant for the identification of online dangerous speech in Kenya:[80]

1. It targets a group of people. It is important to note that a hateful comment about an individual is not necessarily dangerous speech unless it targets the individual as part of a group. In our research, it was observed that dangerous speech towards a group can occur across various lines, including religion, tribe/ethnicity, gender, sexuality, political affiliation and race.
2. It may contain one hallmark of dangerous speech. Three hallmarks that are common in dangerous speech comments, as identified by Susan Benesch,[81] include:

   a. Comparing a group of people with animals, insects or vermin;

   b. Suggesting that the audience faces a serious threat or violence from another group, specifically the same group that is a target of the inflammatory speech ('accusation in a mirror'); or

   c. Suggesting that some people from another group are spoiling the purity or integrity of the speakers' group.
3. It contains a call to action. Dangerous speech more often than not encourages a particular audience to commit acts of violence towards a group of people. These can include calls to kill, beat/injure, loot, riot, and forcefully evict.

Umati Phase I relied on a manual process of collecting and categorising online dangerous speech. Human input proved necessary for contextually analysing and categorising speech statements, which in turn facilitated the creation of an inflammatory speech[82] database. Between October 2012 and November 2013, up to eleven monitors scanned a collection of online sites in seven languages: English and Kiswahili (Kenya's official and national languages respectively); Kikuyu, Luhya, Kalenjin and Luo (vernacular languages from the four largest ethnic groups); Sheng (a pidgin language incorporating Kiswahili, local languages and English); and Somali (spoken by the largest immigrant community).[83] In Phase II, the Umati team has begun work on incorporating more automation in the data collection process where applicable. This is being explored through Machine Learning and Natural Language Processing techniques and tools, which if successful, will significantly increase the scalability and transferability of the Umati project going forward.

78 Benesch, S. (2013). Dangerous Speech: A Proposal to Prevent Group Violence. 23 Feb. Available from: http://voicesthatpoison.org/guidelines. [Accessed 2 Sept. 2014].
79 Not all variables must be present for speech to qualify as dangerous speech. Variables are also not ranked and may carry more or less weight depending on the circumstances. Each instance of speech must be evaluated in terms of the information available.
80 For further analysis see Awori, K. (2013). *Umati Final Report: September 2012-May 2013*. p. 27. Available from: http://www.research.ihub.co.ke/uploads/2013/june/1372415606__936.pdf. [Accessed 2 Sept. 2014].
81 Benesch, S. (2008). Vile Crime or Inalienable Right: Defining Incitement to Genocide. *Virginia Journal of International Law*. 48 (3). Available from: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1121926. [Accessed 2 Sept. 2014].
82 Inflammatory speech is used to refer to all three categories along the continuum: offensive speech, moderately dangerous speech and extremely dangerous speech.
83 The sources list currently covers 80+ blogs and forums, 350+ Facebook users, groups and pages, 400+ Twitter users, all major online Kenyan newspapers and YouTube channels for the five main Kenyan media houses.

Categories of inflammatory speech and their likelihood to catalyse violence

As monitors manually scanned online platforms for incidents of dangerous speech, they recorded the speech acts they perceived to be hateful in an online database. In this process, all dangerous speech statements were translated into English and sorted into three categories (in ascending order of severity):[84]

1. **Category one – offensive speech:** mainly insults to a particular group. Often, the speaker has little influence over the audience and the content is barely inflammatory, with no calls to action. Most statements in this category are discriminatory and have very low prospects of catalysing violence.
2. **Category two – moderately dangerous speech:** comments are moderately inflammatory and made by speakers with little to moderate influence over their audience. Audiences may react differently; to some, these comments may be highly inflammatory, while to others, they may be considered barely inflammatory.
3. **Category three – extremely dangerous speech:** statements are made by speakers with a moderate to high influence over their audience. These statements are seen to have the highest potential to inspire violence, as they tend to constitute an action plan that can be understood and acted upon by the targeted audience. These statements are often stated as truths or orders. Umati categorised all statements with a clear or perceived call to beat, to kill, and/or to forcefully evict a particular group, or an individual because of their belonging to a particular group, as extremely dangerous speech statements.

It is important to note that a causal link is almost impossible to draw between dangerous speech and on-the-ground violence, due to the many factors that contribute to bringing about a physical violent act (see Grayman and Anderson, pp. 25-26). However, speech has the capacity to catalyse or inflame violence. Actors are still legally and morally responsible if they commit violence in response to incitement or dangerous speech. When imminent threats of violence were found during the election period, the Umati team extracted the relevant information and forwarded it by email to a listserv of specific stakeholders. These included donor agencies, Umati partners and Uchaguzi key decision makers who were better equipped with mitigating the threats of violence that Umati collected. This process was triggered five times from January to April 2013 and on-the-ground teams mobilised based on the information passed to them.

Findings

- Over 90% of the inflammatory speech statements that Umati collected in 2013 were from Facebook. This has been attributed to the fact that Facebook is the most popular social media site in Kenya. Umati found however, that other factors come into play that accommodate dangerous speech on Facebook as opposed to the second most popular social media site, Twitter.[85] Most interestingly, a behaviour one of the authors named 'KoT cuffing' was observed on Twitter where '[offensive] tweets not acceptable to the status quo are shunned, and the author of the tweets, is publicly ridiculed. The end result is that the "offender" is forced to retract statements due to the crowd's feedback, and can even close his/her Twitter account altogether.'[86] KoT cuffing, a self-policing behaviour by Kenyans On Twitter (KoT), demonstrates that netizens themselves are capable of employing non-judicial means to counter online dangerous speech.
- Not surprisingly, it was possible to identify those that engaged in dangerous speech online, either via their real names, e.g. by use of their Facebook and Twitter accounts, pseudonyms which can be mapped to their email addresses, or through a traceable history of online activity using tracking software. Umati, however, did not attempt to uncover the true identities of online speakers, and instead focused on observing behavioural patterns of repeat dangerous speech offenders over short periods of time.
- Umati data reflected that in Kenya, ethnicity is a primary lens through which political, economic and social issues are viewed and reacted to by the public. Umati data showed that online discriminatory speech is mostly along ethnic lines. However, as different events transpired through 2013, most notably the Nairobi Westgate Mall attack,[87] Umati data shows that Kenyan online discriminatory speech has escalated along ethno-religious lines. What is crucial to note here is not that discrimination is mostly ethnic or religious,

84 Awori, K. (2013). *Umati Final Report: September 2012-May 2013*. p. 27. Available from: http://www.research.ihub.co.ke/uploads/2013/june/1372415606__936.pdf. [Accessed 2 Sept. 2014]. The full categorisation formula, including the data entry form, can be viewed in the final report.
85 Further discussed in Awori, K. (2013). *Umati Final Report: September 2012-May 2013*. pp. 24-25. Available from: http://www.research.ihub.co.ke/uploads/2013/june/1372415606__936.pdf. [Accessed 2 Sept. 2014].
86 *Ibid.*
87 Daily Nation. (2013). Security forces move to end Westgate mall siege as death toll rises to 62. 23 Sept. Available from: http://www.nation.co.ke/news/Westgate-Mall-attack-alshabaab-terrorism/-/1056/2004630/-/kr74w0/-/index.html. [Accessed 1 Sept. 2014].

but that such discrimination often stems from political, economic and social tensions along various divides. Thus, analysis of dangerous speech should be put into context of other speech online, as rarely do such speech incidents happen in isolation. Moreover, efforts to tackle dangerous speech should focus on addressing the deeper-seated issues that drive people to engage in, disseminate and even act on such speech's provocations.

- While the languages used to disseminate dangerous speech are those that are widely understood in the country, Umati collected some instances of coded language that had been used in past election periods. Additional research is required to investigate this linguistic 'code-switching', which is when a speaker alternates between two or more languages in the context of a single conversation, often to convey a thought or say something in secret.
- Umati Phase II has taken a keen focus on counter-speech, based on emerging phenomena on how 'netizens' are dealing with inflammatory speech online. Umati is monitoring how public conversations take place online over time, how some of these conversations may move towards dangerous speech, and the resultant counter-speech efforts if any. This broader approach will help us better understand self-regulation mechanisms employed by online communities (see Ayala, pp. 17-21). Preliminary self-regulation mechanisms observed online include ridiculing a speaker or a narrative that attempts to inflame hate/misinform/disinform, e.g. the aforementioned KoT cuffing; flooding online spaces with positive counter messages that diffuse tensions arising from hateful messages; and the use of humour and satire to 'hijack' inflammatory narratives.

Conclusions

Observations of dangerous speech should be framed within the context of other conversations online, as inflammatory speech statements rarely happen in isolation. Online dangerous speech is a symptom of the much more complex offline socialisations and perceptions that precede online interaction. We are yet to find concrete instances of online dangerous speech catalysing events offline (see Grayman and Anderson, pp. 22-26). Nonetheless, as 'netizens' congregate and converse online, forming networks around issues of interest, the possibility of organising offline reactions to online conversations is likely.

As part of our third objective in Phase II, we will explore efforts to reduce online dangerous speech through online and offline civic engagement. Umati intends to engage with relevant stakeholders on matters pertaining to freedoms of speech and expression towards better understanding how these are understood and exercised by the Kenyan public. While we are primarily looking at online methods, we will build on experience from *NipeUkweli*[88] (Kiswahili for 'Give me truth'), which is an outreach campaign fashioned to explore proactive ways of mitigating dangerous speech both online and offline.

Going forward, we offer that findings from Umati can provide insight into how humanitarian NGOs can galvanise their crisis prevention efforts and help manage security risks, before and during highly polarised events such as general elections (see Grayman and Anderson, pp. 22-26). One possible avenue could be to promote fissures and spaces where citizens in conflict-prone areas can air out any misconceptions or grievances that would otherwise inform hate/inflammatory/dangerous speech, and even violence.[89] Efforts to tackle dangerous speech (and its consequences) should focus on addressing the deep-seated issues that drive people to engage in, disseminate and act on the provocations of such speech.

88 Njeru, J. N. (2013). *NipeUkweli: Outreach to Sensitize Communities on Dangerous Speech: Summary Report*. iHub Research. 20 March. Available from: http://www.ihub.co.ke/ihubresearch/jb_NipeUkweliSummaryReportMarchpdf2013-11-18-16-07-39.pdf. [Accessed 2 Sept. 2014].
89 A creative example of this is the 'Alternatives to Violence Program', in countries like Kenya and Rwanda: http://www.avpkenya.org. [Accessed 2 Sept. 2014].

From Kenya to Myanmar

Though Umati's methodology was designed to monitor online dangerous speech in Kenya, the project's methodology was adopted in early 2014 for a pilot study of online dangerous speech in Ethiopia. Various elements of the coding form were edited to suit the Ethiopian context.[1] Overall, the methodology was applicable and the same categorisation of dangerous speech into three spectra was employed.

Umati is currently piloting the project in Nigeria, ahead of the 2015 elections. We are working with local Nigerian civil society organisations, offering technical support, as the teams adopt the methodology for their context. The Umati team was also recently in Myanmar, sharing insights on setting up the project with civil society organisations such as MIDO[2] who are keen on monitoring and countering dangerous speech online. As the collection and analysis process continues to be improved in Kenya, the aim is that the methodology will remain explicit enough to be understood and redesigned for other country contexts. Findings drawn from Umati's experience in Kenya can guide organisations in managing risks in contexts where online media is a possible vehicle for catalysing dangerous speech and violence.

For further information on the Umati project, see http://www.ihub.co.ke/umati

1 *Gagliardone, I., Patel, A. and Pohjonnen, M. (2014). Mapping and Analyzing Hate Speech Online: Opportunities and Challenges for Ethiopia. Programme in Comparative Media Law and Policy, University of Oxford. Available from: http://pcmlp.socleg.ox.ac.uk/sites/pcmlp.socleg.ox.ac.uk/files/Ethiopia%20hate%20speech.pdf. [Accessed 2 Sept. 2014].*
2 *http://myanmarido.org/en. [Accessed 2 Sept. 2014].*

Section 2

Communications Technology and its Impact on Humanitarian Programmes

This section looks at first-hand experiences in the use of communications technology at field level for humanitarian programming. Undeniably, communications technology is increasingly altering the way aid agencies operate and deliver assistance. What does this mean for security risk management? We can benefit from communications technology by managing programmes remotely in high-risk environments, but on the other hand, what are the short and long-term consequences of a lesser presence on the ground, or of collecting and storing mass amounts of beneficiaries' data? Managers and security focal points must understand how communications technology is being used in programming if they are to understand risks and opportunities, especially for security risk management.

Whispering when Everyone is Listening

Low-Tech Communications Technology Implementations in High-Risk Contexts

Keith Porcaro / Laura Walker Hudson

Introduction

Technology has the potential to disrupt existing community power structures, rewriting relationships both within a community and outside it. For communities that are particularly isolated or at risk, technology-focused projects can enable data collection, conflict mitigation, and service delivery efforts that would otherwise be impossible due to safety and other logistical concerns, and empower marginalised members of the community to participate in community dialogue and assert their needs.

Although technology can help reduce risk to community members and staff, it can also calcify negative power relationships, particularly if access to technology is limited to certain members of a community (such as male heads of households) – or restricted completely. Further, programmes using technology can create expectations of action that are incongruent with project goals or standards of beneficiary accountability. These risks can be mitigated. Community-aware approaches to programme start-up, execution, and exit can help ensure not only a programme's short-term success, but also its legacy, long after the final evaluation is complete. This article examines relevant case studies and suggests useful programme practices for high-risk implementations, from community outreach and crafting message content to implementation practices that minimise risk to staff, community members, and user data. Finally, this article will discuss defining the success and evaluating the legacy of technology projects in high-risk communities.

Community buy-in and reporting systems: does acceptance matter for technology-based projects?

Community acceptance of and participation in new systems can make or break technology programmes (see Tafere *et al*, pp. 42-44). Established interests may be suspicious of the effect of capacity-building or information leaving their community; and those with less power may risk repercussions for participating or have restricted access to technology through lack of power, freedom or resources. People may raise concerns about how the data will be used and shared (see Kaiser and Fielding, pp. 37-41). Conversely, technology can enable implementers to engineer equal participation from marginalised groups, and to hear from unexpected sources and indirect beneficiaries through open and anonymous communications channels. Striking this balance effectively is crucial for maintaining negotiated access in challenging contexts.

First interactions with the community are a critical moment for setting expectations about a project's outcomes (see Tafere *et al*, pp. 42-44). Technology systems create feedback loops: expectations of action and response that may be outside a project's remit or capability. Communities may participate based on a mistaken belief in the power of programme implementers to create change. A person taking the risk of reporting an incident may experience negative repercussions, especially if no help – or no immediate, specific help – comes as a result of the report.

Efforts to qualify the intended effect of reporting systems may not survive the first word-of-mouth relay. After the 2010 earthquake in Port-au-Prince, Haiti, a local SMS gateway was set up to feed on-the-ground

reports into an online mapping platform.[90] Although it was emphasised that the service was merely informational, rather than an aid request tool, it was not clear that this distinction was meaningfully understood by those who needed help. As a result, many of the incoming messages were discarded for a lack of actionability, relevance or usable location information, and as the approach was new and little understood by traditional humanitarian actors, requests were not directly taken up by aid agencies. Over-promising or failing to accurately set expectations can damage the community and project, as users take risks or expend resources to use a technology system that fails to deliver the help expected, and cease using the technology system as a result.

In one successful project, Voix des Kivus ran an 18-month pilot to monitor local events in Sud Kivu, a province in eastern DRC. The pilot sought to test the effectiveness of obtaining actionable information via SMS from communities that were dangerous or difficult to travel to. In order to ensure higher-quality data, Voix de Kivus employed 'crowd-seeding', where community reporting was routed through pre-identified representatives, each supplied with phones and credit. Due to the sensitive nature of information that was reported, such as acts of sexual violence, it was critical to obtain community buy-in and ensure that marginalised subsets of the community would be able to report.[91]

To achieve this, Voix des Kivus physically visited the target communities to explain the project and procure community consent. Each community selected three members to report incidents via phone: one from the village's traditional leadership, one representative of women's groups, and one elected representative. This enabled villagers to report incidents through the representative they were most comfortable with, and ensured Voix des Kivus would have a reliable trained cohort of reporters. Community members using the system were assured that reporters would further obfuscate sensitive information using a code sheet, which mapped two-digit numbers to a list of events. An additional digit indicated the event's sensitivity and set the degree to which the event was shared with outside parties (see Kaiser and Fielding, pp. 37-41).[92]

The pilot's success was rooted in a deep understanding of community structures, strengths and weaknesses, and the project prioritised those while still remaining practically feasible. That two of the three reporters represented non-traditional power structures potentially built trust in, and fostered the development of, additional community leaders, while respecting existing relationships.

Practical implementation of technology-based programmes for security risk management

Implementation of technology-based programmes in high-risk areas can raise many logistical challenges, particularly when distribution of hardware is necessary. Technology systems will lessen, but not obviate the need to physically visit target communities, and additional relationship-building may be needed to ensure technology is successfully used. Moreover, communities can demonstrate an ability to compensate for local logistical failures if the perceived value of the service is high enough.

In 2011 Infoasaid supported ActionAid to improve the way they communicated with drought-affected communities in Isiolo, Kenya. Infoasaid used SMS, Interactive Voice Response (IVR) and community bulletin systems to improve responsiveness and monitoring of aid reporting, and keep communities informed with critical or educational information, processes that previously required multi-day physical trips from a central office.[93] Although ActionAid Kenya continued to conduct food distributions throughout the project, one displaced community redirected their food distributions remotely when the security situation deteriorated.

250 Nokia phones were distributed to elected relief committees (RCs), along with an equal number of solar chargers. Not all communities took to the new technology. Some stopped responding or never used the system, for uncertain reasons, and some of these were so remote that, due to security and time considerations, it became impractical to return to some communities in order to troubleshoot issues.[94] This may be part of the cost of doing business in complex technology implementations, but does speak to the importance of simplicity for the end user and field-testing equipment before deployment.

90 Meier, P. (2012). How crisis mapping saved lives in Haiti. *National Geographic NewsWatch*. 2 July. Available from: http://newswatch.nationalgeographic.com/2012/07/02/crisis-mapping-haiti. [Accessed 2 Sept. 2014].
91 FrontlineSMS. (2011). Data Integrity Case Study: Voix des Kivus. pp. 1-2. Available from: http://www.frontlinesms.com/wp-content/uploads/2011/08/Case-Study-Voix-des-Kivus-final.pdf. [Accessed 2 Sept. 2014].
92 *Ibid.*
93 Infoasaid/Actionaid Isiolo. (2012). *A Learning Review of the Pilot Communications Project*. p. 4. Available from: http://www.cdacnetwork.org/contentAsset/raw-data/0abadcd6-f55a-459e-9b0e-3bcb9051c3ba/attachedFile. [Accessed 2 Sept. 2014].
94 *Ibid.*, pp. 13-14, p. 16, p. 34.

In this example, hardware failure may have been a contributing factor to some silences – the solar chargers suffered from a high failure rate, and were unable to deliver the current expected to charge multiple phones. However, several RCs independently adjusted, switching from selling the use of the charger to selling use of the phone itself, and not one RC requested financial assistance to use the service – an unexpected success, indicating the community realised and capitalised on the value of the phone itself. Ownership of both the technology and the drought response that the implementation supported were high. When some communities fled as the security situation in the area worsened, one RC reported their new position and requested that food distributions be diverted to the new location. Staff avoided travelling to a dangerous area, and information about security risks was spontaneously provided by the community, enabling the programme to adjust.

Good project planning involves covering as many contingencies as possible, and solutions may not always be technological. Information density and complexity, such as a wide variety of potential events to report, may present challenges that have technology-adjacent solutions (see de Palacios, pp. 51-55). In Mozambique and Zimbabwe, for instance, conservation area security workers patrolling for evidence of poaching were provided with a 52-card deck of playing cards, each of which corresponded to a different event, code, and instructions for reporting the data on a form.[95] Although there are no publicly available case studies, it's possible that security focal points could have regard to information gathered in this way to augment their understanding of the local environment. Thorough understandings of service, community, and logistical dynamics are pre-requisites not only for being able to successfully roll out a new project, but also for developing creative solutions in the face of new challenges.

Protecting people by protecting data

In complex contexts, humanitarian protection efforts that use technology often involve communicating sensitive information over insecure channels. This yields immediate and direct security risks for – and from – community members and staff. Programmes must then operate under the assumption that information and communications may be intercepted or read by hostile actors, from overbearing governments to abusive family members (see Gilman, pp. 8-11; see also Byrne, a. pp. 12-16). Technological solutions such as encryption can technically solve the problem, but raise new complexities and give the impression of having something to hide (see Byrne, b. p. 57). As with much humanitarian work in such contexts, some of these risks can be mitigated with clearly articulated organisational and programme goals and approaches, and a prior consensus about how the data collected will be handled (see Kaiser and Fielding, pp. 37-41).

In general, there are very few case studies of this type of work; those listed here are most of those that the authors are aware of. This is in part due to the nature of the work, and also to the tendency for technology projects to inadequately consider, document, or publish information relating to the impact or negative security and protection implications of data gathering and dissemination. Below, we summarise some lessons learned from colleagues and partners using technology in their work, and considerations documented in our Data Integrity Guide.[96]

National actors, particularly governments, can cause complete disruptions of technology systems at any scale, depending on the threat they perceive. Even if the project is not a direct target, sudden service interruptions can severely disrupt short-term project outcomes. Further, most low-cost technology platforms, including SMS, are inherently insecure data transmission channels. This, coupled with the state's often close relationship with ICT infrastructure companies, means that the perception and content of communications can pose a risk to staff and target communities, as the potential for messages to be intercepted cannot be discounted. Even non-state armed groups in Afghanistan and Somalia have been reported to intercept SMS traffic, a relatively simple technical operation for sophisticated actors (see Gilman, pp. 8-11; see also Byrne, a. pp. 12-16).

High-risk environments are not merely so because of threats from a central government: often, risks are local, from area militias suspicious of foreign-led projects; to community stigmatisation of HIV-positive people; to an abusive husband monitoring a spouse's phone. Discovery of messages on the phone itself can put individuals at risk, and messages to programme participants should omit personal or sensitive information. Good practice can mitigate some of these issues, particularly on the local level. Examples of

95 Le Bel, S. *et al.* (2014). FrontlineSMS as an early warning network for human-wildlife mitigation: Lessons learned from tests conducted in Mozambique and Zimbabwe. *Electronic Journal of Information Systems in Developing Countries.* 60. p. 3. Available from: http://www.ejisdc.org/ojs2/index.php/ejisdc/article/view/1256. [Accessed 2 Sept. 2014].
96 FrontlineSMS. (2011). *User Guide: Data Integrity.* Available from: http://www.frontlinesms.com/wp-content/uploads/2011/08/frontlinesms_userguide.pdf. [Accessed 2 Sept. 2014].

good practice are crowd-seeded reporting (that works in a more restricted way than crowd-sourcing, as pre-selected phone holders are the only ones who can send information), or redacting potentially harmful personal information from messages. Moreover, community members can be advised on good practice, such as deleting sent and received messages as they come in.

Conversely, community members and staff can manipulate project data, and may be incentivised to over- or underreport based on the outcomes expected as a result of their activity, such as receiving more aid due to exaggerated crisis reports. Multi-stakeholder verification can help detect and deter falsification or exaggeration. Even when information is verified, low participation rates can distort the aggregate data picture, especially if it is a function of lack of access to technology for certain groups, rather than lack of interest. With restricted access to communities, these groups and the precise dynamics unfolding on the ground can be hard to spot.

An emerging area of concern is the complex ethics around utilising data contributed by individuals with limited technology experience. General principles of privacy and fair dealing dictate that operators of platforms need informed consent to collect and manipulate people's data (see Kaiser and Fielding, pp. 37-41). However, explaining to someone on the far side of the digital divide precisely where their data will be hosted and treated can be impractical or impossible, making it difficult for those individuals to truly consent. This is an emerging area of work only now being explored by agencies, researchers and policy-makers. Data use should also do no harm, but there are many instances of technologists not understanding the complex risk management strategies that less empowered individuals employ and accidentally publishing or exposing compromising data, putting them at risk. To take a high-tech example, the ill-fated Google Buzz platform automatically and non-consensually exposed relationships between individuals and their contacts, including victims of intimate partner violence seeking help.[97] The unclear legal and regulatory implications of hosting and collecting different kinds of data, often across multiple jurisdictions, represent another emerging concern. Context analysis, caution and a clear understanding of the technical underpinnings of the proposed platform are critical to avoiding early and costly mistakes (see Byrne, b. pp. 56-58).

Conclusion

While technology's democratisation has enabled a new wave of low-cost data collection and information projects to take place, particularly in environments that were too risky to justify a project, it has yet to reduce the competition for participant attention that any implementation faces. There is little data on the real impact that this has on project approaches, and less on the impact that such projects have, as the combined challenges of technology use and difficult operating environments militate against good impact measurement. Like any project, attention and perceptions of value by beneficiaries must be earned, with context-sensitive planning and execution (see Kaiser and Fielding, pp. 37-41; see also Tafere *et al*, pp. 42-44). This is particularly important in high-risk areas, which have increased susceptibility to shocks, and where unexpected difficulties with technology use may derail a project before it gains momentum.

Ultimately, the success of any technology project is dependent on access to the underlying platform, and excluding people from platforms only exacerbates inequality, and thus conflict. Reasons for lack of access are many, particularly in high-risk contexts, and so multi-platform, inclusive, low-tech approaches – SMS, voice systems, community bulletins, etc.– can help give people the widest possible number of options to connect with the implementing organisation. Access to technology can be transformatively empowering for local communities. Although resources may not be available to bring every technology pilot to scale, participatory programmes can help defuse local reluctance toward technology and, anecdotally at least, can increase 'buy-in', a sense of empowerment and community acceptance of programmes. In Kibera, a slum in Nairobi, foreigners began an effort to map the slum and its attendant services, but only found lasting success when Kiberans took ownership over the mapping efforts and outcomes. In the words of one Kiberan, 'When I saw the map for the first time, I was proud. This has not been done by other people. It has been done by me.'[98]

97 Boyd, D. (2010). Privacy, Publicity, and Visibility. Presentation at Microsoft Tech Fest. 4 March. Available from: http://www.danah.org/papers/talks/2010/TechFest2010.html. [Accessed 2 Sept. 2014].
98 Parfitt, B. (2012). Putting yourself on the map. *Geographical*. April. Available from: http://www.geographical.co.uk/Magazine/Community_Mapping_-_Apr_12.html. [Accessed 2 Sept. 2014].

A Principled Approach to Data Management

Lessons Learned from Medair's Experience in Lebanon Using Last Mile Mobile Solutions

Joel Kaiser / Rob Fielding

Introduction

Over the past 25 years Medair has developed expertise delivering emergency assistance to disaster and conflict-affected populations in need of safe water and sanitation, hygiene promotion, health and nutrition services, and secure shelter. Since its first cash transfer programme in 2009, Medair has made a concerted effort to realise the benefits of mobile digital technologies in humanitarian programming. The industry trend in this direction has been accelerated by the rapid increase of mobile phone subscriptions in developing countries. With the spread of mobile connectivity, digital technologies are bringing to humanitarian aid workers an unprecedented capacity for data collection and analysis, which can improve service delivery in humanitarian crises (see Tafere *et al*, pp. 42-44). The most effective use of mobile digital technologies to date for Medair has been via Last Mile Mobile Solutions (LMMS).

LMMS is a software system designed by aid workers that enables humanitarian staff to register people in the affected population, and digitally manage a distribution of relief materials or resources to them. To do this, LMMS has replaced paper-based project forms with digital forms on handheld devices, and has in this way fully automated the process of identifying and tracking the quantity of items, such as cash, hygiene kits, or food rations, that are to be distributed per beneficiary based upon project specifications. LMMS accomplishes this by issuing beneficiaries with computer-readable identity cards. Once registered into the system, beneficiaries can be transitioned into projects using the same identity card, thereby avoiding multiple data entries over time. LMMS strengthens the security and control over the inventory of relief items during a distribution and enables improved accountability through photo verification of households or their authorised proxies. It also supports the added benefit of real time analysis and reporting of relief activities involved in the project.

Using LMMS in the Syrian refugee response has enabled Medair field teams in Lebanon to distribute emergency shelter solutions customised to diverse groups of Syrian refugees without compromising accountability or security of relief items.

Benefits of using software for aid delivery in Lebanon

Medair's emergency response team arrived in Lebanon and conducted emergency assessments and crisis mapping for two weeks in the Bekaa Valley in order to locate and identify refugee families living in informal tented settlements. These assessments not only confirmed the vulnerabilities of a growing demographic, but also the rapid rate of data turnover resulting from the on-going displacement of refugees. The multitude of informal refugee settlements, each with unique needs and assets, created a complex and dynamic context in which the accurate and timely collection and management of assessment data became paramount.

Medair field teams realised that static 'snapshots' of individual settlements could not adequately inform the agile humanitarian operation required by the crisis, and therefore trained assessment teams to perform continual, rolling assessments, supported using Open Data Kit (ODK). This form filling software is an open source system that substitutes the traditional clipboard. It allows conducting surveys or

questionnaires and collecting quantitative and qualitative data in different languages. In Lebanon, national staff collected data in Arabic for identifying the most vulnerable population and creating a list of beneficiaries and their needs. Subsequently they were able to download the information in both English and Arabic in CSV format back in the office. ODK also enabled the real-time mapping of data using ArcGIS (a geographic information system), and the information produced was shared with other actors in the humanitarian community.

Currently, beneficiary identification and distribution teams cover 173 informal settlements in Medair's areas of operation across West and Central Bekaa with shelter and non-food-items needs. This amounts to aid for approximately 29,000 beneficiaries living in 4,611 tents according to latest data collected and mapped using ArcGIS as part of the Countrywide Inter Agency Mapping Platform Version 3.[99]

This software also allowed Medair to use the information for identifying trends more accurately and gaining a more nuanced understanding of the capacities and needs of newly arrived refugees. This understanding enabled the Medair team in Lebanon to customise their projects for diverse refugee groups using a 'relief items catalogue'. Based on the data gathered at the assessment stage, Medair catalogued all relief items available to beneficiaries factoring different needs, or family size or composition, for example. Although beneficiaries do not get to choose the items from a list, having rapid access to up-to-date information has allowed Medair to tailor the distribution of aid to the actual needs of the most vulnerable populations, and provide a faster and more efficient assistance. This was particularly useful given the very fluid situation in which displaced populations were constantly moving (see Porcaro and Walker, p. 35).

At the distribution stage, Last Mile Mobile Solutions comes into play. LMMS enables digital tracking and control of relief items, and streamlines the distribution process, allowing teams to undertake distributions that would otherwise be too complicated and cumbersome to support. Combinations of relief items, such as vinyl sheeting, plastic sheeting, timber of various sizes, plywood sheets, hand tools, and NFI materials such as fire extinguishers, mattresses, blankets, baby kits and kitchen sets can be distributed within a single settlement.

The initial deployment of LMMS in Lebanon focused on distribution projects including shelter and new refugee arrival non-food-items kits as well as the distribution of fire prevention and mitigation equipment. It is anticipated that both WASH and health projects will also benefit from one centralised beneficiary database and registration system using one centralised multi-sectorial assessment and distribution team, with supporting technical staff for each sector. To avoid duplication where uncertainty arises, the Medair team in Lebanon also benefit from being able to crosscheck beneficiaries' names in the field using the LMMS server. Along with the benefit of having instant access to beneficiaries' previous distribution records and knowing exactly what they have received and when, the team can instantly address complaints and distribution inaccuracies raised by beneficiaries.

Handling sensitive information appropriately

The most sacred tenet in data storage is to correctly recognise (and protect) sensitive information, which for humanitarians amounts to any data that directly links to individuals in an affected population. This data must only exist in a limited domain, since any breach could radically jeopardise the personal security of many people and thereby undermine the principle of 'Do No Harm' (see Porcaro and Walker, p. 36). In this way, aid agencies should approach the topic beginning with the protection principles of the Sphere Handbook, specifically the section on managing sensitive information.[100] The Sphere Handbook recommends that humanitarian agencies have clear policies and procedures in place to guide staff on:

1. How to respond to a security breach.
2. How to refer sensitive information, such as incident reports and trend analyses.
3. How data may and may not be shared.
4. How to collect data, including seeking consent to gather information and providing a rationale for why data is being collected.

The data collected by Medair using ODK and LMMS includes vulnerability and demographic indicators, and is therefore sensitive. Add to this fact the sectarian nature of the conflict in Syria, and the security of beneficiary data becomes of paramount importance. The risk to beneficiaries is most related to the use of

99 Howe, A. (2014). LMMS *Lessons Learned in the Syria Regional Crisis.* Beirut: Medair.
100 Schenkenberg van Mierop, E. and Haenni Dale, C. (2011). Protection Principles. In *The Sphere Project: Humanitarian Charter and Minimum Standards in Humanitarian Response.* 3rd ed. Rugby: Practical Action. pp. 29-47.

data for purposes other than those for which they were collected, such as the sharing with or selling of data to third parties, and the inherent security risks of sending and receiving sensitive data via mobile phones.[101] Reports of security breaches at large online companies such as eBay, and even security and anti-virus providers such as Kaspersky and Symantec, offer additional proof that the challenges related to digital data collection and storage are a risk for even the most technologically advanced companies. For humanitarian organisations operating on tight budgets, this challenge can appear insurmountable (see Gilman, p. 9).

The context of the Middle East also presents unique challenges to data management and security. For example, it was originally planned to export monthly list files for cross checking with UNHCR's database to ensure that beneficiary registration information on LMMS was up to date. However, difficulties with the data export process were encountered because the digital tools used to extract the data from the LMMS server did not support Arabic script. Quick workarounds had to be devised in order to fix an otherwise simple checking process.

Adapting Cash Learning Partnership (CaLP) principles to data management

To date, there is no widely recognised guidance on data management in humanitarian operations. However, in an effort to operationalise the Sphere guidance on managing sensitive data, the Cash Learning Partnership (CaLP) has published a set of principles and operational standards for the secure use of personal data in cash transfers. Medair chose to use the CaLP principles, despite the programme not involving cash transfers, out of the belief that they present the best guidance on data management to date. The principles were developed to address the risks associated with the collection, storage, use, and disclosure of the personal data of beneficiaries. They were designed to serve as a minimum standard to ensure the protection of beneficiaries' privacy and personal data, which is defined as 'any data that directly or indirectly identifies or can be used to identify a living individual'.[102]

The principles are based on numerous international and national instruments which enshrine data protection principles, and derive guidance from human rights standards related to privacy and data protection. These are strongly linked to individual autonomy and dignity. The principles are necessary, particularly since a CaLP survey indicated that a majority of respondents reported that their organisation lacked internal data management guidelines. The principles also introduce a Privacy Impact Assessment[103] that serves as an excellent means to inform the planning and implementation of data management. The final section of this paper describes Medair's experience interacting with these principles in the management of sensitive beneficiary data in Lebanon.

> The version of the Privacy Impact Assessment (PIA) adapted by CaLP was initially developed by the U.S. Department for Homeland Security (DHS). DHS considers the PIA process 'inherently necessary for all U.S. Federal Government programmes since 2002.' 'The process of a PIA is to demonstrate that programme managers and system owners have consciously incorporated privacy protections throughout the development life cycle of a system or programme. This involves making certain that privacy protections are built into the system from the initiation of the development, not after the fact, when they can be far more costly or could affect the viability of the project.'

Lessons learned: implementation of data management principles

Medair's digitally collected beneficiary data is significantly more secure than using Excel spreadsheets or paper-based beneficiary lists. Of course, Medair is aware that no system is foolproof and that it is only as good as the personnel who implement it (see Byrne, b. pp. 56-58). To this end, Medair has created Standard Operating Procedures (SOPs), which are periodically refined based on theoretical anticipation of the strengths and weaknesses of the process as implemented, and based on trial and error as experienced by teams in the field. This has produced several lessons learned which highlight that a mutually trustworthy relationship with the beneficiaries is critical when employing digital technologies, and that time spent explaining the use of the technology, supported by easily understood leaflets, has garnered this requisite trust among refugee populations (see Porcaro and Walker, p. 33).

101 Gallagher, I. (2011). Egyptian police use Facebook and Twitter to track down protesters' names before 'rounding them up'. *Mail Online*. Available from: http://www.dailymail.co.uk/news/article-1354096/Egypt-protests-Police-use-Facebook-Twitter-track-protesters.html. [Accessed 10 July 2014].
102 The Cash Learning Partnership. (No date). Protecting Beneficiary Privacy. p. 5. Available from: http://www.cashlearning.org/downloads/calp-beneficiary-privacy-web.pdf. [Accessed 1 Sept. 2014].
103 *Ibid.*

Digital technologies may be difficult to understand and trust for some communities, and key for their success is that beneficiaries understand that personal information is not shared outside the agency (see Porcaro and Walker, p. 36). Medair field teams are very clear in delivering this message, and explain the advantages that these technologies have in protecting people's confidentiality. As mentioned before, an added advantage of LMMS is that plastic card IDs substitute the traditional finger printing signature, which can be seen as impersonal and demeaning by some beneficiaries. LMMS allows a more dedicated approach by aid agencies, which in turn helps communities trust the technology behind it (see Tafere *et al*, pp. 42-44).

Cash Learning Partnership principles for data management: Medair's experience

The principles published by CaLP are paraphrased below, along with a summary of Medair's experience of applying them.

1. *Respect that collection of personal data represents a potential threat to beneficiary privacy.*

This principle is fundamental to the training of Medair's data collection teams. The teams are identified to the refugee community as the sole authority for the collection of personal data, which minimises the risk of fraudulent actors seeking personal data in the name of Medair. A lesson learned is to include additional information on the programme leaflet explaining the use of personal data and steps taken to secure it, as well as the redress mechanism refugees have access to in the event they feel their privacy has been compromised.

2. *Protect by design by ensuring that privacy and protection of beneficiary data are designed into the programme rather than as 'add-ons'.*

This has been highlighted as an area of improvement. For example, there was no specific SOP to address a beneficiary who opted out of providing data for LMMS, and an *ad hoc* work-around had to be created. Undertaking a Privacy Impact Assessment (PIA) would have identified holes in SOPs such as this. However, the SOPs did successfully address database backup, encryption, protection and partition; so for example, those collecting data never have access to full beneficiary records, while multiple verifications protect database backups.

3. *Understand data flows within the programme as well as among organisations in order to mitigate the risks.*

Data Sharing Agreements (DSA) among Medair and third parties, which have been in place from the onset of the programme, define expectations concerning confidentiality of the shared data. However, the difficulty of enforcing such agreements remains and as such, trust among partners becomes critically important.

4. *Ensure the quality and accuracy of the personal data by keeping it up to date and relevant, and ensure that the amount of data is not excessive in relation to its use.*

Medair discovered that very frequent spot checks are necessary to account for both errors by data collection staff and beneficiaries providing incorrect data. By building data triangulation into the process through, for example, comparison with refugee registration papers, these spot checks can be facilitated efficiently. However, a lesson learned was to find a better process for identifying beneficiaries who have moved outside the programme area, since this oversight will ultimately undermine the programme's exit strategy.

5. *Obtain consent or inform beneficiaries as to the use of their data.*

All beneficiaries are informed about the programme and asked for their consent to use and share their personal data. A lesson learned indicated the need for improved monitoring to ensure data collection teams are taking the required time to receive informed consent, since some may proceed through the questioning too rapidly for beneficiaries to comprehend the implications of their participation.

6. *Security standards should be in place for each stage of collection, use, and transfer of data.*

Medair maintains a security focal point who is in sole possession of the database password (with failsafes in place). All data is password-protected and encrypted. As stated earlier, DSAs regulate the use of data for third parties, though monitoring and enforcement of data usage by third parties is not practiced.

7. *Disposal of beneficiary data should be part of an exit strategy; data should not be held longer than required without a clear rationale.*

A review indicated a need for a more robust exit strategy beyond destruction of hardware. Personal data held in the cloud has not been addressed and indeed, the footprint of this data is not clearly understood.

8. *An accountability mechanism should enable beneficiaries to address concerns or complaints about the use of their personal data.*

Although Medair operates a hotline for beneficiary complaints, a review found that beneficiaries were not specifically informed that they have a right to follow up on the use of their data, and that this hotline is one such method. LMMS does enable Medair to track information that has been shared, and with whom. Another lesson learned was to establish an SOP for reporting data loss.

Conclusion

Medair believes that the benefits of digital tools such as LMMS outweigh the risks so long as a principled approach to data management is adopted. The benefits in increased efficiency and effectiveness with digital data entry are tangible: on average a competent and efficient data-entry assistant is able to complete 6 to 8 household registrations per hour using LMMS, or approximately one household registration every 7.5 to 10 minutes.[104] This figure is comparable to paper-recorded data collection, until the lengthy data entry component is factored in and the number of errors that often occur when data is typed into Excel spreadsheets or handwritten onto paper forms. This saving of time directly translates into financial savings in the form of reduced workloads and the need for fewer staff. Such evidence in support of the increased use of digital data collection tools suggests that greater emphasis should be paid to developing consensus and training in data management principles. This would help to ensure that humanitarian agencies located in developing countries, often operating with few resources, are also able to realise the benefits of digital technologies.

104 Howe, A. (2014). *LMMS Lessons Learned in the Syria Regional Crisis.* Beirut: Medair.

Mobile Money Systems for Humanitarian Delivery

World Vision Cash Transfer Project in Gihembe Refugee Camp, Rwanda

Maereg Tafere / Stuart Katkiwirize / Esther N. Kamau / Jules Nsabimana

Section 2

Introduction[105]

One of the factors driving the steady shift towards employing technology is the rapid expansion of the mobile telecommunications system and its potential to reach even remote areas of the world. According to global statistics, there are almost 7 billion mobile-cellular subscriptions,[106] three-quarters of them in developing countries. This creates a new opportunity for cash transfer using mobile phones. Such was the case of Kenya, where this system was used for the first time.[107] Concern World Wide was the first to use mobile phones for bulk cash transfer in early 2008 in response to the Kenyan post-election crisis.

This study is an assessment of a mobile money system (MMS) used to transfer cash to refugees from the Democratic Republic of Congo (DRC) based in Gihembe, Rwanda. It is based on document and literature reviews, as well as group discussions held between 5 May and 6 June 2014. Overall more than 100 refugee families, in mixed groups and in another group involving only women heads of households, were involved in the discussions. Interviews with UNHCR and VISA were also held, and WFP and World Vision were represented in the discussions by groups of 3-5 experts working in the pilot.

This study does not claim to be complete, but describes the opportunities and challenges as observed at the current stage of the project. We therefore recommend further longitudinal study to be carried out to find out the long-term impacts of the system.

Project background

Currently, Rwanda hosts more than 75,000 refugees, most of them from DRC, who arrived at different times. Some are recent arrivals while those in Gihembe, numbering 14,500 (3,500 households), came in 1996. For many years the refugees have been receiving humanitarian services in-kind including food or firewood. There were also instances of using cash vouchers. However, direct cash distribution presented some pitfalls: among others, difficulties for refugees and internally displaced people to use formal banks, and the security challenges associated with accessing remote insecure areas where refugees and disaster victims were mostly located (see Porcaro and Walker, pp. 33-36). These called for the use of alternative means to disburse cash in an accessible and safe manner.

World Food Program (WFP), Office of the United Nations High Commissioner for Refugees (UNHCR), World Vision Rwanda, Bank of Kigali (BoK) and VISA decided to implement a pilot project to test MMS. WFP, UNHCR and World Vision worked together to prepare the refugees, identify and contract merchants and money agents willing to serve the refugees and provide the mobile and cell phones; while VISA and AirTel (mobile communications provider) took responsibility for providing the electronic system (mVISA) and managing the transactions respectively. The project started as a pre-pilot in December 2013 with 177 heads of households. Based on quick information gathered from beneficiaries regarding the levels of satisfaction, the program was then expanded in January 2014 to cover all the 3,500 households (14,500 persons) in the refugee camp. The total amount of money transferred every month amounts to about US$140,000.[108]

105 The authors would like to thank World Vision Rwanda and the staff in Gihembe refugee camp who facilitated the group meetings, and meetings with the partner agencies both in Kigali and the field. We are also grateful to the head of UNHCR office in Gihembe, WFP staff, and the refugee group members who devoted their time during the discussion days.

106 International Telecommunications Union. (2014). *The World in 2014: ICT Facts and Figures.* pp. 1-8. Available from: http://www.itu.int/en/ITU-D/Statistics/Pages/facts/default.aspx. (Accessed 2 Sept. 2014).

107 Datta, D. et al. (2008). Mobile Phone-based Cash Transfers: Lessons from the Kenya Emergency Response. *Humanitarian Exchange Magazine.* 40. October. pp. 37-40. Available from: http://www.odihpn.org/humanitarian-exchange-magazine/issue-40/mobile-phone-based-cash-transfers-lessons-from-the-kenya-emergency-response. (Accessed 2 Sept. 2014).

108 World Vision Rwanda. (2014). Cash transfer project highlights. Unpublished. pp. 1-2.

The MMS uses short message services (SMS), operating on a VISA systems platform, to handle transactions between the refugees and sixteen vendors with a diversified food basket (a diverse range of food products). Money is transferred from BoK to vendors' and money agents' accounts when refugees purchase food or receive money. The vendors and money agents are required to have an account with the BoK, but the refugees are not. SMS texts are automatically sent by the mVISA system informing beneficiaries about the availability of the monthly amount in their e-accounts. The system also updates the amount after every purchase or withdrawal has been accepted. The system provides an option for withdrawal of cash in case the registered vendors don't offer competitive services in both quality and price. If beneficiaries decide to withdraw cash instead of purchasing food directly from the designated vendors, they bear transaction costs. Normally, one transaction is anticipated to be necessary, and thus is free. However, subsequent transaction costs are borne by beneficiaries, the aim being to discourage withdrawal of cash as such withdrawal may not necessarily be for purchasing food.

Results and discussions

The results of the group discussions were positive. The mobile money option provided beneficiaries with several opportunities including the option to purchase their preferred food types, and created a good environment for disaster victims and host communities to interact (through local businesses) leading to more interdependence. Other key benefits included:

- **Safety and security:** in-kind distribution is crowded and messy. Food distribution normally poses security risks to aid workers who manage warehouses, or transport and distribute food to beneficiaries. MMS can help in managing these risks as well as risks to the beneficiaries. In some places, such as Darfur, community leaders *(Sheiks)* take a portion of beneficiary ration from each household as payment for their presumed community services.[109] This ultimately reduces the family's per capita food consumption. The MMS avoids all such possibilities as rations are directly transferred to the beneficiary's e-wallet. The system also benefits vendors and aid workers. Money is directly transferred to vendors' accounts without the need for them to go to banks to make deposits at the end of a good market day. They save time and feel safer as they don't carry large amounts of money.
- **Social cohesion:** initial findings suggest that cash had a positive impact on relationships within households, between households, and even between communities. Refugees consistently reported improved relationships within the community due to reduced amounts of theft and interpersonal loans, both of which were key sources of conflict within the community. Refugees also reported reduced need for illegal firewood collection due to purchasing preferred food items that require less cooking time, which has addressed one of the key sources of conflict with the local community, namely the scramble over natural resources. These changes have positive security implications.
- **Restoring dignity:** standing in a line to receive food rations, or visiting a shop with a food voucher, can be a humiliating moment for families who had their own livelihoods before a crisis. Being in control of their cash using their phones, being able to buy what they want, and when they want, gave beneficiaries a sense of dignity.
- Finally, the system brought a number of actors together (aid agencies, private sector, merchants, and local authorities) to work on the same agenda. These entities worked closely on matters that are relevant to the project including tracking of beneficiary satisfaction, and challenges encountered. Organisational relationships in turn contributed to better understanding of each other's businesses. The involvement of communications companies in the humanitarian sector opens up opportunities for other forms of technology products that improve humanitarian services (see Porcaro and Walker, pp. 33-36; see also Kaiser and Fielding, pp. 37-41).

As is the case for any newly adopted system, some challenges remain. Almost all discussants unanimously mentioned telephone network interruption to be the number one challenge of the system. Since transactions depend on SMS messages, connectivity disruptions caused anxiety to both the vendors and the refugee families. For instance, a beneficiary sends an SMS message to instruct the system to deduct money from his/her account. If

109 World Vision Sudan. (2012). Food distribution monitoring report. Unpublished. pp. 15-20.

connectivity is lost during the transaction period, he/she cannot receive goods until connectivity is restored which can take from few minutes to few hours. In a few cases, World Vision had to intervene by sending messages to the BoK headquarters to resolve hanging SMS messages. Other key challenges raised by discussants were lack of stable power system to recharge mobile phones, illiteracy (difficulty in writing and reading SMS messages, and memorising the five-digit PIN number); and loss of SIM cards and at times of cell phones. In addition, MMS required intensive awareness creation and subsequent sensitisation of beneficiaries (see Porcaro and Walker, pp. 33-36). The project would not have succeeded without an experienced and competent local partner working closely with the beneficiaries.

Some concerns were raised by supporting NGOs on the ground in relation to data security. Owing to the engagement of multiple entities in the process, there were some apprehensions from the organisations regarding the risks associated with electronic storage and sharing of personal and financial data, due to perceived risk of repercussions if data was to fall into the wrong hands. Electronic data is considered more of a risk than printed data as it is potentially easier to move or access. This highlights a lack of protocol for data management among the involved agencies (see Kaiser and Fielding, pp. 37-41).

Conclusion and recommendations

Technologies sponsored and sanctioned by the humanitarian community should be simple to use, cost-effective, reliable and secured (see Porcaro and Walker, pp. 33-36). Security costs that protect the mobile banking system are normally borne by the technology providers (banks and communications companies) and should not be transferred to users. The following precautions may be necessary for a secure money transfer system:

1. Use mobile phones with basic functions (voice and text systems only) and avoid use of smart phones as their systems can be accessed remotely;
2. Ensure adequate beneficiary education on securing SIM cards and PIN codes even from close relatives;
3. Pay closer attention to how stolen or malfunctioning SIM cards are replaced; and
4. Ensure that mobile service provider companies have a proper information security policy that governs access to network elements and information assets by employees, agents or external fraudulent users.

Now that an increasing number of mobile telephone companies provide MMS, humanitarian agencies have the option of engaging the local service provider already most popular among beneficiary populations. A greater number of users would mean a bigger market for the private companies, which opens opportunities for competitive bidding to reduce service costs: MMS providers can offer free cell phones, SIM cards and lower transaction costs if they know they can sustain their business for a longer period of time. In addition, continuous monitoring and evaluation by partners and researchers may contribute to the refinement of the program and smooth integration into the country's economy.

The overall outcome of the quick performance assessment of World Vision's Mobile Money System programme in Gihembe was positive. MMS provided beneficiaries with ease, security, and options to purchase preferred food types. As mentioned above, the system is secured, and allows beneficiaries to use the money in their phones (e-wallet) at an appropriate time. The system also provided opportunities for refugees to create closer relationships with the host community and country. Donors and humanitarian actors on the ground expressed satisfaction; unlike food and cash voucher distribution systems, this technology made their work easier and safer. Envy and mistrust between disaster victims and host communities can be a source of insecurity in environments where resources are scarce and valuable supplies such as food stocks and equipment are controlled by aid agencies. The current system allowed them to mitigate some of the risks associated with in-kind distribution of goods. Relationships between World Vision's field workers and refugee families improved as complaints on resource-related issues lessened.

Section 3

Using Communications Technology for Security Risk Management

This section explores some practical tools that can help mitigate security risks, both digital and physical. As presented in this paper, the challenges and opportunities presented by communications technology are myriad. The technological revolution is far from being entirely negative: new digital tools are presenting important opportunities for security risk management. There are new ways to source, track and interpret security data and new ways to develop alert systems and share security information within organisations.

Communications technologies require some technical knowledge to assess and respond to the risks they bring, a factor that often shuts down practical discussion about such challenges as organisations and staff feel out of their depth, overwhelmed, and intimidated by a sense of general fear whose nature they do not understand. But while it is true that the humanitarian sector is behind the curve and needs to do far more to understand the nature of these risks, there are basic practical steps that can be taken now.

SMS Technology and Bulk SMS Delivery Systems

Their Role in Security Management for the Humanitarian Community

Athalie Mayo

Introduction

Security professionals in the humanitarian sector might frown at over-reliance on cellular telephone technology in high-risk environments, whether the risk landscape is dominated by natural hazards or man-made risks. The emphasis has traditionally been on ensuring the presence of an emergency communications network which consists generally of HF/UHF/VHF or satellite networks. Nonetheless, the implementation of such traditional emergency communications networks is fraught with difficulties ranging from financial constraints to concerns that the visible use of such technology may, conversely, result in the targeting of the user (see Gilman, pp. 8-11; see also Byrne, a. pp. 12-16). More often than not, the nationally recruited staff members of an organisation are those that suffer most from the shortfalls of these systems.

In recent years, the proliferation of cellular phones, expansion of networks, and increase in the provision of services such as bulk SMS distribution have amplified the range of mitigating measures available to the security professional and the staff members under their responsibility. This article seeks to promote further discussion of the challenges and opportunities presented by the use of SMS technology and bulk SMS distribution services for the dissemination of security information, ranging from simple notifications to more advanced mechanisms such as the activation of warden systems.

Traditional emergency communications systems

Benefits of traditional systems

'Knowledge is power' and the gathering and analysis of information is the bedrock of sound security management. Nonetheless, knowledge of an imminent attack or demonstration or inbound typhoon is useless if it cannot be communicated in a timely and efficient manner to those who may be affected (see Porcaro and Walker, pp. 33-36). A fundamental requirement of any security operation in a high-risk environment is therefore a robust communications system that permits exchange of key information as close to real-time as possible.

There is no doubt that resilient, autonomous and 24/7 communications systems are absolutely critical to the provision of efficient security support in high-risk environments. Satellite phones, HF and VHF/UHF networks in varying configurations have provided the foundations of security operations all over the world for years. When implemented fully they represent a significant measure to mitigate against the prevailing risks. Of course, they are not invincible and there are sometimes 'black spots' in satellite phone or HF coverage or human error to contend with. This article does not in any way seek to denigrate the value of these systems which have been proven time and again in humanitarian operations. Rather, the aim is to explore some situations which may perhaps be better supported by alternative or parallel means of communication, namely SMS based systems.

Limitations when supporting locally recruited staff

It is not unusual to find that not all locally contracted staff members working in locations classified as 'high-risk' have been provided with radio handsets or satellite phones as their international counterparts might have been. The rationale behind this varies but is often due to a combination of two factors: a perception that they have their own networks and coping mechanisms as they are living and working in their home environment, and the funding implications of providing equipment and support to such a large number of staff.

Anecdotal evidence from three locations generally acknowledged to be 'high-risk' at the time that the discussions with local staff took place (Darfur 2009, Afghanistan 2011, and Central African Republic 2014) indicated another significant challenge to the roll-out of emergency communications systems to locally recruited staff. Even where the employing organisations had provided local staff with radio handsets or satellite phones, individuals frequently did not use them in the way that had been envisaged by security professionals. Shortfalls included: very low response rate to radio checks, consistent failure to carry radios, radios not being charged, radios not used to broadcast security updates nor used to summon security support *in extremis*.

The reported reasons behind these issues varied according to individual, organisation and location. Of particular concern was the observation that radios and satellites phones can draw negative attention towards the individuals using them and consequently heighten the risk they are facing (see Byrne, a. p. 14). In a location such as Kandahar this scenario may reach life-threatening proportions. If local staff members are seen with such equipment they are immediately recognised as working for international organisations and may be targeted by extremist elements that oppose the work or ethos of their employers.

Elsewhere, for example Bangui, Central African Republic, the local staff members may be more concerned that the communications equipment identifies them as a well paid employee of an international organisation and that they therefore become more vulnerable to criminal activity such as robberies. In some locations, such as Darfur, there are genuine practical hurdles to be overcome. Fluctuations in the community's supply of electricity and the sparsity of some staff members' living accommodation do make it more difficult to keep radios charged.

Confidence in the emergency communications system

Anecdotal evidence also indicates that staff members' use of emergency communications is directly affected by the perceived efficiency of the security staff managing and responding to the communications system. As an example, in Central African Republic, staff members working for a United Nations Agency who were satisfied by the emergency security support received when they had requested it were more prone to using the radios on a regular basis. During a security workshop held for some staff members, it was observed that those staff members who believed that their requests for support had not been appropriately answered on previous occasions were more prone to disregarding the emergency communications equipment and procedures (see Porcaro and Walker, pp. 33-34).

The confidence of staff members will affect their use of any security related communications equipment. Nonetheless, if the equipment or system is not used by them for anything other than security purposes it is more likely to be under-utilised. A staff member will rarely forget their mobile phone as these have become indispensable tools of daily life but the VHF handset may be relegated to an office drawer if it is not considered to have tangible benefits.

Emergency communications in areas prone to low frequency/high impact risks such as earthquake

Chile is a classic example of a location in this category. The security risk landscape of Chile (2011/2012) was comparatively tranquil and marred only by social unrest in the form of demonstrations and property invasions and the ever present risk of earthquake. In 2010 Chile suffered a level 8.8 earthquake but was able to respond very efficiently (compared to Haiti's level 7.0 in 2010 for example) due largely to the experience and organisation of national bodies as well as the relatively higher constructions standards in the country.

Nonetheless, this scenario presents a challenge for security risk management. The 2010 earthquake in Chile did impact the mobile telephone network coverage and reportedly accounting for staff of international organisations took some days despite all best efforts. Clearly, the ideal situation for any organisation is that all staff may be accounted for within hours. Is it, however, sustainable to establish a radio network and issue equipment to all staff in order to be prepared for a low frequency natural hazard? Aside from the financial implications, the challenge of

training staff and ensuring that they are always prepared is considerable as such an environment lacks the regular stimulus (such as kidnappings in Yemen or complex attacks in Iraq) that keep staff dedicated to following procedures and using equipment.

SMS technology

SMS technology as an alternative, or complement to traditional emergency communications systems

In 2013, as reported by UN News Centre, the UN Deputy Secretary General drew attention to global sanitation issues by stating that more people have access to a mobile phone than a toilet.[110] Mobile phones have become cheaper and cheaper as companies seek to expand their networks globally. Even in underdeveloped rural areas imaginative solutions have been sought to support the use of mobile phone technology. SMS (Short Message Service) technologies were first used in the early nineties. Since then they have become second nature to phone owners. They permit the transmission of short messages to multiple recipients on even the most basic model of cellphone. SMS is a two-way system permitting exchange between parties.

In the wake of man-made disasters such as the London bombings the UK Government produced a paper on technical solutions available to ensure resilient communications.[111] The analysis of SMS stated:

> Short Message Service, or SMS, is a 'store and forward system' (…) The implications of this are that if the recipient terminal is unavailable the message is stored by the system for later resend. While most messages are received immediately timing can be unreliable. SMS uses a signalling channel as distinct to dedicated channels, text messages can be sent independently of other services over the network. The signalling channel is less susceptible to congestion.[112]

In summary, the use of SMS is subject to fluctuations in mobile network operability but is more likely to succeed than voice communications during times of high network usage. The United States Federal Communication Commission and Federal Emergency Management Agency recommend the use of data based communication such as SMS.[113] This analysis is supported by experiences of the author in the field. In the wake of earthquakes in Chile or social unrest in Thailand, SMS messages were more likely to reach the recipient than a voice call, although they were also subject to delay.

'Bulk SMS Delivery Systems' have been developed, primarily with sales and marketing activities in mind, and become progressively more sophisticated. These systems allow the distribution of multiple messages to recipients via the internet regardless of the geographical location of the individual. Two way messaging is possible and some of the service providers have developed additional packages that include software for managing address books, contact lists, historical records, etc. The requirement for internet does add a vulnerability to bulk SMS delivery systems but it should be remembered that they may also be accessed and managed remotely. If deprived of the internet locally, a security professional might, for example, request colleagues at alternate locations to send a message on their behalf.

Uses of SMS as measure to mitigate risk

No single technology provides a robust mitigating measure unless it is combined with a clearly structured and appropriately implemented procedure (see Sambuli and Awori, pp. 27-31; see also de Palacios, pp. 51-55). The most obvious example of this is the standard 'radio check'. Distributing radios to staff is of little use if they do not know how to use them or if we do not monitor the functionality of the system. The 'radio check' procedure is therefore one critical element of an emergency communications system. The same concept applies to alternative systems such as those using SMS technology.

Haphazard distribution of SMS is not a solution. Clear guidelines and parameters must be provided to staff if this technology is to be useful (see Byrne, b. pp. 57-58) and, in addition, back-up systems and procedures must be clearly defined and practised. A very basic and crude illustrative example of a back-up system might be the distribution of whistles to staff in earthquake prone areas. As a last resort they at least have something more than their own voice to be able to summon help *in extremis*.

110 UN News Centre. (2013). Deputy UN chief calls for urgent action to tackle global sanitation crisis. 21 March. Available from: http://www.un.org/apps/news/story.asp?NewsID=44452&Cr=sanitation&Cr1=#.VAVs1bxdXXH. [Accessed: 2 Sept. 2014].
111 Cabinet Office Civil Contingencies Secretariat. (Undated). *Ensuring resilient telecommunications: a survey of some technical solutions.* Available from: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/85842/resilient-telecomms-survey.pdf. [Accessed 2 Sept. 2014].
112 The congestion of cellular networks in the wake of incidents or disasters is a well-documented phenomenon. Serious incidents may prompt a surge in usage as telephone users seek to contact their loved ones. In extreme cases (such as 9/11 or the Boston Bombing) this can 'knock out' the voice communications capacity of a network. One example of this is explored in the following article: Albanesius, C. (2013). FCC Probes Post-Bombing Cell Phone Congestion in Boston. *PC Magazine UK.* Available from: http://www.pcmag.com/article2/0,2817,2417891,00.asp. [Accessed 2 Sept. 2014].
113 Fugate, C. and Genachowski, J. (2011). How to Communicate Before, During and After a Major Disaster. *Federal Communications Commission.* Available from: http://www.fcc.gov/blog/fcc-and-fema-how-communicate-during-and-after-major-disaster. [Accessed 2 Sept. 2014].

The following are commonly found examples of the way in which SMS technology is integrated into security systems:

- **Standard, two-way exchange of security information:** SMS permits a discreet and rapid way for information to be exchanged between staff member and security focal point.
- **Security broadcasts:** brief security messages may be rapidly sent to all staff if a bulk SMS distribution system is available, i.e. 'As at 1100 hrs avoid crossroads before airport till further notice. Violent demonstration.'
- **Warden systems:** the standard 'call out tree' can be implemented using any communications technology and SMS is no exception. Security managers or focal points may SMS all wardens who in turn will SMS the staff under their responsibility. Depending on numbers this system can be managed using just cellphones (no bulk distribution system needed) and allows for responses to be fed back up from staff, through wardens to security professional.
- **Alerts:** this article will not explore the many other security related alerts that may be channeled through SMS as well as other media as they are more specialised. Examples of these may be GPS tracking on vehicles or remote monitoring of water quality or seismic conditions.

Staff members do not generally require much training on the use of mobile phones and SMS. Most staff will have their own personal mobile phone even if they have not been provided with a corporate mobile phone, radio, satellite phone or other communications device. SMS uses little battery life and short cuts can be created depending on the phone.

As referred to above, while more resilient than voice communications, the use of SMS technology still depends upon the integrity of the cellular telephone network. The use and specific vulnerabilities of the mobile phone network are fully described in HPN's Good Practice Review (GPR8).[114] With regards to SMS usage, the review highlights a simple procedure that helps to minimise concerns that SMS communications are not received in a timely manner due to network limitations: staff members are requested to SMS acknowledgement of receipt of the communication. GPR8 also reminds us that SMS communications are not secure and should not be used for the passage of sensitive information, a limitation that applies equally to most VHF networks.

Example of effective use of bulk SMS distribution systems

The United Nations in Thailand (2010-2011) made use of a commercially available bulk SMS distribution system. This particular version benefitted from a contact management system that could be updated online by staff members (their own data) or administrators (data pertaining to staff under their responsibility). It therefore provided, *de facto*, a back-up record of staff contact details for security use as the information was hosted on the internet rather than on a few individuals' computers. The level of information security remains to be fully assessed although this particular system required authorisations from the administrator and the use of log-ins and passwords. In addition, the system catered for multiple administrators: overall management by UN Department of Safety and Security (UNDSS), and management of individual agencies' data by their own agency security focal points.

This proved particularly useful during times of tension in Bangkok as the 'hot-spots' in the city were localised; barricades or demonstrations affecting one agency may not necessarily have had any impact on other agencies on the other side of the city. Agency security focal points were able to use the system to send tailored messaged to their staff in addition to the UN-wide messages. As long as internet access is available, this system greatly facilitated the bulk transmission of messages to staff members and their dependents. In parallel to this bulk SMS distribution system, some agencies used SMS in the standard way to activate emergency call-out trees (warden systems) and exchange security related data.

114 Van Brabant, K. *et al.* (2010). *Good Practice Review: Operational security management in violent environments. Number 8 (New edition).* Humanitarian Practice Network. Dec. Available from: http://www.odihpn.org/download/gpr_8_revised2pdf. [Accessed 2 Sept. 2014].

Conclusion

In summary, SMS technology as a tool for enhancing the security of staff may be explored more fully and in greater depth, particularly in relation to the use of bulk SMS distribution software. Its primary disadvantage, dependency on mobile phone network, is clear, but the advantages are multiple: transmission of SMS is cheap, there is little need to buy additional equipment, minimal training is required and existing protocols and procedures can be used or adapted. There is a risk that staff members become over-reliant on the SMS system but security training should emphasise the back-up systems in place. In particular, the use of SMS-based systems will provide additional support to locally recruited staff members who may not be fully covered by other mechanisms.

SMS technology is already widely used, whether officially or unofficially, but it is posited that a great deal more benefit could be extracted from this technology if its implementation as a security measure is reviewed in a more systematic way. As mentioned above, SMS systems are at present inherently vulnerable and therefore will not mitigate risks to the same degree as emergency communications systems based on radio or satellite technology. Over-dependence on SMS and cell phones generally is a concern and conscious efforts must be made to ensure back-up and/or parallel systems are in place. In some locations, where the security situation may be politically or culturally sensitive, it should not be forgotten that SMS and cellular phones are not secure from eavesdropping.

Applicability of Open Source Systems (Ushahidi) for Security Management, Incident and Crisis Mapping

Acción contra el Hambre (ACF-Spain) Case Study

Gonzalo de Palacios

Introduction

Acción contra el Hambre (Action Contre la Faim, ACF-Spain) is a Spanish humanitarian organisation and part of the ACF-International Network. Since its creation in 1995, ACF-Spain has been working in different countries and contexts, where security management is implemented and adapted through GPR8 'Operational Security Management in Violent Environments' (Van Brabant, 2010). For ACF-Spain, incident reporting serves two main purposes: supporting victims of incidents and being able to take the necessary steps in order to prevent the occurrence of new incidents.

In 2008 ACF-Spain started registering incidents from all its countries of operations (15 to 20 countries) in a systematised way using an Excel workbook. Incidents were reported from field sites to the Country Coordination Office and from there to Headquarters in Madrid. Although this was a positive initiative, as it began to provide evidence for identifying trends, victim profiles or most vulnerable locations, it had some limitations in relation to the access of information from countries of operation and the efficiency of the reporting process itself. In order to be able to analyse the information, the data contained in the incident report in Word format had to be transferred manually to the Excel workbook, taking a considerable amount of time. One of the gaps in the registering system ACF-Spain identified at that time was being able to pinpoint on a map where incidents were happening, something that Excel cannot offer. Despite this we managed to generate from our Excel database map layers in KML (Keyhole Markup Language), which allowed us the possibility of viewing through Google Earth where incidents were happening. The process was still very inefficient, with numerous mistakes, and the resulting KML was too heavy. After doing research, we identified various possibilities for incident reporting and mapping, such as open GIS software, Open Data Kit from Google, SharePoint from Microsoft, internal Project Management software and Ushahidi.

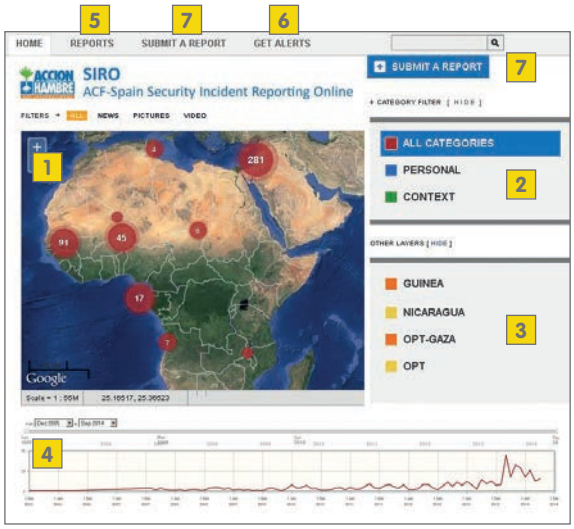
These systems were compared and evaluated. It was determined that an incident reporting system should improve reactivity to support incident victims (see Porcaro and Walker, pp. 33-36); be able to map not only where incidents occurred (see Sambuli and Awori, pp. 27-31); but also statistics from the database, security perimeters and levels, and evacuation routes and maintain a database of security-related information to help ACF-Spain improve its incident reporting system, refine the analysis of trends through the consolidation of information, and ease decision making for security management. In summary, an incident reporting and mapping system should allow registration, consolidation and graphical representation of security incident information. From a technical point of view, other factors were considered, such as cost, licence, bandwidth, access and permissions, authentication, mobile device support, compatibility with other systems, flexibility and adaptability of the tool, the possibility of mapping polygons, routes and areas, the possibility of getting reports and alerts, and the possibility of importing/exporting information from/to other software.

An illustration of the system would be:

The result of the analysis and comparison identified Ushahidi as the system that best suited our needs.

Applicability of Ushahidi in security risk management

Ushahidi,[115] 'testimony' in Swahili, is a web-based platform initially developed in collaboration with Kenyan citizen journalists to map violence in Kenya after the post-election fallout in 2008. We selected Ushahidi because it fulfilled the technical and functional criteria aforementioned. In particular, Ushahidi is an open source platform, so there is no cost related to the procurement of a licence; information is protected with authentication access; is easy to customise without a system administrator; documents, images, photographs and videos can be uploaded; locations where incidents have taken place are easy to identify and placemarks can be added; it can be used on mobile devices (both for sending reports and recording them in the database); it allows encrypted access to the incident register panel and the export/import of information to/from other software; and it offers the possibility to generate graphs from the information contained in the database (only by category in a certain period of time).



A quick look at Ushahidi for NGOs

The main page offers a quick view on a map [1] of the reported incidents. The map represents the total number of incidents or the incidents in a given period (the timeline can be adjusted). These incidents are represented on the map according to categories [2] defined by the system administrator and displayed in different colours or icons. Layers representing areas, locations, meeting points, routes, etc. can appear on the map if uploaded [3]. The layers have to be created first in KML format and can be easily uploaded to the platform. Each layer can be given a colour to represent levels of risk or other categorisation used by the organisation.

There is also a graph [4] that shows the evolution in the reporting of incidents over time. All the reports that have been introduced into the system can be seen [5], and there is also the possibility of viewing reports in a given time range, according to category, country or any other customisable field. It is possible to activate alerts [6] and be informed via e-mail of incidents reported in a particular location. This can also be customised by incident-type.

Section 3

115 The original Ushahidi website was used to map incidents of violence and peace efforts throughout Kenya based on reports submitted via the web and mobile phones. Ushahidi has grown into a global non-profit technology company that aims to change the way information flows in the world and empower people to make an impact with open source technologies, cross-sector partnerships, and ground-breaking ventures. For further information see http://www.ushahidi.com/ [Accessed 1 September 2014].

The online template for reporting incidents [7] is also displayed on the main page. It has some compulsory fields and the exact location of each incident can be pinpointed on a map. The categories for the template are the same ones that are shown on the map [2]. The rest of the template can be customised according to the information that an organisation wants to collect.

The system can be public or password protected. It also has the possibility of administration settings for customising fields and options. The level of access for different users can be set up depending on the criteria determined by the platform administrator.

Reporting a security incident

The ACF-Spain incident report template in Word format was replicated in the Ushahidi incident report web site. This allowed for reports to be made in a more efficient way, as well as offering a single data entry that is transferred directly into a database for extraction and analysis. Who reports an incident is something that can be decided by the organisation, and can depend on internet access, the need for review before information is made public, etc. Once an incident is reported, it will automatically appear in the restricted area (depending on the user privileges and profile) which allows an authorised user or administrator to review the information reported before it is made public – a function available within the organisation and for registered users with a password. The information can be modified by an authorised user in order to ensure the report meets the standards set by the organisation. The incident reporting template has the capacity for private fields, for certain user profiles, as well as public fields. In this way, additional information can be added to the reports by the person reviewing and validating them. An example could be incident severity, which it may be important to harmonise across an organisation and not leave up to the criteria of the person reporting: the theft of a car can be rated as having a high impact in a country with low criminality rates and as low impact in a country with high criminality rates, depending on who reports the incident, but from an organisational security management point of view the impact may need to be rated equally.

The system can be set up so that once an incident is reported, an email is sent to the person in charge of reviewing the incidents, or the report can be automatically validated. Triggers for these different actions can be customised in terms of who submits the report, the location, keywords used, category of incident or when the incident was reported. As mentioned before, each report has to be verified and approved by an authorised user or administrator before the report appears in the public part of the platform. For ACF-Spain it is important to have this option in order to comply with the EU Data Protection Directive (95/46/CE), and to prevent misuse of the platform or the possibility that it might become a way of denigrating staff. If an incident report includes information considered as confidential or affecting the private sphere and image of a person, it can be corrected and the name replaced by a generic denomination.

Because of the sensitivity of the information contained in the Ushahidi platform database installed on the ACF-Spain servers, we decided to password-protect it and maintain it under an https protocol. The platform allows anyone with access to the site to report incidents. However, we decided, from the point of view of internal process, that only Country Directors, Logistics Coordinators or Security Managers could upload/report incidents through the system. The basis for this decision was that the organisation considered it important that security managers at country level were aware of incidents happening in the countries where they were working, and that they should not find out about incidents after Headquarters in Madrid did. Subsequent access to information once the report has been validated is open to the entire organisation.

ACF-Spain has internally classified security incidents into three categories: incidents resulting in direct harm to ACF-Spain (to be reported in all circumstances); incidents with no harm to ACF-Spain but with consequences for its security or operational management (near misses, recommended to report them); and incidents with no harm nor other consequences (interesting to report them). All these types of incidents can be reported through the platform. This is helping us identify trends, training needs, new risks, etc., but can also be used to evaluate the level of risk of new intervention areas or likelihood of incidents through the evidence collected. Real-time information extraction can establish how many incidents have been reported, their type, severity, the number of staff affected and their gender and profiles. This information allows security managers and country directors to compare security incidents between countries of operations.

For instance, traditionally in ACF-Spain most reported incidents have been traffic and criminality related. For the first time in 2014 this pattern has changed due to the work done in different emergencies (Philippines, Middle East) and we have witnessed an increase in threats and harassment towards ACF-Spain staff. The identification of this new trend has allowed us to raise awareness of this fact and to prepare the necessary training and briefing for our staff. Similarly, we noticed an increasing number of traffic related incidents with motorbikes in the Sahel. The identification of this trend allowed us to take different decisions (training of users, hiring of drivers, reinforcing staff awareness) in order to minimise vulnerability to this risk.

Since the introduction of the incident reporting system through the Ushahidi platform, we witnessed a steep increase of incidents being reported (from an average of around 34 incidents per year to around 80). Our initial analysis was that not so many more incidents were happening, but that facilitating the reporting meant more incidents are being reported as consequence. Part of the information provided through Ushahidi is done through drop down menus, check boxes or option buttons, making the reporting simpler and faster. In other words, the complexity of the process can no longer be used as an excuse for not reporting incidents.

This analysis is being confirmed in 2014, where the number of incidents being reported at the time of writing (August 2014) is matching the figures for 2013, the year when the system started being used. However, facilitating reporting through the Ushahidi system was not the only stimulus for more incident reporting, since its use coincided with the creation of a full-time dedicated security manager at ACF-Spain. These figures will have to be confirmed in the coming years through more statistical evidence.

Nevertheless, we are still encountering delays in the reporting of incidents or resistance to the use of the reporting system. The delays in the reporting process are the same ones that were faced prior to installation of the Ushahidi system, most of them not related to the tool itself but to the internal understanding of what ACF-Spain considers incidents, what should be reported, etc. Access to the internet is becoming less of a problem, particularly in country capitals where the reporting is done according to the internal process explained above. Some of the delays in the reporting process may also come from lack of knowledge about the existence of the tool and insufficient appropriation of the tool by persons in charge of reporting (see Porcaro and Walker, pp. 33-34). Access to the platform has been facilitated by providing the URL in different locations of the organisation's intranet. Resistance to its use is not due to the tool itself, but to other factors (change management).

Ushahidi's interaction with other software: representing information

In ACF-Spain the previous reporting system of transferring information from a Word template to an offline Excel database, had been internally questioned because of the inefficiency of the process and the need to be more transparent and be able to share internally what was happening to our teams. Equally, an organisation needs to know how incidents are being managed in order to share lessons learned and practices.

Although as stated above it is possible to access reports according to type of report or location, the graphic and/or statistical representation of incidents has to be complemented with other software. At ACF-Spain we have used Excel 2010 to process the information from an XML file downloaded from

116

116 Information shown here does not necessarily reflect real information about incidents occurring to ACF-Spain.

Ushahidi (although CSV format downloading is also possible). Downloaded information can be drawn from approved reports, verified reports or reports awaiting verification or approval. A time range can also be set up. The information can be represented and managed in many different ways, and we are using it through a 'dashboard' file.

This dashboard is uploaded onto ACF-Spain's intranet so it can be used and consulted by organisation members when preparing briefings, risk analysis, reports, etc. The dashboard can show contextual incidents, direct incidents or both, but could be modified to show other information collected through Ushahidi's online template. At ACF-Spain it shows incidents per month, per year, accumulated at a global organisational level or per country. The file also shows the regularity of security protocol or the security level updates in all the locations where ACF-Spain works (although this information is not collected through Ushahidi).

Conclusions

Since ACF-Spain adopted Ushahidi as platform for incident reporting, we have seen an increase in the number of incidents reported as well as a decrease in the time between the occurrence of an incident and the moment it is reported. This has allowed us to support the victims of incidents better and to react in a timely manner to challenges encountered. There have been cases of incidents being reported through Ushahidi within hours of their occurrence. However, ACF-Spain recommends field teams to use the quickest way possible (telephone in most cases) if a severe incident occurs, in order to be able to provide support to the victims as fast as possible, and later on to provide more detailed information through the online reporting template. In a number of cases, having incidents being reported within hours of their occurrence has allowed us to provide prompt psychological assistance to staff members affected by incidents, as well as the activation of other contingency protocols.

The alert system that the administrator can activate to get a notification when a report has been submitted for validation (which can also be set up so all users receive an alert when a report has been validated) has improved the speed with which information is shared among all staff, from senior management to field teams through HQ support personnel. As a platform it has shown great stability and reliability, and we are currently using only a limited part of its functions and potential, bearing in mind that the platform is being constantly developed through the open source model. The Ushahidi platform can be downloaded directly from its web page. While the creation of templates and statistics does not require advanced computer skills, it does needs the engagement of IT staff for its installation on a server so that it can be used online.

There has been a great improvement in having real time information and in the efficiency of the reporting process. Ushahidi has enough flexibility to accommodate the incident reporting criteria of different organisations as well as the potential to be used for other purposes.[117] Through the use of the system it has been possible to identify potentially dangerous locations, conduct more accurate risk analysis and introduce more appropriate risk mitigation measures, all in a timely manner. However, Ushahidi is only a tool, and should be accompanied by training, awareness, promotion and communication of its added value. As such, ACF-Spain has been conducting briefings, trainings, field visits, communications and reports at internal level to promote the use of Ushahidi for reporting incidents and sharing information.

117 See, for example, http://harassmap.org/en/what-we-do/the-map. [Accessed 1 September 2014].

Measures for Mitigating Cyber-Security Risks

Rory Byrne

As this publication has explored, the current cyber-security environment – where even massively resourced and staffed organisations continue to be the subject of significant cyber-security breaches – poses an uphill challenge to NGOs with limited time, knowledge and resources. There is no one-size-fits-all strategy for hardening an organisation against hostile digital intelligence gathering, particularly since increased security often means decreased convenience. However, establishing a strong baseline and understanding when and how to introduce increased security measures has generally proven to be most effective. Humanitarian agencies also have the advantage of being able to learn mitigation lessons from the human rights world.

The tools and methodologies for information gathering by governments and hostile actors are openly acknowledged and increasingly directed against NGOs. As the experiences covered in this paper indicate, humanitarian organisations are not immune (see Gilman, pp. 8-11; see also Byrne, a. pp. 12-16). However, lessons can and should be drawn from other sectors who have already begun to address the issues of hardening their people and systems against the deleterious effects of unrestrained intelligence gathering. While the detailed discussion of such measures is beyond the scope of this paper, there are some basic strategic actions open to NGOs to help understand, identify and manage the risks.

Understand, model and constantly analyse

Humanitarian organisations are increasingly sophisticated in their analysis of physical security, and are gradually improving coordination efforts and information sharing through structures such as EISF and INSO. However, aid agencies should not forget that they must also understand and apply the same logic to digital threats (see Gilman, pp. 8-11).

Understanding the true nature of digital risks is vital to long-term viability. Organisations should map, audit and constantly update critical information they are mandated to preserve and protect. NGOs also need to understand the lengths and measures hostile actors operating in countries in which they have a presence are prepared to take in order to get access to sensitive information and core competencies (see Gilman, pp. 8-11; see also Byrne, a. pp. 12-16).

Similarly, an internal review should also focus on information that leaves an organisation exposed, such as external emails, financial transactions or travel reservations – such information can be an invaluable source of insight into the comings and goings of an organisation and its people. Because outsiders must be relied upon to ensure the security of the entire organisation, this type of vulnerability represents another layer of risk that has to be accounted for.

Decisions should be driven by realistic risk modelling. For example, following the Snowden revelations, media scrutiny has focused our attention on the highest levels of intelligence gathering, while ignoring or glossing over some of the most common causes of data breaches – for instance, weak passwords, loss of laptops and social engineering. Similarly, many myths exist which hinder protection measures, such as those pertaining to the security of Skype, Blackberry and satellite phones – which depending on your threat model and potential adversary might be considered either highly insecure (versus a government level threat) or highly secure (versus a disorganised local militia).

Information security structures

Digital security is part of, but not the same as, information security. Information security is the wider context of how, why and when information is collected, shared and stored – both digitally and physically. The most sensitive information identified in a previous section should be tightly compartmentalised on a 'need to know basis', with the minimal access that is needed for the purposes of completing work.

Governments and other actors have exploited weaknesses in intelligence handling in a number of ways (see Byrne, a. pp. 12-16). For example, physical access to offices makes placing trojans much easier than remotely hacking into a machine, and failure to securely store or shred sensitive physical data and electronic media often bypasses any checks and balances put in place by the use of sophisticated encryption.

In comparison to human rights groups, humanitarian aid agencies generally have much better physical security management training, implementation and accountability structures. However, these need to be extended to deal with digital security (see Gilman, pp. 8-11). Information security breaches can create long-term damage to an organisation and its staff, and should be treated with the same due diligence as physical security breaches – with appropriate sanctions in place to ensure compliance as necessary. IT departments also need to be properly resourced with the capabilities and capacities to deal with the current threat environment. When outside contractors or suppliers are used for IT systems, they should be thoroughly vetted. Ideally 'red-teaming' or penetration testing of such systems should be conducted in order to identify potential weaknesses.

Select the right tools

Ensuring correct tool selection continues to be one of the most important parts of the success or failure in mitigating the impact of hostile digital intelligence gathering by governments and other actors. Investment in tools that reduce the ability of users to make mistakes (for example, encrypting all hardware automatically before distribution to staff) has proven to be one of the most effective measures for mitigating risk. Understanding the trade-offs between security, usability, functionality and cost are vital. This is particularly important, as many human rights and humanitarian agencies without the requisite skills or expertise in this area have often turned to expensive and off-the-shelf commercial solutions, which often do not meet the actual needs of the organisation (see Gilman, pp. 8-11; see also Byrne, a. pp. 12-16).[118]

Similarly the choice of certain communications technology can also make an organisation a target. VPN connections, for example, are heavily restricted in certain countries and monitored. The Great Firewall of China has been documented to show signs of machine learning to pick up and block foreign VPN traffic and pinpoint where it is coming from.[119] The Tor network,[120] which anonymises and encrypts its traffic to protect user privacy, faces similar challenges. Russia recently came out as publicly targeting the service, offering a $110,000 bounty to crack the network, and recent leaks from other governments show similar efforts. Organisations should bear in mind where they are operating when making a technology choice, as choosing particular systems can make them the target of digital attacks or intrusions into their systems (see Gilman, pp. 8-11; see also Byrne, a. pp. 12-16).

However, this process has become easier in the past few years with the emergence of the Liberation Technology (LibTech) movement.[121] Comprised of a number of technologists, NGOs and donors, it has contributed a significant number of free and open source tools and methods designed specifically with the humanitarian or human rights worker in mind. Organically developed training and management frameworks, based on years of experience in the field, are now available from a number of LibTech organisations.[122] New innovations have allowed humanitarian agencies to bypass some of the growing pains associated with other, less vulnerable, sectors.

Training

Training remains one of the best methods for mitigating the ability of hostile governments and other actors to abuse digital intelligence. A strong foundation must exist within an organisation as the weakest link can often compromise an organisation's entire network. Particularly in places with lower levels of digital literacy, experience shows that training tends to be hit-and-miss, not fit for the purpose, outdated, at too high/low level for the job description, or it does not represent a good fit for the current range of information systems and processes already in place.

118 A good example is the choice of using encryption. Although it is tempting to use it as a blanket across an organisation, if the intention is to use it in places that require licences, like China, Burma, Iran, or Israel, bringing encrypted devices across borders could draw unwanted attention and potentially cause legal issues. Also, even if a licence is not required, the use of encryption can affect relationships with governments, who may see that organisations that claim to be in the country to help, have something to hide. For further information see: Koops, B.-J. (2013). Crypto Law Survey. Available from: http://www.cryptolaw.org. [Accessed 2 Sept. 2014]. JISC Legal Information. (2013). What's the legal position of transporting encrypted equipment abroad? 13 May. Available from: http://www.jisclegal.ac.uk/ManageContent/ViewDetail/ID/2947/Whats-the-legal-position-of-transporting-encrypted-equipment-abroad-13-May-2013.aspx. [Accessed 2 Sept. 2014].

119 Arthur, C. (2012). China tightens 'Great Firewall' internet control with new technology. *The Guardian*. 14 Dec. Available from: http://www.theguardian.com/technology/2012/dec/14/china-tightens-great-firewall-internet-control. [Accessed 2 Sept. 2014].

120 See https://www.torproject.org. [Accessed 2 Sept. 2014].

121 For more information, see Stanford University Center on Democracy, Development, and the Rule of Law. Program on Liberation Technology. http://cddrl.fsi.stanford.edu/libtech. [Accessed 2 Sept. 2014].

122 For example, Tactical Technology Collective and Front Line Defenders. Security in a Box. https://securityinabox.org. [Accessed 2 Sept. 2014].

For example, participants at HQ might be trained in how to use encrypted email software, while their field offices are not; the implication is that security is weakened and hostile elements, if given the chance, will exploit obvious weak spots.

Implementation continues to be a recurring problem for mitigation strategies. With digital training and tools the pace of change is extremely rapid, and the rate at which skills fade, become obsolete, or are forgotten is extremely high. Following up with additional training, online learning, auditing and other methods of reinforcement is necessary to guarantee that proper protocols are being adhered to (see Kaiser and Fielding, pp. 37-41). New employees should be given information security training as part of any induction process. When this is not possible, information access should be limited to only those functions that are necessary to conduct their job.

While training staff in specifics of security is a vital part of the process of mitigating cyber-security risks, it important to involve staff in the non-technical aspects of security – for example not opening email from unknown senders, not responding to phishing emails, not answering social engineering enquiries, not sharing company information with others, or taking care talking about company business outside the company – to explain how protecting an organisation's information and assets is not solely the job of the security professional. Raising awareness in all aspects will be an important part of protecting the organisation.

Prepare for failure

With so much information stored digitally, from mobile phones to servers housed at HQ, it is inevitable that failures will occur. As with any security mitigation effort, preparing for failure is the *sine qua non* of best practices.

Building in resilience, with regular secure offsite backups, is crucial for minimising any damage caused by accident or disruption operations launched by hostile governments and actors – such as the seizure, theft or destruction of computer equipment. In some environments, the additional benefit of doing this outside the country of operation (in countries such as the Netherlands, Finland and Iceland with strong NGO protection laws) is strongly recommended.[123]

Last, but not least, digital security breaches and adverse reputational issues should be integrated into business continuity planning and crisis management practices and procedures. For example, simulations should occur of dealing with potential risks such as a finding a hostile network penetration, critical system failure or dealing with a large leak of sensitive data.

123 When selecting information security tools, another thing that should be noted is local regulation and compliance in regard to information security. Data protection laws are the obvious example. European data protection regulations restrict the transfer of any personal data outside the EU and failure to take that into account can lead to significant fines. Organisations should think about what data they are holding and the implications when moving it between countries. Organisations using cloud services should also carry out a strong audit of where that data is hosted.

Editorial Team and Contributors

Editors

Raquel Vazquez Llorente
Researcher, European Interagency Security Forum (EISF)

Raquel Vazquez is responsible for conducting and coordinating research that helps share and promote best practice amongst the humanitarian sector, with the aim of building the capacity for security risk management. Prior to joining EISF, Raquel worked in Libya, Israel, Bangladesh and the UK for different humanitarian and human rights organisations. She also led field research for a National Geographic project on religious persecution during Pol Pot's regime, and assisted in war crimes investigations during the UN-backed Khmer Rouge Trials in Cambodia and in the Office of the Prosecutor of the International Criminal Court.

Imogen Wall

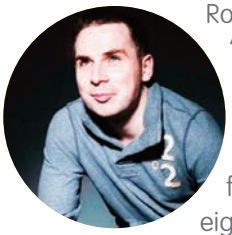
Imogen Wall is a freelance communications consultant who focuses on policy, advocacy and use of communications technology in disaster response. A former BBC journalist, she specialises in the theory and practice of communication as a form of assistance and has designed and implemented projects to this end in a number of emergencies including the Indian Ocean tsunami (Aceh, Indonesia), Haiti, Sudan, East Timor and most recently in the Philippines following Typhoon Bopha. She is the author of a number of policy papers, and has worked for a number of organisations including UNOCHA, UNDP, Save the Children, BBC Media Action, and the World Bank.

Contributors

Daniel Gilman
Humanitarian Affairs Officer, Policy Analysis and Innovation Section, UN OCHA

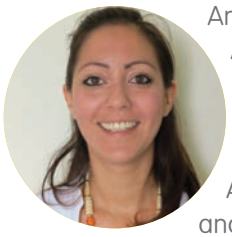
Daniel Gilman works on promoting the development of humanitarian innovations in the wider humanitarian system and within OCHA, as well as other emerging policy issues. He was on the team that produced the OCHA policy report 'Humanitarianism in the Network Age', and is now looking at a range of issues including information security and privacy in humanitarian emergencies, the use of UAVs in humanitarian emergencies, and approaches to financing humanitarian research and development.

Rory Byrne
Founder and CEO of Security First



Rory Byrne is currently building 'Umbrella', the first open source and free mobile tool to manage the physical and digital security of aid workers, journalists and activists in the field. His experience draws on over eight years in the human rights world, and also on his work in the military and as a Certified Ethical Hacker. Previously he helped establish and was Head of Security and Research for the human rights organisation Videre – the world leader in the gathering, verification and distribution of covert camera footage. He has trained hundreds of human rights defenders in areas such as encryption, physical counter-surveillance, covert filming, risk management and secure communications.

Anahi Ayala
Senior Innovation Advisor, Center for Innovation and Learning, Internews



Anahi Ayala is the Senior Innovation Advisor for the Internews Center for Innovation and Learning. For three years prior to this position, she was the Internews Media Innovation Advisor for the Africa Region and Health and Humanitarian Media. As well as in Africa, she has experience working in countries in Asia, Eurasia, Latin America and the Middle East.

Kagonya Awori
Adviser for Umati Project, iHub

Kagonya Awori was the Technical and Research Lead for the first phase of the Umati project. She has also been involved in extending the Umati framework to partners in Myanmar. Her background is in Computer Science and Human-Computer Interaction, and she is currently pursuing a PhD in Computer Engineering at the University of Melbourne, Australia.

Bobby Anderson
World Bank

Bobby Anderson worked in Aceh for three and a half years, most recently as the Post-Conflict Reintegration Programme Co-ordinator for the International Organisation for Migration, where he managed the largest ex-combatant reintegration and stabilisation projects in Aceh. He has also worked in Afghanistan and the former Yugoslavia. Bobby currently works on governance projects in Eastern Indonesia.

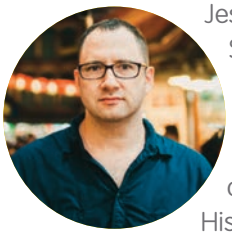
Laura Walker Hudson
CEO, SIMLab

Laura Walker Hudson supports organisations around the world in using mobile technology for social change, drawing on her expertise in humanitarian aid, human rights law and international development. Before coming to SIMLab, Laura worked on international humanitarian policy and quality for the British Red Cross.

Nanjira Sambuli
Research Manager, iHub

Nanjira Sambuli leads the Governance and Technology research pillar of iHub, where she has developed a framework for assessing the viability, verification, and validity of crowdsourcing and also Umati. She is trained as a mathematician with experience as a new media strategist for UN organisations, Africans Act 4 Africa, and Global Power Shift among others. She is also the editor of 'Innovative Africa: The new face of Africa', a series of essays on the emerging African tech landscape.

Jesse Hession Grayman
Assistant Professor in the Division of Sociology, Nanyang Technological University's School of Humanities and Social Sciences, Singapore

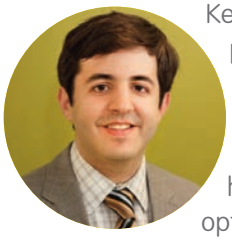


Jesse H. Grayman holds a PhD in Social and Medical Anthropology from Harvard University, and two master's degrees from the University of Michigan: an MPH in Epidemiology and an MA in Southeast Asian Studies. His dissertation, entitled 'Humanitarian Encounters in Post-Conflict Aceh, Indonesia', is an ethnography based on five years of fieldwork that highlights the experiences of Indonesian staff working for international humanitarian agencies in Aceh's post-conflict recovery sector.

Esther N. Kamau
Senior Programme Officer for Humanitarian and Emergency Affairs, World Vision East Africa

Esther N. Kamau has 9 years of experience in development and humanitarian assistance, and has worked as a Development Facilitator and a Program Manager for integrated development programs in Kenya. She holds a Bachelor of Commerce degree in Business Administration and Management from Daystar University, Kenya, an honours degree in Development Studies from University of South Africa (2010) and an MA in Sustainable International Development from Brandeis University (2011).

Keith Porcaro
Legal Project Director, SIMLab



Keith Porcaro works with legal aid providers and governments to integrate mobile technology into legal processes. A lawyer and developer, Keith's background is in helping organisations and individuals optimise around shifting systems. He holds a JD from Duke University and a BSFS from Georgetown University.

Joel Kaiser
Emergency Response Officer, Medair

Joel Kaiser is a PMI® certified project manager and humanitarian emergency specialist with advanced studies in early recovery and complex emergencies, combined with eight years of field experience around the world.

Maereg Tafere
Associate Director East Africa Region, World Vision International

Maereg Tafere has over 28 years of experience in humanitarian and development work. His work experience ranges from managing rural development programs in Ethiopia to country director roles in Burundi (2001-2007) and Sudan (2007-2012). He holds a BSc from Addis Ababa University, an MSc from the Indian Institute of Technology (IIT) and a PhD in environmental management.

Stuart Katkiwirize
Regional Director for Humanitarian and Emergency Affairs, World Vision East Africa

Stuart Katkiwirize has been at the forefront of mainstreaming gender, protection and disaster risk reduction into different disaster management dimensions since 1993. He has experience leading consortia, working across agencies, and working with major donors in implementing large scale lifesaving and livelihood promotion and protection programs, especially in Southern and Eastern African countries. He is pursuing PhD studies at the University of Salford, UK.

Rob Fielding
Technical Programme Officer, Medair

Rob Fielding is a humanitarian and development infrastructure specialist with extensive experience in shelter and settlements, most recently with the Shelter Centre in Geneva. As a Technical Programme Officer at Medair, he leads innovation and research.

Jules Nsabimana
Food Assistance Manager, World Vision Rwanda

Jules Nsabimana has 11 years of experience in humanitarian emergency affairs, disaster risk reduction (DRR), livelihood and resilience programs with a specialisation in food assistance management. He has worked with Catholic Relief Service in DRC, and with World Vision DRC, Burundi, Niger and Mali. He holds a degree in Economics and is pursuing an MBA in Project Management.

Athalie Mayo
Humanitarian Emergency Logistician, World Food Programme

Following six years in the British Army (Intelligence Corps), Athalie Mayo worked in the private sector on security and crisis management for five years and thereafter joined the UN as a Security Officer. She has experience in a number of locations including the Niger Delta, Latin America, Iraq, Haiti, Darfur, and Central African Republic.

Gonzalo de Palacios
ACF-Spain Security Manager

Gonzalo de Palacios has worked for humanitarian organisations in the field and headquarters for over ten years. His work has encompassed logistics, coordination, programming and humanitarian security management. He has a degree in Law and an MA in International Cooperation and Development.

Bibliography and Resources

Bibliography

Albanesius, C. (2013). FCC Probes Post-Bombing Cell Phone Congestion in Boston. *PC Magazine UK.* Available from: http://www.pcmag.com/article2/0,2817,2417891,00.asp. [Accessed 2 Sept. 2014].

Anderson, B. (2013). Gangster, ideologue, martyr: The posthumous reinvention of Teungku Badruddin and the nature of the Free Aceh Movement. *Conflict, Security & Development.* 13 (1), p. 53.

Anderson, B. and Snyder, J. (2013). Coming of Age in the Urban Kampung: Gang Demographics and Territories in Select Jakarta Neighborhoods – Preliminary Findings. A paper presented at the European Association for South East Asian Studies Conference, Lisbon, Portugal, 2-5 July 2013. Available from: https://www.academia.edu/3849904/Coming_of_Age_in_the_Urban_Kampung_Gang_Demographics_and_Territories_in_Select_Jakarta_Neighborhoods-_Preliminary_Findings. [Accessed 1 Sept. 2014].

Arthur, C. (2012). China tightens 'Great Firewall' internet control with new technology. *The Guardian.* 14 Dec. Available from: http://www.theguardian.com/technology/2012/dec/14/china-tightens-great-firewall-internet-control. [Accessed 2 Sept. 2014].

Australian Associated Press. (2013). Egypt NGO says office raided by police. 19 Dec. Available from: http://www.sbs.com.au/news/article/2013/12/19/egypt-ngo-says-office-raided-police. [Accessed 1 Sept. 2014].

Awori, K. (2013). *Umati Final Report: September 2012-May 2013.* Available from: http://www.research.ihub.co.ke/uploads/2013/june/1372415606__936.pdf. [Accessed 2 Sept. 2014]. The full categorisation formula, including the data entry form, can be viewed in the final report.

BBC. (2011). Fake DigiNotar web certificate risk to Iranians. 5 Sept. Available from: http://www.bbc.co.uk/news/technology-14789763. [Accessed 1 Sept. 2014].

BBC. (2012). Vietnamese bloggers deny charges, third in leniency bid. 16 April. Available from: http://www.bbc.co.uk/news/world-asia-17727373. [Accessed 1 Sept. 2014].

Benesch, S. (2008). Vile Crime or Inalienable Right: Defining Incitement to Genocide. *Virginia Journal of International Law.* 48 (3). Available from: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1121926. [Accessed 2 Sept. 2014].

Benesch, S. (2013). Dangerous Speech: A Proposal to Prevent Group Violence. 23 Feb. Available from: http://voicesthatpoison.org/guidelines. [Accessed 2 Sept. 2014].

Blomfield, A. (2011). Syria 'tortures activists to access their Facebook pages'. *The Telegraph.* 9 May. Available from: http://www.telegraph.co.uk/news/worldnews/middleeast/syria/8503797/Syria-tortures-activists-to-access-their-Facebook-pages.html. [Accessed 1 Sept. 2014].

Boyd, D. (2010). Privacy, Publicity, and Visibility. Presentation at Microsoft Tech Fest. 4 March. Available from: http://www.danah.org/papers/talks/2010/TechFest2010.html. [Accessed 2 Sept. 2014].

Cabinet Office Civil Contingencies Secretariat. (Undated). *Ensuring resilient telecommunications: a survey of some technical solutions.* Available from: https://www.gov.uk/government/uploads /system/uploads/attachment_data/file/85842/resilient-telecomms-survey.pdf. [Accessed 2 Sept. 2014].

Communications Commission of Kenya. (2013). *Quarterly Sector Statistics Report: First Quarter of The Financial Year 2013/14 (Jul-Sept 2013).* Available from: http://ca.go.ke/images/downloads/STATISTICS/Sector%20Statistics%20Report%20Q1%202013-14.pdf. [Accessed 2 Sept. 2014].

Daily Nation. (2013). Security forces move to end Westgate mall siege as death toll rises to 62. 23 Sept. Available from: http://www.nation.co.ke/news/Westgate-Mall-attack-alshabaab-terrorism/-/1056/2004630/-/kr74w0/-/index.html. [Accessed 1 Sept. 2014].

Datta, D. et al. (2008). Mobile Phone-based Cash Transfers: Lessons from the Kenya Emergency Response. *Humanitarian Exchange Magazine.* 40. October. pp. 37-40. Available from: http://www.odihpn.org/humanitarian-exchange-magazine/issue-40/mobile-phone-based-cash-transfers-lessons-from-the-kenya-emergency-response. [Accessed 2 Sept. 2014].

Eisen, M. (2014). The Internet of Things Is Wildly Insecure – And Often Unpatchable. *WIRED.* 4 Jan. Available from: http://www.wired.com/2014/01/theres-no-good-way-to-patch-the-internet-of-things-and-thats-a-huge-problem. [Accessed 1 Sept. 2014].

FBI. Intelligence Cycle. Available from: http://www.fbi.gov/about-us/intelligence/intelligence-cycle. [Accessed 1 Sept. 2014].

Fisher, M. (2013). Syria's Pro-Assad Hackers Infiltrate Human Rights Watch Web Site and Twitter Feed. *The Washington Post.* 17 March. Available from: http://www.washingtonpost.com/blogs/worldviews/wp/2013/03/17/syrias-pro-assad-hackers-infiltrate-human-rights-watch-web-site-and-twitter-feed. [Accessed 1 Sept. 2014].

FrontlineSMS. (2011). Data Integrity Case Study: Voix des Kivus. pp. 1-2. Available from: http://www.frontlinesms.com/wp-content/uploads/2011/08/Case-Study-Voix-des-Kivus-final.pdf. [Accessed 2 Sept. 2014].

FrontlineSMS. (2011). *User Guide: Data Integrity.* Available from: http://www.frontlinesms.com/wp-content/uploads/2011/08/frontlinesms_userguide.pdf. [Accessed 2 Sept. 2014].

Fugate, C. and Genachowski, J. (2011). How to Communicate Before, During and After a Major Disaster. *Federal Communications Commission.* Available from: http://www.fcc.gov/blog/fcc-and-fema-how-communicate-during-and-after-major-disaster. [Accessed 2 Sept. 2014].

Gagliardone, I., Patel, A. and Pohjonnen, M. (2014). *Mapping and Analyzing Hate Speech Online: Opportunities and Challenges for Ethiopia.* Programme in Comparative Media Law and Policy, University of Oxford. Available from: http://pcmlp.socleg.ox.ac.uk /sites/pcmlp.socleg.ox.ac.uk/files/Ethiopia%20hate%20speech.pdf. [Accessed 2 Sept. 2014].

Gallagher, I. (2011). Egyptian police use Facebook and Twitter to track down protesters' names before 'rounding them up'. *Mail Online.* Available from: http://www.dailymail.co.uk/news/article-1354096/Egypt-protests-Police-use-Facebook-Twitter-track-protesters.html. [Accessed 10 July 2014].

Goolsby, R. (Undated). On cybersecurity, crowdsourcing, and social cyber-attack. *Policy Memo Series.* 1. Washington, DC: The Wilson Center. Available from: http://www.wilsoncenter.org/sites /default/files/127219170-On-Cybersecurity-Crowdsourcing-Cyber-Attack-Commons-Lab-Policy-Memo-Series-Vol-1.pdf. [Accessed 1 Sept. 2014].

Grayman, J. H. (2014). Rapid response: Email, immediacy, and medical humanitarianism in Aceh, Indonesia. *Social Science & Medicine.* In press. http://dx.doi.org/10.1016/j.socscimed.2014.04.024. [Accessed 1 Sept. 2014].

Halliday, J. (2011). London riots: BlackBerry to help police probe Messenger looting 'role'. *The Guardian.* 8 Aug. Available from: http://www.theguardian.com/uk/2011/aug/08/london-riots-blackberry-messenger-looting. [Accessed 1 Sept. 2014].

Howe, A. (2014). *LMMS Lessons Learned in the Syria Regional Crisis.* Beirut: Medair.

Human Rights Watch. (2011). *World Report 2011: Belarus.* Available from: http://www.hrw.org/world-report-2011/belarus. [Accessed 1 Sept. 2014].

ICRC. (2011). *International Humanitarian Law and the challenges of contemporary armed conflicts.* pp. 36-38. Available from: http://www.icrc.org/eng/assets/files/red-cross-crescent-movement/31st-international-conference/31-int-conference-ihl-challenges-report-11-5-1-2-en.pdf. [Accessed 1 Sept. 2014].

ICRC. (2013). What limits does the law of war impose on cyber-attacks? 28 June. Available from: http://www.icrc.org/eng/ resources/documents/faq/130628-cyber-warfare-q-and-a-eng.htm. [Accessed 1 Sept. 2014].

ICRC. (Undated). Customary IHL. Rule 32. Humanitarian Relief Objects. Available from: http://www.icrc.org/customary-ihl/eng/docs/v1_rul_rule32. [Accessed 1 Sept. 2014].

ICT Statistics Newslog. (2011). Estonians Vote in Parliamentary Election by Mobile Phone. 7 March. Available from: http://www.itu.int/ITU-D/ict/newslog/Estonians+Vote+In+Parliamentary+Election+By+Mobile+Phone.aspx. [Accessed 1 Sept. 2014].

Infoasaid/Actionaid Isiolo. (2012). *A Learning Review of the Pilot Communications Project.* p. 4. Available from: http://www.cdacnetwork.org/contentAsset/raw-data/0abadcd6-f55a-459e-9b0e-3bcb9051c3ba/attachedFile. [Accessed 2 Sept. 2014].

International Crisis Group. (2012). Indonesia: Cautious Calm in Ambon. *Asia Briefing.* 133. 13 Feb. p. 2. Available from: http://www.crisisgroup.org/en/regions/asia/south-east-asia/indonesia/b133-indonesia-cautious-calm-in-ambon.aspx. [Accessed 1 Sept. 2014].

International Telecommunications Union. (2014). *The World in 2014: ICT Facts and Figures.* pp. 1-8. Available from: http://www.itu.int/en/ITU-D/Statistics/Pages/facts/default.aspx. [Accessed 2 Sept. 2014].

Jamieson, D. (2011). London Riots Co-ordinated with BlackBerry Messenger. *TechWeek Europe.* 8 Aug. Available from: http://www.techweekeurope.co.uk/news/london-looting-co-ordinated-with-blackberry-messenger-36303. [Accessed 1 Sept. 2014].

JISC Legal Information. (2013). What's the legal position of transporting encrypted equipment abroad? 13 May. Available from: http://www.jisclegal.ac.uk/ManageContent/ViewDetail/ID/2947/Whats-the-legal-position-of-transporting-encrypted-equipment-abroad-13-May-2013.aspx. [Accessed 2 Sept. 2014].

Kaiman, J. (2013). Hack Tibet. *Foreign Policy.* 4 Dec. Available from: http://www.foreignpolicy.com/articles/2013/12/04/hack_tibet_china_cyberwar. [Accessed 1 Sept. 2014].

Kanere. (2013). Classified Fingerprinting. 30 Nov. Available from: http://kanere.org/2013/11/30/classified-fingerprinting [Accessed 1 Sept. 2014].

Karimakwenda, T. (2012). Civil Society Coalitions issue response to police crackdown. *SW Radio Africa.* 8 Nov. Available from: http://www.swradioafrica.com/2012/11/08/civil-society-coalitions-issue-response-to-police-crackdown. [Accessed 1 Sept. 2014].

Karugu, W. N. and Mwendwa, T. (2007). Vodafone and Safaricom Kenya: Extending the Range and Reliability of Financial Services to the Poor in Rural Kenya. UNDP. Available from: http://growinginclusivemarkets.org/media/cases/Kenya_MPESA_2008.pdf. [Accessed 1 Sept. 2014].

Le Bel, S. *et al.* (2014). FrontlineSMS as an early warning network for human-wildlife mitigation: Lessons learned from tests conducted in Mozambique and Zimbabwe. *Electronic Journal of Information Systems in Developing Countries.* 60. p. 3. Available from: http://www.ejisdc.org/ojs2/index.php/ejisdc/article/view/1256. [Accessed 2 Sept. 2014].

Livingston, S. (2011). Africa's Evolving Infosystems: A Path- way to Security and Stability. *Africa Center for Strategic Studies.* Research Paper No. 2.

Lynch, C. (2013). Somali Militants Live-Tweet Their Deadly Attack on U.N. Compound. Foreign Policy. 19 June. Available from: http://blog.foreignpolicy.com/posts/2013/06/19/somali_militants_live_tweet_their_deadly_attack_on_un_compound. [Accessed 1 Sept. 2014].

Ma'an News Agency. (2012). Israeli forces raid NGO offices in Ramallah. 11 Dec. Available from: http://www.maannews.net /eng/ViewDetails.aspx?ID=546800. [Accessed 1 Sept. 2014].

Marczak, B. *et al.* (2014). Hacking Team and the Targeting of Ethiopian Journalists. *Citizen Lab.* 12 Feb. Available from: https://citizenlab.org/2014/02/hacking-team-targeting-ethiopian-journalists. [Accessed 1 Sept. 2014].

Marczak, B. *et al.* (2014). Mapping Hacking Team's "Untraceable" Spyware. *Citizen Lab.* 17 Feb. Available from: https://citizenlab.org/2014/02/mapping-hacking-teams-untraceable-spyware. [Accessed 1 Sept. 2014].

Marczak, W. R., Scott-Railton, J., Marquis-Boire, M. and Paxson, V. When Governments Hack Opponents: A Look at Actors and Technology. *Citizen Lab.* (Unreleased draft).

McMillan, R. (2012). How the Boy Next Door Accidentally Built a Syrian Spy Tool. *WIRED.* 11 July. Available from: http://www.wired.com/2012/07/dark-comet-syrian-spy-tool. [Accessed 1 Sept. 2014].

McPherson, M., Smith-Lovin, L. and Cook, J. M. (2001). Birds of a Feather: Homophily in Social Networks. *Annual Review of Sociology.* 27 (1). pp. 415-444.

Meier, P. (2012). How crisis mapping saved lives in Haiti. *National Geographic NewsWatch.* 2 July. Available from: http://newswatch.nationalgeographic.com/2012/07/02/crisis-mapping-haiti. [Accessed 2 Sept. 2014].

Moody, J. (2005). Fighting a Hydra: A Note on the Network Embeddedness of the War on Terror. *Structure and Dynamics.* 1 (2). Available from: http://escholarship.org/uc/item/7x3881bs. [Accessed 1 Sept. 2014].

Nakashima, E. and Warrick, J. (2013). For NSA chief, terrorist threat drives passion to 'collect it all'. *The Washington Post.* 14 July. Available from: http://www.washingtonpost.com/world/national-security/for-nsa-chief-terrorist-threat-drives-passion-to-collect-it-all/2013/07/14/3d26ef80-ea49-11e2-a301-ea5a8116d211_story.html. [Accessed 1 Sept. 2014].

Njeru, J. N. (2013). *NipeUkweli: Outreach to Sensitize Communities on Dangerous Speech: Summary Report.* iHub Research. 20 March. Available from: http://www.ihub.co.ke/ihubresearch/jb_NipeUkweliSummaryReportMarchpdf2013-11-18-16-07-39.pdf. [Accessed 2 Sept. 2014].

Ottis, R. (2010). From Pitch Forks to Laptops: Volunteers in Cyber Conflicts. In Czosseck, C. and Podins, K. (eds). *Conference on Cyber Conflict Proceedings 2010.* Tallinn: CCD COE Publications. pp. 97-109. Available from: http://www.ccdcoe.org/publications/2010proceedings/Ottis%20%20From%20Pitchforks%20to%20Laptops%20Volunteers %20in%20Cyber%20Conflicts.pdf. [Accessed 1 Sept. 2014].

Parfitt, B. (2012). Putting yourself on the map. *Geographical.* April. Available from: http://www.geographical.co.uk/Magazine/Community_Mapping_-_Apr_12.html. [Accessed 2 Sept. 2014].

Pierskalla, J. H. and Hollenbach, F. M. (2013). Technology and Collective Action: The Effect of Cell Phone Coverage on Political Violence in Africa. *American Political Science Review.* 107. pp. 207-224. Available from: http://polisci.duke.edu/uploads/media_items/technology-collectiveactioncellphoneviolence.original.pdf. [Accessed 1 Sept. 2014].

Portland Communications. (2012). New Research Reveals How Africa Tweets. 1 Feb. Available from: http://www.portland-communications.com/2012/02/new-research-reveals-how-africa-tweets. [Accessed 2 Sept. 2014].

Rayner, G. and Spencer, R. (2012). Syria: Sunday Times journalist Marie Colvin killed in 'targeted attack' by Syrian forces. *The Telegraph.* 22 Feb. Available from: http://www.telegraph.co.uk/news/worldnews/middleeast/syria/9098175/Syria- Sunday-Times-journalist-Marie-Colvin-killed-in-targeted-attack-by-Syrian-forces.html. [Accessed 1 Sept. 2014].

Richards, J. and Lewis, P. (2011). How Twitter was used to spread – and knock down – rumours during the riots. *The Guardian.* 7 Dec. Available from: http://www.theguardian.com/uk/2011/dec/07/how-twitter-spread-rumours-riots. [Accessed 1 Sept. 2014].

Schenkenberg van Mierop, E. and Haenni Dale, C. (2011). Protection Principles. In *The Sphere Project: Humanitarian Charter and Minimum Standards in Humanitarian Response.* 3rd ed. Rugby: Practical Action. pp. 29-47.

Schmitt, M. N. (ed.). (2013). *Tallinn Manual on the International Law Applicable to Cyber Warfare.* New York, NY: Cambridge University Press.

Scott-Railton, J. (2013). Revolutionary Risks: Cyber Technology and Threats in the 2011 Libyan Revolution. *CIWAG Case Study Series.* Newport, RI: US Naval War College. Available from: https://www.usnwc.edu/getattachment/01e787b8-ee4c-4efb-8c5a-fe02aa2781ba/Scott-Railton-final-for-website.pdf. [Accessed 1 Sept. 2014].

Scott-Railton, J. (2014). Presentation at the 2014 Working Group on Emergency Telecommunications. Available from: http://wget2014.wordpress.com/tag/the-citizen-lab. [Accessed 1 Sept. 2014].

Scott-Railton, J. and Marquis-Boire. M. (2013). A Call to Harm: New Malware Attacks Target the Syrian Opposition. *Citizen Lab.* 21 June. Available from: https://citizenlab.org/2013/06/a-call-to-harm. [Accessed 1 Sept. 2014].

Shapiro, J. N. and Weidmann, N. B. (2013). *Is the phone mightier than the sword? Cell phones and insurgent violence in Iraq.* Department of Politics and Woodrow Wilson School, Princeton University. Available from: https://webspace.princeton.edu/users/esocweb/ESOC%20website%20publications/SW_CellphonesIraq.pdf. [Accessed 1 Sept. 2014].

Shirky, C. (2008) *Here Comes Everybody: The Power of Organizing Without Organisations.* Penguin Press.

Social Bakers Statistics. (2013). Available from: http://www.socialbakers.com/. [Accessed 12 April 2013].

Spyer, P. (2002). Fire without smoke and other phantoms of Ambon's violence: Media effects, agency, and the work of imagination. *Indonesia.* 74. pp. 21-36. Available from: http://cip.cornell.edu/DPubS?service=UI&version=1.0&verb=Display&handle=seap.indo/1106939683. [Accessed 1 Sept. 2014].

Sterling, B. (2012). Amnesty International infested with Chinese Ghost RAT. *WIRED.* 20 May. Available from: http://www.wired.com/2012/05/amnesty-international-infested-with-chinese-ghost-rat. [Accessed 1 Sept. 2014].

Taylor, M. and Hopkins, N. (2013). Amnesty to take legal action against UK security services. *The Guardian.* 9 Dec. Available from: http://www.theguardian.com/world/2013/dec/09/amnesty-international-legal-action-uk-security-services. [Accessed 1 Sept. 2014].

The Cash Learning Partnership. (No date). Protecting Beneficiary Privacy. p. 5. Available from: http://www.cashlearning.org/downloads/calp-beneficiary-privacy-web.pdf. [Accessed 1 Sept. 2014].

Trucano, M. (2009). Checking in with BridgeIT in Tanzania: Using mobile phones to support teachers. World Bank. 25 Sept. Available from: http://blogs.worldbank.org/edutech/checking-in-with-bridgeit-in-tanzania. [Accessed 1 Sept. 2014].

UN News Centre. (2013). Deputy UN chief calls for urgent action to tackle global sanitation crisis. 21 March. Available from: http://www.un.org/apps/news/story.asp?NewsID=44452&Cr=sanitation&Cr1=#.VAVs1bxdXXH. [Accessed: 2 Sept. 2014].

UN. (Undated). Tracnet, Rwanda: Fighting Pandemics through Information Technology. Available from: http://www.un.org/esa/sustdev/publications/africa_casestudies/tracnet.pdf. [Accessed 1 Sept. 2014].

UNDP. (2012). Mobile Technologies and Empowerment: Enhancing human development through participation and innovation. Available from: https://www.undpegov.org/mgov-primer.html. [Accessed 1 Sept. 2014].

UNESCO. (2014). Smart eSOS toilet for emergencies. 8 July. Available from: http://www.unesco-ihe.org/news/smart-esos-toilet-emergencies. [Accessed 1 Sept. 2014].

UNHCR. (2012). Modern technology helps meet the needs of refugees in South Sudan. 27 Dec. Available from: http://www.unhcr.org/50dc5a309.html [Accessed 1 Sept. 2014].

UNHCR. (2014). UNHCR pilots new biometrics system in Malawi refugee camp. 22 Jan. Available from: http://www.unhcr.ie/news/irish-story/unhcr-pilots-new-biometrics-system-in-malawi-refugee-camp [Accessed 1 Sept. 2014].

UNICEF. (2013). Searching for creative solutions in humanitarian action. 21 Oct. Available from: http://www.unicef.org/emergencies/index_70706.html. [Accessed 1 Sept. 2014].

Van Brabant, K. *et al.* (2010). *Good Practice Review: Operational security management in violent environments. Number 8 (New edition).* Humanitarian Practice Network. Dec. Available from: http://www.odihpn.org/download/gpr_8_revised2pdf. [Accessed 2 Sept. 2014].

Weiland, S. (2013). A Threat to Relations: Germany Irate over Russian NGO Raids. *Der Spiegel*. 26 March. Available from: http://www.spiegel.de/international/europe/russian-authorities-raid-german-foundations-and-ngos-a-890969.html. [Accessed 1 Sept. 2014].

World Vision Rwanda. (2014). Cash transfer project highlights. Unpublished. pp. 1-2.

World Vision Sudan. (2012). Food distribution monitoring report. Unpublished. pp. 15-20.

Key Resources

The following links have been provided throughout the publication and can be consulted for further information.

http://cddrl.fsi.stanford.edu/libtech

http://citizenlab.org

http://digitalhumanitarians.com

http://growinginclusivemarkets.org

http://harassmap.org

http://healthmarketinnovations.org

http://ipaidabribe.com

http://myanmarido.org/en

http://voicesthatpoison.org

http://wget2014.wordpress.com

http://www.avpkenya.org

http://www.cashlearning.org

http://www.ccdcoe.org

http://www.cdacnetwork.org

http://www.cryptolaw.org

http://www.danah.org

http://www.frontlinesms.com

http://www.matternet.us

http://www.reclaimnaija.net

http://www.research.ihub.co.ke

http://www.sisiniamani.org

http://www.ushahidi.com

https://securityinabox.org

https://www.torproject.org

Other EISF Publications

If you are interested in contributing to upcoming research projects or want to suggest topics for future research please contact **eisf-research@eisf.eu**.

Briefing Papers

Security Risk Management and Religion: Faith and Secularism in Humanitarian Assistance
August 2014
Hodgson, L. et al. Edited by Vazquez, R.

Security Management and Capacity Development: International Agencies Working with Local Partners
December 2012
Singh, I. and EISF Secretariat

Gender and Security: Guidelines for Mainstreaming Gender in Security Risk Management
September 2012 – *Sp. and Fr. versions available*
Persaud, C. Edited by Zumkehr, H. J. – EISF Secretariat

Engaging Private Security Providers: A Guideline for Non-Governmental Organisations
December 2011 *Fr. version available*
Glaser, M. Supported by the EISF Secretariat (eds.)

Abduction Management
May 2010
Buth, P. Supported by the EISF Secretariat (eds.)

Crisis Management of Critical Incidents
April 2010
Buth, P. Supported by the EISF Secretariat (eds.)

The Information Management Challenge
March 2010
Ayre, R. Supported by the EISF Secretariat (eds.)

Reports

The Future of Humanitarian Security in Fragile Contexts
March 2014
Armstrong, J. Supported by the EISF Secretariat

The Cost of Security Risk Management for NGOs
February 2013
Finucane, C. Edited by Zumkehr, H. J. – EISF Secretariat

Risk Thresholds in Humanitarian Assistance
October 2010
Kingston, M. and Behn O.

Joint NGO Safety and Security Training
January 2010
Kingston, M. Supported by the EISF Training Working Group

Humanitarian Risk Initiatives: 2009 Index Report
December 2009
Finucane, C. Edited by Kingston, M.

Articles

Incident Statistics in Aid Worker Safety and Security Management: Using and Producing them
March 2012
Van Brabant, K.

Managing Aid Agency Security in an Evolving World: The Larger Challenge
December 2010
Van Brabant, K.

Whose risk is it anyway? Linking Operational Risk Thresholds and Organisational Risk Management
June 2010, (in Humanitarian Exchange 47)
Behn, O. and Kingston, M.

Risk Transfer through Hardening Mentalities?
November 2009
Behn, O. and Kingston, M.

Guides

Security Audits
September 2013 – *Sp. and Fr. versions available*
Finucane C. Edited by French, E. and Vazquez, R. (Sp. and Fr.) – EISF Secretariat

Managing The Message: Communication and Media Management in a Crisis
September 2013
Davidson, S., and French, E., EISF Secretariat (eds.)

Family First: Liaison and Support During a Crisis
February 2013 *Fr. version available*
Davidson, S. Edited by French, E. – EISF Secretariat

Office Closure
February 2013
Safer Edge. Edited by French, E. and Reilly, L. – EISF Secretariat

Forthcoming publications

Office Opening Guide

eisf

European Interagency Security Forum

EISF Coordinator
+44 7760 992 239
eisf-coordinator@eisf.eu

EISF Researcher
+44 7925 409 655
eisf-reseach@eisf.eu

www.eisf.eu

design and artwork: www.wave.coop

First published October 2014