5

Digital Risk: how new technologies impact acceptance and raise new challenges for NGOs

Ziad Al Achkar

Introduction

NGOs are increasingly reliant on digital tools to conduct their work. Over the past decade, NGO operators have turned to new tools, software, and processes to collect data, conduct surveys, manage, and oversee projects. NGOs increasingly look towards remote management and digital tools to conduct assessments, monitor areas of interest, or provide cash aid. As a result, today's NGO actor is increasingly digital, with a larger digital footprint.

Every step of the NGO cycle can be traced and tracked digitally. In doing so, NGOs open themselves up to emerging threats that can hamper their operations, target their staff, and crucially disrupt their relationships with the communities they are working with. These threats include digital hacks to disrupt operations, steal sensitive data, and spread mis/disinformation. NGO actors must reckon with this growing reality and examine how digital risk affects their acceptance. Risk emanating digitally endangers the relationships between NGOs and local communities, belligerent actors, and authorities by creating tensions that reduce the ability of organisations to build connections and trust with various stakeholders.

NGOs have to identify how these digital threats and new risks manifest themselves (Dette, 2018). In this article, I show how some of these digital threats impact NGO acceptance, contribute to digital insecurity, and – critically – what approaches can help bolster acceptance and address digital security concerns.

Security in the digital environment

Attacks against NGOs take place in the physical realm through bombardment of facilities, kidnappings, killings, and other targeted attacks. Concurrently, other campaigns occur digitally through misinformation, disinformation, digital attacks, and hacks that impact the ability of NGOs to operate and damage their relationship with local communities, particularly in conflict settings (van Solinge & Marelli, 2021).

Physical attacks and digital attacks share the same ultimate goal: to upend and disrupt aid operations and create distrust between communities and NGOs – especially international organisations or those receiving external funding. While physical attacks represent a much more forceful action that seeks to send clear messages to NGO workers, digital attacks operate in more nuanced and subtle ways that aim directly at affecting acceptance (for a list of cyber and digital risks, see Kalkman, 2018).

Whereas physical risks can be mitigated or reduced by effective security risk management, digital risks are much harder to deal with, and restoring relationships with stakeholders following digital attacks may prove to be challenging and more time-consuming. The tricky nature of digital risks is that they can emanate from any actors, whether local or sitting thousands of miles away; they can be hard to assess, and therefore hard to mitigate; and they can have large-scale digital and physical repercussions that can have an impact on both staff and the people with whom NGOs are working. An organisation's entire operation could be under surveillance without their knowledge, and their data could be used for entirely nefarious reasons.

As NGOs increasingly rely on digital technologies in their day-to-day operations, it is important to reflect on how this transformation can lead to what I call 'digital insecurity'. By digital insecurity, I mean protocols, practices, and behaviours that can increase the risk towards an organisation, its staff, and the communities they work with. This includes practices such as poor encryption protocols; lack of strong data protection policies and practices; poor vetting of third-party actors who provide digital infrastructure and tools, and who get access to collected data; and inadvertent sharing of GPS coordinates of the location of staff and activities. (For a comprehensive list of cyber threats see Agrafiotis et al., 2018.) Digital risk, however, is never constrained to the digital space, and ultimately will have a physical risk and security component. For example, data leaked on refugees or on potential movement of NGO workers in a conflict setting has real physical security ramifications. It is increasingly difficult to uncouple the two, and understanding how digital risks translate into physical risks and harm is key. Below I discuss two types of digital risks – mis/disinformation campaigns and the misuse of data.

Disinformation and misinformation campaigns

The terms 'misinformation' and 'disinformation' are often used interchangeably, but they are not the same thing. Misinformation is when false or out-of-context information or facts are shared and reported as truth. This occurs when people unintentionally share false news or information. On the other hand, disinformation is the deliberate fabrication of information designed for nefarious purposes. Those who engage in disinformation are purposefully doing so with a specific goal or agenda in mind (Starbird, 2020). While the two often go hand-in-hand, it's important to keep in mind the difference and the critical role that intentionality plays.

Due to the ease with which information is disseminated, belligerent actors may target NGOs in disinformation campaigns (Tiller, Devidal & van Solinge, 2021). Social media posts, fake reports, and targeted campaigns against workers spread rumours and disinformation about the nature of their work, their political goals, and about other issues such as health (Elliot, 2019; Fidler, 2019; Peyton, 2020).

These disinformation campaigns, which are becoming increasingly sophisticated in nature, are typically led by groups seeking to discredit the work of NGO actors. Often these campaigns create mistrust between NGO actors and the communities where they are operating by spreading rumours; misrepresenting statements or reports by NGO personnel; fabricating information about the intent of these organisations; or labelling them as providing intelligence support for a foreign government (Gharib, 2017; Hargrave, 2018). As a result, tensions and mistrust between communities and NGO workers can reduce the ability of organisations to operate safely in those environments or develop successful programs.

Disinformation campaigns, in turn, can increase the security risks facing NGOs and communities and affect NGO acceptance. These campaigns and attacks place a target on NGO personnel and the communities where they operate. Critically, these digital campaigns seek to destabilise the relationships that NGOs develop with local communities that are pivotal to their ability to operate and access certain areas. As such, disinformation campaigns affect acceptance by the local communities and turn the relationship into a more hostile and confrontational one (Pereira, 2021). In Syria, belligerent actors launched online campaigns linking a civil society NGO, known as the White Helmets, to terrorist groups. The goal was to discredit their work and fuel conspiracy theories about Western meddling (Solon, 2017). More recently, misinformation about the nature of COVID-19 and vaccines has led to attacks against health workers globally, creating mistrust about the pandemic and questioning the work of health organisations, which ultimately creates harm for the general population and impedes the work of these organisations (Peyton, 2020).

Risks for misuse of data

Organisations also face attacks against their services and digital infrastructure, or misuse of the data collected. As organisations collect more data on vulnerable communities or store information about their programmatic activities online, they become targets for actors looking to access this information (Parker, 2020). This is particularly important in conflict areas where NGOs operate, and where this kind of data is actionable intelligence against either the communities NGOs are working with or the NGOs themselves (*The Guardian*, 2017).

The recent report from HRW on UNHCR's collection of biometric data of Rohingya refugees is an example of this (Human Rights Watch, 2021). UNHCR collected biometric data from Rohingya refugees in Bangladesh, informing the refugees that this was necessary and a required prerequisite for getting aid. UNHCR shared the biometric data with the host government of Bangladesh, who then shared the data with the government of Myanmar – the same government that refugees were fleeing from. This put the lives of the refugees and their families who might still be in the country in grave danger (Rahman, 2017, 2021; Hodal, 2021).

UNHCR, and legal practitioners I've spoken with, note that it is very likely that UNHCR followed protocol and did everything by the book. As a UN agency, their legal mandate with host governments would have likely required them to share the information. This particular incident raises important questions as to whether informed consent processes are the appropriate mechanism to ensure safety and the trust of the beneficiary communities. What is evident here is that even if UNHCR did everything legally, they have fundamentally broken the trust of the population they are working with, damaged their acceptance, and provided a belligerent government with sensitive information and actionable intelligence on people they have actively persecuted. NGOs, therefore, have to be careful about what kind of data they collect, how they store and secure it, and who gets access to it (Saldinger, 2021).

Individuals and communities are paying increasing attention to the practices of organisations, including how they handle any data they have entrusted to them. This is especially true as digital literacy improves around the world. Failure to handle data responsibly has repercussions both for organisations' reputations and their acceptance. The case of UNHCR and Rohingya biometric data collection reflects this. Refugees entrusted UNHCR to safeguard their sensitive information and were led to believe that the informed consent forms they signed precluded sharing the data with the government that was targeting them. This situation has long-term implications as the refugees are likely to require the assistance of UNHCR for months, if not years to come, and it raises concerns as to what the relationship between the two parties will look like moving forward. Therefore, organisations and security officers must demonstrate that they are placing the safety and privacy of individuals, both employees and affected communities, at the centre of their work.

For both of these risks, it's important to remember that NGO reputations transcend borders and territories. This is especially true for multinational organisations that operate in numerous countries. Organisations and security teams need to understand and properly assess these risks and their ability to impact operations. Oxfam International is one of the most recent examples, where staff were accused of sexual exploitation in Haiti and DRC. As a result, Oxfam International's reputation has been tarnished globally, losing the ability to apply for financial support from certain governments, and losing thousands of donors, forcing them to cut back operations (*BBC News*, 2021). The speed and ease with which digital information is reported and shared means that information about poor or unacceptable practices committed by NGO actors in one area of operation could spread to another community or region, or country.

A need for a sector-wide approach

Three strategies in particular would help to address digital risks and, at the same time, increase acceptance.

Building internal capacity and synergies across teams

Digital security involves bolstering the technical capacity of NGOs and their staff as they increasingly operate and rely on digital tools for their day-to-day activities (Marelli, 2020). Donors need to recognise that digital security requires in-house technical expertise that small and medium scale organisations may not have the budget for (Stewart, 2021). Building in-house expertise would help train staff to avoid some of the most common practices of poor digital behaviours and build capacity to spot weaknesses and vulnerabilities in programmatic planning.

IT and security teams need to determine what is feasible or doable within the capacity available to their NGOs and plan accordingly. In some cases, that may mean scaling back the implementation of certain digital solutions to a level that is safely manageable by the organisation. NGOs should operate under the mantra 'If I can't protect it, I shouldn't collect it' as a basis of their digital and data collection operations. Such an approach could involve testing any tools or software before deployment (Gazi, 2020), or conducting an audit of messaging tools and apps that are used to communicate in the field to understand what kind of metadata is generated and who, beyond the two parties involved, may have access to it (see, for example, Van der Merwe, 2020; ICRC, 2018). NGOs should be conducting digital audits to assess weaknesses, risks, and vulnerabilities across their digital infrastructure to mitigate any potential for harm that may come out of their work (Sandvik, Jacobsen & McDonald, 2017).

Showcasing that you take digital security seriously by ensuring that your staff have at least a baseline technical capacity is a key part of gaining acceptance and trust from communities you are working with. Communities need to know that if you are asking them to share sensitive data you have the ability to secure it and protect their privacy. Organisations should be able to answer questions about what they intend to do with the data, how they will manage the risks, and their plans for disposing of the data afterwards. Showing that you take protecting data seriously and have considered the potential harms and risks that can emanate from it goes a long way to building trust and acceptance. This doesn't mean that every person on your staff has to be an expert, but they need to be well versed, at a minimum, with what the digital risks and harms are.

Transparency

Today's digital world requires transparency about practices and sharing of lessons learned. Communities and local actors demand transparency and respect organisations that have proven to be open and good custodians of their data and to care about the digital risks and harms that can emanate from those activities. It is imperative for NGOs to view clear and continuous communication with local communities as a key component of combatting mis/disinformation and improving their digital risk environment.

One of the gaps in the digital security and NGO field at this moment is the lack of clear examples of how insecurity or a breach in digital security leads to physical or psychological harm on NGO workers or beneficiary communities. This stems from a general reluctance to share information about failures and perhaps a lack of trust among NGOs, often driven by competition for the same pool of funding (Schneiker, 2020).

NGOs working with communities should see trust and acceptance as two indispensable pillars for their ability to operate (Stoddard, Haver & Czwarno, 2016). Combatting mis/disinformation requires a multipronged approach, since there is no technical silver bullet to this issue. Instead, it is important to view this issue through a socio-political lens, as what allows mis/disinformation to spread are people and communities. As a result, the emphasis on building trust, and building a strong rapport with communities that is driven by honesty, transparency, and meaningful engagement is key. Local communities should be consulted and involved in data collection, analysis, and implementation of projects and organisation activity through meaningful feedback mechanisms. For example, asking communities to help design programs and data collection practices will be positively reflected on the ground in increased access. Engaging with local communities throughout the process can contribute to building acceptance and fostering a better security risk management environment.

Building a community of practice

The NGO sector is made up of tens of thousands of organisations and lacks a centralised or hierarchical mechanism to coordinate efforts. However, one of the ways that NGOs can be better prepared to deal with new and emerging challenges is by developing communities of practice and networks of experts. These communities can work to develop minimum acceptable standards and protocols that could be scaled up across a large number of organisations. They could focus on specific issues and areas as they relate to acceptance, such as mis/disinformation, network and communication security, data protection, or other digital risks. The challenge is to be prepared to respond to these evolving risks, and a single organisation cannot deal with what is fundamentally a sector-wide issue.

Some of this work is already underway. Some organisations have undertaken efforts to understand how new digital risks – notably mis/disinformation – affect their work and impact on acceptance (See ICRC and DigitHarium, IMC risk assessment guidelines for more information). For example, ICRC's latest report on Misinformation, Disinformation, and Hate Speech (MDH) articulates some steps organisations can take to tackle MDH, such as information ecosystem assessments that can identify who and what levers can be used to help combat MDH. The ICRC report recommends looking at incorporating MDH awareness into protection work, identifying case studies that exemplify best practice, and – importantly – building collaborations across organisations (ICRC, 2021).

Security managers, in coordination with their IT staff, will have to contribute to the development of new knowledge related to digital security risk, disseminate it throughout their organisations, and build networks. The NGO community, and particularly donors, need to emphasise and back these community-wide efforts to build capacity and expertise throughout the sector.

Bibliography

Agrafiotis, I., Nurse, J., Goldsmith, M., Creese, S. and Upton, D. (2018) 'A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate', *Journal of Cybersecurity*. Available at: **https://doi.org/10.1093/cybsec/tyy006** (accessed: 24 May 2021).

BBC News (2021) 'Oxfam: UK halts funding over new sexual exploitation claims', 7 April. Available at: **https://www.bbc.com/news/health-56670162** (accessed: 10 August 2021).

Dette, R. (2018) 'Do No Digital Harm: Mitigating Technology Risks in Humanitarian Contexts', in Hostettler, S., Najih Besson, S., and Bolay, J.-C. (eds) *Technologies for Development*. Cham: Springer International Publishing, pp. 13–29. doi: 10.1007/978-3-319-91068-0_2.

Elliot, V. (2019) 'Ebola responders in Congo confront fake news and social media chatter', *The New Humanitarian*, 2 May. Available at: **https://www.thenewhumanitarian.org/news/2019/05/02/ebola-responders-congo-confront-fake-news-and-social-media-chatter**

Fidler, D. (2019) 'Disinformation and Disease: Social Media and the Ebola Epidemic in the Democratic Republic of the Congo', *Council on Foreign Relations*, 20 August. Available at: **https://www.cfr.org/blog/disinformation-and-disease-social-media-and-ebola-epidemic-democratic-republic-congo** (accessed: 14 June 2021).

Gazi, T. (2020) 'Data to the rescue: how humanitarian aid NGOs should collect information based on the GDPR', *Journal of International Humanitarian Action*, 5(1), p. 9. doi: 10.1186/s41018-020-00078-0.

Gharib, M. (2017) 'In Their Own Words: Why Armed Fighters Attack Aid Workers', NPR, 14 September. Available at: **https://www.npr.org/sections/goatsandsoda/2017/09/14/550944946/in-their-own-words-why-armed-fighters-attack-aid-workers** (accessed: 4 June 2021).

Hargrave, R. (2018) 'Aid groups targeted by fake news, report says', Devex, 14 February. Available at: **https://www.devex.com/news/sponsored/aid-groups-targeted-by-fake-news-report-says-92096** (accessed: 24 May 2021).

Hodal, K. (2021) 'UN put Rohingya "at risk" by sharing data without consent, says rights group', *The Guardian*, 15 June. Available at: **http://www.theguardian.com/global-development/2021/jun/15/un-put-rohingya-at-risk-by-sharing-data-without-consent-says-rights-group**

Human Rights Watch (2021) *UN Shared Rohingya Data Without Informed Consent*. Available at: **https://www.hrw.org/news/2021/06/15/un-shared-rohingya-data-without-informed-consent** (accessed: 10 August 2021).

International Committee of the Red Cross (ICRC) and Privacy International (2018) *The Humanitarian Metadata Problem: "Doing No Harm" in the Digital Era*.

International Committee of the Red Cross (ICRC) (2021) *Harmful Information – Misinformation, disinformation and hate speech in armed conflict and other situations of violence: ICRC initial findings and perspectives on adapting protection approaches*.

Kalkman, J. P. (2018) 'Practices and consequences of using humanitarian technologies in volatile aid settings', *Journal of International Humanitarian Action*, 3(1). doi: 10.1186/s41018-018-0029-4.

Marelli, M. (2020) 'Hacking humanitarians: moving towards a humanitarian cybersecurity strategy', *Humanitarian Law & Policy Blog*. Available at: **https://blogs.icrc.org/law-and-policy/2020/01/16/hacking-humanitarians-cybersecurity-strategy/** (accessed: 24 May 2021).

van der Merwe, J. (2020) *Secure Communication Platforms: Developing A Framework for Assessing the Metadata of Communication Platforms*. Centre for Innovation, Leiden University. Available at: **https://www.centre4innovation.org/wp-content/uploads/2020/04/FINAL_SecCom_09042020.pdf** (accessed: 21 June 2021).

Parker, B. (2020) 'The cyber attack the UN tried to keep under wraps', The New Humanitarian, 29 January. Available at: https://www.thenewhumanitarian.org/investigation/2020/01/29/united-nations-cyber-attack (accessed: 12 May 2020).

Pereira, C. (2021) 'Disinformation Wars and Not So Digital Threats – Global Interagency Security Forum', *Global Interagency Security Forum*, 5 May. Available at: **https://gisf.ngo/blogs/disinformation-wars-and-not-so-digital-threats/**

Peyton, N. (2020) 'Fear, rumours lead to hundreds of attacks on COVID-19 responders', *Reuters*, 18 August. Available at: **https://www.reuters.com/article/us-health-coronavirus-africa-idUSKCN25E2LF** (accessed: 4 June 2021).

Rahman, Z. (2017) 'Irresponsible data? The risks of registering the Rohingya', *The New Humanitarian*, 23 October. Available at: **https://www.thenewhumanitarian.org/opinion/2017/10/23/irresponsible-data-risks-registering-rohingya**

Rahman, Z. (2021) 'Betrayal and denial from the UN on refugee data', *The New Humanitarian*, 21 June. Available at: **https://www.thenewhumanitarian.org/opinion/2021/6/21/rohingya-data-protection-and-UN-betrayal**

Saldinger, A. (2021) 'USAID hack is "wakeup call" for aid industry on cybersecurity', Devex, 4 June. Available at: **https://www.devex.com/news/sponsored/usaid-hack-is-wakeup-call-for-aid-industry-on-cybersecurity-100028**

Sandvik, K. B., Jacobsen, K. L. and McDonald, S. M. (2017) 'Do no harm: A taxonomy of the challenges of humanitarian experimentation', *International Review of the Red Cross*, 99(904), pp. 319–344. doi: 10.1017/S181638311700042X.

Schneiker, A. (2020) 'Why trust you? Security cooperation within humanitarian NGO networks', *Disasters*, 44(1), pp. 25–43. doi: **https://doi.org/10.1111/disa.12363**

van Solinge, D. and Marelli, M. (2021) 'Q&A: Humanitarian operations, the spread of harmful information and data protection'. Available at: **http://international-review.icrc.org/articles/humanitarian-operations-harmful-information-data-protection-913** (accessed: 26 May 2021).

Stewart, S. (2021) 'Opinion: Information security needs to be a priority of international development', Devex, 13 January. Available at: **https://www.devex.com/news/sponsored/opinion-information-security-needs-to-be-a-priority-of-international-development-98861**

Stoddard, A., Haver, K. and Czwarno, M. (2016) 'NGOs and Risk: How international humanitarian actors manage uncertainty', *Humanitarian Outcomes*, February. Available at: **https://www.humanitarianoutcomes.org/publications/ngos-and-risk-how-international-humanitarian-actors-manage-uncertainty**

Starbird, K. (2020) 'Disinformation campaigns are murky blends of truth, lies and sincere beliefs – lessons from the pandemic', *The Conversation*, 28 July. Available at: **http://theconversation.com/disinformation-campaigns-are-murky-blends-of-truth-lies-and-sincere-beliefs-lessons-from-the-pandemic-140677** (accessed: 10 August 2021).

Solon, O. (2017) 'How Syria's White Helmets became victims of an online propaganda machine', *The Guardian*, 18 December. Available at: **http://www.theguardian.com/world/2017/dec/18/syria-white-helmets-conspiracy-theories**

Tiller, S., Devidal, P. and van Solinge, D. (2021) 'The "fog of war" . . . and information', *Humanitarian Law & Policy Blog*, 30 March. Available at: **https://blogs.icrc.org/law-and-policy/2021/03/30/fog-of-war-and-information/**

The Guardian (2017) 'Secret aid worker: we don't take data protection of vulnerable people seriously', 13 June. Available at: **http://www.theguardian.com/global-development-professionals-network/2017/jun/13/secret-aid-worker-we-dont-take-data-protection-of-vulnerable-people-seriously** (accessed: 21 June 2021).

About the author

Ziad Al Achkar

Researcher

Ziad Al Achkar is a Ph.D. Candidate at the Jimmy and Rosalynn Carter School for Peace and Conflict Resolution at George Mason University. His research focuses on the use of digital technologies in support of peacebuilding and humanitarian action and the evolving relationship with the private technology sector. In particular, Ziad researches how the pursuit of legibility shapes and influences the behavior of humanitarian organisations. Ziad Al Achkar has published articles, policy documents, educational guides, and given talks focused on the responsible use of digital technology and remote sensing.