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.

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

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