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

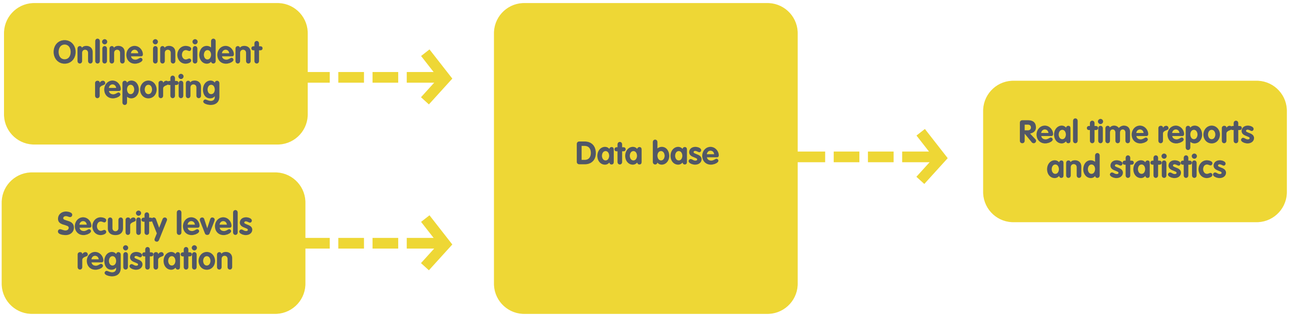
Introduction

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.

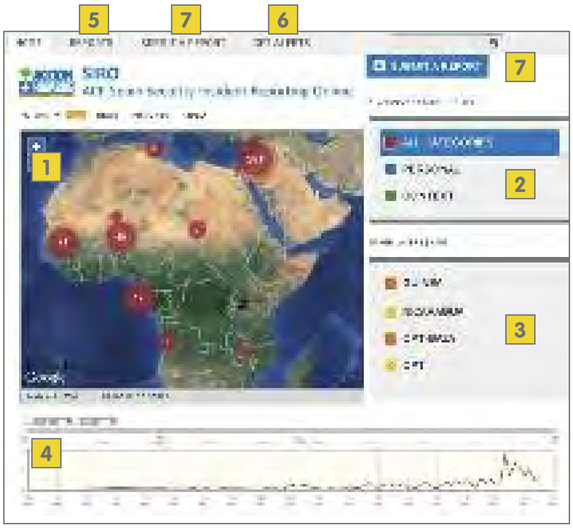
An illustration of the system would be:


Online incident reporting
Security levels registration
Data base
Real time reports and statistics

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.

[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.

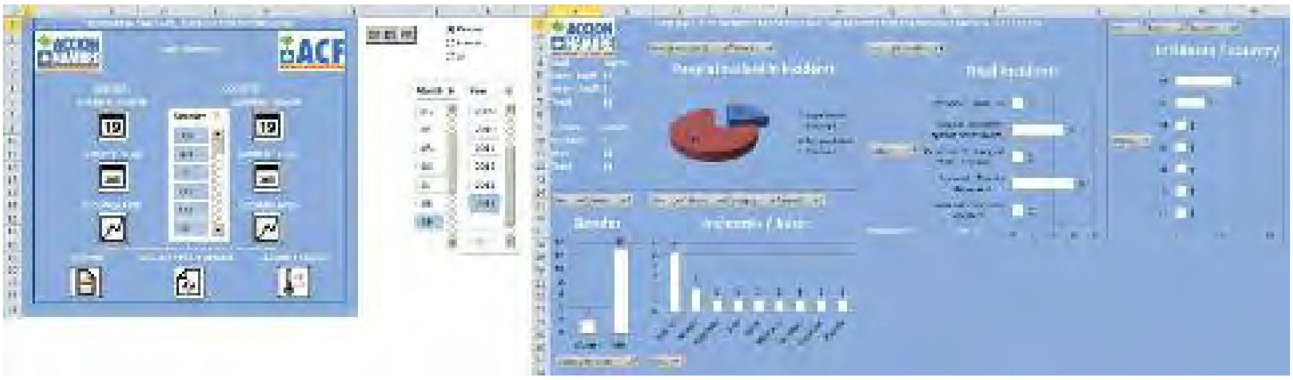
This analysis is being confirmed in 2014, where the number of incidents being reported at the time of writing (August 2014) is matching the figures for 2013, the year when the system started being used. However, facilitating reporting through the Ushahidi system was not the only stimulus for more incident 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.

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

EISF is a member-led grouping and has no separate legal status under the laws of England and Wales or any other jurisdiction, and references to 'EISF' in this disclaimer shall mean the member agencies, observers and secretariat of EISF.

While EISF endeavours to ensure that the information in this document is correct, EISF does not warrant its accuracy and completeness. The information in this document is provided 'as is', without any conditions, warranties or other terms of any kind, and reliance upon any material or other information contained in this document shall be entirely at your own risk. Accordingly, to the maximum extent permitted by applicable law, EISF excludes all representations, warranties, conditions and other terms which, but for this legal notice, might have effect in relation to the information in this document. EISF shall not be liable for any kind of loss or damage whatsoever to you or a third party arising from reliance on the information contained in this document.

© 2014 European Interagency Security Forum

Available at **www.eisf.eu**

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