What makes cybersecurity in humanitarian aid different? Insights from practitioners on key challenges

Anfuso, Chiara; Bartolucci, Andrea; Del-Real, Cristina; Moallem, Abbas

What Makes Cybersecurity in Humanitarian Aid Different? Insights from Practitioners on Key Challenges

Chiara Anfuso[1][0009-0002-7219-840X], Andrea Bartolucci[1][0000-0001-9128-1685] and Cristina Del-Real[1] [0000-0003-3069-4974]

[1]Institute of Security and Global Affairs (ISGA), Leiden University, The Hague, Netherlands

Corresponding author: Chiara Anfuso, c.anfuso@fgga.leidenuniv.nl

Abstract. Humanitarian organizations are increasingly facing cyber threats that put their data and the populations they serve at risk, making effective cybersecurity essential to uphold their mission and values. Yet humanitarian organizations face unique organizational, operational, and normative challenges that hinder cybersecurity. To gain a comprehensive understanding of these challenges, this mixed-method study investigates the key obstacles to effective cybersecurity implementation, drawing on practitioners' experiences. The findings reveal a critical insight: every cybersecurity decision involves difficult trade-offs across a complex web of humanitarian, legal, ethical, and operational priorities. While the study confirms that the humanitarian organizational and operational context poses challenges to implementing conventional cybersecurity measures, practitioners continue to value these practices. This suggests that the key challenge is not their applicability but navigating the complex balance between cybersecurity and humanitarian needs. Treating cybersecurity as a mere checklist is therefore ineffective for these organizations; instead, humanitarian organizations must determine which measures hold the greatest value and how to integrate them without compromising the organization's mission. Accordingly, this study stresses the need to rethink cybersecurity not as an isolated concern, but as an integral element of humanitarian decision-making.

Keywords: Cybersecurity Challenges, Humanitarian Organizations, Mixed method.

1 Introduction

1.1 Cyber Risks in Humanitarian Innovation

Technological innovation has become central to humanitarian work, with tools such as digital data platforms, biometrics, and even Artificial Intelligence (AI) increasingly shaping how aid is delivered [1], [2]. But as humanitarian organizations become more reliant on these technologies and data, they must face a critical vulnerability: heightened exposure to cyber threats.

Recent reports underscore the scale of this risk. As highlighted by Microsoft [3], [4], non-governmental organizations (NGOs) were the fourth most targeted sector by nation-state-affiliated threat actors in both 2024 and 2025. In 2025 Cloudflare [5], [6] also reported nearly 325.2 million cyberattacks per day targeting civil groups and nonprofits, which marked a 241% increase compared to 2024. This surge in attacks indicates that for humanitarian organizations the question is no longer whether they will face a cyber incident, but when.

Humanitarian organizations collect highly sensitive and geopolitically valuable data that makes them attractive targets for both criminals and state threat actors [7], [8], [9], [10]. At the same time, these organizations often struggle to implement robust cybersecurity measures due to unique constraints, such as limited resources and difficult operational environments [10], [11], [12], [13]. It is precisely this dichotomy—being a high-value target with low cybersecurity—that leaves humanitarian organizations highly vulnerable to cyber incidents.

But for a humanitarian organization, the ability to prepare and respond to cyber incidents determines whether the data and tools it relies on safeguard the individuals it strives to protect, or endanger them. When a humanitarian organization collects sensitive information—such as biometrics or medical records—it is not merely handling data; it is holding the identities and fragile positions of at-risk and vulnerable individuals. Robust cybersecurity for humanitarian organizations is therefore not just a technical concern, but a deeply human one, critical to uphold one of their core principles: do no harm [14], [15]. Given these high stakes, cybersecurity must become integral to humanitarian operations to ensure the protection of individuals and their data.

Cybersecurity best practices developed for private companies or other well-resourced organization, however, do not account for the unique needs of humanitarian organizations. Moreover, they do not consider the unique normative and symbolic needs that define humanitarian work, such as adherence to the humanitarian principles. These defining characteristics of humanitarian operations might clash with the implementation of certain cybersecurity measures, requiring adaptation.

The humanitarian example exposes a broader gap in the cybersecurity field, or rather a lack of tailored strategies to address distinctive organizational and contextual realities, particularly in high-risk or low-resource settings. This gap underscores the need for a better understanding of how people, technology, and (operational) contexts interact to shape cybersecurity needs in specific contexts. With this study, we hence raise a central question: what makes cybersecurity in humanitarian aid different?

1.2 The Objective and Subjective Dimensions of Humanitarian Organizations

Humanitarian organizations present characteristics that differentiate them from other types of organizations. Some of these differences relate to their structural and operational aspects; humanitarian organizations often operate in high-risk regions with limited connectivity [13], [16] and usually rely on constrained budgets and resources [11], [17], among other similar obstacles. But an equally important dimension that further distances humanitarian organizations from other sectors lies in their normative and symbolic features. These characteristics include ethical obligations, adherence to the humanitarian principles, and the trust of communities and donors [18], [19], [20]. Such normative elements are important enablers of humanitarian operations; without them, humanitarian organizations risk losing access to crisis-affected regions, funding, and other assets essential to fulfill their mission [21], [22]. Given the importance of these characteristics, humanitarian organizations cannot treat cybersecurity only as a technical concern; rather, the adoption of cyber measures must be deeply linked to mission delivery, trust, and other normative considerations.

This dual aspect of humanitarian organizations makes it essential to examine both their "objective" and "subjective" dimensions. With the objective dimension, we refer to the tangible, verifiable aspects of cybersecurity, including the measures in place as well as the organizational and operational conditions that shape cybersecurity implementation (e.g., budget, staff constraints). In contrast, the subjective dimension captures the perceptions and interpretations of cybersecurity. This includes, for example, the perceived impacts of cyber incidents on organizational reputation, stakeholder trust, or funding, as well as the tendency to underestimate risks. We argue that, to gain a comprehensive understanding of cybersecurity needs, the focus should extend beyond technical concerns to focus on the challenges that arise from both these dimensions. In this article, we hence address both the objective and subjective characteristics of humanitarian organizations to identify the technical, organizational, and operational vulnerabilities that cybersecurity poses, as well as important normative considerations.

1.3 The Current Study

The study has two core aims: (1) to investigate what key cyber challenges humanitarian organizations face; and (2) to gain a deeper understanding of these challenges from the perspective of practitioners, exploring how they experience them and why they consider certain obstacles most important. Existing reports, which provide valuable descriptive quantitative accounts of existing cybersecurity practices, highlight serious cybersecurity gaps across humanitarian organizations (e.g. [10], [23]). Little is known, however, about the underlying causes of these gaps and whether different types of organizations face distinct challenges. Additionally, firsthand practitioners' experiences remain largely unexplored. To address these gaps, the study adopts a concurrent embedded mixed-methods design to offer a foundation for developing more effective strategies tailored to the needs of the humanitarian sector.

2 Methodology

This study presents an analysis of the core challenges to humanitarian cybersecurity, as identified by humanitarian practitioners. It adopts a concurrent embedded mixed-method design, in which a quantitative and a qualitative components are conducted simultaneously [24]. Participants filled in a questionnaire while thinking aloud, while concurrently responding to follow-up questions to collect deeper insights into their questionnaire responses. The quantitative and qualitative phases are described in further detail in Section 2.1.

In an embedded design, one method is dominant, while the other ("embedded") plays a supporting role to enrich or contextualize the main findings [25]. In this study, the qualitative phase constituted the dominant component, while the questionnaire was embedded to structure the discussion, provide descriptive frequencies, and enable comparisons across organizations. Questionnaire responses directly informed the interview questions, with integration occurring during data collection [24], [25] (see Figure 1).

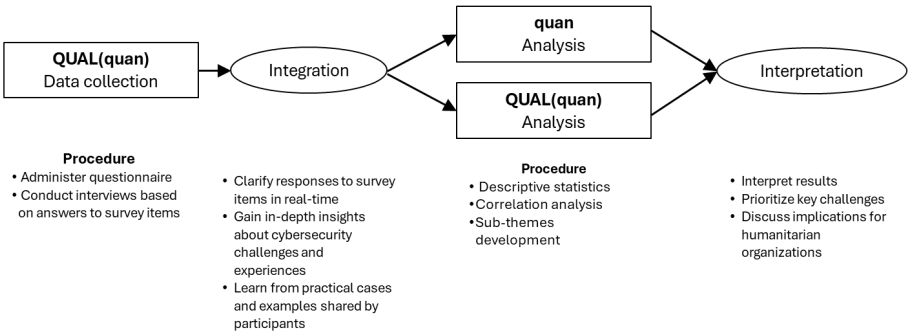

Figure 1: Study procedural diagram (according to Moeller et al. [5]).

2.1 Data collection

We recruited participants through purposive and snowball sampling between December 2025 and January 2026. The inclusion criteria required that participants: (1) were employees of a humanitarian organization, (2) were responsible for cybersecurity and/or data protection within their organization, and (3) were fluent in English to ensure a correct understanding of the questionnaire. Previous scholars have emphasized the importance of focusing on smaller organizations and local contexts due to their higher vulnerability levels [11], [17]; accordingly, we aimed to recruit participants from different organizational types and sizes to capture potential differences and challenges. We did not apply any geographical restrictions.

This study used an identical sample of elite informants (e.g., data protection officers (DPOs), chief information officers (CIOs), heads of information technology (IT)) for both the quantitative and qualitative phases. We recruited participants via email or LinkedIn. Initially, we contacted 105 practitioners through purposive sampling; a follow-up email was sent to all in January 2026. From this sample, eight participants

replied and agreed to participate in the study, and four additional participants were recommended through snowball sampling. The final sample consisted of 12 participants. This sample size aligns with prior research on elite populations and is generally considered sufficient to generate in-depth qualitative insights [26], [27]. Consistent with these studies, we reached thematic saturation around the eighth interview.

Participants were first asked to fill in a questionnaire, which we developed deductively drawing on the key challenges identified in a previously conducted scoping literature review [28]. The questionnaire aimed to examine whether these literature-derived challenges reflect the lived realities of humanitarian organizations, identify possible areas of divergence, or additional challenges experienced by practitioners. It was designed and administered via Qualtrics for online interviews and paper format for in-person interviews. It represented the first phase of the study, with the qualitative design building on the participants' answers to the questionnaire items.

The questionnaire consisted of three core blocks: (1) objective characteristics, including implemented cybersecurity measures, organizational and operational challenges; (2) subjective characteristics, capturing the perceived impact of a cyber incident on organizational reputation, stakeholder trust, and funding, and the tendency to underestimate cyber risks; and (3) demographic characteristics, such as organizational type, work setting, and number of employees. The full questionnaire is provided in the Appendix.

We conducted interviews with participants while they were answering the questionnaire. The interviews aimed to explore the issues in greater depth and allow for the emergence of new insights beyond those identified in the literature. Examples of questions asked include: “Can you think of a situation in which this condition affected cybersecurity in your organization?” or “Can you explain why you ranked this factor as the most important?”

In total, we conducted four in-person interviews and eight online interviews via Microsoft Teams. All interviews were conducted with one participant at a time by one researcher (CA) to ensure consistency. Interviews lasted on average 45 minutes (including the time to fill out the questionnaire). All interviews were audio-recorded (following consent provided by participants before the interview) except one.

2.2 Data analysis

We analyzed the questionnaire responses in R (version 2024.09.0+375) using the tidyverse suite (readr, dplyr, tidyr, ggplot2). We calculated descriptive statistics for categorical variables (frequencies and percentages) and continuous variables (means, standard deviations, medians, and ranges). We further categorized organizations by size (small, medium, large, very large) based on the number of employees. To examine relationships among variables (e.g., funding and trust), we used Spearman’s rank-order correlations. To illustrate possible variations, we also visualized the distribution of the perceived cyber incident likelihood across organization size categories using a jitter plot.

Quantitative results were complemented with the insights collected with the qualitative interviews. We analyzed the interview data in Atlas.ti (version 23.4.0) using an inductive thematic approach [29]. Table 1 presents the core themes and identified sub-themes.

Table 1: Identified Themes and Sub-Themes.

Dimension	Questionnaire Core Themes	Interviews Sub-Themes
Objective	Implemented cybersecurity measures	(Insufficient) Training
		Limited cybersecurity personnel
		Learning from best practices
	Organizational challenges	Support from senior management
		Cybersecurity only as a technical issue
		Pace of cyber change
	Operational challenges	Headquarters versus field difficulties
		Nature of humanitarian aid
Subjective	Perceived cyber incident impact (reputation, trust, funding)	Type of incident
		Type of data
		Size of the incident
		History/frequency of incidents
		Type of response
		Leniency of donors
	Organization attitude towards cybersecurity	Cyber incident exposure

We structured the results and discussion section around the core themes of the questionnaire. Results are presented narratively, first outlining relevant quantitative results and then deepening these findings with qualitative insights and discussing the identified sub-themes.

2.3 Ethical considerations

The project was subject to appropriate ethical review at Leiden University (Ref: 2025-11-20-C. Anfuso-V2-6384). Before beginning the study, participants were provided with an information sheet and asked to sign a consent form, including permission to audio-record. Participation was voluntary, and participants were informed that they could withdraw at any time without consequences. To ensure anonymity, neither participants' nor organizations' names were recorded; we instead used pseudonyms for both data storage and reporting (e.g., Participant 1, Participant 2).

2.4 Limitations

The core limitation of this study lies in its quantitative component. This phase was designed to support the qualitative insights rather than to generate statistically robust results. The sample size was based on qualitative saturation, resulting in a small sample that was insufficient to make strong quantitative inferences. Consequently, the quantitative data could only provide descriptive results and could not be used to draw inferential insights. Despite these limitations, adopting this design allowed us to

identify the key cybersecurity challenges and, at the same time, contextualize them through participants' narratives. Combining this data allowed us to interpret the statistical results alongside the participants' lived experience, producing a more comprehensive understanding of the main challenges faced by humanitarian organizations.

3 Results and Discussion

3.1 Participants characteristics

Table 2: Individual-level demographic characteristics of the sample (n = 12)

Individual-level characteristics	*n*	*%*
Age	12	
Sex		
Male	9	75
Female	3	25
Job length		
1-2 years	2	16.7
3-5 years	4	33.3
6+ years	6	50.0
Work setting		
Headquarters/coordination	12	100
Field-based	0	
Mixed/rotates	0	

Table 3: Organization-level demographic characteristics of the sample (n = 12)

Organization-level characteristics	*n*	*%*
Organization type		
International NGO (INGO)	7	58.3
UN agency	4	33.3
National NGO	1	8.3
Local NGO	0	0
Number of employees	12	
Number of volunteers	7	
Organization size		
Small (<100 employees)	1	8.3
Medium (<5000 employees)	8	66.7
Large (<10000 employees)	2	16.7
Very Large (>10000 employees)	1	8.3

Table 2 and Table 3 present the demographic characteristics of the sample. At the individual level, participants were predominantly male, and most had worked in the organization for more than six years. Participants' ages ranged from 26 to 62 years (M = 44.8; SD = 10.7). All participants were based at organizational headquarters. Future

research should expand this sample by including field-based personnel, whose experiences may differ from those of headquarters staff, providing a more comprehensive understanding.

At the organizational level, most organizations were international NGOs (INGOs). The sample included organizations of varying sizes, ranging from approximately 30 employees to about 18,000 employees (M = 3894.2; SD = 5009). Most organizations did not rely on volunteers, with only one reporting about 500 volunteers (M = 71.6; SD = 188.9).

3.2 Objective Dimension

Implemented measures. Figure 2 presents the cybersecurity measures implemented across participating organizations.

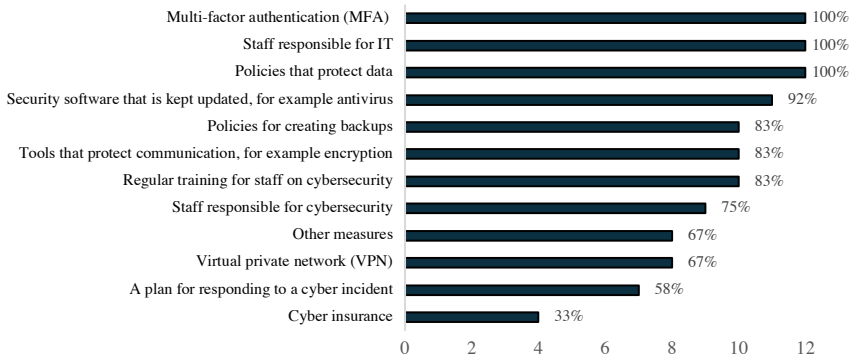

Figure 2: Implemented cybersecurity measures (n = 12)

All organizations reported having data protection policies, designated IT staff, and MFA in place, while cyber insurance and formal cyber-incident response plans were among the least implemented measures. Eight participants reported implementing additional measures beyond those listed, including data classification frameworks (e.g., public, internal, confidential, highly confidential), role-based access controls with individual user accounts, access and activity logging, and regular audit reviews. Some organizations were also exploring advanced solutions, such as machine learning and AI-based tools, for continuous network monitoring and threat detection.

Regarding *cybersecurity training*, although ten participants reported that their organization implemented such training, the interviews revealed that these programs often presented significant gaps. Most organizations provided an annual e-learning or Moodle-based course; others required staff to undergo an introductory training at the beginning of employment, which was neither mandatory nor enforced. Five participants reported offering multiple types of regular training for all staff, including an annual cyber awareness week and phishing simulations. Nevertheless, despite this more regular and comprehensive training, four of the five participants reported very poor test results across all members of staff, and questioned the training's efficacy. Similarly, while 12 participants reported having staff responsible for IT and nine reported having staff responsible for cybersecurity, the interviews revealed important limitations. All

participants, in fact, expressed concerns about *shortages of IT and cybersecurity personnel*. This shortage represented a particular concern for smaller organizations, which often had only one individual responsible for IT, who often combined this role with other functions. Nonetheless, all participants expressed concerns regarding the scarcity of cybersecurity personnel, irrespective of the organization's size.

During interviews, we asked participants how they selected and prioritized cybersecurity measures to implement in their organizations, and they reported drawing on *best practices* from both the humanitarian sector and other industries. The most frequently cited sources included the IT and private sectors, critical infrastructure, and hospitals. Some organizations also looked at frameworks such as the CIS Controls, ISO standards, and NIST guidelines; Participant 2 explained that implementing these measures has become easier as more humanitarian CIOs come from the private sector, bringing relevant experience with them. Several organizations also reported relying on Microsoft and its cybersecurity guidelines or outsourcing their systems to IT service providers, a practice that participants generally viewed as efficient. Nonetheless, two practitioners expressed concerns about potential losses of data sovereignty and the risks that could arise if Microsoft services were to become suddenly unavailable.

Beyond concerns about data sovereignty, some participants argued that cybersecurity measures developed for the private sector do not always fit humanitarian needs. As Participant 8 explained, certain measures may not work in conflict settings or in environments with limited internet connectivity. Similarly, Participant 3 observed that humanitarian organizations cannot strictly follow certain regulations, such as GDPR requirements, as these were not written with NGOs in mind but rather for large technology companies. Despite recognizing these limitations, Participant 5 argued that drawing on private industry's best practices still can be useful:

> We're no more special than a private industry. … If you think of the private sector and the amount of data that your bank has or your insurance provider or your doctor has, it's as much or more than what the humanitarian sector is ever going to have or should have. … Sometimes we think we're special. … I don't think, in today's era, that the humanitarian sector very often needs to even custom-build tools. They can use tools that are available and configure them. …The way that our business runs might be different, but I think we can adapt what's available.

While opinions differed on the full applicability of private-sector practices, many participants agreed and emphasized the importance of learning and knowledge sharing within the humanitarian sector itself. As highlighted by participants, looking at what other NGOs are doing is essential, as these measures are compatible with budgets and operational capacities. To this end, participants noted the usefulness of sector-specific knowledge-sharing platforms, such as NetHope.

These findings indicate a growing commitment to cybersecurity, but they also highlight practical difficulties associated with effective implementation. When we asked participants whether their organizations had encountered challenges in implementing any of these measures, 11 of 12 (92%) confirmed that they had. The specific nature of these challenges is discussed in the following sections.

Organizational Challenges. Table 4 and Figure 3 present the organizational challenges to cybersecurity, ranked by priority.

Table 4: Organizational challenges by average priority (n = 11)

Priority	Organizational challenges	Average Rank
1	Other priorities are seen as more urgent, for example, mission needs	2.27
2	Limited budget or funding	2.36
3	Insufficient IT or cybersecurity staff	2.64
4	Lack of cybersecurity expertise in the organization	3.73
5	Old or outdated systems and technologies	4.09
6	Strong dependence on volunteers	5.91

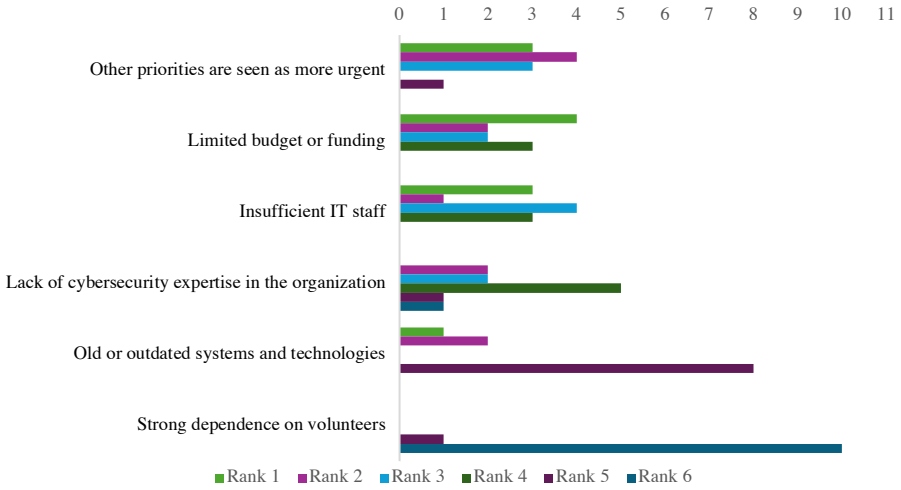

Figure 3: Participants' ranking of organizational challenges.

While lack of funding, personnel shortages, and other organizational priorities were identified as core challenges across participants, the interviews revealed two additional obstacles to effective cybersecurity implementation: (1) lack of support from senior management, and (2) cybersecurity being perceived only as a technical concern. Participants described these challenges as the underlying cause of the other issues and as the real obstacles to effective cybersecurity implementation.

Ten out of 11 participants flagged *support from senior management* as crucial to avoid most of the listed cybersecurity challenges. Participant 8, for example, suggested

that if senior management recognized cybersecurity as a significant concern for the organization, funding would become available; this funding, however, is often directed toward priorities that senior management deems more important. This idea was supported by Participant 9, who reported strong senior management support and, consequently, no difficulties in obtaining funding or resources for cybersecurity.

Such a lack of understanding from senior management also leads to not taking cybersecurity skills and expertise seriously. As stressed by Participant 11, many organizations may have robust cybersecurity policies and systems in place, yet—as shown by the phishing simulations' and training results—most staff members know very little about cybersecurity. He argued that maintaining a decent baseline level of cybersecurity awareness should be a requirement for employees working in organizations dealing with such complex operations and data. The limited cybersecurity expertise across employees, however, is often tolerated because senior staff and management do not fully recognize its importance.

Linked to the lack of senior management support is the challenge of employees perceiving *cybersecurity only as a technical concern*. Participants expressed frustration with the general lack of understanding that IT is not a standalone unit and that cybersecurity issues are not an exclusive responsibility of the IT or cybersecurity department. Participant 12 indicated that a core challenge remains convincing everyone to take cybersecurity seriously, stressing that an IT-only approach is not sufficient. As Participant 10 affirmed:

> Training colleagues, training people, educating people in general about cybersecurity, and how to be aware of protecting yourself. This is the main challenge. It's not technology, it's human.

This human factor becomes even more critical given the *rapid pace of cyber change*. As Participant 9 noted, "For every wall, there's a bigger ladder." Organizations must constantly adapt as cybercriminals develop new methods. This constant change, however, makes implementing new policies or technologies difficult, since—as indicated by Participant 10—people naturally resist change. In this respect, Participant 11 warned of another important related aspect: poorly implemented new technologies can introduce additional vulnerabilities. This need for constant innovation and reliance on new tools hence means that even innovation itself can become a source of risk.

Together, these findings show that the challenges to effective cybersecurity implementation extend well beyond technical and resource-related constraints. Limited budgets and capacity shortages remain significant obstacles; the most critical challenges, however, stem from human and organizational factors, especially insufficient senior management support and a narrow perception of cybersecurity as a purely technical issue. Consequently, overcoming funding, resource, and other technical constraints requires, above all, a change in senior management and an organization-wide understanding that cybersecurity is crucial to humanitarian work.

Operational Challenges. Table 5 and Figure 4 present the key operational challenges to cybersecurity as prioritized by participants.

Table 5: Operational challenges by average priority (n = 11)

Priority	Operational challenges	Average Rank
1	Working in unsafe or unstable locations (e.g., conflict zones)	2.64
2	Weak and unreliable internet or damaged infrastructure	2.82
2	Difficulty making sure no outside actors can access sensitive information	2.82
4	Restrictions from authorities, armed groups, or local policies	3.09
5	Strong dependence on local partner organizations	3.64

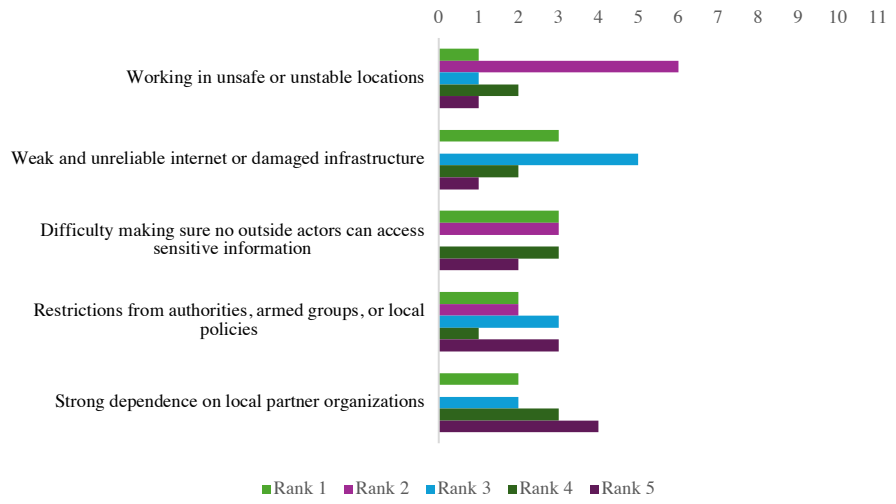

Figure 4: Participants' ranking of operational challenges.

Compared to the organizational challenges, participants struggled more with clearly prioritizing operational challenges, most of which they perceived as relevant to humanitarian work. The interviews ultimately revealed that the core umbrella issue often stems from the *contrasts between headquarters and field/regional offices*.

Participants noted that while differences between headquarters and field offices exist for most systems and practices, these discrepancies are especially evident for cybersecurity. Field office work, in fact, comes with additional difficulties that often increase the organization's vulnerability to cyber incidents. Participants referred to issues of censorship, limited internet access, and even cases of phones being taken away and then given back by local authorities. As Participant 1 explained, "When the network is disconnected, we lose the ability to collaborate with people on site, who must make do with what they have at hand." These conditions often conflict with standards developed for and with headquarters in mind, meaning cybersecurity measures are more difficult to maintain in certain regional offices.

Participants also highlighted that operating across multiple countries comes with tensions arising from different cultures, cybersecurity understanding, and legal requirements. One clear example is the GDPR. As explained by Participant 3, while in Europe the GDPR governs how personal data should be handled, local authorities in some countries expect full access to information about beneficiaries and operations. This, of course, contrasts with European headquarters' requirements and creates a constant balancing act: organizations must protect sensitive data to comply with GDPR, but they also need to satisfy local authorities and legal requirements. This challenge extends beyond data protection concerns to issues with websites and online tools access that are heavily restricted in some countries; such restrictions force practitioners to ask difficult questions: Should they provide colleagues with the digital platforms they would normally rely on? And if so, how would they do it without breaking the law of the country of operation or exposing sensitive information?

Even the *nature of humanitarian aid* itself was identified as an additional vulnerability to fieldwork. As Participant 12 emphasized, "We don't exist to be cyber secure. We exist to help people." Participant 6 argued that this inclination to help creates additional risks when deployed to a particular country. As he explained, humanitarian workers are naturally inclined to help others, and working in a humanitarian organization further reinforces this mindset: once you enter the organization, you are trained into its culture, and it becomes part of how you think and act. But this service-oriented mindset can increase staff vulnerability to social engineering attacks, as malicious actors exploit trust and compassion to gain access to information. In sum, the humanitarian ethos itself risks becoming a source of vulnerability to cyber incidents.

Although difficulties arising from fieldwork in certain regions were identified as a core concern by most participants, one of the most compelling insights to emerge from the interviews came from discussions about the least significant operational challenge. Unlike most participants, Participant 11 identified "Strong dependence on local partner organizations" as the primary challenge to humanitarian cybersecurity. As he explained, even when a humanitarian organization maintains robust internal cybersecurity standards, the practices adopted by local partners can introduce significant vulnerabilities. For example, data may be stored in unsecured Excel files, shared via email with multiple recipients, or kept on USB drives left in offices, all practices entirely beyond the humanitarian organization's control. Given that his organization worked with local partners in nearly every location, the participant emphasized that these risks would be far more likely to occur than the other listed challenges.

This observation prompted a broader reflection on how cybersecurity should be understood within the humanitarian context. As Participant 11 noted, cybersecurity is just one element of an organization's overall risk profile. This is particularly important for a humanitarian organization, which must balance cybersecurity with a range of considerations—including legal, ethical, and humanitarian factors—as well as with stakeholders' perceptions of cybersecurity measures. In practice, this means that cybersecurity does not always align with humanitarian needs. For example, an organization might want to use certain tools to increase cybersecurity, but these may be

poorly received by communities or difficult to implement in conflict settings. In brief, as Participant 11 emphasized, treating cybersecurity in isolation is neither practical nor feasible; instead, it must be considered within the broader organizational and operational context:

> One thing I've seen in the past is that… people go through and say, 'Oh, the organizations are doing this; they need to do XYZ cybersecurity measures, and then everything will be better in the world.' And they've not looked at a big part of the puzzle… I think it is really about trying to be less idealistic about them and much more practical.

This practicality, according to Participant 11, involves prioritizing the implementation of measures that are likely to reduce the biggest risks while remaining cost-efficient, especially given the budget constraints affecting the humanitarian sector. Addressing the poor cybersecurity practices of local partners, for example, may not sound as "flashy" or innovative as implementing high-profile, expensive technical solutions, but would likely yield better results. This perspective led him to raise a crucial question:

> The real challenge will be: what is the best-value cybersecurity action that organizations can take? That, really, is the question of the day—not what can we do, but what is the best-value thing that we can do?

3.3 Subjective Dimension

Impact of a Cyber Incident: Reputation, Trust, and Funding. We asked practitioners about the perceived impact of a cyber incident on three core aspects: the organization's (1) reputation, (2) trust, and (3) future funding (see Table 6).

Table 6: Perceived impact of a cyber incident on the organization (n = 12)

Impact area	Strongly disagree (1)	Disagree (2)	Somewhat disagree (3)	Neither agree nor disagree (4)	Somewhat agree (5)	Agree (6)	Strongly agree (7)
Reputation	0	0	1	0	0	6	5
%			8.3			50.0	41.7
Trust	0	0	1	1	3	5	2
%			8.3	8.3	25.0	41.7	16.7
Funding	0	0	0	4	3	3	2

Impact area	Strongly disagree (1)	Disagree (2)	Somewhat disagree (3)	Neither agree nor disagree (4)	Somewhat agree (5)	Agree (6)	Strongly agree (7)
%				33.3	25.0	25.0	16.7

Concerning reputation, 11 out of 12 participants (92%) agreed or strongly agreed that a cyber incident would harm their organization (*Mdn*: 6). Only one participant somewhat disagreed; as explained by Participant 12, his organization had recently faced a cyber incident, and its reputation had not suffered. Consequently, if before he would have agreed that a cyber incident would impact the organization's reputation, his opinion had changed following the incident. This perception was not shared by other participants whose organizations had faced a cyber incident, who still believed it would impact their reputation.

Participants also leaned toward agreement for the impact of a cyber incident on trust; compared to reputation, however, there was more variation in answers, with participants' ratings ranging from somewhat disagree to strongly agree (*Mdn* = 6). Participants explained this variation by highlighting a fundamental difference between trust and reputation: whereas reputation was described as a short-term concern, trust was viewed as a long-term issue for a humanitarian organization. Participant 1 noted that although the immediate organization's reputation might suffer in the aftermath of a cyber incident, trust depends on the organization's ability to handle it. In other words, organizations have limited control over the immediate reputational impact of a cyber incident but can influence its effect on trust. Because of this, Participant 1 argued that a cyber incident could even have a positive impact on trust if the organization demonstrated its ability to handle it effectively.

Similarly, responses to the impact on funding ranged from neutral to strong agreement (*Mdn* = 5.5). When answering this question, participants often associated potential funding impacts with losses in reputation and trust. This pattern was partially supported by Spearman's rank-order correlations, which showed a positive association between perceived funding impact and reputation (ρ = .39, p = .21), and a strong positive association between perceived funding impact and trust (ρ = .66, p = .018). These results indicate that participants who reported greater perceived impacts on reputation or trust also tended to report greater perceived impacts on funding.

One aspect on which participants disagreed regarding future funding opportunities was the *leniency of donors* following a cyber incident. Three participants felt that donors would recognize that NGOs are not large tech companies or banks and are doing their best to manage cybersecurity within their capacity. Participant 1 disagreed with this idea, arguing that donors would likely expect the same level of security as any other organization handling sensitive data. Similarly, Participant 11 noted that donors fund organizations to strengthen their cybersecurity; inadequate or insecure systems would therefore likely reflect negatively on the organization.

The interviews with participants on these three aspects revealed five interrelated sub-themes that emerged as key drivers of a cyber incident's impact on a humanitarian

organization: (a) the type of incident, (b) the type of data compromised, (c) the size of the incident, (d) the frequency/history of incidents, and (e) the type of response.

When thinking about the extent to which a cyber incident would harm their organization, most participants argued that it would depend on the *type of incident*. Participants explained that humanitarian organizations cannot realistically prevent certain incidents (e.g., state-sponsored attacks) and that relevant stakeholders would be understanding in such instances. But, as highlighted by Participant 9, there is a difference between being targeted by a state actor and lacking basic cybersecurity measures like MFA or being negligent. As put by Participant 10:

> When you come to me saying, "Oh, sorry, sorry, I had a car accident, I was driving, and somebody hit me." [Then I say] Okay, no problem. But if you come to me, "yeah, well, I was drinking, and I was driving fast, and somehow I hit something in the middle of this". Those are not the same incident.

Various participants closely linked the type of incident to the *type of data* compromised. Practitioners agreed that the more sensitive the data collected, the more cybersecurity should be a priority for a humanitarian organization; as a result, not being able to protect this data would lead to a bigger impact. For example, Participant 7 indicated that a website defacement might be perceived as morally wrong but generally understandable by stakeholders. In contrast, a breach exposing LGBTI+ beneficiaries' data in a high-risk country for this group would significantly damage the organization; as Participant 10 further explained, such an incident would also affect how beneficiaries perceive the organization: if their data is compromised, they may refuse aid in the future due to fear that their information could be accessed by the government.

Along with the concerns about data sensitivity, Participant 9 raised an important question of whether the *size of the incident* would matter more than the type of data compromised. As asked by the participant, "What if you had the medical records for 10 people versus 100,000 names and addresses? Which one is heavier? It's really hard to … put an algorithm around that." Similarly, Participants 10 and 12 flagged that the *frequency or history of incidents* could be an important element. For instance, Participant 12 noted that, while their organization had not faced repercussions following a recently experienced cyber incident, they were worried that repeated incidents could have more serious impacts, especially if reported in the press.

Ten participants also agreed that the extent of a cyber incident's impact would likely depend on the *humanitarian organization's response.* Participant 3, drawing on her previous experience with a donor organization, explained that donors focus less on whether an NGO has experienced a cybersecurity incident and more on how the organization handles it. In line with this view, Participant 6 added that the organization's response influences donor decisions because their primary concern is not data being compromised but avoiding negative publicity. Poor handling of an

incident could therefore lead donors to reconsider funding to protect their own reputation.

Overall, these results show that the impact of a cyber incident on reputation, trust, and funding depends on multiple interrelated factors and highlight the need for humanitarian organizations to prepare and respond effectively to mitigate such an impact.

Organizations' attitudes towards cybersecurity. Table 7 provides an overview of participants' perceptions of their organizations' attitude towards cybersecurity risks.

Table 7: Perceived organization's cyber risks (n = 12)

Attitude towards cybersecurity	Strongly disagree (1)	Disagree (2)	Somewhat disagree (3)	Neither agree nor disagree (4)	Somewhat agree (5)	Agree (6)	Strongly agree (7)
Cybersecurity is taken seriously	0	0	0	3	3	4	2
%				25.0	25.0	33.3	16.7
Underestimates cyber incident likelihood	1	2	0	2	4	3	0
%	8.3	16.7		16.7	33.3	25.0	

To the question of whether their organization took cybersecurity seriously, participants' responses ranged from neutral to strongly agree (*Mdn* = 5.5). Nonetheless, when asked whether their organizations underestimated the likelihood of a cyber incident, answers were more varied, from strongly disagree to agree (*Mdn* = 5). There were no relevant differences based on the organization's size (see Figure 5).

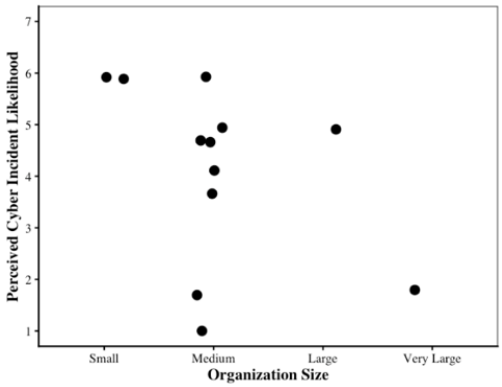

Figure 5: Jitter plot of organization size and perceived cyber incident likelihood.

When explaining why their organization underestimated the likelihood, participants mentioned an interesting factor: *the organization's exposure to a cyber incident*. Most

participants noted that their organization underestimated the possibility of a cyber incident simply because they had never faced one. Surprisingly, some participants even viewed this exposure as a positive event; Participant 12 stated that the incident that his organization faced was "the best that could have happened," as it immediately led to increased awareness and additional funding. Participant 9 shared a similar view:

> As an organization, the best thing that can happen to you is to have a near miss
>
> or some type of event that might be low impact but high visibility.

Participants explained that, in the aftermath of a cyber incident, everyone suddenly becomes very conscious of cybersecurity, including senior management. Consequently, this immediate visibility often accelerates the implementation of cybersecurity measures. Participants noted that, however, this heightened awareness tends to last briefly, only during the initial and most intense moments of the incident. Once resolved, upper management often reverts to the attitude that such an incident is unlikely to happen again.

Interestingly, Participant 4 noted that an organization does not necessarily need to experience a cyber incident directly for awareness to increase; simply hearing about cyber incidents in similar organizations can have a positive impact. The type and size of the organization, however, seemed to play an important role in this regard. Participant 4, who worked for a small humanitarian organization, explained that incidents in organizations like the International Committee of the Red Cross (ICRC) had not raised cybersecurity awareness in her organization. She suggested that organizations like the ICRC are "too far from reality" for smaller organizations. Instead, she argued that hearing about incidents in closer, more comparable organizations would provoke a stronger sense of concern. This idea underscores the value of sharing experiences and lessons learned within the humanitarian sector to enhance cybersecurity awareness.

4 Conclusion

The findings of this study reveal that humanitarian organizational and operational realities pose challenges to the implementation of cybersecurity measures developed for the private sector, as we initially assumed. Nevertheless, practitioners continue to value these practices, suggesting that the central issue is not their applicability, but rather how to navigate the complex balance between cybersecurity and humanitarian needs.

Humanitarian cybersecurity is not "different" simply because private-sector practices fail to translate or adapt; it is different because humanitarian organizations operate within a complex web of competing priorities. Budget constraints, resource limitations, and complex operational environments are real challenges to cybersecurity, but the true obstacle lies in finding the right balance: deciding when cybersecurity must take precedence over mission imperatives and when compromise is necessary.

Reflecting on these findings, we realize that we have been mistakenly approaching the issue as if cybersecurity were a mere checklist, focusing only on which measures

are implemented and what hinders their adoption. In doing so, we overlook that humanitarian organizations face constant trade-offs: cybersecurity must be balanced alongside legal, ethical, operational, and humanitarian considerations. Too little cybersecurity can compromise operations and endanger individuals, but too much can equally undermine missions and erode trust with communities or host countries. The critical question should hence not be whether to implement more cybersecurity measures, but which measures carry the greatest value and how to integrate them without undermining the organization's mission. As such, these findings stress the need to rethink cybersecurity not as an isolated concern but as one element in the broader realm of humanitarian decision-making.

Acknowledgments. The authors wish to thank the humanitarian practitioners who kindly participated in the study and shared their valuable insights. This study was supported by the Dutch Ministry of Education, Culture, and Science through the Starter Grants Program (grant number FGGA/2023-0044). It forms part of the project "Securing Humanitarian Operations: Preparedness and Response to Cyber Crises in Aid Delivery."

Disclosure of Interests. The authors have no competing interests to declare that are relevant to the content of this article.

Appendix – Full Questionnaire

Questions

Objective characteristics
Organizations apply cybersecurity measures to avoid incidents or to respond quickly when problems occur. These measures can include technologies (firewalls and antivirus), data protection (backups), or people-focused activities (cybersecurity awareness training), among others.

Q1 Which of the following measures are currently in place in your organization? **Select all the measures you have implemented.**

- Policies that protect data
- Regular training for staff on cybersecurity
- A plan for responding to a cyber incident
- Tools that protect communication, for example, encryption
- Staff responsible for IT
- Staff responsible for cybersecurity
- Policies for creating backups
- Cyber insurance
- Multi-factor authentication
- Security software that is kept updated, for example, antivirus
- Virtual private network (VPN)
- Other measures
- We don't have any cybersecurity measures in place.

Q2 Thinking about your organization's attempts to apply **at least one** of these cybersecurity measures, have you experienced any obstacles or difficulties during implementation?

- Yes, we faced difficulties
- No, we didn't face difficulties
- We have not attempted to implement any cybersecurity measures

Q3 Which of the following factors limits your organization's ability to implement cybersecurity? Rank all factors **from most to least important.**

_____ Limited budget or funding

_____ Insufficient IT or cybersecurity staff

_____ Strong dependence on volunteers

_____ Other priorities are seen as more urgent, for example mission needs

_____ Old or outdated systems and technologies

_____ Lack of cybersecurity expertise in the organization

Q4 Which of the following conditions make cybersecurity difficult in your organization? Rank all factors **from most to least challenging.**

_____ Working in unsafe or unstable locations (e.g., conflict zones)

_____ Weak and unreliable internet or damaged infrastructure

_____ Restrictions from authorities, armed groups, or local policies

_____ Difficulty making sure no outside actors can access sensitive information

_____ Strong dependence on local partner organizations

Subjective characteristics

Next, we would like you to share your perceptions of cybersecurity in your organization and the potential impacts of a cyber incident.

Please read the following statements regarding your organization's cybersecurity and indicate your level of agreement.

Q5 A cyber incident would harm my organization's reputation.

- Strongly disagree
- Disagree
- Somewhat disagree
- Neither agree nor disagree
- Somewhat agree
- Agree
- Strongly agree

Q6 A cyber incident would reduce the trust that key stakeholders have in my organization

- Strongly disagree
- Disagree
- Somewhat disagree
- Neither agree nor disagree
- Somewhat agree
- Agree
- Strongly agree

Q7 My organization underestimates the likelihood of a cyber incident

- Strongly disagree
- Disagree
- Somewhat disagree
- Neither agree nor disagree
- Somewhat agree
- Agree
- Strongly agree

Q8 Cybersecurity is taken seriously across my organization.

- Strongly disagree
- Disagree
- Somewhat disagree
- Neither agree nor disagree
- Somewhat agree
- Agree
- Strongly agree

Q9 A cyber incident would harm my organization's future funding opportunities.

- Strongly disagree
- Disagree
- Somewhat disagree
- Neither agree nor disagree
- Somewhat agree
- Agree
- Strongly agree

Demographics

Q10 What type of organization do you work for?

- UN agency
- International NGO (INGO)
- National NGO
- Local NGO
- Other _____

Q11 Is your organization part of the Red Cross and Red Crescent Movement?

- Yes
- No
- I don't know

Next, we would like to know about the number of paid employees and volunteers working for your organization

Q12 How many paid employees work for your organization?

- Approximately _____
- I don't know

Q13 How many volunteers work for your organization?

- Approximately _____
- I don't know

Q14 What is your current job title? _____

Q15 What is your primary regional focus?

- Africa
- Asia
- Europe
- Latin America and the Caribbean
- North America
- Oceania

Q16 What is your primary work setting?

- Field-based
- Headquarters/coordination
- Mixed/rotate

Q17 How long have you been working for your organization?

- Less than 1 year
- 1–2 years
- 3–5 years
- 6+ years

Q18 What is your sex?

- Male
- Female
- Prefer not to say

Q19 In which **month** were you born? _____

Q20 In which **year** were you born? _____

References

[1] L. Arendt-Cassetta, "From digital promise to frontline practice: new and emerging technologies in humanitarian action." United Nations Office for the Coordination for Humanitarian Affairs (OCHA), Apr. 19, 2021.

[2] A. Beduschi, "Harnessing the potential of artificial intelligence for humanitarian action: Opportunities and risks," International Review of the Red Cross. [Online]. Available: https://international-review.icrc.org/articles/harnessing-the-potential-of-artificial-intelligence-for-humanitarian-action-919

[3] Microsoft, "Microsoft Digital Defense Report 2024." 2024. [Online]. Available: https://www.microsoft.com/en-us/security/security-insider/threat-landscape/microsoft-digital-defense-report-2024#modal-dialog

[4] Microsoft, "Microsoft Digital Defense Report 2025." 2025. [Online]. Available: https://www.microsoft.com/en-us/corporate-responsibility/dmc/en-us/corporate-responsibility/cybersecurity/microsoft-digital-defense-report-2025/

[5] Cloudflare, "Impact Report 2025." 2025. [Online]. Available: https://cf-assets.www.cloudflare.com/slt3lc6tev37/7koyyovVxIqK8zdG1pqo6O/dfcbbde950394c61855befd9bf083a28/Impact-Report-2025-Final.pdf

[6] J. Woolbright, "Celebrating 11 years of Project Galileo's global impact." Jun. 12, 2025. [Online]. Available: https://blog.cloudflare.com/celebrating-11-years-of-project-galileo-global-impact/

[7] A. Fitz-Gerald and J. Hennebry, "Protecting civilians in a data-driven and digitalized battlespace: toward a baseline humanitarian technology infrastructure," *Front. Hum. Dyn.*, vol. 6, Jan. 2025, doi: 10.3389/fhumd.2024.1465594.

[8] K. B. Sandvik, "The centralization of vulnerability in humanitarian cyberspace: The ICRC hack revisited," in *Humanitarian extractivism*, Manchester University Press, 2023, pp. 38–56.

[9] L. Arendt-Cassetta, A. Omond, T. van Benthem, and Y. Shura, "Virtual Risk, Tangible Harm: The Humanitarian Implications of Cyber Threats." OCHA, 2022.

[10] NetHope, "State of Humanitarian and Development Cybersecurity Report." 2025.

[11] K. Saeedi, M. Hassan, S. Alarifi, and H. Almagwashi, "An intuitive approach to cybersecurity risk assessment for non-governmental organizations," *Transform. Gov. PEOPLE PROCESS POLICY*, Oct. 2024, doi: 10.1108/TG-08-2024-0201.

[12] R. Vhikai, E. Mugoni, A. P. Mataka, and F. Saruchera, "Digitalisation and efficient humanitarian logistical operations in Zimbabwe," *Cogent Soc. Sci.*, vol. 10, no. 1, p. 2321725, Dec. 2024, doi: 10.1080/23311886.2024.2321725.

[13] B. Parmadi and K. Ramli, "Transforming Humanitarian Response with IoT in Conflict Zones: Field Insights, Ethical Frameworks, and Deployment Challenges," *Int. J. Electr. Comput. Biomed. Eng.*, vol. 3, pp. 157–187, May 2025, doi: 10.62146/ijecbe.v3i1.112.

[14] K. B. Sandvik, K. L. Jacobsen, and S. M. McDonald, "Do no harm: A taxonomy of the challenges of humanitarian experimentation," *Int. Rev. Red Cross*, vol. 99, no. 904, pp. 319–344, Apr. 2017, doi: 10.1017/S181638311700042X.

[15] B. Hayes, "Migration and data protection: Doing no harm in an age of mass displacement, mass surveillance and 'big data,'" *Int. Rev. Red Cross*, vol. 99, no. 904, pp. 179–209, Apr. 2017, doi: 10.1017/S1816383117000637.

[16] N. Ermicioi, "Factors Affecting Nonprofits' Information Security Readiness During Crises: A Study of COVID-19's Impact on Small and Medium Nonprofit Organizations (NPOS) in the DMV Area," Marymount University, 2020.

[17] N. Ermicioi and M. Xiang Liu, *Cybersecurity In Nonprofits: Factors Affecting Security Readiness During Covid-19*, 2022.

[18] S. Le Blond, A. Cuevas, J. R. Troncoso-Pastoriza, P. Jovanovic, B. Ford, and J.-P. Hubaux, "On Enforcing the Digital Immunity of a Large Humanitarian Organization," in *2018 IEEE Symposium on Security and Privacy (SP)*, May 2018, pp. 424–440. doi: 10.1109/SP.2018.00019.

[19] M. Marelli, "The SolarWinds hack: Lessons for international humanitarian organizations," *Int. Rev. Red Cross*, vol. 104, no. 919, pp. 1267–1284, Apr. 2022, doi: 10.1017/S1816383122000194.

[20] Z. Al Achkar, *Digital Risk: how new technologies impact acceptance and raise new challenges for NGOs*, 2021.

[21] K. B. Sandvik, "The humanitarian cyberspace: shrinking space or an expanding frontier?," *Third World Q.*, vol. 37, no. 1, pp. 17–32, Jan. 2016, doi: 10.1080/01436597.2015.1043992.

[22] M. Marelli, "Hacking humanitarians: Defining the cyber perimeter and developing a cyber security strategy for international humanitarian organizations in digital transformation," *Int. Rev. Red Cross*, vol. 102, no. 913, pp. 367–387, Apr. 2020, doi: 10.1017/S1816383121000151.

[23] CyberPeace Institute, "Cyber Resilience for NGOs: A Collective Intelligence effort | CyberPeace Institute," Dec. 2024. [Online]. Available: https://cyberpeaceinstitute.org/news/publications/cyber-resilience-ngos-collective-intelligence-effort/

[24] A. K. Moeller, J. W. Creswell, and N. Saville, Eds., *Second language assessment and mixed methods research*. in Studies in language testing, no. 43. Cambridge: Cambridge University Press, 2016.

[25] J. W. Creswell and V. L. Plano Clark, "Choosing a mixed methods design," in *Designing and conducting mixed methods research*, in 1st ed. , SAGE Publication, 2006, pp. 58–86.

[26] S. K. Ahmed, "Sample size for saturation in qualitative research: Debates, definitions, and strategies," *J. Med. Surg. Public Health*, vol. 5, p. 100171, Apr. 2025, doi: 10.1016/j.glmedi.2024.100171.

[27] S. K. Sharma, S. K. Mudgal, R. Gaur, J. Chaturvedi, S. Rulaniya, and P. Sharma, "Navigating Sample Size Estimation for Qualitative Research," *J. Med. Evid.*, vol. 5, no. 2, p. 133, Jun. 2024, doi: 10.4103/JME.JME_59_24.

[28] C. Anfuso, A. Bartolucci, C. Del-Real, and S. Kuipers, "Cybersecurity Threats, Challenges, and Strategies in Humanitarian Operations: A Scoping Review," 2025. doi: 10.2139/ssrn.5884603.

[29] V. Braun and V. Clarke, "Using thematic analysis in psychology," *Qual. Res. Psychol.*, vol. 3, no. 2, pp. 77–101, Jan. 2006, doi: 10.1191/1478088706qp063oa.