Cyber-Warfare and Humanitarian Space

Daniel Gilman

Introduction[2]

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

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

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

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

Increasing vulnerability of humanitarian organisations

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

[2] The views expressed in this publication are those of the author alone, and do not reflect the position of the United Nations. Material for this report was drawn in part from the forthcoming OCHA publication 'Humanitarianism in the Age of Cyberwarfare'. The author would also like to thank John Scott-Railton of Citizen Lab for his expertise and support, without which this paper would not have been possible.

[3] See http://digitalhumanitarians.com. [Accessed 1 Sept. 2014].

[4] See Kanere. (2013). Classified Fingerprinting. 30 Nov. Available from: http://kanere.org/2013/11/30/classified-fingerprinting; UNHCR. (2012). Modern technology helps meet the needs of refugees in South Sudan. 27 Dec. Available from: http://www.unhcr.org/50dc5a309.html; UNHCR. (2014). UNHCR pilots new biometrics system in Malawi refugee camp. 22 Jan. Available from: http://www.unhcr.ie/news/irish-story/unhcr-pilots-new-biometrics-system-in-malawi-refugee-camp. [All accessed 1 Sept. 2014].

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

[6] See http://en.wikipedia.org/wiki/Cyberwarfare. [Accessed 1 Sept. 2014].

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

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

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

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

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

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

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

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

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

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

The paramilitarisation of cyber-warfare: the case of Syria

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

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

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

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

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

[16] See http://www.matternet.us. [Accessed 1 Sept. 2014].

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

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

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

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

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

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

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

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

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

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

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

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

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

Conclusions

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

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

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

[23] Furthermore, cyber-warfare does not have to produce permanent, physical destruction to be considered an 'attack'. See ICRC. (2011). *International Humanitarian Law and the challenges of contemporary armed conflicts*. pp. 36-38. Available from: http://www.icrc.org/eng/assets/files/red-cross-crescent-movement/31st-international-conference/31-int-conference-ihl-challenges-report-11-5-1-2-en.pdf. [Accessed 1 Sept. 2014]. See also ICRC. (2013). What limits does the law of war impose on cyber-attacks? 28 June. Available from: http://www.icrc.org/eng/resources/documents/faq/130628-cyber-warfare-q-and-a-eng.htm. [Accessed 1 Sept. 2014].

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

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

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

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

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.

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