CYBERSECURITY

VS

Humanitarian Organizations

On a Collision Course ?

DH Network
Digital Humanitarian Network

AUGUST 2018

Licensing Information

CYBERSECURITY AND HUMANITARIAN ORGANIZATIONS: ON A COLLISION COURSE?

by

Emma Amaral (emma.m.amaral@gmail.com)
Master of Global Affairs (MGA) Candidate 2019
University of Toronto

Andrej Verity (verity@un.org | @andrejverity)
Office for the Coordination of Humanitarian Affairs (OCHA)
United Nations

Design

Jiahui Du (jd3399@tc.columbia.edu)
MA in Instructional Technology and Media
Teachers College, Columbia University

This document was made possible
with the support of UN-OCHA

CONTENTS

EXECUTIVE SUMMARY

Humanitarian organizations are collecting increasing amounts of data from crisis-affected populations on both the individual and community level. This data is informing more evidence-based interventions, creating more advanced tools such as interactive maps and other infographics, and informing predictions of future humanitarian crises. However, the responsibility of handling valuable data makes humanitarian organizations a new target for cyber attacks, potentially putting people's lives at risk. As cyber attacks such as hacking or denial of service attacks against civil society continue to increase, the humanitarian sector has not kept pace with the necessary corresponding security infrastructure or policies. Furthermore, cyberwarfare will add even more complexity and logistical challenges to the crises to which humanitarians respond. Along with ethical issues such as the data-related rights of affected populations and the "do no harm", the humanitarian sector risks its very legitimacy in the world's increasingly digital future, if it does not act sufficiently on privacy and security concerns.

This report outlines the various steps humanitarian organizations can take to increase their cybersecurity, ranging from the individual level to the organizational and sector-wide. They include:

1. Conduct risk assessments
2. Build capacity: Staff expertise and training
3. Partner with the private sector when the benefits outweigh the risks
4. Change the organizational structure
5. Improve the basic standards of cybersecurity practices
6. Increase responsibility on donors for security funding and reducing stigma
7. Improve communication between humanitarian organizations
8. Improve data policy as a whole and be consistent
9. Develop an emergency contingency plan

Organizations should avoid reacting in the following manner:

1. Address cybersecurity by introducing new technologies
2. Wait until there is a serious breach of trust in the humanitarian sector
3. Adopt a 'one size fits all' approach
4. Become overwhelmed

The cybersecurity landscape is, by its technological nature, in a continuous arms race between offensive and defensive capabilities. The humanitarian sector must acknowledge that it is operating within this landscape, and therefore incorporate responsible structural changes that will allow organizations to continue to do their life saving work effectively. Although it is not feasible for resource-constrained organizations to keep up with the most current cybersecurity defensive technologies, there are practical steps that can be implemented (beginning with increased awareness) that will allow them to leverage the potential of data while minimizing associated harms. This report is informed by experts in the civil society, cybersecurity, and humanitarian fields, and quotes obtained in the research process are provided throughout the report for greater context. Content presented in boxes is meant to provide the reader with supplementary information.

INTRODUCTION

The focus of this paper is to alert humanitarian organizations and related bodies such as UN-OCHA to increasing cybersecurity threats, and to recommend steps that will minimize risks to organizations and the people they serve. The 2014 report published by OCHA titled "Humanitarianism in the Age of Cyber-warfare" noted that among other factors, the information that humanitarians collect in the future would be shaped by "the extent to which political or criminal groups target humanitarian operations, as well as the level of government surveillance."[1] For several reasons since, cybersecurity threats have become more prevalent and consequential, including in their aim towards humanitarian organizations.

First, states (along with sponsored non-state groups) have increased; there is an increasing reliance on and collection of data by humanitarian organizations; and a near ubiquitous reliance on information and communications technology (ICT) for national infrastructure that is also used in a humanitarian response (such as transportation, water and sanitation systems, financial institutions, etc.). Even a cursory Google search surfaces many statements by experts concurring that the cybersecurity threat landscape is becoming more complex. One comprehensive resource is the Center for Strategic and International Studies (CSIS), which has compiled an extensive timeline of "significant cyber incidents since 2006."[2] The evidence of attempted and successful cyber attacks against humanitarian organizations in recent history suggests that the field has not developed more cyber secure practices since the 2014 report.

"Since the 2014 OCHA cybersecurity report, humanitarian organizations are now a more informed cohort, and there is greater emphasis on community involvement regarding data use. However, this has not translated into practical applications of security practices."- Interviewee

The cyber attacks compiled by CSIS are extremely varied and seem to attempt to accomplish different goals: financial hacking to steal cryptocurrency or other funds; to obtain data to then sell; to spread disinformation or "fake news" (to weaken support for policies; to influence elections; to promote disunity, etc.); to attack infrastructure; to gain strategic information and intellectual property (from other states or competing private companies); to target and surveil specific people and/or organizations (such as UN personnel; journalists; or political opponents); while some random style attacks seem aimed only at disruption and promoting chaos.

1. Gilman, D. (October 2014) "Humanitarianism in the Age of Cyber-Warfare: Towards the Principled and Secure Use of Information in Humanitarian Emergencies," OCHA Policy and Study Series. https://www.unocha.org/sites/unocha/files/Humanitarianism%20in%20the%20Cyberwarfare%20Age%20-%20OCHA%20Policy%20Paper%2011.pdf, accessed May 2018.
2. "Significant Cyber Incidents," Center for Strategic & International Studies. https://www.csis.org/programs/cybersecurity-and-governance/technology-policy-program/other-projects-cybersecurity, accessed May 2018.

Hacking and other cyber warfare tools are becoming increasingly affordable and accessible. Authoritarian and democratic governments alike are increasingly regulating and controlling activity on the internet. Surveillance and interception technologies have become so accessible that even poorer governments and other non-state actors can use these tools against their adversaries.[3] Private companies that develop a sophisticated range of cyber technologies, such as Verint,[4] Gamma International, and Hacking Team,[5] are known to sell military grade hacking tools to regimes accused of human rights abuses. Blue Coat Systems Inc. is one of many companies which produces devices that can "implement politically motivated restrictions on access to information, and/or to monitor private communications," including intercepting encrypted technologies.[6] Citizen Lab has traced these devices to 83 countries, some in the midst of armed conflict. Furthermore, publically available "how to" instructions on cyber attacks can turn any sympathetic ally with a computer into a hacker. When the group Anonymous attacked the UN as part of their #OpStopTheUN campaign, they released a list of specific targets and created tutorial videos on how to attack these websites. Similarly, the Syrian Electronic Army provided denial of service software on their Facebook page for allies to download and use against certain media targets.[7] Distributed Denial of Service attacks, or DDoS, refer to coordinated efforts to disrupt internet-dependent services, making them unavailable to users.

Cyberspace is an expanding battleground between a wide array of actors, beyond traditional kinetic conflict: Deibert and Railton of the Citizen Lab state that "all actors to armed conflict today increasingly are better equipped and more savvy about how to exploit big data for nefarious ends."[8] In the 2011 Libyan civil war, pro-government actors such as the Libyan Electronic Army targeted opposition groups over cyberspace, with DDoS attacks, malware, and hacking among others.[9] Cybersecurity is now considered the most significant threat faced by the United States, as listed in the annual assessment sent to Congress from the Director of National Intelligence, Dan Coats.[10] In July 2018, Coats stated that the "warning lights are blinking red again", comparing the ongoing and pervasive cyber attacks facing digital infrastructure in the country to the warning signs present in the months prior to the 9/11 terrorist attacks. Coats clarified that although cyber attacks have recently centered around election meddling and undermining American democracy (as 12 Russian military

3. Sandvik, K.B. (2016) "The humanitarian cyberspace: shrinking space or an expanding frontier?", Third World Quarterly 37(1): 17–32. accessed June 2018.
4. "Privacy International uncovers widespread surveillance throughout Central Asia, exposes role of Israeli companies" (November 2014) Privacy International. https://privacyinternational.org/press-release/1186/privacy-international-uncovers-widespread-surveillance-throughout-central-asia, accessed June 2018.
5. Toor, A. (February 2016) "European companies sold powerful surveillance technology to Egypt, report says," The Verge. https://www.theverge.com/2016/2/24/11104524/egypt-surveillance-nokia-finfisher-hacking-team-spyware, accessed June 2018.
6. Williams, P. & Fiddner, D. (August 2016) "Cyberspace: Malevolent Actors, Criminal Opportunities, and Strategic Competition," (p. 338) United States Army War College Press. https://ssi.armywarcollege.edu/pdffiles/PUB1319.pdf, accessed June 2018.
7. Ibid (p. 351).
8. Ibid (p. 336).
9. Ibid (p. 347).
10. Perlroth, N. & Sanger, D. (May 2018) "White House Eliminates Cybersecurity Coordinator Role," The New York Times. https://www.nytimes.com/2018/05/15/technology/white-house-cybersecurity.html, accessed July 2018.

intelligence agents have been indicted for), critical infrastructure is at stake as well.[11] IT professionals predict that future cyberthreats will become more ubiquitous, automated, and sophisticated. The rise of Artificial Intelligence will enable this escalation: computers could be trained through machine learning to automatically detect new ways of compromising computer systems that are very difficult to uncover.

"The sophistication of cyber attacks increases like Moore's Law, it's exponential. The minute they find out something works, it gets run across the web, dark net, internal circle, word of mouth. They all help each other." -Interviewee

A related topic that is increasingly receiving attention and concern is use of disinformation as part of a larger information warfare strategy. This is undoubtedly an increasing threat to humanitarian organizations, who rely on maintaining trust from the general public, donors, and beneficiaries to fulfill mandates. For example, the White Helmets (also known as the Syria Civil Defence) became targets of a sustained misinformation campaign to discredit them and their work. Although it is an important topic, this report focuses on cybersecurity in the sense of hacking, data breaches, and surveillance. However, it is important to acknowledge that these are becoming harder to disentangle. In 2017, John Scott Railton reported on a technique called "tainted leaks." According to Railton, David Satter, a journalist and critic of the Kremlin, had documents stolen from him through a phishing campaign. Satter's emails were modified with false information and "leaked" by a self-proclaimed pro-Russian hactivist group, in a manner that supported and seemingly provided evidence for the propaganda of the Russian government.[12]

The Internet of Things (IoT) refers to devices that are connected to the Internet, from kitchen appliances to play toys and infrastructure such as bridges and power plants. There are billions of these devices constantly amassing data, as some wearable technologies are physically located on people 24 hours a day, and other devices record audio from inside people's homes. By 2020 it is estimated that the IoT will range between 20 to 50 billion devices. Even the humanitarian sector is using "humanitarian wearables" to deliver data informed aid. The IoT will bring a new range of cybersecurity vulnerabilities, as they are often produced with little to no built-in security or follow up security updates for the device.

11. Stracqualursi, V. (July 2018) "US intelligence chief: 'The warning lights are blinking red again' on cyberattacks," CNN. https://www.cnn.com/2018/07/14/politics/director-of-national-intelligence-dan-coats-cyberattacks-russia/index.html, accessed July 2018.
12. Hulcoop, A. et al. (May 2017) "Tainted Leaks: Disinformation and Phishing With a Russian Nexus," The Citizen Lab. https://citizenlab.ca/2017/05/tainted-leaks-disinformation-phish/, accessed June 2018.

Cybersecurity obligations of humanitarian organizations

"The things we need aren't about technology, they're about political will and about rights."- Nathaniel Raymond

Humanitarian organizations have a duty to "do no harm" while supporting communities in need. This ethos must extend to the protection of sensitive data that organizations collect and/or handle from cyber attacks as well. The Signal Program by the Harvard Humanitarian Initiative[13] grounded this concept in legal theory. The following rights of beneficiaries have been derived from international law, with number two and three being the most relevant to this report.

1. The right to access, generate, communicate, and benefit from information during crisis;
2. **The right to protection from threats and harms resulting from the use of information and communications technologies and data during crisis;**
3. **The right to data privacy and security;**
4. The right to data agency; and
5. The right to redress and rectification.

The Harvard Humanitarian Initiative followed the identification of these rights with a report outlining nine corresponding obligations that humanitarian organizations must adhere to if they are to uphold basic principles and standards of humanitarianism.[14] The three most relevant to this report include ensuring competence, capacity, and capability throughout humanitarian information activities (HIAs). Humanitarian organizations must ensure that they have the technical skills to properly secure data to fulfill their duty of care to beneficiaries, as well as the responsibility to ensure that any new technologies can be properly secured. Secondly, humanitarian organizations have a responsibility to identify and minimize adverse effects through the course of an HIA, including the various ways that beneficiaries may be exploited, targeted, or discriminated against because of their "information or data generated through humanitarian activities." And finally, humanitarian organizations must ensure data privacy and security, before, during, and after the implementation of a humanitarian information activity. According to the report,

"Failure to realize this obligation increases the potential for irrevocable harms affecting the protection status of vulnerable people, such as refoulement, arbitrary detention, trafficking, torture and disappearance, extrajudicial killings, and social and economic exclusion and exploitation. Additional harm may arise due to loss of dignity, financial loss, and the burden of guarding against future harms. Further, in certain circumstances this may cause violations of other rights, such as the right to data agency."

---

13. Greenwood, F. et al. (January 2017) "The Signal Code: A Human Rights Approach to Information During Crisis," Harvard Humanitarian Initiative. https://hhi.harvard.edu/publications/signal-code-human-rights-approach-information-during-crisis, accessed June 2018.
14. Campo, S. et al. (May 2018) "Signal Code: Ethical Obligations for Humanitarian Information Activities," (p.14) Harvard Humanitarian Initiative. https://hhi.harvard.edu/publications/signal-code-ethical-obligations-humanitarian-information-activities, accessed June 2018.

Humanitarian organizations also have a responsibility to maintain the public's trust, for long term viability. A publicized case of the inappropriate use of data on the scale of Facebook's Cambridge Analytica scandal could be devastating to the humanitarian sector, especially if it has negative consequences for beneficiaries' safety and well being. Blowback could be in the form of legal consequences, or a loss of trust in cases where organizations acted unethically but not to the extent of breaking international data protection laws (or because they enjoy legal immunity, as is the case for international organizations). Yahoo was fined £250,000 for inadequately preventing a 2014 hack that compromised the personal data of 500 million users and was only revealed two years later.[15] The UK Information Commissioner's Office acknowledged that cyber attacks will happen as cybercriminals become more sophisticated and harder to defend against, but that "organizations must take appropriate steps to protect the data of their customers to this threat." Responsibly guarding against cyber attacks is important for humanitarian organizations lacking public support and trust. Organizations that irresponsibly handle data, cover up cyber attacks and data breaches, and fail to notify affected beneficiaries risk their long term survival.

"We've watched the incredibly quick erosion of trust in the tech sector for their inability to do what we're talking about."- John Scott Railton

15. Gibbs, S. (June 2018) "Yahoo fined £250,000 for hack that impacted 515,000 UK accounts," The Guardian. https://www.theguardian.com/technology/2018/jun/12/yahoo-fined-hack-ico-uk-accounts-russia, accessed June 2018.

A RECENT HISTORY OF ATTACKS

"Vulnerabilities of humanitarian activists, journalists, and other participants in conflict situations have been documented in so many disparate situations that one must conclude that it is too simple to make an argument that digital technologies are inherently benign."[16]

Documented cyber attacks against humanitarian organizations and actors have increased in recent years as predicted by scholars in 2011.[17] It is important to note that the following list is not all inclusive, as most cyber attacks go unreported or unnoticed.

2018.7

In June 2018, an Amnesty International staff member was targeted by mobile spyware produced by the NSO Group, a private Israeli cyber intelligence firm.[18] The baited message included a tip about a protest at the Saudi embassy in Washington, sent to the staff member over WhatsApp. During their investigation, Amnesty International found that a Saudi activist had received similar messages. The suspicious messages were shared with the Citizen Lab, who has been tracking the NSO Group's Pegasus spyware since 2016. The Citizen Lab's analysis found that the messages were part of the Pegasus infrastructure, which has been used in previous attacks against Ahmed Mansoor, a human rights defender from the United Arab Emirates, and Mexican lawyers, activists, and scientists.[19]

"This is the new normal for human rights defenders."- Joshua Franco, head of technology and human rights for Amnesty International.[20]

2018.3

In March of 2018, a United Nations incident report confirmed that the UN panel tasked with enforcing trade sanctions against North Korea was targeted in a series of hacks by a state actor. These cyber attacks compromised the email accounts of panel members including their email messages.[21]

16. Williams, P. & Fiddner, D. (August 2016) "Cyberspace: Malevolent Actors, Criminal Opportunities, and Strategic Competition," (p. 358) United States Army War College Press. https://ssi.armywarcollege.edu/pdffiles/PUB1319.pdf, accessed June 2018.
17. Ferris, E. (2011) "Megatrends and the future of humanitarian action," (p.923) International Review of the Red Cross, pp 915938 doi:10.1017/ S181638311200029X, accessed June 2018.
18. "Amnesty International Among Targets of NSO-powered Campaign" (August 2018) Amnesty International. https://www.amnesty.org/en/latest/research/2018/08/amnesty-international-among-targets-of-nso-powered-campaign/, accessed August 2018.
19. Marczak, B., Scott-Railton, J., Deibert, R. (July 2018) "NSO Group Infrastructure Linked to Targeting of Amnesty International and Saudi Dissident," The Citizen Lab https://citizenlab.ca/2018/07/nso-spyware-targeting-amnesty-international/, accessed August 2018.
20. Osborne, S. (August 2018) "Amnesty International reveals employee targeted with Israeli spyware," The Independent. https://www.independent.co.uk/news/world/middle-east/amnesty-international-israel-spyware-human-rights-nso-group-a8473266.html, accessed August 2018.
21. Whoriskey, P. (March 2018) "The U.N. issued trade sanctions against North Korea. Then hackers infiltrated it," The Washington Post. https://www.washingtonpost.com/news/wonk/wp/2018/03/06/the-u-n-issued-trade-sanctions-against-north-korea-then-hackers-infiltrated-it/?noredirect=on&utm_term=.67e59e831e05, accessed August 2018.

2017.8
2018.2

Computer security technology company McAfee uncovered a phishing campaign titled "Operation Honeybee," targeting humanitarian aid organizations through infected Microsoft Word documents. This operation ran from August 2017 to February 2018 and used North Korean political and humanitarian topics to entice victims to open decoy documents, such as one titled "International Federation of Red Cross and Red Crescent Societies – DPRK Office."[22] According to McAfee, the attacker targeted organizations involved in humanitarian aid on the Korean peninsula.

2017.11

The aforementioned CSIS compilation identified a Vietnamese hacking group that targeted cyber espionage campaigns against several organizations, including human rights and civil society organizations in November 2017.[23]

2016

In 2016 a Russian entity engaged in a "major cyber espionage campaign" targeting human rights organizations, among others.[24] One target included the Syrian Observatory for Human Rights. The objective of the cyber attacks seemed to be to stifle the outgoing flow of information on Syria's humanitarian crisis, and the extent of Russia's involvement in military operations in the country. The attacks were reported to be well organized with state support, using malware to "**erase data, spread false information using official accounts and give access to NGOs contacts, including highly sensitive targets.**"[25]

2016

In 2016 British surgeon Dr. David Nott, who virtually guided medical operations in Syria, suspected that a hacker used information from his computer to attack a Syrian underground operation room.[26] BBC News broadcasted a story of Dr. Nott's remote efforts to help the besieged hospital by giving real time instructions to surgeons via Whatsapp and Skype. Dr. Nott believes that this led to the hacking of his computer because of the timing and the precision of a "bunker bomb" a few weeks later that shut down the hospital. According to Dr. Nott, who has since stopped advising doctors over the internet, "the operation was the only time coordinates came out of that operating theatre."

22. Sherstobitoff, R. (March 2018) "McAfee Uncovers Operation Honeybee, a Malicious Document Campaign Targeting Humanitarian Aid Groups," McAfee. https://securingtomorrow.mcafee.com/mcafee-labs/mcafee-uncovers-operation-honeybee-malicious-document-campaign-targeting-humanitarian-aid-groups/, accessed June 2018.
23. "Significant Cyber Incidents," Center for Strategic & International Studies. https://www.csis.org/programs/cybersecurity-and-governance/technology-policy-program/other-projects-cybersecurity, accessed June 2018.
24. "Russia mounts major cyber-espionage campaign against Syrian organisations," (February 2016) The New Arab. "https://www.alaraby.co.uk/english/news/2016/2/21/russia-mounts-major-cyber-espionage-campaign-against-syrian-organisations, accessed June 2018.
25. Ibid.
26. Dixon, H., Majid, A., & Swinford, S. (March 2018) "How hackers 'led warplanes to Syrian hospital' after targeting British surgeon's computer," The Telegraph. https://www.telegraph.co.uk/news/2018/03/20/british-surgeon-helped-syrian-operations-hacked-reveal-secret/, accessed July 2018.

A case that alarmed several humanitarian organizations was the discovery of major security vulnerabilities of Red Rose, an online data storage and management platform and app provider for humanitarian responders.[27] Major clients such as Catholic Relief Services (CRS) and other aid agencies use Red Rose's web-based system to manage their cash and voucher transfers to beneficiaries. After conducting competitiveness intelligence, Mautinoa reported that it identified multiple security problems. Although Red Rose denied this, Mautinoa claims that these problems exposed vulnerable people to "very significant risks": they were able to enter CRS's cloud-based server and access "names, photographs, family details, Personal Identification Numbers (PINs) and map coordinates for more than 8,000 families receiving assistance from the NGO in West Africa." Mautinoa was also able to access CRS's administrative dashboard, allowing them to view and edit financial and personal details, and to download data; the system contained financial records amounting to around $4 million dollars, donated by agencies such as USAID and the European Commission.[28]

2015

Since 2015, CISCO's Tactical Operations team has been installing WiFi networks across a total of 75 sites in Greece, Slovenia and Serbia to provide connectivity for refugees on the move. According to CISCO, their cloud security software blocks an average of 2,000 cyberthreats per day: "as cyberthreats are becoming more advanced and prevalent, and data privacy and protection is vital for the refugee population, the importance of building cybersecurity protections into the network architecture cannot be understated."[29]

2014.10

In October 2014 the Syrian Electronic Army hacked the official UNICEF Twitter page, sending out seven tweets and changing the cover photo on the account. The tweets described the bombing attack on a school in Homs by the "moderate opposition." UNICEF quickly noticed the tweets and deleted them, and publically attributed the hacking to the SEA.[30]

27. Parker, B. (November 2017) "Security lapses at aid agency leave beneficiary data at risk," The New Humanitarian. https://www.irinnews.org/investigations/2017/11/27/security-lapses-aid-agency-leave-beneficiary-data-risk, accessed July 2018.
28. Ibid.
29. Ramrayka, L. (March 2017) "Company focus: Delivering Critical Cybersecurity for Refugees," News Deeply. https://www.newsdeeply.com/refugees/articles/2017/03/02/company-focus-delivering-critical-cybersecurity-for-refugees, accessed July 2018.
30. Jha, A.K. (October 2014) "UNICEF's Twitter Account hacked by Syrian Electronic Army," Tech Worm. https://www.techworm.net/2014/10/unicef-twitter-account-hacked.html, accessed July 2018.

Why are cyber attacks against humanitarian organizations increasing?

"Data allows you to do things at scale, whether that be help people or harm people, even at a population level."- Interviewee

Civil society has always been targeted by powerful state or non-state actors for surveillance and intelligence gathering because of the nature of their work. However, this has shifted from traditional methods such as planting spies in organizations to the new medium of cyber attacks. In John Scott Railton's report, he notes two reasons that certain governments target civil society targets civil society with cyber attacks:[31]

1 Domestic and foreign civil society can be seen as a threat to a regime by exposing corruption and other "cover ups" and abuses of power, and for "mobilizing people into organized opposition."

2 Civil society can be seen as an extension of the West and therefore embody Western interference into local affairs. This has serious implications for humanitarian organizations who are operating in areas where they are not welcome, such as the Syrian imposed ban on the provision of aid to opposition held areas.[32] Another hostile actor is Boko Haram (considered a terrorist group by the US) operating in areas around Nigeria, whose mandate is to target anything deemed "western."[33]

Other reasons include:

"If you collect it, they will come."- John Scott Railton

3 Humanitarian organizations are relying on and collecting more data regarding social media, biometrics, and financial information to deliver aid. However, the gaps between these new practices and legal and ethical frameworks, along with the lack of professional skills in digital data management, are a "disaster waiting to happen."[34] One audit of an international organization found that their web-based computer system did not adequately protect sensitive personal data, and could put vulnerable people at risk. An expert in data protection noted that storing a large amount of personal information in one database was "alarming" and made this sort of computer system a "natural target."[35]

31. Hulcoop, A. et al. (May 2017) "Tainted Leaks: Disinformation and Phishing With a Russian Nexus," The Citizen Lab. https://citizenlab.ca/2017/05/tainted-leaks-disinformation-phish/#part4, accessed August 2018.
32. Borger, J. (April 2014) "Syria: UN urged to defy Assad on aid or risk lives of hundreds of thousands," The Guardian. https://www.theguardian.com/world/2014/apr/28/legal-experts-urge-united-nations-ignore-assad-ban-aid-syria-rebels, accessed July 2018.
33. "Who are Nigeria's Boko Haram Islamist Group?" (November 2016) The BBC. https://www.bbc.com/news/world-africa-13809501, accessed July 2018.
34. Scarnecchia D.P. et al. "A Rights-based Approach to Information in Humanitarian Assistance". PLOS Currents Disasters. 2017 Sep 20 . Edition 1. doi: 10.1371/currents.dis.dd709e442c659e97e2583e0a9986b668, accessed July 2018.
35. Parker, B. (January 2018) "Exclusive: Audit exposes UN food agency's poor data-handling," The New Humanitarian. https://www.irinnews.org/news/2018/01/18/exclusive-audit-exposes-un-food-agency-s-poor-data-handling, accessed July 2018.

"Every time you see a major conflict, humanitarian data is of prime importance to the warring parties."- Interviewee

4 The data that humanitarian organizations collect and store can be valuable to malicious actors and harmful to beneficiaries. Data breaches can benefit a range of actors, from states to criminal organizations with financial motives. Although humanitarian organizations may determine that the data they are collecting is not enough to identify or cause beneficiaries harm, it can be combined with other data sets in a way that can, and is hard to predict: dubbed the mosaic effect.[36] NGOs are increasingly seen as legitimate surveillance targets because they can "go where the intelligence community can't", and even if they could, accessing existing lists is cheaper than recreating them. States currently have the capabilities to fuse together humanitarian datasets to inform their military operations, and in the future more non-state actors will acquire the capabilities to analyze data in a similar way. Furthermore, potentially dangerous data for beneficiaries extends beyond just personally identifiable data, like names, date of birth, and gender. Demographically identifiable data that can identify entire communities and villages, and real time data on their location (such as the coordinates of refugee camps) is even more valuable for malicious actors.

5 In recent major conflicts strategic targeting of civilians has increased with seemingly no consequences. The nature of warfare has moved away from legal obligations to avoid harming civilians, enshrined in International Humanitarian Law. For example, the use of hunger and famine as a military tool drives populations to relocate. Humanitarian data that outlines which areas experience food insecurity and the transportation of food supplies can be translated into malicious military objectives, such as the targeting of key roads or ports. In the event of civilian targeting, humanitarian organizations collect and hold the data that indicate how successful these campaigns are by tracking human suffering. Although civilians may remain the ultimate targets, humanitarian organizations could be targeted if they are providing relief to these populations.

"You're always kind of reacting: there's no cure for everything. All they need to do is be lucky once, whereas on the defence side you need to get lucky every time."- Interviewee

6 Attackers have an unfair advantage. Humanitarian organizations are disproportionately threatened by cyber attacks when compared to states and private corporations. This is because of pressure to keep overhead costs low, and to deploy as much money as possible directly to the field to help beneficiaries. On the other hand, states and sponsored groups have enormous budgets to spend on amassing data, especially if they consider people fleeing violence to be "national security threats" or more disturbingly, potential targets.[37]

"The awareness isn't there. Security is perceived as a hassle and an impediment to development... something that prevents teams from being "agile" and able to prototype ideas quickly."- Interviewee

36. Greenwood, F. et al. (January 2017) "The Signal Code: A Human Rights Approach to Information During Crisis," Harvard Humanitarian Initiative. https://hhi.harvard.edu/publications/signal-code-human-rights-approach-information-during-crisis, accessed June 2018.
37. Tan, E. (December 2017) "The difference between Humanitarian Data Security and Corporate Data Security is…" Medium. https://medium.com/@emersontan/the-difference-between-humanitarian-data-security-and-corporate-data-security-is-11072dd4d0cf, accessed June 2018.

7 There remains a lack of awareness among humanitarian staff regarding cyber security practices. In a 2017 audit of the UNHCR, the report notes that "the majority of reported cyber-security incidents arise from a lack of awareness of information security issues among employees and others using IT systems."[38]

In many of these cases, attributing cyber attacks is very difficult and can take months. Along with political considerations, this makes it difficult for victims to condemn attackers in a timely way after attacks occur; depending on the sophistication, a forensic investigation needs to be done before someone can be definitively accused of launching the attack. To add to the confusion, attribution in cyber attacks is very difficult. For example, there are "false flag attacks" where attackers intentionally leave signals that falsely incriminate other hackers. In addition, states often use proxies in cyber attacks that are commonly criminal networks, obscuring the nature and extent of their involvement in the attack.

Considerations for the humanitarian community

"Most international staff I know who are working in the humanitarian field aren't paying attention to cybersecurity. Why is that? For starters, it's an issue rooted in the security community which humanitarians have traditionally tried to maintain at arm's length."- Elizabeth Ferris[39]

The humanitarian community has not historically focused on cybersecurity. There are multiple reasons for this: it is considered to be in the domain of security, a tricky area for organizations striving to remain neutral; because humanitarians consider themselves to be "the good guys" and therefore unlikely to become targets (although this has unfortunately been disproven by armed attacks in the physical realm); and finally, because humanitarian organizations are already under pressure and scrutiny to keep their overhead costs low, meaning less spending towards IT.[40] However, over the next five years experts predict there will be a proliferation of targeted cyber attacks against humanitarian organizations at all levels of sophistication, including the increased misuse of stolen data to scare displaced people away from refugee camps and the tracking of defectors.

"Wherever there's a conflict you will find targeted hacking. Humanitarian organizations are not really addressing this as a threat to their core mission, and yet it is."- John Scott Railton

What are the implications if this data gets compromised for vulnerable populations?

According to Emerson Tan, humanitarian data security cannot be overstated because lives are at stake when it comes to personally identifiable data of refugees, persecuted minorities, and

38. "Report of the Independent Audit and Oversight Committee, 2016-2017," (August 2017) UNHCR. http://www.unhcr.org/59c4e2147.pdf, accessed June 2018.
39. Ferris, E. (June 2014) "Why Humanitarians Should Pay Attention to Cybersecurity," Brookings. https://www.brookings.edu/blog/up-front/2014/06/02/why-humanitarians-should-pay-attention-to-cybersecurity/, accessed June 2018.
40. Ibid.

others fleeing violence.[41] For example, Syrian refugee data collected by an agency for e-voucher distribution, including names, photos, and GPS location data, could provide the Assad regime with a list of suspected people who lived in opposition held areas. These refugees could be considered rebels and targeted, or simply never be able to return home.[42]

Volker Schimmel, a staff with the UNHCR, echoes this concern in an interview, stating, "Especially in the beginning, there was—at least on the official propaganda side-a big push by Syrian authorities to pursue refugees as traitors to the regime."[43] The UNHCR is leading an initiative in Jordan where hundreds of thousands of Syrian refugees are located. The initiative uses biometric data to deliver aid. Refugees receive humanitarian aid money through an ATM (known as "cash based transfers") that scans their irises.[44]

The UNHCR operations in Jordan were deemed "unsatisfactory" overall by an internal audit in 2015, a grade also given to the "safeguarding of assets." According to the report, the UNHCR "sent Excel-based beneficiary lists to its bank on an encrypted CD. The lists were prone to manual errors and could easily have been hacked and tampered with. Similarly, the CD was not a safe media as it was vulnerable to the risk of data corruption." The report noted that this occurred because the UNHCR had not "identified and assessed the key risks pertaining to cash payments." It provided the agency with recommendations to improve the security of their cash based transfers that it has since acted upon.[45]

An audit of an international organization's management platform found that staff were collecting more personal information from beneficiaries than needed, including recording their religion-an alarming finding considering the mass violence perpetrated against Rohingya Muslims in Myanmar, a country the audit team visited.[46] There is precedent for the use of hacking to release sensitive lists, including a case that lead to the first combined charges of hacking and terrorism-something officials say "represents the increasing prominence of cyberwarfare." A hacker affiliated with ISIS hacked a private company in the United States to obtain the names and personal information of US military and government officials. This information was passed onto ISIS who tweeted the list, along with a statement that these people would be lethally targeted.[47]

Humanitarian staff are also at risk of having Humanitarian staff are also at risk of having their own identities compromised by malicious actors.This threat of harm against staff or their loved ones has serious consequences for the morale of the organization.

Biometric data of vulnerable individuals that gets in the wrong hands can be cross checked against different humanitarian datasets to create "biometric kill lists." This would endanger beneficiaries indefinitely as identifiers like irises or thumbprints cannot be changed to avoid detection. In terms of privacy, biometric data is also very useful for state surveillance purposes, and states can make requests for this information that cannot be refused.

41. Tan, E. (December 2017) "The difference between Humanitarian Data Security and Corporate Data Security is…" Medium. https://medium.com/@emersontan/the-difference-between-humanitarian-data-security-and-corporate-data-security-is-11072dd4d0cf, accessed June 2018.
42. Ibid.

BEYOND DATA BREACHES: HOW CYBER ATTACKS COULD MAKE IT MORE DIFFICULT FOR HUMANITARIAN ORGANIZATIONS TO OPERATE

"When life-saving aid isn't delivered on time and to the right beneficiaries, people can die. This dependency makes us vulnerable."- Elizabeth Ferris, Brookings Institute[48]

"Humanitarian organizations must ask, what is the worst case scenario and what are our contingency plans?" -Daniel Scarnecchia

In 2011 humanitarian scholars predicted that because of evolving technological sophistication including cyber attacks, there existed the possibility of a future "catastrophic event, which would overwhelm both national capacity and the international humanitarian system."[49] The ubiquity of infrastructure that relies on ICT (both specific to the humanitarian sector and more generally, such as airport traffic control systems or electrical power grids) and the difficulty of distinguishing between military and civilian targets can cause cyber attacks to strain the humanitarian system and paralyze disaster response. Although these attacks are unpredictable and almost impossible for humanitarian organizations to prevent, organizations should nonetheless prepare for potential disruptions.

Humanitarian organizations, like those in the vast majority of sectors, would find their ability to operate severely hindered if their Internet or servers went down in a cyber attack. For example, humanitarian aid is increasingly cash-based, relying on a technological network of digital money, mobile networks,

43. O'Donovan, C. (December 2015) "Tracking Refugees Puts A Vulnerable Population At Risk," Buzzfeed News. https://www.buzzfeednews.com/article/carolineodonovan/tracking-refugees-puts-a-vulnerable-population-at-risk, accessed June 2018.
44. Ibid.
45. "Audit of the operations in Jordan for the Office of the United Nations High Commissioner for Refugees," (June 2015) United Nations Office of International Oversight Services. https://oios.un.org/page/download/id/310, accessed June 2018.
46. Parker, B. (January 2018) "Exclusive: Audit exposes UN food agency's poor data-handling," The New Humanitarian.https://www.irinnews.org/news/2018/01/18/exclusive-audit-exposes-un-food-agency-s-poor-data-handling, accessed July 2018.
47. Weiner, R. (September 2016) "Hacker who sent 'kill list' of U.S. military personnel to ISIS: 'I feel so bad,'" The Washington Post. https://www.washingtonpost.com/local/public-safety/hacker-who-sent-kill-list-of-us-military-personnel-to-islamic-state-i-feel-so-bad/2016/09/23/dc0ba0ea-8196-11e6-b002-307601806392_story.html?utm_term=.11dcf1f8157b, accessed June 2018.
48. Ferris, E. (June 2014) "Why Humanitarians Should Pay Attention to Cybersecurity," Brookings. https://www.brookings.edu/blog/up-front/2014/06/02/why-humanitarians-should-pay-attention-to-cybersecurity/, accessed June 2018.
49. Ferris, E. (2011). "Megatrends and the future of humanitarian action," (p.923) International Review of the Red Cross, 93, pp 915938 doi:10.1017/ S181638311200029X, accessed June 2018.

online banks and ATMs, etc. Going back to the first of five rights articulated in the Signal Code, beneficiaries have the right to access, generate, communicate, and benefit from information during a crisis. This means that humanitarian organizations must consider how they will maintain this flow of information in the event of a cyber attack such as a Distributed Denial of Service. Furthermore, with increased reliance on online sources of information for disaster response coordination, organizations should consider if and how they could operate if this resource no longer existed.

Cyber attacks on critical infrastructure could have crippling effects on the humanitarian sector. They could prevent or disrupt an entire range of humanitarian activities, such as the ability of organizations to communicate with field staff; the delivery of aid into affected areas; the use of GPS technology to map a disaster response; and the maintenance of infrastructure such as hospitals and life-saving equipment. Cyber attacks of this nature would create crisis situations that are very difficult to predict or plan for. Humanitarian organizations may be faced with helping entire populations that have been plunged into darkness overnight, or handling the fallout from a chemical or nuclear accident. For example, the death toll after the 2017 Hurricane Maria in Puerto Rico was much higher than initially reported, and largely stemmed from the lack of electricity in the weeks following the hurricane.[50]

In terms of electrical power grids, US officials have warned that over the past two years, "Russian government cyber actors" have targeted "government entities and multiple U.S. critical infrastructure sectors," spanning from energy to nuclear, water and aviation.[51] According to the US Energy Secretary, cyber attacks are "literally happening hundreds of thousands of times a day."[52] This is all too familiar in Ukraine, which experienced a massive power outage in 2015, and other attacks since across almost every sector, also attributed to a foreign state.[53]

Large scale devastation could arise from the hacking of nuclear or chemical plants, which are already being scoped out by cyber attackers. In October 2017 a simulated cyber exercise took place in Sweden, where hackers flooded the cooling system of a nuclear power plant. This technically sophisticated exercise, involving the UN's International Atomic Energy Agency, demonstrated the physical damage that could be inflicted by a cyber attack on critical infrastructure.[54] It followed a real attempted cyber attack launched by sophisticated hackers against a petrochemical plant in Saudi Arabia. Investigators believe the intent of the attack was to trigger an explosion that would have likely resulted in significant casualties. The Schneider's Triconex controllers that were compromised in Saudi Arabia are also used in about 18,000 plants globally, from nuclear and water treatment

50. Kishore, N. et al. (July 2018) "Mortality in Puerto Rico after Hurricane Maria," The New England Journal of Medicine. https://www.nejm.org/doi/full/10.1056/NEJMsa1803972#figures_media, accessed July 2018.
51. Dlouhy, J. A. (March 2018) "Russian Hackers Attacking U.S. Power Grid and Aviation, FBI Warns," Bloomberg. https://www.bloomberg.com/news/articles/2018-03-15/russian-hackers-attacking-u-s-power-grid-aviation-fbi-warns, accessed July 2018.
52. Ibid.
53. Greenberg, A. (June 2017) "How an Entire Nation Became Russia's Test Lab for Cyberwar," Wired. https://www.wired.com/story/russian-hackers-attack-ukraine/, accessed July 2018.
54. Lyngaas, S. (January 2018) "Hacking nuclear systems is the ultimate cyber threat. Are we prepared?" The Verge. https://www.theverge.com/2018/1/23/16920062/hacking-nuclear-systems-cyberattack, accessed July 2018.

facilities to oil and gas refineries and chemical plants.[55] The United States has experienced an ongoing hacking of companies' computer networks that operate nuclear power stations such as the Wolf Creek Nuclear Operating Corporation in 2017. Although Wolf Creek officials claimed that no operations systems were breached and there was no threat to public safety, investigators reported that hackers tried to map out computer networks for future attacks.[56]

Aside from an increasing reliance on technology, digital humanitarians also tap into a supply chain of user-generated content to acquire information and make decisions. This user-generated content makes humanitarian organizations susceptible to cyber attacks because of the dangerous assumption that all actors using a system are trustworthy and that upstream data doesn't need to be checked for malicious content as it comes in. False, or unverified reports, could be part of a calculated strategy to confuse or spread misinformation. There remains a tension between releasing information in a timely fashion with the amount of vetting that needs to be done.

55. Perlroth, N. & Krauss, C. (March 2018) "A Cyberattack in Saudi Arabia Had a Deadly Goal. Experts Fear Another Try," The New York Times. https://www.nytimes.com/2018/03/15/technology/saudi-arabia-hacks-cyberattacks.html, accessed July 2018.
56. Perlroth, N. (July 2017) Hackers Are Targeting Nuclear Facilities, Homeland Security Dept. and F.B.I. Say," The New York Times. https://www.nytimes.com/2017/07/06/technology/nuclear-plant-hack-report.html, accessed July 2018.

WHAT STEPS CAN HUMANITARIAN ORGANIZATIONS TAKE TO IMPROVE THEIR CYBERSECURITY PRACTICES?

According to researchers, cybersecurity is most accurately conceptualized as a holistic and comprehensive strategy where all of an organization's functions and procedures are designed to protect critical information.[57] Therefore, there needs to be a coordinated plan across entire organizations to improve cybersecurity.[58] These plans should be assessed as broad and reinforcing systems (overlapping layers of defence), not by individual features.[59] Organizations should have a realistic and simple cybersecurity "roadmap" that will be implemented within a set timeframe and that can be clearly communicated to all staff.[60] Furthermore, organizations should be continuously reviewing and evaluating their cybersecurity practices.

1. Conduct risk assessments

An important place to start when designing a new program or collecting data in the field is to create a risk assessment. Threat modeling is a similar practice and a term used by the security community, where each identified threat is matched with mitigation measures. It is commonplace in the private sector but needs to be adopted by the humanitarian community in a formalized fashion. This is important because cybersecurity practices are context specific and will look different for every humanitarian organization in different scenarios.

- Risk assessments should be informed by input from locals in the region where organizations are operating. Risk assessments should include considerations such as: the types of data being collecting; extent of damage if data is improperly accessed; actors who could benefit from gaining access to data; potential methods of accessing data; and current safety protocols. Risk assessments should be repeated at regular intervals proportionate to the level of risk initially assessed.

    1. Understand the spectrum of risk for potential data breaches. The implications could vary from monitoring financial statements more closely to concern for the lives of field staff and/or beneficiaries.

57. Bailey, T., Kaplan, J.M., & Rezek, C. (July 2015) "Repelling the cyberattackers," McKinsey. https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/repelling-the-cyberattackers, accessed July 2018.
58. Choi, J. et al. (July 2017) "Hit or myth? Understanding the true costs and impact of cybersecurity programs," McKinsey. https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/hit-or-myth-understanding-the-true-costs-and-impact-of-cybersecurity-programs, accessed July 2018.
59. Bailey, T., Kaplan, J.M., & Rezek, C. (July 2015) "Repelling the cyberattackers," McKinsey. https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/repelling-the-cyberattackers, accessed July 2018.
60. Choi, J. et al. (July 2017) "Hit or myth? Understanding the true costs and impact of cybersecurity programs," McKinsey. https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/hit-or-myth-understanding-the-true-costs-and-impact-of-cybersecurity-programs, accessed July 2018.

2. Risks should be assessed against benefits that the project would deliver. For example, organizations should consider what harm beneficiaries would experience if a specific project or technology was not used at all.

- Instead of trying to protect everything, identify what the most sensitive data is and prioritize cybersecurity practices accordingly. Data can be categorized into levels such as "public", "private", and "classified" information. Each level of data categorization should correspond to a checklist of security features.

Insights from the risk assessment can inform what the appropriate balance between security and functionality should be. It is important to not become overly fixated on the very rare but crippling attacks, such as those conducted by warring parties. A more common and non-technical risk involves the physical seizure of equipment where data is stored, such as laptops. Humanitarian organizations that cross between checkpoints where this activity is reported must consider how to mitigate against this risk.

"If you make your security 100%, you won't be operationally functional. So you have to find a middle ground."- Interviewee

2. Build capacity: Staff expertise and training

"Organizations have a surprisingly high rate (from 40-60%) of their staff falling for targeted suspicious links and messages. This is true across sectors, including in the humanitarian space."- John Scott Railton

According to McKinsey, almost 80% of technology executives surveyed reported that their organizations could not keep pace with the increasingly sophisticated technology utilized by attackers.[61] Data hygiene practices can be easily improved through increased training for humanitarian staff and can go a long way (the Red Rose leak was attributed to a simple password issue).

- A culture of data security needs to be widespread in the organization. Everyone is a data steward and responsible for the organization's cybersecurity, not just the IT department.

1. Staff should be aware that even if they are not a conspicuous or high-profile member of the organization, they may be targeted as a means of hacking or surveilling someone of interest in the organization. The targeted person will have much lower scrutiny regarding materials that come their way from a trusted or internal colleague. In the hacking of the Democratic National Committee, campaign chairman John Podesta was targeted as a method of entry to get to presidential nominee, Hillary Clinton.

---

61. Bailey, T., Kaplan, J.M., & Rezek, C. (July 2015) "Repelling the cyberattackers," McKinsey. https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/repelling-the-cyberattackers, accessed July 2018.

2. Cybersecurity measures can be seen as cumbersome steps that slow down the ability of the organization to function. However, the easier it is for staff to access the data they are working with, the easier it is for external actors to as well.

- Promote password safety. If staff are using weak passwords, or an all-purpose password, then all other efforts for security may be undermined.

  1. Passwords should be updated every six months and different ones should be used for different purposes. One option to keep track is using a "password manager" which is stored on an encrypted cloud. Another option is to create passwords with sufficient complexity from the beginning, such as a "passphrase": a combination of a few words that make sense to the user but are otherwise illogically and randomly connected. For example, a combination of four different favourite books and movies would read: "outsiders 1984 dracula rent." According to one estimate, this passphrase would take 24,471 centuries to crack.[62]

  2. One misconception is that administrative users have to use the "administrator" user log in, as the default setting does. In fact, this should be changed as soon as possible.

  3. Two- (or multi-) factor authentication provides a second layer of security beyond entering one's username and password to access an account.

  There are different types of two-factor authentication that can supplement a username and password with varying degrees of security. They include a physical key that plugs into a USB port; a one-time password app; an SMS-based text message; and biometric ID.[63] These methods have different pros and cons, but the latter two are considered the least desirable for various reasons. SMS is discussed further below.

- Provide ongoing training for staff to minimize "internal vulnerabilities."[64] These practices should be well integrated into the organization's daily operations.[65] Staff should be encouraged to request assistance or advice whenever necessary, and be given practical and realistic steps to follow.

- Stay up to date. Staff with the highest proportion of cybersecurity related responsibilities must keep themselves informed and communicate main points to the rest of the organization. This may include networking with others across humanitarian organizations;

62. Hearn, M. "Why should I use a random passphrase?" https://www.useapassphrase.com/, accessed September 2018.
63. "What is the best type of multi-factor authentication for me?" Access Now. https://www.accessnow.org/cms/assets/uploads/2017/09/Choose-the-Best-MFA-for-you.png, accessed July 2018.
64. Choi, J. et al. (July 2017) "Hit or myth? Understanding the true costs and impact of cybersecurity programs," McKinsey. https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/hit-or-myth-understanding-the-true-costs-and-impact-of-cybersecurity-programs, accessed July 2018.
65. Bailey, T., Kaplan, J.M., & Rezek, C. (July 2015) "Repelling the cyberattackers," McKinsey. https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/repelling-the-cyberattackers, accessed July 2018.

subscribing to newsletters from IT security companies; or simply following them on social media to stay informed of the most important highlights regarding vulnerabilities or new attacks.

- Consider external hires. Humanitarian organizations must first determine whether hiring a cybersecurity professional is realistic and affordable. Ideally this person would have experience or knowledge of the humanitarian sector as well. In the private sector it is customary to have a position called the "chief information security officer" (CISO) who oversees all things cyber. Humanitarian organizations may be able to fill this role from "nontraditional talent pools" such as recruits from the military or intelligence communities, or skilled problem solvers from within in the organization.[66]

- Foster a diverse team with different perspectives. Staff from various backgrounds within the organization could contribute unique considerations to the cybersecurity conversation, as this topic crosses many domains beyond ICT such as politics, policy, data collection and analysis. A diverse team would also provide broader insights into social engineering threats. A team can be considered 'diverse' when it is comprised of multiple, distinct cultural backgrounds and has gender parity.

3. Partner with the private sector when the benefits outweigh the risks

Partnerships with the private sector can provide the knowledge and expertise humanitarian organizations need, especially on a short term basis or in an emergency. However, these partnerships should not be seen as scalable long term solutions to secure humanitarian organizations. They are not a substitution for improving internal cybersecurity practices. It is also important for humanitarian organizations to realize that the private sector is motivated by profit, not necessarily by humanitarian principles.

- The first step is determining whether there are open source tools available, and whether there are free or affordable services that private companies provide to humanitarian organizations. There are also a number of non-profit organizations that specialize in helping civil society with cybersecurity.

- Experts from the private sector can be very helpful in implementing cybersecurity best practices, and it is beneficial to have one staff oversee this process rather than multiple part time staff. However, whether or not these cybersecurity practices are effective depend entirely on whether organizations continue to implement them on their own.

- When partnering with the private sector, humanitarian organizations should keep certain things in mind, such as remaining in control of data: how much data will the company have

66. Ibid.

access to, and hold on to after the partnership? The concept of sparsity (for organizations to only collect and keep the minimum amount of beneficiary data that is needed: practices that also reduce liability), goes against collecting large data sets that companies require for advanced analytics and Artificial Intelligence.

- ***"We are trading data with the private sector to get free stuff."- Nathaniel Raymond***
  Humanitarian organizations partner with large private companies such as Google and Digital Globe to aggregate and analyze the data they collect. This means that beneficiaries' data are being commodified without their informed consent, and will serve as "training data" for these companies. The commodification of beneficiaries' information to help private companies make money is not in line with the humanitarian principles of impartiality and independence.

Furthermore, humanitarian organizations may lose control over what their aggregated data will be used for. For example, if humanitarian data provides insights into behavioural patterns of a certain population, companies can potentially sell this data to other clients such as the military or defence contractors, looking to develop weaponry with more accurate targeting. Palantir is considered a potentially useful data analytics tool for humanitarian organizations, while its primary objective is "as a multidiscipline U.S. defense and intelligence agency data aggregator."[67]

- Humanitarian organizations should consider how important principles are conceptualized in the private sector. This includes informed consent versus a simplistic understanding of consent; what is considered an acceptable level of risk for beneficiaries; and what is an acceptable rate of failure.

- Private companies working on a "pro bono" basis, and without a formal agreement may not be a reliable source of support over time. They can see a change in leadership to someone less inclined to help humanitarian organizations.

- There is an excitement towards data collection and technology among humanitarian organizations that can be slightly naive. Funders are under pressure to look innovative and forward thinking, leading to investments in risky and exciting new technologies. However, there needs to be more investment in the capacity to secure existing technologies, which may not necessarily come from the private sector.

  "The tech world has recognized the humanitarian space as a consumer with deep pockets." -John Scott Railton

67. Williams, P. & Fiddner, D. (August 2016) "Cyberspace: Malevolent Actors, Criminal Opportunities, and Strategic Competition," (p. 332) United States Army War College Press. https://ssi.armywarcollege.edu/pdffiles/PUB1319.pdf, accessed June 2018.

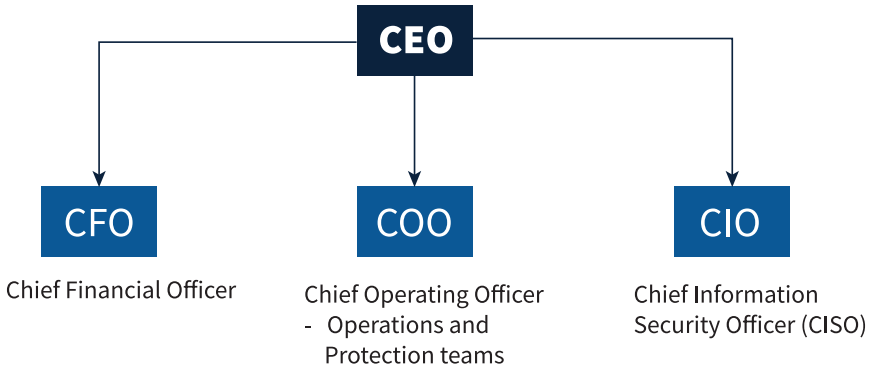
4. Change the organizational structure

"Technical capacity usually isn't the main problem. The broad issue is that you don't have the governance structures in place to properly manage the technical capacity or the data that the organization holds. Leadership and management don't have an understanding of this or the potential ethical issues: this may be through no fault of their own, but it hasn't been prioritized yet." - Daniel Scarnecchia

"It's not just technical- it's deeply organizational. If you stick to the technical, it will enable leadership to kind of step back."- John Scott Railton

Increase the communication between cybersecurity professionals such as the IT department and the head of organizations like CEOs (or the equivalent). This is required for both sides to compromise regarding their interests: maximizing security and managing operations, respectively.[68] It also allows organizations to coordinate and respond more rapidly when necessary, such as in the case of a cyber attack.[69] This can be achieved by developing more streamlined communication and the regular reporting of risk levels and the status of cybersecurity systems from IT to the decision makers. IT professionals should ensure that cybersecurity jargon is made easy for non-technical staff to understand.

Many humanitarian organizations have the same structural hierarchy as for-profit corporations. This structure silos different employees who need to be communicating better. Overall, employees in charge of the protection of beneficiaries and information security should both have better communication flows with top decision makers. The link from IT to the top is especially important because IT staff may not realize that the threats they are detecting are related to political threats or geopolitical events in the region they are operating in, a connection that leaders of the organization can provide.



68. Choi, J. et al. (July 2017) "Hit or myth? Understanding the true costs and impact of cybersecurity programs," McKinsey. https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/hit-or-myth-understanding-the-true-costs-and-impact-of-cybersecurity-programs, accessed July 2018.
69. Bailey, T., Kaplan, J.M., & Rezek, C. (July 2015) "Repelling the cyberattackers," McKinsey. https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/repelling-the-cyberattackers, accessed July 2018.

This is the traditional hierarchy of organization. To build an organizational culture of cybersecurity, the CISO should be part of the protection team and communicate more with the COO and the CEO. The CISO should be able to halt new programs and data collection practices that put beneficiaries at risk. This would help ensure that organizations embed digital security within their humanitarian initiatives.

5. Improve the basic standards of cybersecurity practices

Humanitarian organizations should never compromise on IT Security in the rush to "get things done." We may rush into a digital solution that in the end just worsens the problem we are trying to resolve."- Interviewee

"It always starts with a trickle, but you can spread this cost over the entire sector rather than specific organization if you establish a minimum set of technical standards."- Daniel Scarnecchia

- Keeping track of data is difficult but necessary. Digital information is "non-rivalrous", meaning "it can be copied and used by more than one person (or algorithm) at a time." Unlike other commodities, the non-rivalrous nature of data makes it easy to use for unintended purposes, and it is not always clear to owns it.[70]

  > There is currently a lack of oversight within organizations. Organizations need to know exactly what data they are in possession of and where it is stored. It is easy for different staff to make copies of an Excel spreadsheet, and for the organization to lose track of all the copies that exist.

- Penetration testing, also referred to as red teaming (when you attack your own system/network/data to see what the vulnerabilities are), can ultimately strengthen an organization's cybersecurity.[71] Until this testing is conducted, the humanitarian sector will not necessarily be aware of vulnerabilities in the software being used. Experts have noted that had Red Rose conducted penetration testing, they would have likely identified and removed the vulnerabilities that Mautinoa was able to exploit.

- Loading tests can determine the loading time of different pages. This is important in determining whether the pages can handle extreme traffic in the case of an emergency, such as a page with a list of local hospitals after a natural disaster. If these pages are identified beforehand, a cache system can be installed that will manage heavy traffic without paralyzing the web page.

---

70. "Data is giving rise to a new economy," (May 2017) The Economist. https://www.economist.com/briefing/2017/05/06/data-is-giving-rise-to-a-new-economy, accessed July 2018.
71. Lyngaas, S. (January 2018) "Hacking nuclear systems is the ultimate cyber threat. Are we prepared?" The Verge. https://www.theverge.com/2018/1/23/16920062/hacking-nuclear-systems-cyberattack, accessed July 2018.

- Do not neglect the security of smartphones. Experts predict that mobile phones will be the most popular mode of cyber attacks in the future, as they can easily be turned into surveillance tools and are accessible to large amounts of information resources. However, there is still a widespread belief that these devices are better protected and less targeted than other devices, leading more people to focus on securing their laptops and neglecting their mobile security. As hackers move from baiting users with fake apps containing malware to launching back-end attacks through mobile operating systems like iOS and Android, these attacks will become more difficult to defend against or even detect.[72]

> The recent hacking of Reddit's SMS two-factor authentication system serves as a reminder that if an SMS text message is intercepted, this authentication system can be easily overcome.[73] Reddit used this log-in system for staff members, requiring them to enter a one-time passcode sent to their phones along with their username and password. Once hackers gained access to the phone numbers, they were able to access to usernames, passwords, and email addresses.

> There are many reasons why using SMS as a secondary authentication step is not ideal in terms of privacy and security.[74] Attackers can access text messages by counterfeiting SIM cards, infiltrating phone carriers, or rerouting text messages in transit. Civil rights activist DeRay Mckesson had his email addresses and Twitter account breached after hackers called his phone carrier and successfully reset his SIM by impersonating him. Hackers then received the SMS text message meant for Mckesson and bypassed his two-factor authentication.[75]

- Prioritize system maintenance.

"Once a security patch is released to fix a critical vulnerability, you should apply it within a couple hours, or else you'll be compromised within about a day."- Interviewee

1. Systems need to be kept up-to-date. The latest version of a software package should be installed to protect from security vulnerabilities that may exist in older versions; where it is not feasible to run the latest version of the software the latest security patches released by vendors must be applied. The defaults on packaged software should always be updated (e.g., default password).

---

72. Glassberg, J. (August 2018) "3 trends hackers at Black Hat and DEFCON are watching," Yahoo Finance. https://finance.yahoo.com/news/3-trends-hackers-black-hat-defcon-watching-104212581.html, accessed August 2018.
73. Gibbs, S. (August 2018) "Reddit user data compromised in sophisticated hack," The Guardian. https://www.theguardian.com/technology/2018/aug/02/reddit-user-information-usernames-passwords-email-addresses-hack, accessed August 2018.
74. White, N. & Li, A. (December 2017) "We need to talk...about SMS-based two step authentication," Access Now. https://www.accessnow.org/need-talk-sms-based-two-step-authentication/, accessed July 2018.
75. Conger, K. (2016) "How activist DeRay Mckesson's Twitter account was hacked," Tech Crunch. https://techcrunch.com/2016/06/10/how-activist-deray-mckessons-twitter-account-was-hacked/, accessed July 2018.

2. Due to the grant-based nature of humanitarian organizations, it is common practice to purchase a computer system and then customize it. It is important for organizations to also budget for the ongoing maintenance of programs and software to keep them up-to-date.

- Take advantage of audits and checklists

  1. Audits should be conducted at least once a year by a party unrelated to the operations or development teams.

  2. Security audits and checklists should be integrated into the initial planning stage of any new product to ultimately save time. Once the product is already built, implementing security checklists may no longer be feasible for humanitarian organizations. One way to complete the checklist process more efficiently includes automating, such as setting up automated weekly reports; configuration management; and the application of a patch after a security release.

  3. Determine how often the checklist needs to be updated, and schedule time and assign responsibility for making the necessary checks on defaults.

  4. If possible, apply a higher level of security protection than is required for a specific type of data, as long as this does not inhibit the functioning of the organization.

- Use open source tools with an active community and commitment to security, which is possible for any budget. More information is provided in the Annex.

"It's worth it and it's okay to go slowly. Don't be too overwhelmed by these security checklists. You can implement them slowly and methodically (for example, try to check off 2 new security features per month)."- Interviewee

6. Increase responsibility on donors for security funding and reducing stigma

Humanitarian staff are stretched thin as they typically work in dangerous and hostile environments. The responsibility for prioritizing cybersecurity should be placed on donors and the decision makers.

- Funding around cybersecurity needs to increase. Educating donors on cybersecurity threats is one way to ensure funding for this measure becomes a core part of budgeting. Funding for the physical safety of humanitarian staff was also once neglected, but attitudes have changed dramatically since then.

1. *"Organizations must say, "I can't do this job anymore as I would like to because I'm constantly hindered in my mission because of these new threats. I need money, people, and policy." All things are required, kind of a "self help.""- Interviewee*

2. *"The ongoing cost of checking backups and performing disaster recovery tests does not get budget allocation; or staff time priority."- Interviewee*

3. Funding earmarked for cybersecurity should consist of a guaranteed minimum amount. Donors must accept that this is a new budget line, and funding for cybersecurity should not vary based on whether or not an organization has been the victim of a cyber attack in the past.

There is a hard balancing act between being transparent about security, versus trust, brand, and reputation concerns. If you get security wrong and announce a breach, this hurts your brand. In many cases, management would likely not want to publicize a leak/attack."- Interviewee

- Funders should reduce the stigma of reporting. Commend the IT department for identifying the hack and responding, instead of stigmatizing organizations for reporting the cyber attack (which is virtually inevitable to happen at some point).

- Critical incident reporting needs to become more mainstream, but how this should be operationalized remains up for debate. Funders need to make the disclosure of an attempted or successful cyber attack more feasible for humanitarian organizations, such as providing more money after the incident for damage control. Unlike other sectors, there is no legal requirement for humanitarian organizations to disclose this information, nor is there yet an ethical norm. In this unregulated environment, it is important that humanitarian organizations feel supported in disclosing to their funders when an attack has happened, and share best practices with others.

    1. There is ongoing debate as to who should be included within the circle of trusted people privy to the critical incident reporting, as transparency must be balanced with avoiding further harm to beneficiaries. For example, reporting an incident of a state-sponsored cyber attack should not provide a playbook for other governments looking to do the same thing. Ideally, the humanitarian sector would develop an ombudsman type entity or a neutral forum for critical incident reporting.

    2. Some experts argue that funders should make critical incident reporting mandatory to improve transparency, by stipulating it in their terms when they provide grants. Others worry this will cause organizations to downplay incidents.

    3. Some experts feel that sharing critical incident reporting within the humanitarian sector will come about organically with the maturity of the field. For example, the financial sector is much more developed in this kind of sharing, but as long as the industry has existed they have dealt with fraud in some form. A level of inevitable financial loss is acknowledged, not stigmatized.

- As long as humanitarian organizations view the data they hold as a competitive advantage for obtaining continued and increased funding, they will not share this data or information with others. Donors should address this obstacle by encouraging humanitarian organizations to develop data sharing policies.

"You can't get to true sharing as long as humanitarian organizations think it's an existential risk to share with other organizations."-Interviewee

7. Improve communication and coordination between humanitarian organizations

- Humanitarian organizations should share information regarding cyber attacks, especially with organizations that have less resources and capabilities. An alert in the sector may prompt others to pay closer attention and investigate whether they have already been hacked. There is currently no early warning system of a potential cyber attack, meaning multiple humanitarian organizations can be exploited by the same vulnerability.

    1. This would help track cyber attacks and trends. When organizations in Ukraine were affected by foreign hacking campaigns, they realized once they started communicating with each other that they were all affected by a common vulnerability.[76]

    2. There are ways organizations can share helpful information with each other without giving away too much information. For example, they can share what their updated cybersecurity defensive practices are, without necessarily sharing that they have been attacked. They can also share information about the latest security patches.

- There is a lot of "snake oil" in the private security industry. Humanitarian organizations should share information on which private companies are the most helpful and effective, especially those that successfully managed to thwart an attempted cyber attack.

    "They all say do no harm. You can't do no harm if you don't know what the harms are."-Nathaniel Raymond

- Increased communication and collaboration between humanitarian organizations would increase awareness regarding cyber threats common to certain regions and conflicts.

76. Greenberg, A. (June 2017) "How an Entire Nation Became Russia's Test Lab for Cyberwar," Wired. https://www.wired.com/story/russian-hackers-attack-ukraine/, accessed July 2018.

8. Improve data policy as a whole and be consistent

"Don't make it easy for the bad guys."- Interviewee

- There is an ongoing tension between collecting more data with detailed breakdowns to deliver individualized aid to beneficiaries, and collecting less data but providing more generic and potentially mismatched aid. For example, in-depth needs assessments shed light on communities such as those with disabilities or different ethnic groups. This balance must be debated within organizations and reflected in their data policies.

- At minimum this should include clear policies around how much and what type of data should be collected and stored, especially when responding in areas with heavy government surveillance or when there is likely to be pushback for political reasons. These decisions should not be left to front line staff: many of the decisions on what data to collect are currently being made in the spur of the moment.

- Humanitarian organizations should have a clear data retention policy. Humanitarian organizations need to either protect or destroy sensitive data that could be useful militarily, to ensure that the amount of harm compromised data can do is minimal.

- Develop a policy around data sharing. This should include constraints around sharing sensitive data and data anonymization practices. Humanitarian organizations need to take precautions when partnering with other organizations that might not have adequate cybersecurity defenses on their platforms. This should also serve as an incentive for strong cybersecurity practices, as organizations may stop receiving information from partners if they are seen as negligent with data.

  > Staff should know what their roles are and decision making capabilities around sharing data. This may protect them if they are not given such privileges: if an external source is applying pressure on them to share data, they are protected by their organizational policy and can instead forward the request to their superiors.

- Organizations should have a good data backup policy and a recovery policy in the case of lost data. Data should be stored offline with regular back ups.

- Determine the PTO (point in time recovery) and RTO (recovery time objective). In the case of data loss this will inform what time stamp of the data it should be replaced with and how quickly this replacement must happen.

- Develop data anonymization practices so that the data used by the organization is less risky for beneficiaries.

- Develop safe on-boarding and off-boarding practices for personnel, so that sensitive information is not leaving the organization and all new staff are trained in relevant policies.

9. Develop an emergency contingency plan

- Know what to do if you were hacked. This includes knowing who to contact in your organization and what to do with the affected infrastructure. Know what external organization can be contacted for assistance.

- A denial of service attack can be especially disruptive in a time of high traffic, such as during a disaster response when other organizations or beneficiaries may need to access real time data. One option is to serve critical information through alternate websites.

- The majority of humanitarian organizations do not have the technical capacity to recover from a cyber attack in a timely manner to minimize damage.

"Disaster recovery exercises are generally deprioritized in favour of building new features. There is a "set and forget" mentality prevalent in organisations."- Interviewee

- Actively monitor for attacks. This includes:

  1. Watching the error logs on servers, and reading the reports. Ensure your server logs provide a list of successful logins and failed login attempts. Check for suspicious activity such as an unauthorized person signing in under "test" or "admin."

  2. Get reports on incidents where people tried to access the website in a way that mimics a known vulnerability (something that has already been patched). This does not necessarily mean that the organization was specifically targeted: it could be automated bots simply scanning through websites to probe which one has a vulnerability.

- If a cyber attack has been verified: respond.

  1. Shut down the service and get it offline by immediately unplugging the server from the network until it can be analyzed by a professional, such as a forensic analyst. Once the compromised system is isolated it can no longer be controlled remotely.

  2. Determine the nature of the attack: is the software that runs the server under attack (more serious implications) or the website?

  3. If a website has been taken down, determine what to safely back it up with. One option is the original code stored in source control (a location where only developers can modify).

  4. Go through the audit logs in detail to get more information about how the attack happened.

5. The forensic analyst will provide more information about the attack, such as whether a data breach occurred. In this instance, an organization would follow their data policy procedures, which involves determining what data was stolen and which beneficiaries need to be notified.

"After a data breach the worst thing you can do is pretend it never happened and never notify anyone."- Interviewee

- Practice with drills to prepare. A lack of preparedness mixed with adrenaline can lead to poor decision making in emergency situations.

WHAT NOT TO DO

1. Address cybersecurity by introducing new technologies

"We cannot code our way out of this. We need to know how to use the technologies we already have."- Nathaniel Raymond

Sean McDonald cautioned that technology was "only one piece of the puzzle", despite the fact that some are attempting to "code around the difficult process of building shared cultural and operational infrastructure."[77] There can be an attraction towards new and disruptive technologies in the humanitarian field, but that will not address the underlying problem of cybersecurity.

In terms of new technology, there needs to be a greater respect for humanitarian principles and standards in the design and development process so that cybersecurity considerations do not have to be retroactively applied. New technology that has the potential to improve cybersecurity, if handled properly, include blockchain and new methods of encryption.

> ***"Secure practices are feasible for humanitarian organizations to implement, but they are usually not top-of-mind when staff are developing and building a new product. As a result, products need to be retrofitted to add security features in, which can be a lot more expensive than adding in the necessary checks up front."- Interviewee***

77. Parker, B. (January 2018) "Exclusive: Audit exposes UN food agency's poor data-handling," The New Humanitarian. https://www.irinnews.org/news/2018/01/18/exclusive-audit-exposes-un-food-agency-s-poor-data-handling, accessed July 2018.

2. Wait until there is a serious breach of trust in the humanitarian sector

"It's going to take the data version of 9/11 for us to have this conversation: a Goma level incident."- Nathaniel Raymond

Trust is slowly gained and quickly lost. As affected populations become more technically sophisticated, their understanding and awareness of the risks associated with their data increases. Because humanitarian organizations are stewards of this data, maintaining people's trust in their ability to handle it properly is critical. Humanitarian organizations should be proactive about ensuring that a high profile event does not occur that would put lives at risk and compromise the sector's long term viability.

3. Adopt a one size fits all approach

Find a balance between cybersecurity measures that do not slow down innovation or hinder the ability for users to access the product. More security is not always the right answer. For example, password protection on medical equipment in emergency rooms imposes a time delay that would result in lives lost. However, it is important to note that some level of hinderance is inevitable while new policies are implemented, such as rules around passwords and access rights.[78]

4. Become overwhelmed

"There is no bad investment. Nation states start with the basic, cheap stuff when they want to hack."- Interviewee

Both the media and the security industry can overwhelm the public and civil society into thinking that cyber attacks are inevitable and resistance is futile. However, even moderate improvements to cybersecurity practices can go a long way. Malicious actors are using their least sophisticated tools because these are sufficient. This can be compared to the panic and international attention paid to Ebola, when from a public health perspective the common cold is responsible for far more deaths.[79] Organizations may not be able to ward off a zero day attack, but there are many other empowering steps they can take that will repel the majority of attacks.

---

78. Bailey, T., Kaplan, J.M., & Rezek, C. (July 2015) "Repelling the cyberattackers," McKinsey. https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/repelling-the-cyberattackers, accessed July 2018.
79. Bollier, S. & Haddad, M. (December 2014) "Infographic: Just how deadly is Ebola?" Al Jazeera. https://www.aljazeera.com/indepth/interactive/2014/08/infographic-deadly-ebola-epidemic-west-africa-20148248162913356.html, accessed July 2018.

CONCLUSION

As the data economy continues to grow and integrate into the world economy, the humanitarian sector exists within the context of this trend. Market research firm IDC predicts that by 2025 the data created and copied every year, called the "digital universe", will reach 180 zettabytes: 180 followed by 21 zeros.[80] The humanitarian sector has been using digital data such as Excel spreadsheets for many years and will likely continue to do so for many more; the novel use of sources of data such as biometrics, social media data, and Call Detail Records will provide humanitarian organizations with new insights.

However, the public's awareness of the tradeoffs inherent in the increased use of data is also increasing. As Bruce Shneier puts it, data is a "toxic asset" because the longer it is in one's possession, the greater the liability. Companies and both domestic and foreign governments want access to it, and it is very difficult to secure from motivated attackers or employee error.[81] Risks of data breaches range from public embarrassment; expensive lawsuits; and criminal charges for private companies: and as humanitarians have noted, extends to real harms for affected populations. There are different ways to mitigate against these risks that humanitarian organizations can employ, from collecting less data to begin with; deleting data that is no longer necessary; and using more cybersecure practices.

80. "Data is giving rise to a new economy," (May 2017) The Economist. https://www.economist.com/briefing/2017/05/06/data-is-giving-rise-to-a-new-economy, accessed July 2018.
81. Schneier, B. (March 2016) "Data is a toxic asset, so why not throw it out?" CNN. https://www.cnn.com/2016/03/01/opinions/data-is-a-toxic-asset-opinion-schneier/index.html, accessed July 2018.

ANNEX

A summary of threats

There is a wide range of cyber attacks that will affect different staff to varying degrees. Most attacks are launched with a low level of sophistication and involve social engineering, such as phishing emails or texts that are tailored to look legitimate to the receiver. The following is not a comprehensive list of threats, which are constantly evolving, but rather a highlight of the most common and their characteristics.

• Faulty passwords

Automated bots can enter different combinations of passwords at lightning computational speeds. Those who use the same password for different platforms, or never change default passwords, are at a greater vulnerability.

• Social engineering

This includes phishing emails or texts. Social engineering refers to the manipulation of users to that trust is developed with the hacker, resulting in the user willingly providing their personal information.[82] This could include personalized emails; impersonation of technical support; impersonation of someone trusted from the user's personal network; etc.

This can be very serious because phishing pages can lead users to enter their password credentials into a fake site, allowing the hacker to store them for later use. This was the type of hack used on the Democratic National Committee.[83]

• Viruses and worms

Viruses and worms are self-replicating pieces of malicious code that are downloaded to a user's computer without their knowledge. Viruses spread to other computers by attaching to files, whereas worms scan for vulnerabilities and report them back to the author of the worm code.

• Automated bots scanning WiFi networks

Not necessarily serious. This is akin to someone looking at your door as they drive around the block. Yes, they may be checking you out, but you're not necessarily a target in the crowd. Automated bots that detect a vulnerability on a computer can be replaced by humans who then

82. Abramson, J. (March 2016) "RSA Conference 2016: IoT is Everywhere… So Are the Vulnerabilities," Symantec. https://www.symantec.com/connect/blogs/rsa-conference-2016-iot-everywhere-so-are-vulnerabilities, accessed July 2018.
83. Gilbert, B. (October 2016) "Hillary Clinton's campaign got hacked by falling for the oldest trick in the book," Business Insider. http://www.businessinsider.fr/us/hillary-clinton-campaign-john-podesta-got-hacked-by-phishing-2016-10, accessed September 2018.

proceed with a more sophisticated hack. Hackers may be using your computer for its strong connectivity to use it as an infected host to then attack others.

• Distributed Denial of Service attacks

These require a very low level of sophistication: all that is required is the IP address of the victim.

Not necessarily serious. It is akin to having the storefront of your window smashed: it looks bad but the business is normally fine. However, it could be very serious in a disaster response setting. If beneficiaries or other humanitarian organizations need to access a website with real time data to inform critical decisions, any delay caused by a DOS attack is very problematic. This type of attack could also be diversion for something else, such as a hacker "sneaking" into the system. DOS attacks can also be used to extort victims or for "hactivist" purposes.[84]

• Malware

This includes ransomware, where victims are extorted for a ransom payment in order to regain access of their software or data. It also includes spyware which can monitor the users' activity and steal personal information and data.

• Zero day exploits

This occurs when a hacker exploits a previously unknown vulnerability, meaning there has been no security patch issued and to which all users are vulnerable. There are "zero days" to defend against these types of attacks: they are rare and require high sophistication to execute.

Accessible tools for reference

The Engine Room refers to the plethora of people and organizations working to provide security support for civil society as the "digital security support ecosystem."[85] This section seeks to highlight key accessible resources available to the humanitarian community to improve cybersecurity.

The following tools are not immune to hacking, but are considered safer than others. For example, Drupal experienced a security bug that would have allowed hackers to install software on any system that ran Drupal. However, vendors are constantly on the lookout for security vulnerabilities, and when detected they develop a corresponding security patch and release it for users to install.

---

84. Abramson, J. (April 2016) "DDoS Attacks: Bigger, Stronger, Scarier," Symantec. https://www.symantec.com/connect/blogs/ddos-attacks-bigger-stronger-scarier, accessed July 2018.
85. Rahman, Z. et al. (March 2018) "Ties that Bind: Organisational Security for Civil Society," (p. 4) The Engine Room. https://www.theengineroom.org/wp-content/uploads/2018/03/Ties-that-Bind-Full-Report.pdf accessed July 2018.

Once the security patch is installed, it allows administrators of the software to see who was trying to break into their system and exploit the bug.

One expert informed that this feature on one of his tools revealed that hackers were not actually trying to steal data, but rather had financial motivations and were trying to run Bitcoin miner software. Another feature of these tools is the automated scanning of logs for suspicious behaviour: for example, if there are five failed logins within 10 seconds from one source address, this is likely not coming from a human, and this user would be automatically blocked. This defence should always be supplemented with human follow up, as a user deemed to be suspicious or with malicious intent should also be manually stopped from accessing the website entirely, or all websites run by the organization.

1) Humanitarian ID. Communicating over this platform will remove some of the risk of social engineering threats, since this platform can verify users. It removes some of the ambiguity of who to trust
2) Jenkins (an open source automation server tool)
3) Drupal
4) ELK software
5) Pingdom
6) Open Web Application Security Project (OWASP) provides a good starting point for organizations without previous audits. It is what the OICT standard at the UN is based on[86]
7) Gophish
8) Encrypted communication: Signal; Wire.com (for conference calls); Whatsapp
9) Two-Factor authentication apps: Authy and Duo security
10) YUBIKey
11) Google advanced protection kits
12) Cryptomaker
13) The Citizen Lab's Net Alert
14) The Citizen Lab's Security Planner
15) Martin Shelton's Signal for Beginners

• Organizations that can assist with cybersecurity

1) The Harvard Humanitarian Initiative is developing a training for humanitarian organizations on capacity development.
2) Access Now
3) Front Line Defenders
4) Tactical Technology Collective
5) Electronic Frontier Foundation
6) Privacy International
7) InterNews
8) Security Without Borders

86. "OWASP Foundation," Open Web Application Security Project. https://www.owasp.org/index.php/Main_Page, accessed July 2018.

List of interviews

This report is informed by a review of publicly available resources and semi-structured interviews with professionals and researchers in the field of humanitarianism and security. Thank you very much to all who generously provided their time and expertise.

Lilian Barajas	UN OCHA
Emma Hogbin	UN OCHA contractor
Emerson Tan	Mautinoa Technologies
Enrico Vigliani	World Food Program
Peter Lieverdink	UN OCHA contractor
Serban Teodorescu	UN OCHA contractor
Michel Oosterhof	Splunk
Daniel Stauffacher	ICT4Peace
Matt Prudente	Security consultant
John Scott Railton	The Citizen Lab
Daniel Scarnecchia	Harvard Humanitarian Initiative
Nathaniel Raymond	Harvard Humanitarian Initiative
Thomas Braun	UN Office for Information and Communication Technology
Matt Mitchell	Global Journalist Security
Daniel Gilman	UN OCHA
Zara Rahman	The Engine Room
Peter Micek	Access Now
Mike Murray	Lookout
Mila Romanoff	UN Global Pulse
Kristin Bergtora Sandvik	University of Oslo