gisf

Humanitarian Security in an Age of Uncertainty: the intersection of digital and physical risks.

GISF Research Article

Global Interagency Security Forum (GISF) - January 2024

The Global Interagency Security Forum (GISF)

The Global Interagency Security Forum (GISF) is a diverse network of organisations active in the fields of humanitarian aid, international development, human rights, and environmental protection, who value security risk management (SRM) as an important element of their operations and program delivery. In a rapidly changing global landscape, GISF values the importance of continuous documentation, adaptation, and innovation of SRM policy and practice. Therefore, we take an inclusive approach to SRM and don't believe in 'one-size-fits-all' security. We recognise that different staff face different risks, based on the diversity of their personal profile, position, context, and organisation. In summary, we are the leading SRM network and a one-stop-shop for information sharing, knowledge management, coordination, and collaboration.

Acknowledgements

This Article was authored by an independent consultant and curated by Dan Ford and Panos Navrozidis. We would like to give special thanks to Tara Arthur, Tolani Ubhi-Mohideen and Dimitri Kotsiras for their editorial and design support.

This Article was designed by Antoine Marinot.

About this Article (Scope of Work)

GISF is launching a new research project on the topic of security in a digital world, aiming to explore the ways in which security risk management in the aid sector is changing in response to the opportunities and risks stemming from the evolving digital world in which aid is delivered and NGOs are operating.

As part of this project, GISF is publishing an article that 'sets the scene', looking at the (a) external threats in the digital world, (b) internal vulnerabilities in the digital world, and (c) the application of the NGO security risk management triangle in the digital world.

While the article raises critical issues and questions, and proposes some practical recommendations for NGO security advisors' work, this article does not touch on all matters around digitalisation and technological developments in-depth, but rather provides a bird's-eye view of trends NGO security advisors must consider and prepare for; for example, NGOs potentially being increasingly affected by misinformation and disinformation.

The project aims to:

- Set the scene for other projects as part of security in a digital world by highlighting some of the key issues that aid organisations face concerning this topic that future projects can further investigate.

- Identify overall geopolitical trends, note the relationship of these trends with digitalisation and technological innovation, and discuss what this means for how NGOs need to manage the safety and security of their staff and projects.
- Discuss practical ways in which these trends could change the ways in which NGO security advisors need to think about security risk management now and in the future.
- Propose practical and tangible recommendations for those working on security risk management and in the aid sector to address these issues.

Methodology

This article was developed in two phases. Initially, an external consultant interviewed experts from NGOs, members, and the private sector. Subsequently, GISF worked on the consolidated notes received to develop this long article, which integrates some of the interview findings.

Suggested citation

GISF. (2023) Humanitarian Security in an Age of Uncertainty: The Intersection of Digital and Physical Risks. Global Interagency Security Forum (GISF).

Disclaimer

GISF CIC is a limited company, registered in England and Wales with registered number 14937701. Our registered office is at Romero House, 55 Westminster Bridge Road, London, England, SE1 7JB. GISF CIC is a member-led organisation. While references to 'GISF CIC' in this disclaimer shall include GISF's members, observers, its secretariat, and administrative staff, the views or opinions expressed do not necessarily represent the views of donors or of GISF CIC's individual member organisations.

The information contained in this publication is for general information purposes only. The information is provided by GISF CIC and while we endeavour to keep the information accurate and complete, we make no representations or warranties of any kind, express or implied, about its completeness, accuracy, reliability or suitability.

Any reliance you place on such information is therefore strictly at your own risk. You should obtain professional or specialist advice before taking, or refraining from, any action based on the content of this information. In no event will we be liable for any loss or damage, including without limitation, indirect or consequential loss or damage in connection with its use.

This publication was produced by the Global Interagency Security Forum through a three-year cooperative agreement funded by the U.S. Agency for International Development under Agreement ***No. Award No. 720FDA20GR00341***

This article is made possible by the generous support of the American people through the United States Agency for International Development (USAID). The contents are the responsibility of the Global Interagency Security Forum and do not necessarily reflect the views of USAID or the United States Government.

Table of Contents

1 Introduction

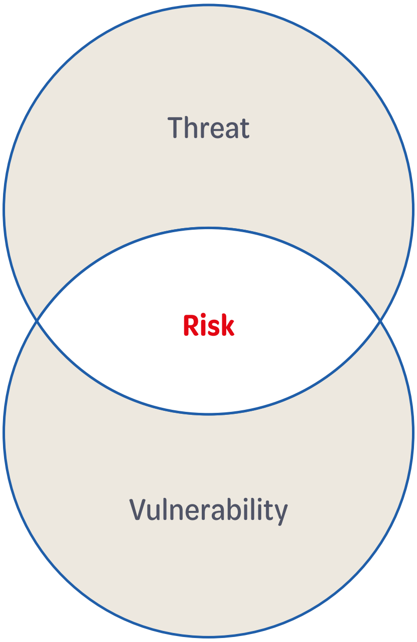
1.1. A discussion about digital technology and humanitarianism

Technology presents both risks and opportunities for humanitarian actors. Among its advantages is increased access to information, early-warning systems, assistance, and services. Technology can also help individuals communicate more efficiently with people across the world. Ultimately, digital technologies, found at all levels of humanitarian organisations and their operations,[1] allow these organisations to 'gather data, distribute aid, get feedback and provide personalised services' (NRC, 2022) to improve their operations.

This paper examines how digital technology interacts with traditional SRM language, concepts, and approaches. It analyses both the dangers posed by advances in digital technology and the benefits such technology can have on the humanitarian SRM sector.

The paper starts by discussing the nature of digital threats in changing geopolitical environments, including the modernisation of warfare (though this is not a critical element of this article); it then considers the internal vulnerabilities of NGOs. This is followed by a section studying the ways in which the NGO security risk management triangle (acceptance, protection, deterrence) relates to digital considerations. The article closes with a set of recommendations.

Figure 1: The relationship between threat, risk, and vulnerability



[1] The Global Interagency Security Forum (GISF) takes a broad definition of humanitarian actors that includes development and human rights agencies. However, due to the experts interviewed, emphasis has been placed on conflict and disaster settings.

1.2. External digital threats

What is a threat in the digital world?

*"A threat is anything that could exploit a vulnerability, which could affect the confidentiality, integrity, or availability of one's systems, data, people, and more **(Kidd, 2022)**".*

A threat also occurs when an adversary or attacker has the opportunity, capability, and intent to negatively impact the victim's operations, assets, workforce, or customers.

A diverse group of threat actors can use digital tools and new technologies to attack individuals and organisations. As a result, by increasing their reliance on digital technology, humanitarians open themselves up to numerous vulnerabilities, threats, and risks (A. Schroeder et al., 2021).

State and non-state actors increasingly use digital technologies, including online media, to advance their interests within larger geopolitical competition and conflict.[2] Rapidly developing technologies like artificial intelligence (AI), cyber and 5G/4G technologies, supply chains, and the interdependencies that underpin these technologies are influencing geopolitics, diplomacy, warfare, and more (Ringhof & Torreblanca, 2022). Since humanitarians commonly deliver aid in and around these contexts, they are increasingly likely to be exposed to direct threats from nefarious actors exploiting digital technology to harm others or, given the integration of digital data, suffer when an organisation is the target of a cyberattack. Ultimately, the implications of such attacks can threaten the safety and security of humanitarian staff and their operations.

Humanitarians increasingly face serious security risks stemming from mis- and disinformation. Social media, accessible by millions, allows for the rapid spread and promotion of fake news. Humanitarian organisations must, therefore, consider how online mis- and disinformation manipulate how the broader public views their mandate and activities, and how this could impact the security of humanitarian staff.

This article discusses external threats through the lens of three main pillars:

1. **Global geopolitical developments and digital advancements in warfare.**
2. **Disinformation, misinformation, and malinformation.**[3]

- Misinformation:the information shared is misleading, but the source disseminating it has no intent to harm.
- Disinformation:the information shared is false and the source is deliberately attempting to manipulate facts.

[2] This was also highlighted by an interviewee.

[3] See Mooser (2023) for more details.

- Malinformation:the information shared is partially true; the intent is to harm a person or organisation by revealing private information.

3. **Private sector dependency on new digital services and products.**

1.3. Internal digital vulnerabilities

As a result of emerging threats in the digital realm, organisations must recognise and provide a more significant role for digital security in their SRM. It is also essential that traditional IT security protocols, such as password management, data minimisation, and protections against hackers, should be spread evenly across an organisation's operations, including those occurring in local settings. For example, INGOs should work to ensure that local IT security measures are in place when forming partnerships with local actors.

What is a digital vulnerability?

A typical digital vulnerability[4] is a weakness, flaw, or other shortcoming in a system (infrastructure, database, or software), but it can also exist in a process, set of controls, or simply just the way that something has been implemented, deployed, or operated by one's staff. Another element is the lack of resources to monitor the vast amount of mis/disinformation targeting an organisation or individual.

This article discusses internal digital vulnerabilities through two main pillars.

1. **Hard or technical digital vulnerabilities: from traditional IT security to transversal risks in digital technologies used in programs and operations.**

- Traditional IT security encompasses the technical elements for internal cyber and digital security measures organisations must take. Password management, data protection, and protection against cyberattacks and hacks are included in this category.
- Digital technologies in program delivery include all the digital tools used to ensure the program effectively takes shape and achieves its objectives on the ground, where the program is implemented.
- The digitalisation of operations and logistics includes all digital technology used to conduct an organisation's operations, including technology used to support communication, human resources, and contracting.

[4] See Kidd (2022) on different types of vulnerabilities.

2. **Soft or non-tech vulnerabilities: people, data hunger, investments, and adaptations.**

- Poor digital literacy (people)

  The inability to critically evaluate digital information means that staff lack the knowledge to protect themselves from digital threats, making them more likely to suffer from a targeted digital attack.

- Over-reliance on data

  As large data sets can tell an incomplete story, relying too heavily on data can lead to decision-making that fails to sufficiently consider nuanced, qualitative, and contextual elements.

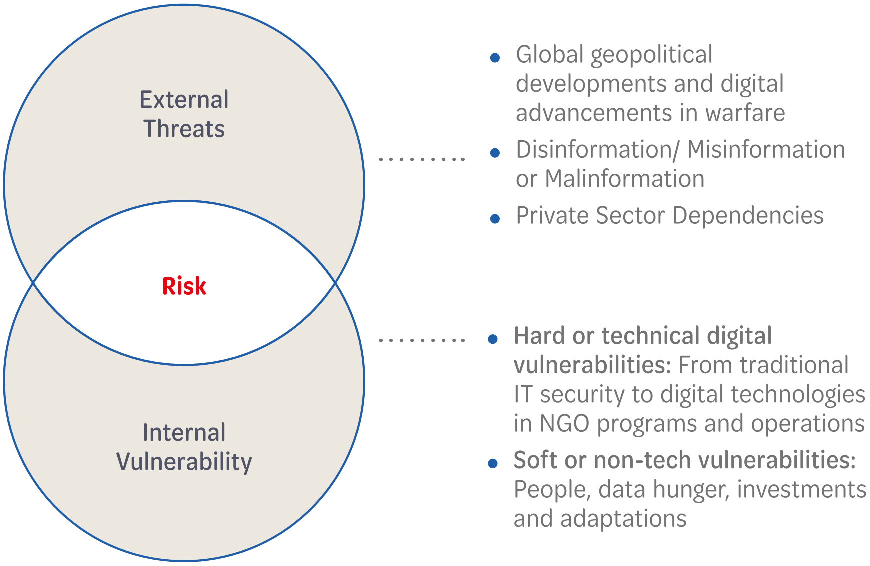
- Differing investment priorities

  Donor priorities inevitably significantly influence an NGO's spending and investment decisions. Without proper security funding, an organisation cannot sufficiently protect against digital security threats, which often require heavy capital investments.

- Organisational structure and management adaptations

  Organisations commonly integrate new technologies into their current processes, policies, and other aspects of management without assessing risk. However, integrating new technology often requires changing internal structure and management to protect against the novel vulnerabilities brought on by incorporating the latest technology into the organisation's operations.

Figure 2: Risk equation in the digital world: Risk = Threats x Vulnerabilities



- Global geopolitical developments and digital advancements in warfare
- Disinformation/ Misinformation or Malinformation
- Private Sector Dependencies

- **Hard or technical digital vulnerabilities:** From traditional IT security to digital technologies in NGO programs and operations
- **Soft or non-tech vulnerabilities:** People, data hunger, investments and adaptations

2 External threats in the digital world

‘Good security risk management like good programming, requires a solid understanding of the environment in which you operate’ ***(Global Interagency Security Forum, n.d.).***

The environment in which humanitarian aid workers operate is changing, and digital technology is becoming more ubiquitous and increasingly integral to humanitarian operations. This section will examine how the external context in which humanitarians operate changes as digital technology becomes more pervasive and how this influences the production of relevant context analyses by SRM practitioners.

2.1. Navigating a changing landscape of global geopolitics and warfare

The real and potential impact of digital risks on the security of aid workers and affected communities is not a new area of exploration (Al Achkar, 2021; Harper & Dobrygowski, 2022; Rodenhäuser et al., 2022). This article analyses how advancing digital technology increases the risks facing humanitarians operating in a digital world. Importantly, conflicts today combine ‘traditional’ kinetic warfare with digital elements of cyber[5] and information[6] warfare, making the risks to humanitarian staff working in and around these conflicts increasingly difficult to navigate.

The overall geopolitical power dynamic and the relationships between the major powers

[5] ‘Cyber warfare involved the actions by a nation-state or international organisation to attack and attempt to damage another nation’s computers or information networks through, for example, computer viruses or denial-of-service attacks’ (RAND, n.d.). Cyberwarfare is often viewed as a field within information warfare.

[6] ‘Information warfare is an operation conducted in order to fain an information advantage over the opponent. It consists in controlling one’s own information space, protecting access to one’s own information, while acquiring and using the opponent’s information, destroying their information systems and disrupting the information flow’ (NATO Defence Education Enhancement Programme, n.d.).

of the world, such as China, Russia, the United States (US), and India, is changing. These states use both hard and soft tools to project their power.[7] Within this context, the world has seen a rise in authoritarianism and democratic backsliding, the polarisation of politics, a great-power conflict in Europe blocking food aid, economic sanctions, and energy supplies being weaponised.[8]
As humanitarians are increasingly responding to proxy wars and regional conflicts stemming from geopolitical power shifts, they are operating in an increasingly dynamic and politicised environment and must take security precautions to navigate through it safely.

As great powers are strategically shifting from the 'global war on terror' to an era of 'strategic competition',[9] larger military conflicts, like the war in Ukraine, are likely to occur (Card et al., 2022; Schroeder, 2019; Slim, 2022). Historically, these large-scale international military conflicts lead to higher levels of civilian and military casualties and a higher number of refugees and internally displaced people (IDPs), all of which increase the demand for humanitarian aid. Increasingly complex, protracted crises, which frequently overlap, strain available resources. Addressing these crises becomes more difficult over time as funding gets constantly redirected to new crises elsewhere.

The effects of climate change are likely to intensify geopolitical competition and its consequences for humanitarian organisations. According to the US National Intelligence Council, the 'intensifying physical effects [of climate change] will exacerbate geopolitical flashpoints', especially cross-border tensions.

The impact of climate change will be most acute in developing countries, 'increasing risks of instability and need for humanitarian assistance' (National Intelligence Estimate, n.d.). Humanitarian organisations will respond to an increasing number of natural disasters across all regions and, in some cases, in areas where there will be an overlap between the protracted conflicts arising from strategic competition between states and natural disasters (National Intelligence Estimate, n.d.).

In addition to the added dynamics of climate change and conflict-induced disaster response, historically recognised protections afforded to humanitarians are increasingly being challenged. As traditional and emerging powers attempt to exert their influence globally, their views of humanitarianism proliferate, including in disaster and conflict settings. Although Western powers have in the past used the foreign aid and humanitarian sectors to advance their geopolitical objectives,

[7] Hard power can be defined as 'the use of a country's military power to persuade other countries to do something' (Cambridge Dictionary, n.d.-a). Soft power can be defined as 'the use of a country's cultural influence to persuade other countries to do something' (Cambridge Dictionary, n.d.-b).

[8] See UN Security Council (2022) and Reuters (2022).

[9] Strategic competition refers to the ways in which great powers such as China and Russia combine economic, diplomatic, military, and technological power to influence the international system and other countries (Card et al., 2022).

the attempt by China, Russia, and others to do the same is occurring in conjunction with their effort to question the notion that humanitarians are neutral actors undertaking aid work to help save and improve lives, making these workers more vulnerable to being targeted in geopolitical conflicts.[10]

As a result of these changing global norms and influences, the traditional principles humanitarians have relied upon for decades to ensure they can operate safely and effectively are being challenged. Additionally, protections afforded to humanitarians under International Humanitarian Law (IHL) are also being questioned by countries that have not historically supported IHL.

Digital advancements are also evident in warfare. Drones now allow militaries to aggressively surveil and attack adversaries without risking the safety of their personnel. Similarly, Open-Source Intelligence (OSINT), which is the review of publicly available information found on the internet to gather a sophisticated understanding of a person, place, or event, is increasingly used by actors to gain intelligence on adversaries. Using social media and posting videos online provides ample evidence to OSINT experts to determine one's location and movements. Meanwhile, as AI becomes more widely used in warfare, critical decisions about who and where to attack are made by algorithms that can produce information quicker than people can. Not only does this technology further complicate warfare, but it also increases the rapidity with which key militaristic decisions are made and allows individuals to deflect blame for military mistakes–such as the mistaken targeting of innocent civilians or aid workers–onto a sophisticated algorithm, rather than a military or government figure.

2.2. Misinformation & disinformation in the sphere of humanitarian aid

Misinformation is defined as false or inaccurate information,[11] whereas disinformation is the deliberate falsification of information with the intention of misleading others.[12] While misinformation and disinformation are not new risks to humanitarian actors, they have become more pervasive in recent years. They are spreading faster and more widely and are amplified by the increasing use of digital tools, including messaging apps such as WhatsApp and Telegram, and social media platforms, such as Facebook and X, formerly Twitter.

[10] According to the Humanitarian Advisory Board 'China's approach to humanitarian aid is different to traditional donors in terms of decision-making, funding processes, and delivery. At the operational level, these differences can challenge existing norms' (Humanitarian Advisory Group et al., 2019). A study by Jonathan Robinson reveals that Russian humanitarian aid is 'heavily influenced by the state, is symbolic, and urban focused'. It is also 'influenced by the context to which Russia is responding' (Robinson, 2007).

[11] 'false information that is spread, regardless of whether there is intent to mislead' (Library Guides: News: Fake News, Misinformation & Disinformation, 2022).

[12] 'deliberately misleading or biased information; manipulated narrative or facts; propaganda' (Library Guides: News: Fake News, Misinformation & Disinformation, 2022).

The physical security implications of misinformation and disinformation are far reaching. At the political level, they can undermine the norms, values, and principles foundational to humanitarian operations and protections afforded under IHL. At the ground level, they can create divisions between aid workers and the communities they serve while also leading to the direct targeting of humanitarian staff.

Research investigating the different rates at which true and fake news stories spread on X found that 'falsehood diffused significantly farther, faster, deeper and [more] broadly' than true information (Vosoughi et al., n.d.) As digital media becomes more pervasive, fake news evolves and spreads in unprecedented ways, with consequences for the security of individuals (Pearn & Verity, 2022). This makes the risks arising from mis- and disinformation among the most difficult to mitigate.

Two interviewees highlighted that the spread of misinformation is one of the greatest risks to the physical security of in-country humanitarians. A lack of access to reliable information in an uncertain and 'fearful [online] environment' makes it difficult for people to effectively make decisions using digital tools and online media (Tuckwood, 2019). Not only is it challenging to dig through the misinformation to gather accurate news online, but it also can directly disrupt humanitarian work. Among the day-to-day issues that affect the safety of staff and programmes is widespread misinformation about the work of an organisation proliferating via online media.[13]

Like misinformation, the impact of disinformation is also growing. In an online environment characterised by an abundance of information and a large quantity of misinformation, disinformation tactics become more effective (Xu, 2021). Disinformation can take various forms, including accurate information surrounded by false contexts, manipulation of original content, or completely fabricated information.[14] Used against humanitarians, 'these attacks are designed to sow division and confusion, disparage targeted organisations and their leaders, and promote inaccurate views about the communities they support' (Oh & Adkins, 2018).

A notable example of the threat of false information to humanitarian organisations is the case of Syria and the White Helmets (otherwise known as the Syrian Civil Defence). This group of civilian volunteers rescue civilians caught between warring parties in Syria's civil war. They also document war crimes committed by Bashar al-Assad's regime and the Russian military. Due to the White Helmets' success, they became targets of a Kremlin-backed disinformation campaign, claiming that footage shared by the group was faked, the hospitals attacked were run by terrorists, and the White Helmets were themselves tied to terrorists (The Syria Campaign,

[13] From an interviewee.

[14] A very worrying development in this area is the growth of generative AI that can create realistic images, audio, writing samples and videos (deepfakes), See: https://medium.com/@lennartfr/deepfakes-and-the-world-of-generative-adversarial-networks-bf6937e70637

2017.). The Syria Campaign, a human rights organisation opposing Assad and the Russians, reported that on X alone, bots and trolls targeting the White Helmets reached 56 million people during 2016 and 2017. The impact of this campaign was so severe that it contributed to the US State Department's decision to freeze aid to the group in 2018, demonstrating the tangible effect of a well-coordinated disinformation campaign.

The current conflict in Ukraine provides insight into how the issue of mis- and disinformation continues to play out in the context of geopolitical conflict. After Russia invaded Ukraine in February 2022, Europe experienced the largest influx of refugees and migrants since World War II. Russia's reported use of indiscriminate weapons and the purposeful targeting of civilians, humanitarians, and vital non-military infrastructure have put many civilians in harm's way. Within this context, individuals and organisations that pro-Russia groups believe undermine the Russian offensive have faced targeted disinformation attacks, including aid workers (van Sant, 2022). For example, online disinformation campaigns attempted to undermine the ICRC's work in the region by spreading disinformation claiming the ICRC was moving Ukrainians into Russia when, in fact, they were helping Ukrainians relocate to other Ukrainian cities (ICRC, 2022c).

2.3. Private sector dependency on new digital services and products

Regardless of the degree to which IT is outsourced, all humanitarian organisations are somehow embedded in digital supply chains. Based in the UK, the National Cyber Security Centre explains that supply chains are large and complex, as organisations rely on many suppliers to provide different products, systems, and services. It goes on to explain that 'effectively securing the supply chains can be hard because vulnerabilities can be inherent, or introduced and exploited at any point in the supply chain' (UK National Cyber Security Centre, 2018).

The reliance on an increasing number of vendors opens organisations up to supply chain attacks where hackers infiltrate 'through an outside partner or vendor that provides components of the system' (Marelli, 2022). As humanitarian organisations integrate more digital technologies provided by third parties, the vulnerabilities that can be exploited by threat actors increase. Among the challenges that arise here is reputational risk. If a humanitarian organisation's data is compromised due to a security lapse on the part of a vendor, the organisation's reputation could be damaged. This could make it more difficult for the organisation to raise funds and operate effectively.

Overreliance on outside suppliers can also lead to vendor lock-in, which prevents organisations from switching to a new vendor due to incompatibility with other products in use, lack of interoperability between different technologies, no market alternative, or inability to afford alternative vendors. With vendor lock-in, should the supplier cease to exist, security support, such as updates for detected vulnerabilities, will no longer be available, making an organisation's systems more vulnerable to digital attacks.

As organisations integrate more and more digital technologies into their operations, they become exposed to a broad range of threat actors seeking to exploit their data or ability to deliver programmes. These vulnerabilities exist not only internally, with staff targeted by phishing, hacking, misinformation, or disinformation, but more broadly, as part of the supply chains humanitarian organisations rely on when using third-party technology. Failure to recognise and mitigate against these digital threats not only endangers an organisation's data and technology but can manifest in physical risk when threat actors leverage stolen data to attack humanitarians in the physical space.

3 Internal vulnerabilities in the digital world

Digital technology further complicates internal vulnerabilities. Digital data exist indefinitely and can be accessed from nearly anywhere in the world. As a result, there are no geographic or temporal limitations for many of the external threats and internal vulnerabilities resulting from digital technology. Actors can exploit vulnerabilities or conduct targeted attacks from far outside the geographic area of a specific operation and well into the future (GISF, 2021).

As the contexts in which humanitarian organisations deliver assistance to crisis-affected communities evolve, so do the types of vulnerabilities, threats, and risks aid workers face.

3.1. Hard or technical digital vulnerabilities: from traditional IT security threats to transversal risks in digital technologies used in programs and operations.

As more humanitarian operations are digitised, hacking and phishing threats become increasingly prevalent. One successful phishing or hacking attempt can grant access to a wide variety of digital systems existing within an organisation and those hosted by third parties, such as cloud databases.

3.1.1 Phishing

Phishing is not a new threat and continues to rise, with over three billion phishing emails sent daily (Palmer, 2021; Microsoft, 2022). Phishers use deceptive messages, most often in email, text, or over the phone, to convince victims to release information about themselves or their organisation that can be used to gain access to sensitive information, such as passwords, personal identifiable information, and financial accounts.

3.1.2. Hacking

In addition to phishing, threat actors can also gain access to sensitive information by hacking the IT systems of an organisation through both hardware and software attacks (Marelli, 2022). In 2021, three-quarters of the exploits/digital hacking tools that Google detected were developed by commercial companies and available for purchase.[15] By gaining access to an organisation's digital systems through hacking or phishing, threat actors aim to extort organisations or individuals, gather information, freeze

[15] Interview with cyber security practitioner.

systems, and in some cases manipulate data and install viruses to forcibly slow down or halt an organisation's work.

3.1.3. Understanding the digital threat actors

The threat actors involved in hacking and phishing can be divided into two main groups: 1) state actors or state-sponsored groups and 2) non-state criminal groups. The incentives of each group differ, but both generate serious security concerns for humanitarian actors. A variety of alternatively motivated hackers exist but are not specifically considered here.

State and state-sponsored actors tend to target primarily human rights organisations and less humanitarian and development NGOs as part of their broader geopolitical objectives. Threat actors can act to hinder the work of organisations if they believe these groups pose a danger to the state's geopolitical strategy and objectives. A simple act, such as freezing an organisation's access to its own data, could disrupt its operations. Although such attacks have historically occurred against human rights groups and state-operated institutions, the increasingly complex geopolitical terrain surrounding humanitarian disasters increases the likelihood that humanitarian and development professionals will face similar threats soon.

Among the threats humanitarians might face in the coming years include non-state criminal groups targeting them partly for financial or other benefits, as has happened to human rights groups. Dangerous actors may enter digital systems to access internal data and information about an organisation's staff or the people to whom they deliver aid. Actors can then use this information to imitate the hacked organisation or its staff, enabling fraud and social engineering—the use of deception and manipulation to get someone to divulge confidential information—in phishing campaigns, in which they use fake names, information, and pretexts in an attempt to manipulate individuals into giving them money.

3.1.4. Types of damage suffered

There are two primary ways in which humanitarian organisations can suffer from digital attacks. The first is by being the direct target of a digital attack. The second is by suffering collateral damage from an attack targeting a third party that houses some or all of the organisation's digital information.

The dangers of being the direct target of a digital attack are evident in the 2021 attack on the International Committee of the Red Cross (ICRC). In January 2022, the ICRC announced that their systems, containing the confidential information of more than 515,000 people, had been the target of a highly sophisticated attack. This hack required highly skilled individuals to exploit an 'unpatched critical vulnerability'. In this case, the goal was to gain access to information, though what happened to this sensitive data is still unknown. As of June 2022, the ICRC had not been contacted by the threat actor, nor had there been a ransom request (ICRC, 2022a; Worley, 2022). The risk to the data subjects could be both physical (their locations were part of the data accessed) or digital (the data can be used for phishing attempts or extortion).

Another way in which threat actors can attempt to disrupt an organisation's operations through a direct attack is by conducting a ransomware attack. Ransomware is a form of malware that cuts a user's access to vital systems and information on their computer and digital servers. Given the time-sensitive and lifesaving work many humanitarian organisations conduct, the sudden halting of operations can have deadly consequences. For example, a ransomware attack on the UK National Health Service (NHS) in 2022 limited the NHS' ability to use critical digital technology, hindering its ability to communicate with ambulance dispatches, emergency prescription services, and urgent treatment centres (Milmo, 2022). Ultimately, the impact of such attacks is felt most sharply by those relying on the lifesaving assistance organisations provide.

While the two aforementioned hacks directly target organisations delivering critical humanitarian and public services, the 2020 SolarWinds hack is an example of how humanitarians can suffer as part of the collateral damage resulting from a digital attack on a third party housing the organisation's data.

In 2020, a cyber operation was launched against SolarWinds—an American IT company that was part of the digital supply chain providing IT management services and cloud storage to various organisations. By targeting SolarWinds, hackers were able to gain access to the data of private companies and organisations as well as US government agencies. Hackers accessed the data of these actors not by targeting each organisation individually but by identifying and attacking a single weakness in SolarWinds, opening the door to the company's customer base.[16] Although hackers may have only aimed to gain access to the networks, systems, and data of the US government or specific private companies, all those who stored their data on SolarWinds, including humanitarian organisations, were exposed (Marelli, 2022).

3.1.5 Protecting against external digital threats: fixing your blind spots

Digital threat actors increasingly view humanitarian organisations as easy targets because they struggle to protect themselves.[17] Even as IT and digital security improves, threat actors often look to take advantage of human fallibility. Threat actors seek to increase their success in one of two ways. Either they increase the number of targets by widening the range of targets, or they rely on social engineering to more effectively target victims. The more information the threat actor holds about individuals, the more sophisticated and effective their attacks can be.

[16] 'A supply chain attack occurs when someone infiltrates your systems through an outside partner or provider with access to your systems and data' (Korolov, 2021).

[17] From an interviewee.

Since phishing targets an individual through emails and other forms of communication—many of which are digital—protecting against phishing requires strong digital literacy at the staff level; each staff member must be aware of the signs of a phishing attempt to avoid handing over sensitive information. Protecting against phishing also requires good digital hygiene practices, such as using strong passwords, antivirus software, and avoiding downloading content from suspicious websites. Limited staff training on digital security as well as insufficient prioritisation and funding of digital security increases exposure to successful phishing attempts.[18]

At the organisational level, appropriate protection against phishing includes implementing access limitations on internal systems to limit the number of people who know or have access to sensitive information. By limiting who has access to information, the organisation is limiting the number of individuals who could reveal sensitive information while falling prey to a phishing attack.

Hacking and phishing have implications for the physical security of humanitarian staff and aid recipients. Humanitarian organisations hold many types of data, often including, but not limited to, addresses, contact details (including next of kin or emergency contacts), biometrics, bank accounts, and personal information, such as the religion or sexual orientation of the individual. This data, combined with knowledge of the location or travel itinerary of an individual, can help threat actors find and target humanitarian staff by carrying out kidnappings, robberies, and other types of physical violence. Additionally, sensitive information gathered during interviews with refugees or IDPs, such as political or religious affiliation, is often stored in emails, online databases, or virtual chats, which can easily be used by police and government officials to justify detention.

All the above demonstrate the need for interoperability between systems across organisations as well as how traditional IT security interlinks with technologies selected for program implementation or to support operations and logistics. Often, programs or logistics will deploy new smart systems (fleet tracking, digital cash, biometrics, etc.) without extended discussion with their IT departments, thus increasing their vulnerabilities and potentially increasing their physical risks. When new digital technologies are introduced, organisations should mainstream an assessment which includes knowledge provided by the IT department, the safety and security team, and the respective program or operations team (technology owner) to prepare for unforeseen threats and mitigate any risk. This can be a quick and inexpensive exercise as part of standard operating procedures (SOPs).

[18] 'Digital hygiene is a phrase used to refer to the practice of cleaning up your electronic/information assets and regularly updating them. This process includes knowing how to choose your password, organising files on your laptop, and adjusting settings on our email and social media accounts, all as a part of an effort to ensure greater security' (SeaGlass Technology, 2020).

3.2. Soft or non-tech vulnerabilities: poor digital literacy (people), over-reliance on data, differing investment priorities, and poor organisational adaptations

Discussions around digital vulnerabilities often focus on breaching software and hardware technology. However, proper day-to-day use of those systems, adherence to internal processes, digital SOPs, and overall increased staff capacity also play a crucial role in protecting against digital threats.

The four major non-tech vulnerabilities existing within people and processes, as discussed in this article, are: poor digital literacy, over-reliance on data, differing investment priorities, and poor organisational adaptations.

3.2.1. Poor digital literacy

Digital literacy can be defined as *'the ability to identify and use technology confidently, creatively, and critically to meet the demands and challenges of life, learning, and work in a digital society,'* including but not limited to the ability to 'manage your online identity as well as your security and privacy' (**Coldwell-Neilson, n.d.**).

Digital literacy includes the ability to critically evaluate digital information—such as that found on social media platforms—and to know how to use information found online correctly and productively to advance the organisation's interests. Not believing mis- and disinformation on social media and instead identifying accurate information is an example of good digital literacy; someone with poor literacy might find themselves repeatedly believing fake news found online.

Without good literacy, staff lack the knowledge to protect themselves from digital threats, which makes them more likely to suffer from a targeted digital attack. Digital literacy also gives staff the knowledge needed to practice good digital hygiene, which can help them avoid suffering from digital and physical security risks. Working to ensure all staff understand the nature of the external threats they face and the internal vulnerabilities that can be exploited is, therefore, critical to protecting against digital dangers.

3.2.2. Over-reliance on data

The second non-technical vulnerability comes from an over-reliance on data. An interviewee expressed concerns about widespread 'magical thinking' that all answers to complex questions can be found through large-scale data collection and analysis. As the usage of large data sets becomes more common throughout the sector, experts could begin relying too heavily on data that tells an incomplete story, thus not considering all the necessary factors when making decisions regarding the security of staff and programmes. Although essential and helpful, data alone cannot answer every question or provide a solution to every problem; relying too heavily on it in isolation can lead to poor decision-making, which can endanger the organisation, its staff, and those it serves.

Data incorrectly applied has many limitations. For example, relying on self-selected samples to produce information about a group can lead to biased and incorrect findings that are not representative of the broader group. Also, relying heavily on open-source technology can lead to the collection of misinformation and incorrect data found on social media and other openly accessible platforms. Using flawed data to make operational, research, and logistical decisions can endanger the safety of staff members. For example, false reports on social media of migrant flows could lead humanitarian organisations to use resources to transport staff through dangerous terrain to the stated location, only to find out upon arrival that the information was incorrect. As a result, humanitarian organisations must be aware of the dangers posed by false information and data online and validate all information before using it to make critical decisions.

3.2.3. Differing investment priorities

Donors, senior management, and the rest of the staff in a humanitarian organisation have differing priorities and perspectives regarding integrating digital tools into humanitarian action. Donor priorities inevitably have a significant influence on an NGO's spending and investment decisions.

Without proper security funding, an organisation cannot sufficiently protect against digital security threats, which often require heavy capital investments. Given this, organisations must further prioritise funding their digital security and must make the argument to donors that humanitarian organisations operating in an increasingly digital world require sufficient funding. Monitoring the sheer volume of mis/disinformation data in any given context and its impact on acceptance is, for example, a new area of focus that very few organisations have the resources to invest in.

Interviewees expressed that humanitarian organisations often do not view data as an asset that needs to be valued to the same degree as physical assets, such as cash and vehicles. Even when an organisation's internal policies cover data security, the concept is often still not fully embraced by senior management.

3.2.4. Organisational structure and management adaptations

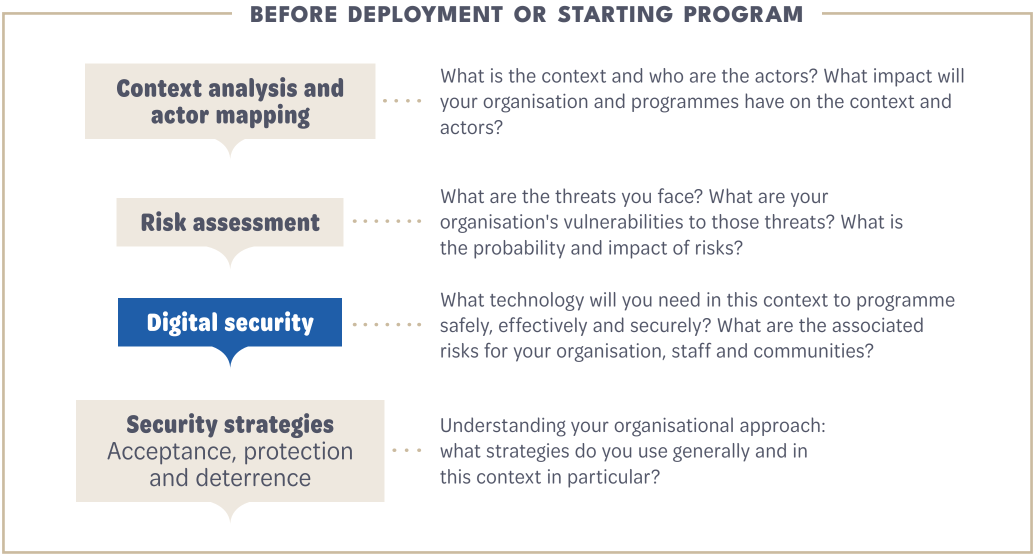
The fourth vulnerability is inappropriate organisational structures and management practices. Experts engaged in digital innovation in the sector highlight that organisations commonly integrate new technologies into their current processes, policies, and other aspects of management without assessing the risks. Integrating new technology, however, often requires a change in internal structure and management to protect against the novel vulnerabilities brought on by integrating the new technology into the organisation's operations. By not adapting internal structures and management when integrating new technologies, the organisation might not fully realise the benefits of the new technology, nor adequately position itself to mitigate and manage threats.

4 Applying the NGO security risk management triangle in the digital world

This section will examine the relevance of the NGO security risk management triangle in the digital world. Here, we discuss how security strategies, contingency plans, incident reporting procedures, and critical incident management can be adapted to consider the interaction of digital and physical risks as digital technology becomes more pervasive in humanitarian action.

To begin with, it is important for security professionals to include digital threat assessments more explicitly in security risk assessments. Digital security threats should be considered part of an organisation’s security risk analysis and thus should be integrated into security risk assessments across the humanitarian sector. Risk assessments should consider the specific digital security threats in a digital world without borders in other countries and regions. Risk assessments should respond to security challenges, no matter where they occur.

Figure 3: Assessing digital security risk (GISF, 2015)



BEFORE DEPLOYMENT OR STARTING PROGRAM

Context analysis and actor mapping: What is the context and who are the actors? What impact will your organisation and programmes have on the context and actors?

Risk assessment: What are the threats you face? What are your organisation's vulnerabilities to those threats? What is the probability and impact of risks?

Digital security: What technology will you need in this context to programme safely, effectively and securely? What are the associated risks for your organisation, staff and communities?

Security strategies Acceptance, protection and deterrence: Understanding your organisational approach: what strategies do you use generally and in this context in particular?

4.1. Security Triangle

Physical security strategies are built around the three pillars of the security triangle: acceptance, protection, and deterrence. These three elements aim to support security experts as they seek to mitigate and manage risk whilst enabling humanitarian actors to continue their work. The digital context in which an organisation operates must be integrated into its security strategy, whichever of the three elements they utilise.

4.1.1. Acceptance

Acceptance can be defined as 'building a safe operating environment through the consent, approval and cooperation from individuals, communities, and local authorities' (GISF, 2020). It is a widely used strategy to mitigate risk. The humanitarian principles of humanity, neutrality, impartiality, and independence facilitate access and acceptance by creating an environment in which stakeholders consent to the presence and activities of humanitarian organisations. These principles are the foundation for the legitimacy and consent underpinning effective humanitarian work.

Some of the barriers organisations face when trying to achieve acceptance stem from the fact that the communities served often do not trust the humanitarian organisations delivering aid. Increasingly, we see digital campaigns, such as mis/disinformation campaigns, directly or indirectly undermine the relationship between the community served and the humanitarian organisations and staff working there (GISF, 2021).

In the face of digital disinformation campaigns seeking to undermine the legitimacy of humanitarian workers, humanitarians can take steps to improve trust. Organisations can attempt to counter online mis/disinformation campaigns by using the same platforms to promote in local languages how communities benefit from the organisation's work. Rather than responding back and directly engaging with those digital profiles, organisations can take control of the narrative through mass communication campaigns that focus on their lifesaving activities, quantifying the results of their work.

Furthermore, communities that can physically identify humanitarian workers are more likely to trust them.[19] This is partly because they can identify these individuals as serving the interests and needs of the local populations. Moreover, many belligerents and armed groups respect the IHL norm of not physically attacking humanitarians, who are defined under IHL as being neutral, non-aggressive actors. As such, they avoid aggressive confrontation with humanitarians when they see a humanitarian organisation's emblem; though, not all threat actors respect this norm. The recent work by the ICRC to develop a digital emblem is an important first step towards bringing their emblem, an important factor in establishing trust and acceptance as well as deterring aggressive behaviour, from the physical realm into the digital space (ICRC, 2022b).

[19] From an interview with an expert in data responsibility and digital innovation.

Unfortunately, establishing trust and achieving acceptance will remain a challenge in an online environment, even when digital emblems are widely used. Spoof accounts and phishing emails will include humanitarian-created digital insignia, fake email addresses, and varying levels of personnel-specific information to trick the recipient into handing over sensitive information. Moreover, respect for the digital emblem and its effectiveness as a mechanism for ensuring physical and digital security is further complicated by the current geopolitical context, which, as aforementioned, provides heightened challenges to IHL and the principles upon which humanitarianism relies.

4.1.2. Protection

According to GISF, protection is defined as 'reducing the impact, but not the threat, by reducing the vulnerability of the organisation' (GISF, 2020). As many interviewees highlighted, protection tends to focus on the physical security of staff working in the community. When it comes to ensuring digital security, on the other hand, organisations typically focus on implementing protective IT security measures at headquarters but fail to implement similarly comprehensive digital security measures across all of the organisation's operations and geographic locations. This makes staff more vulnerable to digital security threats.

To ensure sufficient protection in the digital space, the humanitarian sector must work to translate the protections derived from humanitarian principles and IHL from the physical world to the digital realm. Under IHL, humanitarians must not be targeted by state and military actors; this is also true in the digital realm.

Unfortunately, measures humanitarians take in the physical world to protect against attacks are more challenging online. For example, humanitarian organisations try not to locate their operations next to a military base to reduce their vulnerability and avoid getting caught in the crossfire of kinetic attacks in the physical world. Achieving a similar distance in the digital realm is not as straightforward due to the lack of geographic boundaries inherent in the digital space. Humanitarian organisations frequently rely on the same infrastructure and suppliers as governments and militaries (dual-use technology). As such, when a government's or military's digital servers are attacked, the humanitarian organisations sharing the digital infrastructure with the government will be vulnerable to an attack as well, even if these organisations are not the direct target. To combat this vulnerability, humanitarians can use different infrastructure and suppliers than those used by governments and militaries, thus making them less likely to suffer from a digital attack targeting a government or military actor.

4.1.3. Deterrence

Humanitarian deterrence can be defined as 'reducing the risk by containing the threat with a counter threat' (GISF, 2020). Deterrence strategies are typically used as a last resort when acceptance and protection strategies fail. Among the most popular deterrent strategies include reporting illegal attacks to local police or international courts and the cessation of aid activities (Childs, 2013).

Some experts argue that the only way to use deterrence to maintain the principles of impartiality and neutrality is to cease aid activities. However, to quote an interviewee, 'deterrence is not really an option' when looking at digital actions. This is partly because many actors from a wide variety of backgrounds can launch digital attacks, which are often difficult to identify, and they might be aiming to bring aid activities to a halt.

4.2. Contingency plans, incident reporting, and critical incident management

As mentioned above, humanitarian organisations often view data as less valuable than physical assets. This impacts the development of contingency plans and how incidents are reported and managed.

To illustrate, if a set of NGO-branded clothing or an NGO-marked vehicle is stolen in a humanitarian context, the theft will often prompt two responses. The first deals with the theft of the asset itself, exploring how it happened and adjusting processes to prevent future thefts. The second response is to look at the potential risks of having an external actor use these assets to falsify their identity and pretend to be a humanitarian worker, which could damage the NGO's reputation acceptance strategy, and leave them facing increased risk. In response, the NGO will seek to mitigate those subsequent risks. Stolen data can create a similar domino effect of subsequent dangers, and planning for crises involving digital security should be approached in the same way.

Even when these digital elements of contingency planning are integrated into an organisation's 'on-paper' protocols, a culture must be created to ensure that data and digital issues are not ignored when responding to a crisis. Interviewees mentioned that some organisations had not made contingency plans on what to do with their data (regarding local staff and communities) as the Taliban approached Kabul in 2021, forcing them to make quick decisions on the fly. Contingency plans and incident management must have clear directives on what decisions need to be made regarding the handling of digital equipment and data. For example, should data be 'removed' from the country by being placed on cloud servers? Is the threat actor still able to target that data? If so, should the data be deleted? These assessments must be built into contingency plans, and rigorous training on these digital elements must be conducted.

5 Recommendations

The humanitarian sector is just starting to discuss how it will adapt to the changing context of digital threats and vulnerabilities within which humanitarians operate. As these discussions continue, this section provides recommendations for the sector.

5.1. A seat at the table of enterprise risk management

The interdisciplinary nature of digital security issues necessitates that, whether through a procurement process or a partnership where an organisation receives free services, all decisions made about the use of technology at all levels need to be viewed through the lens of SRM. In several interviews, experts highlighted that SRM specialists do not always have a seat at the table at the highest levels of an organisation. When they do, their advice is often overlooked. Given the interdisciplinary nature of the aforementioned digital security threats, organisations must provide a seat for SRM professionals at the table when discussing various issues relating to their organisation and its security. Preferably, SRM experts should gain a seat at the table in both meetings involving high-level executives as well as board meetings. Beyond simply offering an honorary place for SRM experts in these discussions, high-level executives and board members should actively seek the advice of SRM experts when it comes to all operational and programmatic issues, including as they relate to digital technology. Approaching this from an enterprise risk management perspective can offer a solid framework for identifying internal vulnerabilities and mitigation measures. An interdisciplinary, comprehensive, and multi-layered risk matrix should address concerns that arise from the use of digital technologies in programs and operations.

5.2. Hiring of people with interdisciplinary experience and building interdisciplinary teams

SRM requires a holistic and interdisciplinary approach to bring together all departments in order to build effective mitigation and crisis preparedness strategies. This requires creating job roles and hiring people with interdisciplinary knowledge who are able to ‘speak the language’ of all the experts, such as the language used in operations, IT, physical security, fundraising, and advocacy. One cannot be expected to be an expert in all these areas, but having a broad knowledge of the various risk elements of the sector is increasingly necessary.

Some organisations have already begun to implement this holistic, interdisciplinary approach. The International Federation of the Red Cross and Red Crescent Societies (IFRC) Solferino Academy has developed the Data Playbook, a vital tool for improving organisational data literacy (IFRC, 2022). When recruiting for their new digital security officer and implementing changes to how digital security is approached, an interviewee indicated that their organisation did not recruit purely on IT skills, but instead considered a more comprehensive skillset for new hires. In this example, the security team worked with the communications and advocacy teams to ensure roles were filled by someone whose cross-functional knowledge met the needs of a changing world.

5.3. Investing in capacity building and processes

For the last 10 years, much of the investment around digital technologies has focused on innovation of the digital tools themselves and not the people who use them or on mitigating the associated risks, especially as it relates to in-country staff and local partners. People are still the core of organisations, and investment in them should be equal to the technology.

Access to (digital) security training should be equitable across the sector, regardless of location or position. Not only should staff at headquarters receive constant training on new technology and digital security threats, but organisations must make a concerted effort to provide sufficient training to in-country staff and work to ensure the staff of local organisations with whom they partner also receive proper training to protect against digital security threats. This may sound and read as a basic recommendation for bigger and well-resourced NGOs, but it is often the case for smaller partners. If a local partner organisation does not provide sufficient training to its staff, international NGOs must work with their partners to ensure all national staff receive equitable security training on digital, and other issues. Also, where possible, INGOs should take advantage of their digital security infrastructure and promote risk sharing with local organisations. Doing so will help advance the security interests of local partners.

5.4. Sharing of information, good practices, and lessons learnt

Beyond simply protecting against the threats posed by digital technology, humanitarian organisations should take advantage of the benefits of an increasingly digitalised world. Digital technology offers an opportunity to streamline the sharing of information within and between organisations and communities.

6 Bibliography

Al Achkar, Z. (2021). Digital Risk: how new technologies impact acceptance and raise new challenges for NGOs. Global Interagency Security Forum (GISF), https://gisf.ngo/wpcontent/uploads/2021/12/Digital_Risk_how_new_technologies_impact_acceptance_and_raise_new_challenges_for_NGOs.pdf.

al-Jablawi, H. (2018). The White Helmets Struggle Without US Funding. Atlantic Council, https://www.atlanticcouncil.org/blogs/syriasource/the-white-helmets-struggle-without-us-funding/

Cambridge Dictionary. (n.d.-a). Hard Power. Cambridge Dictionary, https://dictionary.cambridge.org/dictionary/english/hard-power

Cambridge Dictionary. (n.d.-b). Soft Power. Cambridge Dictionary, https://dictionary.cambridge.org/dictionary/english/soft-power

Card, B., Grace, R. and Sable, T. (2022). Humanitarian Access, Great Power Conflict, and Large-Scale Combat Operations. Center for Human Rights and Humanitarian Studies (CHRHS), Brown University‘s Watson Institute for International and Public Affairs, https://watson.brown.edu/chrhs/files/chrhs/imce/research/HA-GPC-LSCO_Report-February-2022.pdf.

Carothers, T., & Press, B. (2022). Understanding and Responding to Global Democratic Backsliding - Carnegie Endowment for International Peace. Carnegie Endowment for International Peace, https://carnegieendowment.org/2022/10/20/understanding-and-responding-to-global-democratic-backsliding-pub-88173

Childs, A. K. (2013). Cultural Theory and Acceptance-Based Security Strategies for Humanitarian Aid Workers. Journal of Strategic Security, 6(1), 64–72, https://doi.org/10.5038/1944-0472.6.1.6

Coldwell-Neilson, J. (n.d.). What is Digital Literacy? - Developing Employability. Developing Employability, https://developingemployability.edu.au/educators/what-is-digital-literacy/

Cole, A., & Olympiou, P. (2022). Risk Management & Decision Making Under Uncertainty During the Afghanistan Crisis 2021, https://www.humanitarianoutcomes.org/sites/default/files/publications/cole_olympiou_risk-management-decision-making-under-uncertainty-during-the-afghanistan-crisis-2021.pdf

CyberPeace Institute. (2022). Submission on the Protection of the Humanitarian Sector. Open-Ended Working Group on Security of and in the Use of Information and Communications Technologies 2021-225, https://cyberpeaceinstitute.org/news/submission-on-the-protection-of-the-humanitarian-sector-2/

Cybersecurity & Infrastructure Security Agency. (n.d.). Cybersecurity and Physical Security Convergence. CISA, https://www.cisa.gov/sites/default/files/publications/Cybersecurity%20and%20Physical%20Security%20Convergence_508_01.05.2021_0.pdf

Elliot, V. (2022). Humanitarian organisations keep getting hacked because they can't spend to secure data. Rest of World, https://restofworld.org/2022/humanitarian-organizations-hack/

European Civil Protection and Humanitarian Aid Operations. (n.d.). Cash transfers. ECHO, https://civil-protection-humanitarian-aid.ec.europa.eu/what/humanitarian-aid/cash-transfers_en

Global Interagency Security Forum (GISF). (n.d.). What is humanitarian security risk management? GISF, https://gisf.ngo/about/what-is-humanitarian-security-risk-management/

Global Interagency Security Forum (GISF). (n.d.). Essential NGO Security Resources, Tools and Templates. GISF, https://www.gisf.ngo/toolbox-pwa/

Global Interagency Security Forum (GISF). (2015). Security To Go (Module 3). GISF, https://gisf.ngo/wp-content/uploads/2015/09/EISF_Security-to-go_guide_Module-3_Risk-assessment-tool.pdf

Global Interagency Security Forum (GISF). (2020). Security To Go: A Risk Management Toolkit for Humanitarian Aid Agencies. GISF, https://www.gisf.ngo/resource/security-to-go/

Global Interagency Security Forum. (2021). Achieving Safe Operations through Acceptance: Challenges and opportunities for security risk management. GISF, https://www.gisf.ngo/resource/achieving-safe-operations-through-acceptance/

Harper, N., & Dobrygowski, D. (2022). Why the humanitarian sector must make cybersecurity a priority. World Economic Forum, https://www.weforum.org/agenda/2022/01/why-humanitarian-sector-cybersecurity-a-priority/

Humanitarian Advisory Group, International Council of Voluntary Agencies (ICVA), and Innovation Center for Risk Governance at Beijing Normal University, & Zhang, D. (2019). Positive Disruption? China's Humanitarian Aid, https://humanitarianadvisorygroup.org/wp-content/uploads/2020/12/HH_China-Practice-Paper_Final-December-2019.pdf

Independent Consultant. (2022). From Cyber Attacks to Bot Farms: The Top Tech Threats Humanitarians Face in Ukraine. The New Humanitarian, https://www.thenewhumanitarian.org/opinion/2022/03/09/from-cyber-attacks-to-bot-farms

International Committee of the Red Cross (ICRC). (2022a). Cyber-attack on ICRC: What We Know. ICRC, https://www.icrc.org/en/document/cyber-attack-icrc-what-we-know

International Committee of the Red Cross (ICRC). (2022b). Digitalising the Red Cross, Red Crescent and Red Crystal Emblems. ICRC, https://www.icrc.org/en/document/icrc-digital-emblems-report

International Committee of the Red Cross (ICRC). Misinformation about ICRC activities for people affected by conflict in Ukraine. (2022c). ICRC, https://www.icrc.org/en/document/false-information-about-icrc-ukraine

International Federation of the Red Cross (IFRC). (2022). Data Playbook. IFRC, https://preparecenter.org/wp-content/uploads/2022/11/DTPB_V1.pdf

Jaikaran, C. (2022). Cybersecurity: Deterrence Policy. Congressional Research Service, https://crsreports.congress.gov/product/pdf/R/R47011

Kidd, C. (2022). Vulnerabilities, Threats & Risk Explained. Splunk, https://www.splunk.com/en_us/blog/learn/vulnerability-vs-threat-vs-risk.html

Korolov, M. (2021). What is a supply chain attack? Why to be wary of third-party providers. CSO Online, https://www.csoonline.com/article/3191947/supply-chain-attacks-show-why-you-should-be-wary-of-third-party-providers.html

Lamensch, M. (2022). For Syria’s White Helmets, the Ukraine War Is Déjà Vu. Centre for International Governance Innovation, https://www.cigionline.org/articles/for-syrias-white-helmets-the-ukraine-war-is-d%C3%A9j%C3%A0-vu/

Library Guides: News: Fake News, Misinformation & Disinformation. (2022). UW Bothel and Cascadia College, https://guides.lib.uw.edu/bothell/news/misinfo

Lough, O., et. al. (2022). Social media and inclusion in humanitarian response. Overseas Development Institute, https://odi.org/en/publications/social-media-and-inclusion-in-humanitarian-response-and-action/

Marelli, M. (2022). The SolarWinds hack: Lessons for international humanitarian organisations. International Review of the Red Cross, 104(919), 1267–1284, https://doi.org/10.1017/S1816383122000194

Marquardt, A., & Lyngaas, S. (2022). Ukraine suffered a comms outage when 1,300 SpaceX satellite units went offline over funding issues. CNN Politics, https://edition.cnn.com/2022/11/04/politics/spacex-ukraine-elon-musk-starlink-internet-outage/index.html

Merriam Webster Dictionary. Deterrence. (n.d.). Merriam-Webster, https://www.merriam-webster.com/dictionary/deterrence

Microsoft. (2022). Microsoft Digital Defense Report 2022, https://www.microsoft.com/en-gb/security/business/microsoft-digital-defense-report-2022

Milmo, D. (2022). NHS ransomware attack: what happened and how bad is it? The Guardian, https://www.theguardian.com/technology/2022/aug/11/nhs-ransomware-attack-what-happened-and-how-bad-is-it

Mooser, A. P. E. (2023).How to manage (mis) information in humanitarian operations. Frontline Negotiations, https://frontline-negotiations.org/blog-how-to-manage-misinformation-in-humanitarian-operations/

National Intelligence Estimate. (n.d.). Climate Change and International Responses Increasing Challenges to US National Security Through 2040. Director of National Intelligence, https://www.dni.gov/files/ODNI/documents/assessments/NIE_Climate_Change_and_National_Security.pdf

NATO Defence Education Enhancement Programme. (n.d.). What is information warfare? https://www.nato.int/nato_static_fl2014/assets/pdf/2020/5/pdf/2005-deepportal4-information-warfare.pdf

Norwegian Refugee Council. (2022). Digitising humanitarian aid. NRC, https://www.nrc.no/perspectives/2022/digitising-humanitarian-aid/

Oh, S., & Adkins, T. L. (2018). Disinformation Toolkit. InterAction, https://www.interaction.org/wp-content/uploads/2019/02/InterAction_DisinformationToolkit.pdf

Palantir. (n.d.). Palantir Impact | Delivering Lifesaving Assistance with WFP, https://www.palantir.com/impact/world-food-programme/

Palmer, D. (2021). Three Billion Phishing Emails Are Sent Every Day. But One Change Could Make Life Much Harder for Scammers. ZD Net, https://www.zdnet.com/article/three-billion-phishing-emails-are-sent-every-day-but-one-change-could-make-life-much-harder-for-scammers/

Parker, B. (2017). Security lapses at aid agency leave beneficiary data at risk. The New Humanitarian, https://www.thenewhumanitarian.org/investigations/2017/11/27/security-lapses-aid-agency-leave-beneficiary-data-risk

Pearn, K., & Verity, A. (2022). Mis & Disinformation - Handling the 21st Century Challenge in the Humanitarian Sector. DH Network, https://reliefweb.int/report/world/mis-disinformation-handling-21st-century-challenge-humanitarian-sector-february-2022

RAND. (n.d.). Cyber Warfare, https://www.rand.org/topics/cyber-warfare.html

Reuters (2002). Russia using energy as weapon, White House says about Nord Stream shutdown. Reuters, https://www.reuters.com/business/energy/russia-using-energy-weapon-white-house-says-about-nord-stream-shutdown-2022-09-02/

Ringhof, J., & Torreblanca, I. (2022). The Geopolitics of Technology: How the EU Can Become a Global Player. European Council on Foreign Relations, https://ecfr.eu/publication/the-geopolitics-of-technology-how-the-eu-can-become-a-global-player/b

Robinson, J. (2007). Russian Foreign Humanitarian Assistance Identifying Trends Using 15 Years of Open-Source Data. Marine Corps University, https://doi.org/10.36304/ExpwMCUP.2022.05

Rodenhäuser, T., Staehelin, B., and Marelli, M. (2022). Safeguarding humanitarian organisations from digital threats. Humanitarian Law & Policy Blog, https://blogs.icrc.org/law-and-policy/2022/10/13/safeguarding-humanitarian-organizations-from-digital-threats/

Schroeder, W. A. (2019). NATO at Seventy: Filling NATO's Critical Defense-Capability Gaps. Atlantic Council Scowcroft Centre for Strategy and Security, https://www.atlanticcouncil.org/wp-content/uploads/2019/04/NATO_at_Seventy-Filling_NATOs_Critical_Defense-Capability_Gaps.pdf

SeaGlass Technology. (2020). What Is Digital Hygiene? https://www.seaglasstechnology.com/what-is-digital-hygiene/

Shaheen, K. (2018). "Heartbroken" White Helmets Say They Fled Syria Fearing Assad Reprisals. The Guardian, https://www.theguardian.com/world/2018/jul/24/white-helmets-says-volunteers-fled-syria-fearing-assad-reprisals

Slim, H. (2022). Solferino 21 Warfare, Civilians and Humanitarians in the Twenty-First Century. Hurst & Co, https://www.hurstpublishers.com/book/solferino-21/

The Guardian. (2022). Pentagon considering paying for Musk's Starlink network in Ukraine. The Guardian, https://www.theguardian.com/world/2022/oct/17/pentagon-starlink-ukraine-musk-funding

The Syria Campaign. (2017). Killing The Truth, https://thesyriacampaign.org/wp-content/uploads/2017/12/KillingtheTruth.pdf

Tuckwood, C. (2019). Hagiga Wahid – Stopping harmful misinformation in Uganda and South Sudan. The Sentinel Project, https://thesentinelproject.org/2019/03/08/hagiga-wahid-stopping-harmful-misinformation-in-uganda-and-south-sudan/

UK National Cyber Security Centre. (2018). Supply chain security guidance, https://www.ncsc.gov.uk/collection/supply-chain-security

United Nations. (2020). DO and SMT Handbook: A guide for Designated Officials for Security and Security Management Teams. UN Department of Safety and Security, https://www.un.org/sites/un2.un.org/files/2021/03/undss-do_handbook_2020.pdf

UN Security Council. (2022). Russian Federation's Suspension of Participation in Black Sea Grain Initiative Risks Impacting Global Food Prices, Top Officials Tells Security Council.Reliefweb, https://reliefweb.int/report/world/russian-federations-suspension-participation-black-sea-grain-initiative-risks-impacting-global-food-prices-top-officials-tells-security-council

US Department of Defense. (2018). Summary of the 2018 National Defense Strategy of the United States of America, https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf

van der Merwe, J., Spierings, J., & Al Achkar, Z. (2019). What would it take for a company like Palantir to become an acceptable ally?. Centre for Innovation, https://www.centre4innovation.org/stories/what-would-it-take-for-a-company-like-palantir-to-become-an-acceptable-ally/

van Sant, S. (2022). Russian Disinformation Targets Aid Workers. Foreign Policy, https://foreignpolicy.com/2022/08/01/russia-disinformation-ukraine-syria-humanitarian-aid-workers/

Vazquez Llorente, R., & Wall, I. (2016). Communications Technology and Humanitarian Delivery Challenges and Opportunities for Security Risk Management. European Interagency Security Forum (EISF), https://www.gisf.ngo/resource/communications-technology-and-security-risk-management/

Vosoughi, S., Roy, D., & Aral, S. (2018). The spread of true and false news online. Science, https://www.science.org/doi/10.1126/science.aap9559

Worley, W. (2022). Exclusive: ICRC Says Cyberattack Was “State-like” in Nature. Devex, https://www.devex.com/news/exclusive-icrc-says-cyberattack-was-state-like-in-nature-102593

Xu, R. (2021). You can’t handle the truth: misinformation and humanitarian action. ICRC Humanitarian Law & Policy, https://blogs.icrc.org/law-and-policy/2021/01/15/misinformation-humanitarian/

gisf

Global Interagency Security Forum

GISF Research and Programmes Manager
T: +44 (0)20 7274 5032
E: research@gisf.ngo

www.gisf.ngo