Trends in Intelligence Gathering by Governments

Rory Byrne

Introduction[26]

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

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

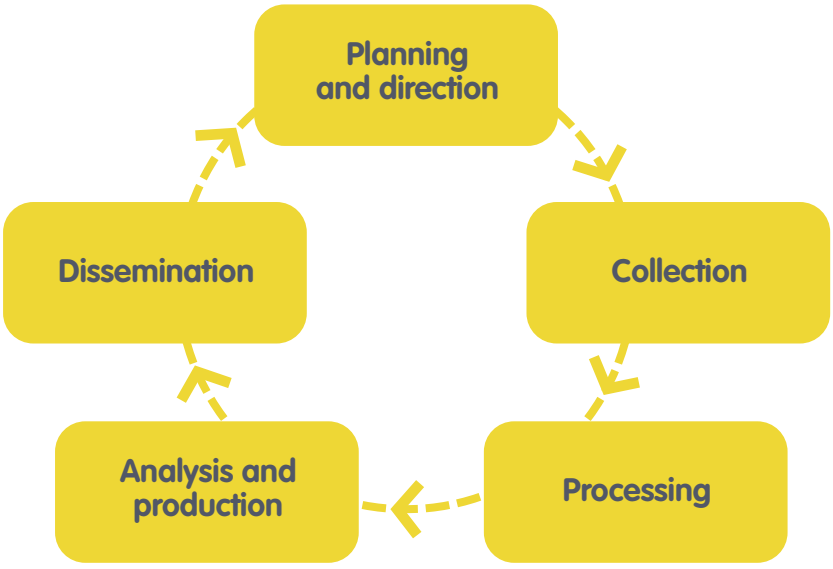
The intelligence cycle

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

Planning and direction

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

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



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

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

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

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

Collection

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

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

Background

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

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

Waterholes

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

Certificates

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

Mobile phones

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

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

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

Physical access

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

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

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

Processing

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

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

Analysis and production

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

Dissemination

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

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

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

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

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

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

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