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.

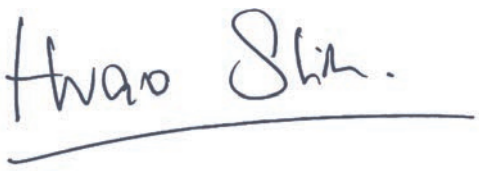
Computer software, mobile phones, smart phones and tablets are all making a huge impact on the delivery of humanitarian assistance and protection. People affected by conflict and disaster are also communicating their situation directly to humanitarian agencies and the wider world on Facebook, in tweets 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.

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

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