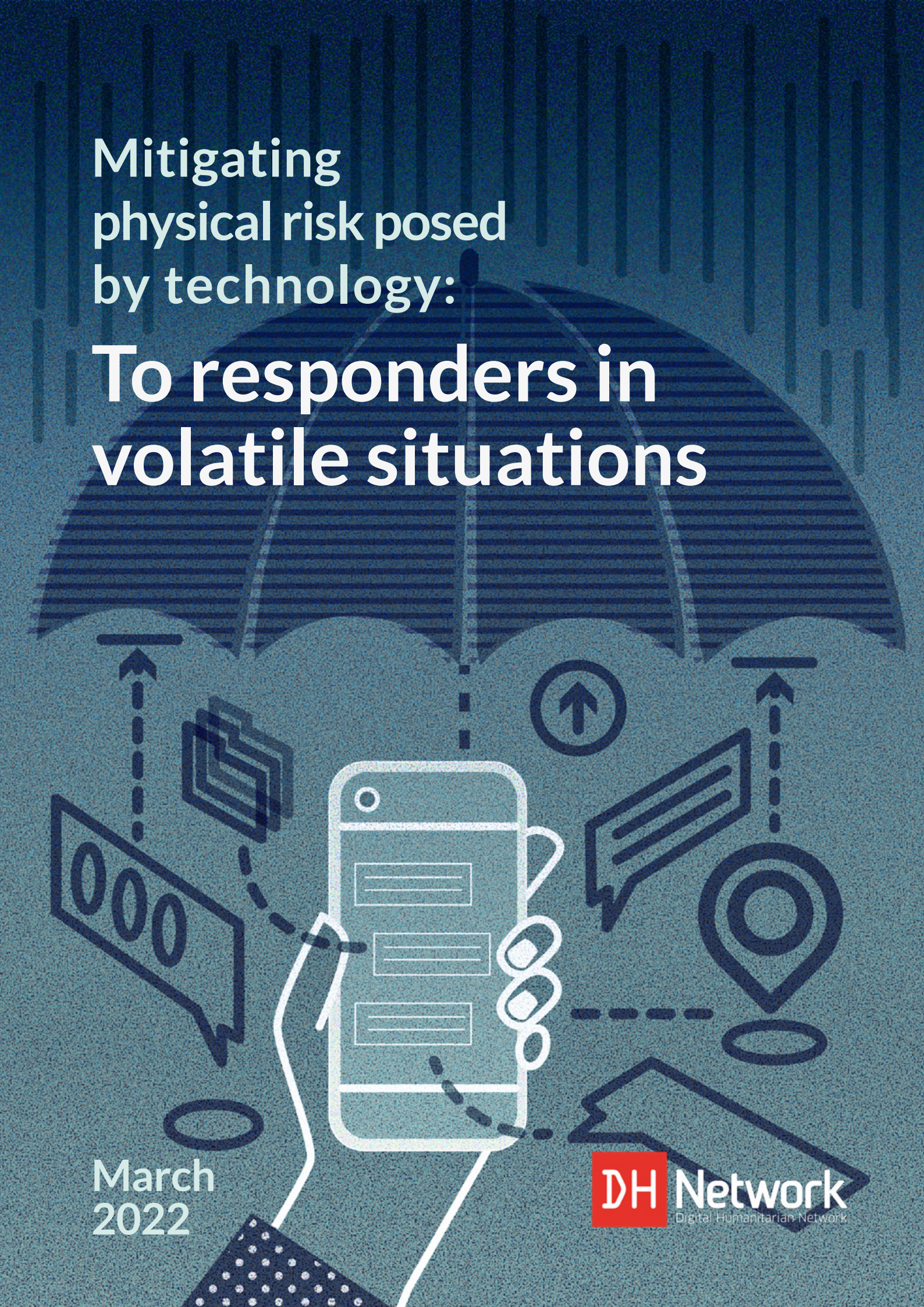
Mitigating physical risk posed by technology:

To responders in volatile situations



March 2022

DH Network
Digital Humanitarian Network

Licensing Information

Mitigating physical risk posed by technology: **To responders in volatile situations**

By

Sarah A Jabbar (sara.abdulrahman@mail.utoronto.ca | LinkedIn)
Munk School of Global Affairs & Public Policy, University of Toronto

Kristen Pearn (kristen.pearn@mail.utoronto.ca | LinkedIn)
Munk School of Global Affairs & Public Policy, University of Toronto

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

Design

Alexandra Sternin | alexsternin.com

This document was made possible with the support of

OCHA

Table of Contents

Acknowledgements

We extend our deepest gratitude to the individuals who took the time to meet with us and share their thoughts and experiences regarding the safety and security risks that digital technologies pose to humanitarian responders in volatile contexts. This report would not have been possible without their contributions.

Name	Organization
Albert Abou Hamra	UNOCHA
Arzu Hatakoy	UNAMA
Ibrahim El Haddad	UNOCHA
Lloyd Cederstrand	UNOCHA
Robert MacTavish	UNICEF
Satoko Nakagawa	UNOCHA, ReliefWeb.int
Yakoubou Mounkara	UNOCHA

Methodology

We conducted a brief literature review[1] of the safety and security risks that digital technologies pose to humanitarian responders stationed in volatile contexts. Although it was not our initial intention to focus on one particular case study, the Taliban taking control of Afghanistan in August 2021 coincided with the production of this report. The precarious situation of humanitarian responders stationed in Afghanistan offered a unique insight into what the humanitarian sector and the larger ecosystem are doing to address the safety and security risks that digital technologies pose to humanitarian responders. We conducted seven semi-structured interviews with humanitarian responders who are currently stationed in or have experience working in multiple volatile contexts, including Afghanistan.

The Issue of Importance

What is it?

In humanitarian emergencies, information communication technologies (ICTs), such as mobile phones and web-based platforms, offer powerful tools for communicating with communities, performing remote needs assessments, conducting advocacy efforts, and general data collection. One interviewee expressed that in today's information landscape, it is almost impossible to perform humanitarian assistance operations effectively without ICTs. A growing body of literature attests to the many benefits that ICTs can offer to help humanitarian relief efforts in terms of efficiency, effectiveness and accountability.[2] These benefits are especially pronounced in volatile and hard-to-reach areas, because ICTs can provide communications channels for humanitarians and affected populations to send and receive life-saving information.

1 Based on the limited sources available.

2 Dette, Rahel. "Do No Digital Harm: Mitigating Technology Risks in Humanitarian Contexts," Technologies for Development, 16 June 2018, pp. 13–29, doi:10.1007/978-3-319-91068-0_2.

The interviewees identified other benefits including:

- ICTs help humanitarian organizations coordinate with other partners during relief efforts.
- ICTs allow humanitarian organizations to collect timely information and data from the field and effectively communicate it to responders on the ground. The Who Does What Where (3W) information management tool was notably mentioned for the way it assists with coordination efforts.[3]
- ICTs can enhance the safety and security of humanitarian responders through web forms or cell phones that increase remote connection.
- ICTs allow responders to communicate remotely with communities that they cannot access (i.e. during the Ebola outbreak and COVID-19 pandemic).
- ICTs enable reciprocal humanitarian access: humanitarian workers can access the affected population, and vice versa.

For years following the September 11 attacks, researchers, activists and policymakers alike raised concerns that the mass collection, storage and analysis of sensitive biometric data pose significant risks to privacy rights[4] and human rights.[5] The potential consequences of poorly implementing technology-based projects can lead to unintended consequences that can be detrimental and even lethal for humanitarian responders and affected populations.[6] Recognizing the potential challenges and risks associated with ICTs can help humanitarians avoid the pitfalls of sensitive data collection and unintended harm.

ICTs are known to introduce complications in a number of ways. For instance, digital tools alter the interaction between aid staff and recipients, which can add to and exacerbate crises or conflict dynamics.[7] The digitization of communications introduces new security and privacy risks, as data transmitted on electronic devices or networks become susceptible to third-party interception and breaches, sometimes unwittingly.[8] However, such challenges entangled with using ICTs for humanitarian purposes have not been adequately researched or addressed in

3 For more information on the 3W tool, please visit: https://emergency.unhcr.org/entry/42801/who-does-what-where-3w.

4 Hu, Margaret. "Biometric ID Cybersurveillance." Indiana Law Journal, vol. 88, 26 June 2013. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2041946.

5 Hu, Margaret. "The Taliban Reportedly Have Control of US Biometric Devices – a Lesson in Life-and-Death Consequences of Data Privacy." Yahoo! News, Yahoo!, August 2021. news.yahoo.com/taliban-reportedly-control-us-biometric-122757450.html; "Steps to Protect Your Online Identity from the Taliban: Digital History and Evading Biometrics Abuses." Human Rights First, 17 August 2021. www.humanrightsfirst.org/resource/steps-protect-your-online-identity-taliban-digital-history-and-evading-biometrics-abuses.

6 Dette, Rahel. "Do No Digital Harm: Mitigating Technology Risks in Humanitarian Contexts," Technologies for Development, 16 June 2018, pp. 13–29, doi:10.1007/978-3-319-91068-0_2.

7 Ibid.

8 Ibid.

literature and practice.[9] Some believe this is because safety and security are not part of the agenda when utilizing digital technologies. Others say that the humanitarian community has not fully grasped the whole issue of data safety in order to mitigate some of the risks.

ICT Security Concerns

A few interviewees noted how some humanitarians lack the digital literacy and training necessary to understand the nature of the threat. The interviewees referred to specific examples, such as humanitarian staff publicizing their activity online in an attempt to connect with affected communities in high-risk countries, resulting in their movements being tracked or staff being kidnapped by malevolent actors. Another example involved a humanitarian convoy moving towards a remote area that had not been accessed in some time, while the agency's communications team publicized the movement on social media. Unfortunately, this public sharing allowed malevolent actors to track and detain the convoy and confiscate its supplies.

Some interviewees discussed the risks of humanitarian agencies and their partners collecting information about digital devices to triangulate reporting about a particular humanitarian crisis in an attempt to inform the relief effort. The interviewees claimed the collection of such sensitive data can make everyone with a digital device a potential target for malevolent actors.

The security of the in-country network was also discussed in two ways. First was the Government's powerful control of the Internet. It is no secret that over the past few years, multiple Governments have taken control of the Internet in their respective countries, with the main purpose being to suppress protests and civil disobedience.[10] [11] [12] [13] Such blackouts heighten a responder's risk when they can no longer communicate with colleagues and/or authorities. Second was the security of information travelling over the Internet and mobile network. Highlighting the seriousness of information being intercepted, interviewees outlined instances where actors have refused to share important information out of fear that the in-country network was insecure. According to the interviewees, it is impossible to guarantee the security of sensitive data online, especially within volatile contexts.

9 Ibid.

10 Arthur, Charles. "Egypt Cuts Off Internet Access." 28 January 2011. Accessed 7 December 2021. https://www.theguardian.com/technology/2011/jan/28/egypt-cuts-off-internet-access.

11 Gohdes, Anita R., Sophie Dyer and Likhita Banerji. "In Dozens of Countries, Governments Rely on Internet Shutdowns to Hide Repression." 4 December 2020. Accessed 7 December 2021. https://www.washingtonpost.com/politics/2020/12/04/dozens-countries-governments-rely-internet-shutdowns-hide-repression/.

12 Statt, Nick. "Myanmar's government shuts down internet indefinitely in response to protests." 1 April 2021. Accessed 7 December 2021. https://www.theverge.com/2021/4/1/22362767/myanmar-military-government-internet-shutdown-blackout-protest-free-speech.

13 Mitra, Esha, and Julia Hollingsworth. "India cuts internet around New Delhi as protesting farmers clash with police." 3 February 2021. Accessed 7 December 2021. https://www.cnn.com/2021/02/01/asia/india-internet-cut-farmers-intl-hnk/index.html.

Humanitarian Mitigation Measures Against ICT Security Concerns

When asked about security measures the humanitarian sector is taking to protect the sensitive data of international and national humanitarian staff, there was a divergence of opinions among the interviewees. Some reported that cybersecurity measures are a high priority, while others suggested the existing cybersecurity measures are not commensurate with the threat.

Those who claimed that cybersecurity measures are a high priority for humanitarian organizations referenced examples, such as UNOCHA's "Data Responsibility"[14] and Somalia's "Information-Sharing Protocol".[15] Such sharing protocols dictate which data sets are accessible and to whom, thus helping prevent breaches of sensitive information. According to one interviewee, there can be a whole variety of non-humanitarian requests where information and data security need to be considered. For example, there have been instances of de facto Governments requesting information about humanitarian staffers for taxation purposes and the UN declining such requests to protect the sensitive information of its staff.

Interviewees discussed a range of products and services used in the field. Humanitarian ID[16] was outlined as an example of ensuring better security by centralizing authentication with a single team that has the capacity to focus on the intricate technical details versus having every single website worry about authentication-related security issues. A tool such as Primero allows for the encryption of shared information and keeps up-to-date records of users to prevent prolonged access. However, the interviewees noted that such approaches and products have not yet been mainstreamed across the humanitarian sector.

One interviewee explained how much information a responder needs to share about themselves just to be part of the sector. For example, each response effort requires individuals to check in with clusters. This generates a lot of information about humanitarian staffers that is not necessarily being well managed, as evidenced by these contact lists being posted online during complex emergencies. Other interviewees were even more critical of the current landscape. Some stated that the humanitarian sector has taken a reactive approach to cybersecurity threats, and they cited the example of ReliefWeb employees working to remove contact lists, photographs and other identifiable information from its platform.

14 For more information on OCHA's Data Responsibility efforts, visit: https://centre.humdata.org/data-responsibility/.

15 For more information on Somalia's Information Sharing Protocol (September 2021), visit: https://reliefweb.int/report/somalia/somalia-information-sharing-protocol-september-2021.

16 Humanitarian ID is available at https://humanitarian.id.

Overall, interviewees expressed genuine concerns about issues they felt should be second nature or prioritized by management. Two regularly highlighted concerns were data exposure and breaches due to the lack of security infrastructure and training in place; and humanitarian staffers' lack of caution when posting on social media platforms outside the workspace.

Safety and Security of National vs. International Staff

There was a consensus among the interviewees that national staff often face more added challenges working for humanitarian organizations than international staff do. According to the interviewees, national Governments require UN staff to register on a meta list, which puts national staff at a higher risk of surveillance and retaliation in comparison to international staff. The interviewees also noted that national staff cannot be evacuated during times of emergency.

The situation in Afghanistan is one example in which national staff are at greater risk of surveillance and retaliation, in this case by the Taliban. Such rapidly changing situations create major risks for all staff. As we saw in the Afghanistan situation, some humanitarian organizations had to retroactively scrub their sites of any identifiable information to help mitigate the risk.

According to Politico reports, around 720 international staff were given the option to evacuate. However, there was little support to evacuate approximately 3,000 Afghan UN humanitarian workers.[17] One interviewee explained part of the challenge for the UN: Member States are responsible for nationals, which means the UN can evacuate only international staffers. Some agencies, such as UNICEF, received backlash as they reportedly requested their national staff to continue working under the slogan "stay and deliver".[18] Other agencies encouraged their staff to step back from their duties for their personal safety. Some interviewees strongly objected to the facts of these reports, stating that although international humanitarians were indeed given the option to evacuate, the number of evacuees was limited. One interviewee pointed out that UNOCHA increased the number of its staff in Afghanistan in response to recent events.

Many interviewees stressed that the UN should advocate for the immunity of its national staff in high-risk countries. They also said that if national staff are arrested, senior UN staffers must deliberate with the host Government to ensure the immunity and protection of its national staff.

17 Heath, Ryan. "U.N. Secretary General Admits Taliban Reprisals Against Staff Have Begun." Politico. 24 August 2021. Accessed 15 September 2021. https://www.politico.com/news/2021/08/24/un-taliban-reprisals-506791.

18 Ibid.

Future Considerations

The interviewees expressed various ideas and recommendations to improve the current security measures:

- Assess the current digital landscape to consider the potential opportunities available in terms of improving and increasing protection measures.
- Initiate **digital-literacy training programmes** to raise awareness of data privacy and protection. In several cases, humanitarian workers have shared information online with other colleagues, jeopardizing and exposing mission details. Some interviewees stressed that humanitarian staff need to be acutely aware that the information they post on social media platforms can put their lives and the lives of those around them at significant risk.
- Install an **easy-to-use secure communication platform** between headquarters and the field officers for Internet security, data sharing and tools, and privacy issues.
- Leverage a **single, secure platform where possible**. However, keep in mind the risk of that single platform being compromised and how your organization will respond if such a breach happens.
- Create **common digital security standards**. This includes sharing existing systems that are leading the way on privacy and security.
- Invest in **dedicated capacity-building for digital security**, and place security in the centre of discussions about technology.
- Conduct **regular risk assessments** of the platforms used. There are standard risk assessments for the physical safety of digital assets and standard penetration tests for digital technologies.

Additional Considerations

Private Sector's Role

The consensus among the interviewees is that the private sector has a significant role to play, since it has the platforms, technical expertise and resources to be a valuable partner. As one interviewee stated, those working in the private sector "are the champions in the digital sphere."

One interviewee shared an experience to help illustrate the role the private sector can play. In 2017, approximately 500 people were killed by a massive truck explosion in Mogadishu, Somalia.[19] Following the terrorist attack, private telecommunications company Hormuud worked alongside UN and humanitarian partners to help responders communicate with the affected people.[20] The interviewee who shared this story did not know how secure or safe its platform was. However, they acknowledged the private sector's role in ensuring the safety and protection of humanitarians and the need to employ the private sector in some cases.

In a more recent example, Reuters reported that for security purposes, Google has temporarily locked email accounts affiliated with the Afghan Government following the Taliban's takeover.[21]

There are multiple instances where the humanitarian sector cooperated with private companies, such as Google and Facebook. However, the interviewees acknowledged that private companies' objective is to make a profit, and collaboration efforts are not always successful. Such a dynamic means that humanitarian organizations must exercise caution and work with private sector companies that have established a degree of reputational trust.

Resources

Although the humanitarian sector has long prioritized the physical safety of humanitarian staff, the consensus among interviewees is that the sector lags behind in investing in the digital safety and security of its staff. As technologies and cybersecurity threats continue to grow and evolve, so does the need for the humanitarian sector to invest in mitigation measures and soft protections.

19 Burke, Jason. "Mogadishu truck bomb: 500 casualties in Somalia's worst terrorist attack." 16 October 2017. Accessed 7 December 2021. https://www.theguardian.com/world/2017/oct/15/truck-bomb-mogadishu-kills-people-somalia.

20 For information on Hormuud's other humanitarian efforts, visit: https://somaliainvestor.so/hormuud-telecom-foundation-csr-champions/.

21 Satter, Raphael. "Google Locks Afghan Government Accounts as Taliban Seek Emails." Reuters. Thomson Reuters, 3 September 2021. Accessed 15 September 2021. https://www.reuters.com/world/asia-pacific/exclusive-google-locks-afghan-government-accounts-taliban-seek-emails-source-2021-09-03/?taid=6132d1feeca2670001c45b36&utm_campaign=trueAnthem:+Trending+Content&utm_medium=trueAnthem&utm_source=twitterurce=twitter.

Conclusion

In recent years, the information landscape has changed considerably. While presenting new opportunities for humanitarian responders to connect with remote and hard-to-reach communities, it has also introduced new risks to the physical safety and security of humanitarian personnel.

Although the humanitarian sector has undertaken some initiatives, including data responsibility and information-sharing protocols, most interviewees agreed that more resources must be directed towards expanding and strengthening (digital) protection measures. Such efforts could range from implementing digital-literacy training programmes to conducting continuous risk assessments of online platforms. Such measures will help ensure the digital protection and physical safety of humanitarian responders, especially those stationed in highly volatile contexts.

Sources

Arthur, Charles. "Egypt Cuts Off Internet Access." 28 January 2011. Accessed 7 December 2021. https://www.theguardian.com/technology/2011/jan/28/egypt-cuts-off-internet-access.

Burke, Jason. "Mogadishu truck bomb: 500 casualties in Somalia's worst terrorist attack." 16 October 2017. Accessed 7 December 2021. https://www.theguardian.com/world/2017/oct/15/truck-bomb-mogadishu-kills-people-somalia.

Dette, Rahel. "Do No Digital Harm: Mitigating Technology Risks in Humanitarian Contexts," Technologies for Development, 16 June 2018, pp. 13–29, doi:10.1007/978-3-319-91068-0_2.

Gohdes, Anita R., Sophie Dyer and Likhita Banerji. In Dozens of Countries, Governments Rely on Internet Shutdowns to Hide Repression." 4 December 2020. Accessed 7 December 2021. https://www.washingtonpost.com/politics/2020/12/04/dozens-countries-governments-rely-internet-shutdowns-hide-repression/.

Heath, Ryan. "U.N. Secretary General Admits Taliban Reprisals Against Staff Have Begun." Politico. 24 August 2021. Accessed 15 September 2021. https://www.politico.com/news/2021/08/24/un-taliban-reprisals-506791.

Hu, Margaret. "Biometric ID Cybersurveillance." Indiana Law Journal, vol. 88, 26 June 2013. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2041946.

Hu, Margaret. "The Taliban Reportedly Have Control of US Biometric Devices – a Lesson in Life-and-Death Consequences of Data Privacy." Yahoo! News, Yahoo!, August 2021. news.yahoo.com/taliban-reportedly-control-us-biometric-122757450.html.

Mitra, Esha, and Julia Hollingsworth. "India cuts internet around New Delhi as protesting farmers clash with police." 3 February 2021. Accessed 7 December 2021. https://www.cnn.com/2021/02/01/asia/india-internet-cut-farmers-intl-hnk/index.html.

Satter, Raphael. "Google Locks Afghan Government Accounts as Taliban Seek Emails." Reuters. Thomson Reuters, 3 September 2021. Accessed 15 September 2021. https://www.reuters.com/world/asia-pacific/exclusive-google-locks-afghan-government-accounts-taliban-seek-emails-source-2021-09-03/?taid=6132d1feeca2670001c45b36&utm_campaign=trueAnthem:+Trending+Content&utm_medium=trueAnthem&utm_source=twitterurce=twitter.

Statt, Nick. “Myanmar’s government shuts down internet indefinitely in response to protests.” 1 April 2021. Accessed 7 December 2021. https://www.theverge.com/2021/4/1/22362767/myanmar-military-government-internet-shutdown-blackout-protest-free-speech.

“Steps to Protect Your Online Identity from the Taliban: Digital History and Evading Biometrics Abuses.” Human Rights First, 17 August 2021. www.humanrightsfirst.org/resource/steps-protect-your-online-identity-taliban-digital-history-and-evading-biometrics-abuses.


DH Network
Digital Humanitarian Network