Cybersecurity threats, challenges, and strategies in humanitarian operations: a scoping review

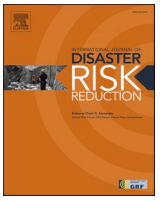
Anfuso, C.; Bartolucci, A.; Real, C. del; Kuipers, S.

International Journal of Disaster Risk Reduction 137 (2026) 106082

Contents lists available at ScienceDirect

International Journal of Disaster Risk Reduction

journal homepage: www.elsevier.com/locate/ijdrr



Cybersecurity threats, challenges, and strategies in humanitarian operations: A scoping review

Chiara Anfuso *, Andrea Bartolucci, Cristina Del-Real, Sanneke Kuipers

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

ARTICLE INFO

Keywords:
Digitalization
Humanitarian aid
Humanitarian organizations
Cyber threats
Cyber preparedness
Cyber response

ABSTRACT

Humanitarian organizations increasingly rely on digital tools and data with the promise of faster and more efficient aid delivery. But digitalization comes with a critical drawback: a heightened exposure to cyber threats. The data breach experienced by the International Committee of the Red Cross in 2022 is a clear example of this risk, but not an isolated one. The incidents recorded during the conflicts in Ukraine and Gaza show that cyberattacks against humanitarian organizations have become an alarming reality of modern conflict. A cyber incident on a humanitarian organization harms the protection of the identities and positions of vulnerable groups. There is therefore an urgent need to recognize cybersecurity as a core pillar of humanitarian aid. This PRISMA-ScR review maps cyber threats, challenges, and strategies in humanitarian aid. It identifies a range of cyber threats to humanitarian organizations, including cyberattacks, surveillance, and mis/disinformation concerns. Still, it reveals notable lacks in terms of cyber preparedness and response, as well as a complete absence of knowledge on crisis communication strategies. Despite the importance of strengthening cybersecurity being recognized, the findings highlight that humanitarian organizations face unique challenges which often hinder the effective implementation of cyber strategies. Given the identified gaps in both existing research and practice, this review stresses the importance of developing solutions tailored to the distinctive features and needs of the humanitarian sector. To this end, this study provides a base for further investigation, with the key themes, gaps, and proposed research avenues guiding immediate focus for this underexplored field.

1. Introduction

In the wake of emergencies, humanitarian organizations work to deliver aid to people in need as fast and efficiently as possible. In recent years, the sharp increase in people requiring humanitarian assistance has prompted these organizations to adopt advanced technologies and tools to better meet the needs of affected communities [1,2]. These efforts include the digitalization of (personal) data collection and the leveraging of emerging technologies such as artificial intelligence (AI), unmanned aerial vehicles (UAVs), and biometrics [2–4]. This shift towards digitalization represents a significant transformation in the work of humanitarian organizations.

The digitalization of aid delivery promises to enable faster and more efficient operations [5–8]. However, it also increasingly exposes humanitarian organizations to cyber threats. In January 2022, the International Committee of the Red Cross (ICRC) experienced a major data breach that affected more than 500,000 individuals connected to the Restoring Family Links platform services

* Corresponding author.
E-mail address: c.anfuso@fgga.leidenuniv.nl (C. Anfuso).

https://doi.org/10.1016/j.ijdrr.2026.106082
Received 20 November 2025; Received in revised form 25 February 2026; Accepted 2 March 2026
Available online 6 March 2026

Table 1
Keywords used for the database search (Web of Science, PubMed, and PsycINFO).

Key concept	Keywords
Humanitarian aid	humanitarian aid OR humanitarian assistance OR humanitarian organi?ation* OR humanitarian relief OR humanitarian support OR humanitarian sector OR aid sector OR disaster relief OR disaster aid OR NGO OR NGOs OR non-governmental organi?ation* OR Intergovernmental organi?ation* OR IGO OR IGOs
(AND)	
Cybersecurity	cyber OR cyber incident* OR cyberattack* OR cyber breach* OR data breach* OR cyber security OR cyber preparedness OR cyber response OR cybersecurity governance OR cyber risk management OR cyber operation* OR cyber crisis communication OR cyber risk* communication

globally [9,10]. The digital platform was designed to store sensitive information about missing persons and vulnerable individuals separated from their families. As such, not only did the breach disrupt the ICRC's operations—it also endangered the individuals relying on the platform, further compromising their already precarious condition [11–13]. Paradoxically, one of the platform's key strengths—its extensive collection of personal data—amplified the impact of the breach, resulting in the exposure of a large amount of sensitive information.

The data breach at the ICRC is not an isolated incident. Rather, it exemplifies a growing trend of cybersecurity threats against humanitarian organizations. For example, during the recent wars in Ukraine and the Gaza Strip, cyberattacks have significantly disrupted relief operations [14,15]. Reported cyberattacks include phishing attempts spreading false information on evacuation plans [15], malware interfering with the provision of essential supplies [15]; [13], and distributed denial of service (DDoS) attacks slowing down the ability to receive donations [16,17]. In the case of Ukraine, hackers allegedly linked to the Russian Federation and Belarus have stolen refugee data and used information on their movements to spread disinformation [15].

The reported cybersecurity incidents in Ukraine and Gaza show that cyberattacks against critical infrastructure and humanitarian organizations have become an alarming reality of modern conflict. This rising threat is further illustrated by Cloudflare [18], which reported nearly 325 million daily attacks on civil society groups and nonprofits, marking a 241% increase compared to 2024. These cases highlight a critical downside of the humanitarian sector's digitalization: while digital tools improve efficiency and coordination, they also introduce serious vulnerabilities that can compromise the sensitive information of the individuals that humanitarian organizations aim to protect.

The impact of a cyber incident on a humanitarian organization extends far beyond immediate operational or financial issues, striking at the essence of humanitarian aid: protecting the most vulnerable [19]. Cyber incidents can disrupt the delivery of life-saving assistance, expose people to long-term risks, and potentially exacerbate existing humanitarian crises and geopolitical tensions [20,15]. Beyond reducing the effectiveness of aid delivery, these attacks raise concerns about the potential long-term misuse of the exposed data, including the re-victimization of already at-risk populations [21]. The extensive collection of personal information, especially through the adoption of new technologies such as biometrics, can be weaponized for targeted violence and persecution [22,23]. In this context, humanitarian organizations may find themselves at risk of inadvertently contributing to the misuse of this information, breaking the trust of vulnerable communities, and compromising the ethical foundation of their own work [24]. This increasing frequency and severity of cyber threats underscore the urgent need to recognize cybersecurity as a core pillar of humanitarian aid delivery and protection of sensitive data.

Cybersecurity governance experts, both in academia and practice, have explored a range of solutions for effectively preparing for and responding to cybersecurity incidents. This research encompasses several areas, including technical measures (e.g., [25,26]), policy recommendations (e.g., [27–30]), training and awareness (e.g., [31–34]) as well as studies on legal and ethical dimensions of cybersecurity (e.g., [35,36]). Many of these best practices, however, emerge from the private sector and do not fully address the distinct characteristics and challenges of the humanitarian context [37–40]. Unlike private companies, humanitarian organizations often operate with limited resources, in insecure or unstable environments, and serve highly vulnerable people [41–44].

Despite the increasing exposure to cyber threats, research on cybersecurity in the humanitarian sector has largely centred on the benefits of digitalization or the implications of cyber operations under International Humanitarian Law (IHL) (e.g., [45,46]). Many of the critical perspectives on the potential risks and challenges have emerged in grey literature and the blogosphere rather than in peer-reviewed academic works [47]. To address this gap, this paper presents a scoping literature review that examines the current state of knowledge on cyber preparedness, response, and communication strategies in the humanitarian sector.

2. Methodology

2.1. Literature search

This scoping review was conducted according to the Preferred Reporting Items for Systematic Reviews and Meta-analyses extension for scoping reviews (PRISMA-ScR) [48]. Given the explorative nature of the research, a scoping review was the most appropriate choice to provide a comprehensive overview of the main sources and evidence available on the topic [49]. Scoping reviews are recognized as essential in identifying key themes and gaps in the literature [50], making this approach ideal for defining future research directions for this underexplored topic [51].

We followed a four-step approach to identify eligible literature on cyber threats, digitalization challenges faced by humanitarian organizations, and cyber strategies: (1) search of electronic databases, (2) search via Google Scholar, (3) backward and forward review,

Table 2
Sources' inclusion and exclusion criteria.

Field	Inclusion criteria	Exclusion criteria
Organization focus	Humanitarian agencies or organizations delivering humanitarian aid; (I)GOs; NGOs; NPOs explicitly mentioning role in humanitarian aid	For-profit organizations; organizations not explicitly mentioning their role in humanitarian aid delivery
Topic focus	Digitalization of humanitarian efforts, data protection and/or cybersecurity concerns (possibly) impacting the effective delivery of humanitarian aid	Ontological, epistemological, and ethical perspectives of digitalization of humanitarian efforts; IHL application and other legal concerns
Content	Currently implemented cybersecurity preparedness, responses, communication strategies and/or risks related to the digitalization of humanitarian efforts	Cybersecurity preparedness, responses, and communication strategies exclusively concerning specific types of new technologies (e.g., UVAs, blockchain, AI) or related risks; proposed frameworks/models to deal with the digitalization of humanitarian aid
Source type	Journal (empirical and non-empirical) articles; book chapters; peer-reviewed articles; policy briefs, conference papers; working papers; organizational reports; doctoral dissertations	Editorials; abstract only; blog posts; (research) posters; commentaries
Language	English	Non-English
Full-text availability	Full text available	Full text not available

and (4) contact with corresponding authors.

We conducted the electronic database search between February 2024 and August 2025 using the following databases to access scientific publications: (a) Web of Science, (b) PubMed, and (c) PsycINFO. We obtained access to the databases through Leiden University. Table 1 shows the complete list of search terms used, combining keywords to define the concepts of humanitarian aid and cybersecurity.

Subsequently, we used Google Scholar to expand the research by including grey literature such as working papers, conference papers, and organizational reports on the topic [52]. We expanded this search in February 2026 with key terms derived from the database search strategy through the Publish or Perish software (see Supplementary Material file 1 for the full queries). We run ten different queries, and following common practice in systematic reviews, we retrieved the top 100 relevance-sorted results from each query [53], yielding a total of 1000 records for screening.

After screening this initial set of records, we performed a backward and forward review of the studies included from the database and Google Scholar search to identify additional relevant literature. In December 2024, we contacted the corresponding authors of eligible studies and asked if they knew of other records relevant to the research objectives; 8 of them replied and provided additional sources. All the records identified through these processes were included in the screening process.

2.2. Eligibility criteria

The inclusion and exclusion criteria applied to each record are presented in Table 2. No temporal restrictions were imposed.

For this review, humanitarian aid was defined as the provision of assistance, relief, and protection to individuals and communities affected by crises [54,55]. This definition encompasses a broad spectrum of organizations providing humanitarian aid, including those responding to various types of emergencies (e.g., disasters, conflict, hunger, etc.), offering various types of relief (e.g., medical and healthcare assistance, education, etc.), and different organizational forms, including (inter)governmental (IGOs), non-governmental (NGOs), and non-profit organizations (NPOs) explicitly mentioning their role in humanitarian aid delivery.

2.3. Source selection

The screening process consisted of two stages: (1) title/abstract screening and (2) full-text screening. We created a screening tool for both the title/abstract and full-text screening to standardize the process (see Supplementary Material file 2). Before proceeding with the screening, we conducted an intercoder reliability (ICR) test to ensure consistency. Two researchers (CA and CDR) independently classified 30 randomly selected abstracts according to the screening tool. The level of agreement between the two researchers was calculated using Fleiss' kappa [56]. The ICR revealed a Fleiss' kappa's value of $\kappa = 0.789$, which corresponds to a substantial level of agreement between researchers [56]. As such, it was deemed sufficient for the first author to proceed with the full list of titles, abstracts, and full-text screening.

2.4. Data extraction and synthesis of results

Data were extracted based on (1) author(s); (2) year of publication; (3) type of document (4) organization's characteristics, needs, and contexts of operation; (5) main threats and vulnerabilities of digitalization to humanitarian aid efforts; (6) existing cyber preparedness, (7) response and (8) communication strategies to deal with cyber incidents (or reported shortcomings thereof); and (9) recommendations for future cybersecurity efforts and research directions. We summarized the main characteristics of the studies included in the review in a table, visually indicating the extent to which they address these core topics (see Table 3). A detailed version of the data extraction sheet is provided in Supplementary Materials file 3.

The findings of the review are structured according to the main elements identified during the data extraction process, which we

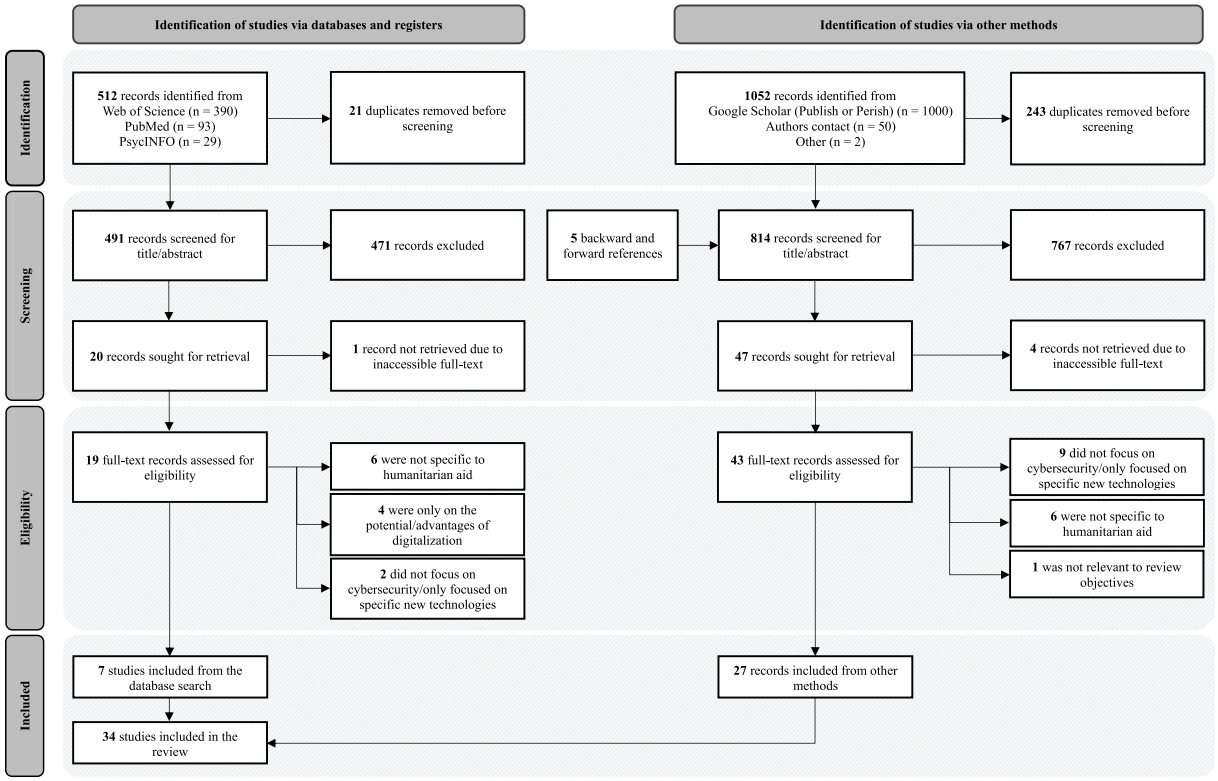


Fig. 1. PRISMA 2020 flow diagram for new systematic reviews which included searches of databases, registers and other sources.

grouped inductively under four key themes: (1) common and emerging cyber threats against humanitarian organizations, (2) challenges of cyber incidents to humanitarian aid efforts, (3) implemented cybersecurity strategies and key shortcomings, and (4) areas of improvement and recommendations for future cybersecurity measures. We synthesized the results of surveys investigating the cybersecurity strategies implemented across the sector in Table 4, reporting compliance with these measures. We also characterized the key recommendations extracted during the review in Table 5 according to the People-Process-Technology (PPT) model to clarify the distinct requirements needed to enhance humanitarian organizations' capacity to manage cyber threats (e.g., [57,58]).

2.5. Limitations

Scoping reviews provide a descriptive account of available research, allowing the identification of key themes and gaps in this underexplored field [49,76,77]. They, however, are at risk of bias arising from the search process and study selection [77]. To reduce such a risk of bias, we standardized the research as much as possible by following the PRISMA-ScR guidelines and conducting an ICR before proceeding with the screening and data extraction. Furthermore, scoping reviews do not appraise the quality of evidence collected [49]. As such, the results of the studies discussed in this review might be limited in validity and generalizability. Such a limitation stresses the need for more methodological rigor and primary data collection to support stronger, evidence-based results to verify and refine the studies' insights. To this end, this review offers a starting point for further investigation, and its findings remain relevant for guiding future research directions.

3. Results and discussion

The search yielded 1569 records, of which 512 articles retrieved via the database research, 1000 via Google Scholar, five via backward and forward review, and 50 through contact with corresponding authors. Additionally, the first author received recommendations for two reports through contact with experts. While these reports were not retrieved via the literature search steps, they were included in the screening process because of their high timeliness and relevance to the research objectives.

Concerning the sources retrieved via the database search, 491 articles were excluded at the title/abstract screening stage. Subsequently, of the 19 studies included in the full-text review, 12 (63%) were deemed ineligible for inclusion based on the established criteria. Seven studies ultimately met the criteria for inclusion in the review.

Following the database search, we proceeded with screening the studies retrieved via alternative methods. At this stage, 243 duplicates were removed before screening. 767 sources were then excluded at the title/abstract screening stage. Among the 47 reports included in the full-text review, 4 were not retrieved due to inaccessible full text, and 16 records were excluded due to failure to meet

Table 3
Included records' characteristics and data extracted.

#	Author(s)	Date	Type of Document	Organization's Characteristics	Cyber Threats	Cyber Preparedness	Cyber Response	Crisis Communication	Future Recommendations
1	Al Achkar	2021	Report	◪	◪	○	○	○	●
2	Arendt-Cassetta et al.	2022	Report	◪	●	●	◪	○	●
3	Bell & Liu	2023	Academic article	○	○	◪	○	○	●
4	Byrne	2014	Report	◪	◪	◪	○	○	●
5	de Bruin & Von Solms	2017	Conference paper	●	◪	◪	○	○	●
6	CyberPeace Institute	2024	Report	○	◪	●	◪	○	●
7	Duffield	2013	Working paper	○	◪	◪	◪	○	○
8	Duffield	2016	Academic article	○	◪	◪	○	○	○
9	Elshani	2023	Report	○	○	●	◪	○	●
10	Ermicioi	2020	Doctoral dissertation	◪	◪	◪	○	○	●
11	Ermicioi & Liu	2022	Conference paper	●	○	◪	○	○	●
12	Fitz-Gerald & Hennebry	2025	Academic article	◪	●	◪	○	○	●
13	Gilman	2014	Report	◪	●	◪	◪	○	●
14	Gilman	2014	Report	○	●	◪	○	○	●
15	Hayes	2017	Academic article	◪	●	○	○	○	●
16	Kalkman	2018	Academic article	◪	◪	◪	○	○	●
17	Le Blond et al.	2018	Academic article	●	●	●	◪	○	●
18	Loukas et al.	2013	Academic article	○	◪	○	○	○	●
19	Marelli	2020	Academic article	●	◪	◪	○	○	●
20	Marelli	2022	Academic article	◪	◪	○	○	○	●
21	Martin et al.	2022	Academic article	◪	●	○	○	○	●
22	Meier	2011	Academic article	○	◪	◪	○	○	○
23	Mierzwa & Scott	2017	Report	◪	◪	●	○	○	●
24	Parmadi & Ramli	2025	Academic article	◪	◪	◪	○	○	●
25	Powazek & Pierson	2024	Report	◪	◪	●	○	○	●
26	Saeedi et al.	2024	Academic article	◪	◪	◪	○	○	●
27	Sandvik	2016	Academic article	◪	◪	◪	○	○	○
28	Sandvik	2023	Book chapter	●	●	●	○	○	○
29	Sandvik et al.	2013	Report	○	●	●	○	○	●
30	Sandvik et al.	2014	Academic article	◪	◪	○	○	○	●
31	Sandvik et al.	2017	Academic article	◪	●	○	○	○	●
32	Vhikai et al.	2024	Academic article	◪	●	◪	○	○	●
33	Vitaliev	2009	Development brief	◪	●	◪	○	○	●
34	Willitts-King et al.	2019	Working paper	○	●	◪	○	○	●

Note.

● Element is discussed in detail and/or substantiated with empirical examples.
◪ Element is mentioned but no further explanation, details, or empirical examples are provided.
○ Element is not discussed.

the established inclusion criteria. As a result of these screening processes, 27 studies retrieved via alternative methods were included in the review. The final synthesis encompassed a total of 34 sources, with 27 records (79%) identified via alternative methods. A complete overview of the screening stages, including reasons for exclusion, is provided in Fig. 1.

Table 3 presents an overview of the key characteristics of each included study and indicates the extent to which they address the core topics of this review.

Most of the identified studies addressed the humanitarian sector as a whole and did not focus on any specific organization or region. One publication was from the International Federation of the Red Cross and Red Crescent Societies (IFRC) and eight studies on the ICRC, resulting in predominant attention to the International Red Cross and Red Crescent Movement. No trends based on the publication year were found.

Regarding document characteristics, 17 (50%) were academic articles. The remaining literature included (policy) reports (n = 10), working papers (n = 2), conference papers (n = 2), one book chapter, one professional development brief, and one doctoral dissertation. With respect to methodological approach, 11 sources (32%) employed empirical research designs.

3.1. Common and emerging cyber threats against humanitarian organizations

The literature highlighted how the expansion of humanitarian organizations' digital reach has resulted in an amplified exposure and surge in cyber threats [8,19,47,64,72,74,78,79,74]. We categorized these threats into three types: (1) direct and indirect cyberattacks, (2) the co-option of data for surveillance purposes, and (3) the spread of mis- and disinformation.

Direct and indirect cyberattacks. The literature shows that cyberattacks against humanitarian organizations mainly consist of the deliberate targeting of humanitarian systems and data (direct attacks) or attacks when humanitarian organizations are not the primary targets but become indirect victims of attacks directed at partner organizations or critical civilian infrastructure (indirect attacks) [19]. Marelli [71] argues that the latter is especially high in the event of supply chain attacks, where humanitarian organizations may suffer collateral damage due to their reliance on the same digital supply chains as the primary targets.

The analysed literature identifies a series of direct attacks against humanitarian organizations. The most common types typically involve malware infections, social engineering [60], distributed denial-of-service (DDoS) attacks, and website compromises [60,61]. But these are not the only ones. In a survey based on several listservs focused on technology leadership in NPOs, Mierzwa and Scott [42] revealed that 26 out of 53 respondents had experienced ransomware incidents. In addition, in a survey distributed to 68 NPOs in San Francisco, Powazek and Pierson [43] revealed phishing attacks as an especially frequent intrusion, affecting 71% of respondents. These emerging threats align with Arendt-Cassetta et al.'s [19] report, which warned of an increase in direct cyberattacks against humanitarian organizations.

Co-option of data for surveillance purposes. Humanitarian organizations handle highly sensitive and geopolitically valuable data [80], making them attractive targets for state actors, armed groups, and criminal organizations [19,41,64,74,65,69,80]. The growing value of this data has raised significant concerns about what Hayes [78] refers to as 'aiding surveillance'. Backed by several other sources, Hayes' study implies that, without due diligence and robust policies, humanitarian data systems can inadvertently facilitate and support mass and government surveillance [47,72,78,65,69,81,82]. Any form of personal information, whether inherently sensitive or not, can expose individuals to targeting based on ethnicity, religion, medical history, or other vulnerable factors [72]. Especially in times of conflict, a data breach can lead to the exploitation, discrimination, and persecution of at-risk communities [19, 64,65] or particular ethnic groups [72,73]. The collection of biometric data in refugee settings represents a particular risk; as evidenced by instances of Rohingya refugees in Bangladesh and Myanmar, and Central African Republic refugees in Congo and Kenya, host or donor governments can demand that humanitarian organizations share biometric data for cross-matching between national databases [8,19,82]. This cross-checking with sensitive data may, in turn, lead to dangerous consequences, including the targeting of entire communities, forced repatriation, or even the creation of so-called 'kill lists' [19]. Le Blond et al. [80] also warned that medical data is especially valuable as it often contains information that armed groups or state actors can exploit to track whether high-profile targets have been treated or detained.

The military origins of some of the technologies, coupled with the sensitive data collected, may also render humanitarian actors legitimate targets [66,83]. The increase in cyber warfare and the proliferation of cheap and user-friendly digital tools across less technologically sophisticated countries make this development especially relevant. The easy access to digital tools has altered the dynamics of modern conflicts, giving rise to more politically motivated hacking [73], which renders humanitarian actors increasingly vulnerable to cyberattacks and digital surveillance.

Spread of mis- and disinformation. Sandvik [84] explained that while humanitarians have always been vulnerable to rumors and propaganda, this risk has been amplified by social media's instant global reach. Humanitarian organizations increasingly rely on social media platforms such as X and Facebook, where communities and individuals can share valuable and timely information [5,85]. However, while these platforms are easily accessible, they also allow anyone to post critiques of humanitarian organizations' responses, speculations about perceived affiliations with local armed actors [74,60,84] or other controversial opinions that could reflect negatively on the organizations [62]. Especially in fragile and conflict-ridden regions, such false information spread about the actions and intentions of humanitarian actors can have severe consequences. It can damage the organizations' credibility or portray them as supporters of conflict rather than impartial aid providers [60,84,59]. Social media or other communication tools can be exploited to spread malicious rumors, incite panic, or disrupt coordination [64,73,67]. For instance, disinformation campaigns in Syria severely damaged the credibility of the White Helmets by falsely portraying them as al-Qaeda affiliates [19]. Similarly, in the Democratic Republic of Congo, conspiracy theories spread on social media led to communities attacking Ebola centres [19], endangering humanitarian workers and further complicating the efforts to mitigate the outbreak. These examples showcase how misinformation and disinformation can jeopardize the work and safety of humanitarian actors, incite panic, and undermine communities' acceptance.

3.2. Challenges of cyber incidents to humanitarian aid efforts

Humanitarian organizations face unique challenges in the cyber domain due to their distinctive needs and operational contexts. These can be grouped into three key categories: (1) normative and reputational challenges, (2) operational challenges, and (3) resources and capacity challenges.

Normative and reputational challenges. The reputation of humanitarian actors is built on the core principles of neutrality, impartiality, and independence [71,60,80]. Breaching these principles can therefore severely disrupt their reputation, eroding trust and potentially compromising the effectiveness of aid delivery [41,80,59,75]. Consequently, as stressed by Sandvik et al. [82], these responsibilities must extend to the digital domain.

The humanitarian principles confer privileges and immunities to humanitarian organizations across countries of operation, enabling them to carry out their mandate [72,69,84,75]. Humanitarian organizations also commit to the 'do no harm' imperative as an essential and inviolable requirement to ensure their actions do not have adverse impacts or create new risks for individuals and populations [78,82]. However, Gilman [73] observed that the emergence of cyber warfare, as seen in the crises in Syria and Libya, has complicated the capacity to uphold neutrality and other core humanitarian principles. These developments in the digital domain thus raise important normative and reputational challenges for humanitarian organizations.

Operational Challenges. Humanitarian organizations often operate in highly volatile and insecure settings [44,83] and depend on local conditions and limitations, including unstable connections, infrastructure damage, and problems with power supplies [41,65]. In such contexts, certain digital and technological choices can increase the vulnerability to cyber threats [66]. For instance, aid beneficiaries may be unable to use technology freely or safely in detention facilities or countries with strict technological controls [80]. In some cases, these strict controls may even apply to humanitarian workers who, for instance, as noted by Le Blond et al. [80], may be asked by armed groups to surrender their mobile phones during meetings.

Humanitarian organizations might also struggle to maintain exclusive control over the information collected [72,79,82]. As highlighted by several participants from various ICRC operational units interviewed by Le Blond et al. [80], humanitarian work highly depends on the extensive collection of sensitive information. However, this data often exceeds the capacities for effective management and storage, and without the proper safeguards, risks being stolen or misused by threat actors [64,72,79,65,82].

Resources and Capacity Challenges. Even with robust strategies in place, a single user error can compromise the entire system. This requires strong databases and server security, along with comprehensive awareness and training for all staff to prevent cyber incidents [44,72]. Delivering such training to aid workers, however, often proves difficult due to high costs and poor internet connections [83]. As emphasized by numerous sources, the implementation of information security policies and proper staff training is often constrained by limited budgets [41,43,44,86,70]. In a survey of NPOs in the DC-Maryland-Virginia area, Ermicioi [41] revealed that donors frequently give specific requirements when it comes to funding, meaning many organizations do not have the freedom to invest in cybersecurity. Humanitarian organizations are also frequently understaffed and highly reliant on volunteers, resulting in a lack of dedicated IT and cybersecurity staff [41,43,60,86]. Small humanitarian organizations are therefore particularly vulnerable to cyber threats due to the limited resources and smaller staff sizes [19,41,86,70].

3.3. Implemented cybersecurity strategies and key shortcomings

The assessment of current cybersecurity practices within the humanitarian sector has received little attention in scholarly discourse. Academic research has focused extensively on International Humanitarian Law (IHL) applications in the digital domain, but has left assessments of practical cybersecurity strategies mostly unaddressed [19,75]. Additionally, the humanitarian sector has devoted substantial efforts to understanding the symbolic and legal challenges arising from the digitalization of their operations, such as concerns over “doing no harm” and “digital dignity” [8]. In spite of their importance, Sandvik et al. [60] had warned that this approach might be insufficient to address the fast-paced cyber developments affecting the humanitarian sector. This claim is reflected by the findings of this review, which indicate that, despite some progress toward establishing data protection policies and basic cybersecurity tools, the humanitarian sector seems to remain insufficiently protected against cyber threats. The strategies identified in the literature, along with the main shortcomings, can be categorized under three key areas: (1) technical policies, (2) organization structure, staff training, and awareness, and (3) communication strategies.

Technical policies. The humanitarian sector has taken a series of steps towards strengthening cybersecurity policies. In particular, substantial efforts have been taken to adopt and standardize data protection policies across the sector, with initial efforts seeing the development of the SPHERE Standards or individual organizations' policies, such as the 2010 International Organization for Migration (IOM)'s Data Protection Manual [87,88]. These guidelines have consistently been revised to ensure responsible data management across all phases of humanitarian action [19]. A significant step to promote a responsible approach to technology and data management came in 2017 with the establishment of the OCHA Centre for Humanitarian Data. Furthermore, in 2021, the United Nations (UN) launched the first Operational Guidance on Data Responsibility in Humanitarian Action, focusing on the safe and ethical management of data in operations [89]. Additionally, the ICRC has devoted substantial efforts to designing robust cyber strategies, including the development of Guidelines on Data Protection [19,74,90] and the establishment of the digital emblem; however, experts warn that this measure is insufficient to stop ransomware attacks or state-sponsored cyber threats [65].

Although these advancements mark important progress, it is important to recognize that cyber threats are evolving faster than these measures. Most of these cybersecurity strategies are thus somewhat dated and might not accommodate recent risks. Data volumes in the humanitarian sector are outgrowing responsible data management and security [19]. Moreover, Sandvik [74] noted that aid workers often ignore and view several of these organizations' procedures as impractical. This is supported by the findings of a CyberPeace Institute's [61] survey of 25 Dutch NGOs, which revealed that only 28% of the organizations have fully implemented data protection policies.

These gaps in policy implementation reflect a broader concern in the humanitarian sector, which, according to various sources, is also lagging behind in terms of practical strategies to manage cyber threats [69,73,84]. In a study distributed to 53 NPOs and NGOs, Mierzwa and Scott [42] found that these organizations often employ basic tools to protect their technologies. Commonly implemented policies include procedures for creating backup copies of data [62,63], ensuring the physical security of sensitive information (e.g., locked file cabinets), and policies for the destruction or disposal of sensitive data [80,63]. Nevertheless, these policies often lack sophisticated encryption or security tools and rely on outdated systems [19,61,65,73]. For example, Sandvik [84] mentioned that many humanitarian organizations still used Excel spreadsheets to produce data for decision-making purposes. The ICRC appears to be one of few organizations implementing full-disk encryption in all laptops [80]. A survey conducted by Elshani [63] among 48 NGOs based in Kosovo also revealed that 50% of these organizations lacked any policies or regulations for managing and mitigating cyber risks. These results indicate that, despite some advancements in basic cyber capabilities, humanitarian organizations might still be unprepared to deal with cyber threats.

Organization's structure, staff training, and awareness. The reviewed sources highlight shortcomings in established guidelines, training, and dedicated information technology (IT) staff across organizations. In a questionnaire distributed to employees of ten aid organizations in Harare, Vhikai et al. [44] found that many organizations lack robust guidelines or professional standards for the use of information technologies. These findings are supported by a survey of NPOs and NGOs by Mierzwa and Scott [42], which revealed that 49% of organizations lacked a formal cybersecurity unit. Powazek and Pierson [43] found similar results, with 47% of NPOs in San Francisco having a designated IT unit, of which 21% with only a single full-time IT staff. Additionally, several records warned that staff members often lack training and awareness on the nature of cybersecurity threats [41,69,73,66,70]. This concern is reflected by the findings of surveys mapping currently implemented cybersecurity strategies across organizations delivering humanitarian aid, as

Table 4
Results of surveys mapping currently implemented cybersecurity strategies (in %).

Element	Source			
	Mierzwa & Scott (2017) ((I)NGOs & NPOs, n = 53)	Elshani (2023) (NGOs in Kosovo, n = 48)	CyberPeace Institute (2024)[b] (NGOs in the Netherlands, n = 25)	Powazek & Pierson (2024) (NPOs in San Francisco, n = 68)
Cyber threats				
Reported cyberattack	50[a]	17	-	85
Technical policies				
Backups	-	-	40	-
Cyber insurance coverage	-	-	28	-
Cybersecurity framework	51	50	-	-
Data protection policy	-	-	28	-
Disaster recovery plan	-	-	36	-
Encryption	-	11	32	-
Firewalls	-	-	36	-
Incident response plan	-	38	28	-
Internal audit	-	0	-	-
Inventory of assets	-	38	32	-
Multi-factor authentication (MFA)	-	29	32	84
Password manager	-	-	28	-
Regular software updates	-	-	-	50
Risk assessment procedure	-	8	-	-
Up-to-date security software (e.g., antivirus)	-	60	48	-
Virtual private network (VPN)	-	23	-	-
Staff, training, and awareness				
Designated IT staff/access	51	35	32	47
(Phishing) simulations	-	-	36	-
Training	53	0	44	48

Low compliance (0% - 33%)
Medium compliance (34% - 66%)
High compliance (above 67%)

Notes: [a] Percentages (%) correspond to the number of organizations implementing cybersecurity measures. [b] Results from the CyberPeace Institute (2024) refer to organizations in full adoption/compliance with measures.

Table 5
Measures to implement to strengthen cybersecurity (detailed recommendations in Appendix A).

Measure	Management Pillar			Source(s)
	People	Process	Technology	
Community of practice to fight mis/disinformation	X			[43,44,59]
Countering rumors strategies		X		[44,60,59]
Transparency		X		[44,59]
Strong foundational training	X			[19,42,61,62,63]
Cybersecurity governance structures	X	X		[19,61]
Strengthen partnerships	X	X		[19,64,65]
Routine secure offsite backups		X	X	[42,66,67,68]
Cybersecurity frameworks leveraging		X		[61,69,70,68]
Risk modelling-based decision-making		X		[66,67]
Business continuity planning		X		[42,66,62]
Simulations	X			[42,66]
Internal reviews	X	X		[66]
Critical information auditing		X		[66]
Risk-based information classification		X		[66]
Encryption protocols			X	[42,71,61,69,65,62,63]
Dedicated VPS/VMs			X	[61]
Dark Web monitoring		X	X	[61]
MFA and password management			X	[61]
Incident response plan	X	X		[61]
Behavior research and training	X			[42,70,63]
Digital safety advocacy	X	X		[63]
Design public education campaigns	X	X		[64]
Threat landscape understanding		X		[72,73]
Privacy protection guidelines		X		[72,74,65]
Ethical committees	X			[72]
Data anonymization and/or aggregation			X	[72]
“Zero Trust” approach	X	X	X	[75]
“Digital humanitarian space”			X	[75]
Supplier dependencies reduction		X		[71]
Cybersecurity coverage in insurance policies		X		[42]
Community-focused approaches	X			[65]
Risk and vulnerability assessment	X		X	[60]

shown in Table 4.

Communication strategies. None of the sources analysed provided information on the communication strategies adopted by humanitarian organizations to manage cyber incidents. Given the critical role communication plays during cyber incidents and crises, particularly in maintaining reputation and trust with key stakeholders, these results highlight an important gap in current research. This gap underscores the need for greater attention and research into crisis communication within the humanitarian sector.

3.4. Areas of improvement and recommendations for future cybersecurity measures

The sources included in this review outlined various recommendations aimed at strengthening humanitarian organizations' ability to prepare for and respond to cyber incidents. We organized these recommendations according to the People-Process-Technology (PPT) model to clarify the distinct requirements needed to enhance humanitarian organizations' capacity to manage cyber threats (e.g., [57,58]) (see Table 5).

Even though there is no one-size-fits-all strategy for protecting an organization from cyber threats [66], these measures can establish a foundation for strengthening cybersecurity in humanitarian organizations. As can be inferred from the majority of "people" and "process" recommendations, cybersecurity measures must extend beyond technical strategies. Although the humanitarian sector has focused on strengthening technical policies, a greater attention to the "people" and "process" aspects could offer a more valuable solution to strengthening cybersecurity in the humanitarian sector, especially given the resource constraints and difficulties in investing in cybersecurity technologies.

4. Research agenda

This review identified several gaps in the existing research and practice of cybersecurity in humanitarian aid delivery. Sandvik et al. [60] observed that the humanitarian sector remained insufficiently protected against fast-evolving cyber threats. Despite some progress in establishing basic cybersecurity measures, our review finds that this concern persists, and we expect this challenge to be even more pronounced in the context of AI. Its rapid development and adoption are likely to amplify existing vulnerabilities, introduce new risks, and create entirely new challenges for humanitarian operations, highlighting the urgent need for further research [3]. We are hence presented with an array of avenues for investigation to expand knowledge on this important but currently overlooked topic. While, given its underexplored nature, there are several opportunities to advance the subject, we find three research directions especially relevant: (1) crisis communication and reputation management, (2) obstacles in cybersecurity implementation and tailored strategies, and (3) context-specific cyber response.

A first research avenue should aim to gain knowledge on crisis communication and its effects and limitations for humanitarian organizations. Despite being significantly overlooked by the existing literature, crisis communication is a key component in (cyber) crisis management (e.g., [39,91,92]). This is especially true for the humanitarian sector, where losing trust with key stakeholders can be detrimental to an organization's image as well as its operations. Humanitarian organizations depend on donations to sustain their missions [93,94]. Furthermore, communities' acceptance is essential to reach individuals in need, without which humanitarian workers may encounter hostility or obstacles to delivering aid [95,96]. As such, trust and reputation become key enablers of humanitarian operations, making timely and effective communication crucial. How do the stakeholders' perceptions of a humanitarian organization change following a cyber incident? And how can humanitarian organizations manage reputational risks and rebuild trust? Future research should map existing internal and external communication strategies and assess whether these are effective in maintaining and/or restoring reputation after a cyber incident. Studies should also investigate whether existing frameworks, such as the Situational Crisis Communication Theory (SCCT), can help humanitarian organizations maintain their image during a cyber crisis. While these models have proven effective in mitigating reputational damage and maintaining stakeholder trust [91,97,98], their applicability in the context of cyber incidents within humanitarian organizations remains to be explored.

A second promising research avenue is based on the recognition that humanitarian organizations present unique features that hinder cybersecurity implementation. As discussed in this review, conventional cyber strategies and procedures are often perceived as costly and impractical by aid workers and, as a result, are not fully adopted. These obstacles in implementing cybersecurity strategies must be considered when designing strategies for humanitarian organizations. Some studies have already begun developing frameworks tailored to their features, underscoring this recognition that the humanitarian sector has distinct cybersecurity needs (e.g., [99,100]). Future research should delve deeper into how the characteristics of humanitarian organizations create distinctive challenges to the effective implementation of conventional cybersecurity strategies. Such findings would help identify the sector's key needs and design tailored cybersecurity approaches. For example, one direction identified in this study involves exploring cybersecurity measures that extend beyond technical strategies [57,101]. Given the difficulties in investing in cybersecurity due to the limited resources, prioritizing "people" and "process" aspects can offer a more valuable solution to strengthening cyber preparedness and response across the humanitarian sector. Various studies have suggested that these strategies can be more easily adapted compared to the technological ones and can hence be better tailored to meet the specific constraints that humanitarian organizations face (e.g., [57,101,102]). Research in this area offers an opportunity to develop measures that are not only practical but also aligned with the operational and contextual realities of humanitarian organizations.

Finally, a third research avenue should focus on expanding knowledge of cyber response, with particular attention to specific organizational features within the sector. Most of the literature tends to focus on the humanitarian sector as a whole, treating it as a uniform unit of analysis. However, this approach leads to overlooking some of the critical distinctions that may shape how organizations (should) respond to cyber crises. Various factors, such as the type of cyber threats faced, organizational features, and the type of

Table 6
Key knowledge gaps and research avenues.

Area	Relevance and Key Findings	Knowledge Gaps	Research Avenues
Crisis communication and reputation management	• Crisis communication is a key component in (cyber) crisis management. • Losing trust and reputation with key stakeholders can be detrimental to an organization's image and its operations.	• No knowledge of crisis communication strategies. • Unclear how cyber incidents affect stakeholder trust and reputation in humanitarian contexts.	• Map existing internal and external communication strategies in humanitarian organizations. • Evaluate whether these are effective in maintaining and/or restoring reputation after cyber incidents. • Test established frameworks and models (e.g., SCCT) in these contexts.
Obstacles in cybersecurity implementation and tailored strategies	• Humanitarian organizations present unique features (e.g., volatile operational environment, limited resources, competing mission priorities) that hinder effective cybersecurity implementation. • Conventional cyber strategies and procedures are often seen as costly and/or impractical	• Limited understanding of how unique organizational features hinder cybersecurity implementation. • Lack of tailored strategies that take into account these obstacles. • Main focus on technical strategies, but less on people and process aspects of cybersecurity.	• Identify key obstacles in cybersecurity implementation and investigate how cyber strategies can be adapted to accommodate these challenges. • Expand research on people and process aspects of cybersecurity in humanitarian settings.
Context-specific cyber response	• Main focus on cyber preparedness, leaving cyber response largely unexplored.	• Limited knowledge of cyber response strategies. • Studies mainly on large organizations or the humanitarian sector as a whole, overlooking specific characteristics and leaving smaller organizations understudied. • No investigations on the key distinctions that shape cyber response, including (a) type of cyber threat (e.g., ransomware, DDoS), (b) organizational features (e.g., size, region of operation), and (c) type of data collected/compromised (e.g., at-risk groups, mission data).	• Investigate key distinctions that shape how organizations (should) respond to cyber crises • Devote more attention to smaller organizations and local contexts. • Foster collaboration between academia and practitioners through the creation of safe spaces to share experiences with cyber incidents.

data compromised, can impact the required cyber response strategies. Developing robust cyber response measures requires a deeper understanding of unique organizational structures, operational contexts, and related vulnerabilities. The literature especially highlights the importance of devoting further attention to smaller organizations [86,70] and focusing on local contexts with unique infrastructure, social, and political dynamics [44]. Addressing these gaps requires a closer collaboration between academia and practitioners. To achieve this, we recommend creating safe spaces for humanitarian organizations to share their experiences with cyber incidents freely; these platforms would enable researchers to strengthen evidence-based research within the sector. Table 6 provides a summary of the identified knowledge gaps and research avenues.

These research avenues are not only relevant to cybersecurity concerns in humanitarian operations but also closely linked to the broader objectives of established disaster risk reduction frameworks. For instance, the Sendai Framework for Disaster Risk Reduction emphasizes strengthening disaster risk governance, preparedness, and communication [103]. As humanitarian and disaster operations increasingly depend on digital technologies and data, effectively managing cyber risks becomes essential to achieving these priorities. Similarly, ISO 22301 provides a structured approach to business continuity planning and incident response that can be enhanced by incorporating cybersecurity considerations tailored to humanitarian and disaster management contexts [104]. Viewed in line with these existing frameworks, cybersecurity should be understood as an integral component of disaster risk reduction, thereby ensuring that organizations can maintain operations even in the event of a cyber incident.

5. Conclusion

As the humanitarian sector goes digital with the promise of increased efficiency and speed in reaching people in need in the wake of disasters, it gets unavoidably caught in the cyber threat landscape. For organizations whose core mission lies in protecting vulnerable individuals, any cyber incident compromising the highly sensitive data collected or disrupting humanitarian operations carries potentially devastating consequences. Given their critical role during emergencies, ensuring humanitarian organizations can effectively prepare for and respond to cyber incidents is crucial to future crisis management efforts.

This scoping review mapped the cyber threats, challenges, and currently implemented cybersecurity strategies across the sector. The findings revealed serious gaps in both existing research and practice, particularly stemming from the lack of measures addressing the unique challenges faced by humanitarian organizations. As such, this review stresses the importance of developing solutions tailored to the distinctive features and needs of the humanitarian sector. To this end, this study provides a base for further investigation, with the key themes, gaps, and research avenues identified guiding immediate focus for this underexplored field.

CRediT authorship contribution statement

Chiara Anfuso: Writing – original draft, Visualization, Methodology, Formal analysis, Data curation, Conceptualization. **Andrea Bartolucci:** Writing – review & editing, Supervision, Methodology, Conceptualization. **Cristina Del-Real:** Writing – review & editing, Supervision, Methodology, Conceptualization. **Sanneke Kuipers:** Writing – review & editing, Supervision.

Declaration of generative AI in scientific writing

During the preparation of this work, the author(s) used ChatGPT to improve English language quality and address writing-related issues such as grammar, clarity, and style. After using this tool, the author(s) carefully reviewed and edited the content as needed and take full responsibility for the content of this publication.

Funding

This research 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."

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgments

The authors thank the authors who responded to our inquiries and recommended supplementary sources that contributed to the comprehensiveness of this review.

Appendix A. Supplementary data

Supplementary data to this article can be found online at https://doi.org/10.1016/j.ijdrr.2026.106082.

Appendix A. Areas of improvement and measures to implement to strengthen cybersecurity

Measure to Implement	Management Pillar			Source(s)
	People	Process	Technology	
Build a community of practice to fight mis/disinformation as well as strategic alliances with technological firms and social media verification analysts capable of augmenting information and "(pre)bunking" narratives	X			[43,44,64,59]
Incorporate effective strategies to swiftly and efficiently counter or dispel rumors in the humanitarian toolkit		X		[44,60,59]
Enhance transparency		X		[44,59]
Invest in strong foundational training	X			[19,42,61,62,63]
Establish a comprehensive cybersecurity governance structure, including policies and practices on basic cyber hygiene, asset inventories, and regular risk assessments	X	X		[19,61]
Strengthen partnerships between governments, international organizations, NGOs, local actors, the private sector, civil society, and academia	X	X		[19,64,65]
Foster resilience through routine secure offsite backups		X	X	[42,66,67,68]
Leverage existing cybersecurity frameworks like the NIST Risk Management Framework (RMF) or the ISO (International Organization for Standardization) 22301:2019 or tailored models to enhance the capability to prepare for and respond to disruptions		X		[61,69,70,68]
Ensure decision-making is driven by realistic risk modeling evaluating the impact of cyber threats from the likelihood of a disaster to financial losses and casualties		X		[66,67]
Integrate digital security breaches into business continuity and crisis management plans		X		[42,66,62]
Conduct simulations to prepare for potential risks such as hostile network penetration or sensitive data leaks	X			[42,66]
Conduct internal reviews focused on identifying information that possibly exposes the organization, such as external emails, financial transactions, or travel reservations	X	X		[66]
Map, audit, and constantly update the critical information mandated to preserve and safeguard		X		[66]
Develop clear information classification procedures to categorize data systematically based on risks		X		[66]

(*continued on next page*)

(*continued*)

Measure to Implement	Management Pillar			Source(s)
	People	Process	Technology	
Establish security standards and encryption protocols for both hardware and software, as well as regular IT system updates			X	[42,71,61,69,65,62,63]
Establish dedicated Virtual Private Servers or Virtual Machines (VPS/VMs) and cloud-hosted email platforms providing better security than shared hosts			X	[61]
Invest in the dark web monitoring to detect leaked credentials		X	X	[61]
Implement MFA for critical systems and use password managers to store password securely			X	[61]
Develop a formal incident response plan with clear roles and procedures	X	X		[61]
If constrained by funding, rely on less costly solutions based on behavior research and approach focused on educating and training staff	X			[42,70,63]
Be more vocal and proactive in advocating for digital safety	X	X		[63]
Design public education campaigns focused on enhancing digital and media literacy	X	X		[64]
Ensure awareness of possible threats before any intervention in the digital sphere	X	X		[72,73]
Develop clear guidelines that integrate privacy protection strategies into all stages of the program cycle, from the project design to data collection, storage and sharing		X		[72,74,65]
Establish ethical committees to assess the risks posed to the stored information	X			[72]
Anonymize and/or aggregate data to safeguard personal information			X	[72]
Build trustworthy and resilient systems out of untrustworthy components, as proposed by the “Zero Trust” approach	X	X	X	[75]
Develop unique assets such as a “digital humanitarian space” akin to a “sovereign cloud” or a “digital embassy”			X	[75]
Reduce strong supplier dependencies		X		[71]
Add cybersecurity coverage to existing insurance policies		X		[42]
integrate community-focused approach that includes local people in the development and implementation of IoT solutions	X			[65]
Conduct assessments focused on existing vulnerabilities in the critical information infrastructure of the organizations	X		X	[60]

Data availability

Data will be made available on request.

References

[1] OCHA, New and Emerging Technologies are Improving Humanitarian Action | Global Humanitarian Overview, Global Humanitarian Overview, 2021. https://2021.gho.unocha.org/global-trends/new-and-emerging-technologies-are-improving-humanitarian-action.

[2] L. Arendt-Cassetta. From digital promise to frontline practice: New and emerging technologies in humanitarian action, OCHA, New York, 2021, April.

[3] A. Beduschi, Harnessing the potential of artificial intelligence for humanitarian action: opportunities and risks, Int. Rev. Red Cross (2022). https://international-review.icrc.org/articles/harnessing-the-potential-of-artificial-intelligence-for-humanitarian-action-919.

[4] Z. Rahman, P. Verhaert, C. Nyst, *Biometrics in the Humanitarian Sector.* the Engine Room Ans Oxfam, 2018.

[5] * M. Duffield, Disaster-Resilience in the Network Age Access-Denial and the Rise of Cyber-Humanitarianism, 2013 [DIIS Working Paper].

[6] E. Ferris, Why Humanitarians Should Pay Attention to Cybersecurity, Brookings, 2014. https://www.brookings.edu/articles/why-humanitarians-should-pay-attention-to-cybersecurity/.

[7] OCHA, Global Humanitarian Overview 2023, 2022.

[8] * B. Willitts-King, J. Bryant, K. Holloway, The humanitarian “digital divide”, in: Humanitarian Policy Group Working Paper, 2019. en/publications/thehumanitarian-digital-divide.

[9] ICRC, Sophisticated cyber-attack targets red cross red crescent data on 500,000 people. International committee of the red cross. https://www.icrc.org/en/document/sophisticated-cyber-attack-targets-red-cross-red-crescent-data-500000-people, 2022.

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

[11] Central Tracing Agency, Towards safer digital services: the CTA data breach one year on, Missing Persons Global Response (2023). http://missingpersons.icrc.org/news-stories/towards-safer-digital-services-cta-data-breach-one-year.

[12] J. Devanesan, Experts analyze the massive red cross data breach, TechHQ (2022). https://techhq.com/2022/01/anguish-and-suffering-experts-analyze-the-massive-red-cross-data-breach/.

[13] S. Lyngaas, Cyberattack on Red Cross Compromised Data of over 515,000 ‘Highly Vulnerable People’ | CNN Politics, CNN, 2022. https://www.cnn.com/2022/01/19/politics/red-cross-cyberattack/index.html.

[14] ICRC, Cyber Operations During Armed Conflicts, 2021. https://www.icrc.org/en/document/cyber-warfare.

[15] L. Howard, The Ukraine War & Cyberattacks Targeting Refugees and Humanitarian Organizations, Henry M. Jackson School of International Studies, 2023. https://jsis.washington.edu/news/the-ukraine-war-cyberattacks-targeting-refugees-and-humanitarian-organizations/.

[16] Global Voices MENA, Human rights organizations call for an immediate physical and digital ceasefire in Gaza, Global Voices (2023). https://globalvoices.org/2023/10/31/human-rights-organizations-call-for-an-immediate-physical-and-digital-ceasefire-in-gaza/.

[17] Z. Siddiqui, Hackers hit aid groups responding to Israel and Gaza crisis, Reuters (2023). https://www.reuters.com/world/middle-east/hackers-hit-aid-groups-responding-israel-gaza-crisis-2023-10-13/.

[18] Cloudflare, Impact report 2025. https://cf-assets.www.cloudflare.com/stl3lc6tev37/7koyyovVxIqK8zdG1pqo6O/dfcbbde950394c61855befd9bf083a28/Impact-Report-2025_Final.pdf, 2025.

[19] * L. Arendt-Cassetta, A. Omond, T. van Benthem, Y. Shura, Virtual Risk, Tangible Harm: the Humanitarian Implications of Cyber Threats, OCHA, 2022.

[20] OCHA Centre for Humanitarian Data, Guidance Note on the Implications of Cyber Threats for Humanitarians, 2023.

[21] S. Lyngaas, Aid Groups Helping Ukraine Face Both Cyber and Physical Threats, CNN, 2022. https://edition.cnn.com/2022/04/23/politics/humanitarian-aid-ukraine-war-cyberattacks/index.html.

[22] J.K. Nwankpa, Registering refugees using personal information has become the norm – but cybersecurity breaches pose risks to people giving sensitive biometric data, The Conversation (2023). http://theconversation.com/registering-refugees-using-personal-information-has-become-the-norm-but-cybersecurity-breaches-pose-risks-to-people-giving-sensitive-biometric-data-208166.

[23] B. Wille, The Data of the Most Vulnerable People is the Least Protected, 2023 [Human Rights Watch], https://www.hrw.org/news/2023/07/11/data-most-vulnerable-people-least-protected.

[24] E. Rushing, Protecting Civilians Against Digital Threats: Four Worrying Trends and Recommendations to Address them, Humanitarian Law & Policy Blog, 2023. https://blogs.icrc.org/law-and-policy/2023/10/19/protecting-civilians-digital-threats-four-worrying-trends/.

[25] European Union Agency for Cybersecurity (ENISA), Best Practices for Cyber Crisis Management, 2024.

[26] G. González-Granadillo, S. González-Zarzosa, R. Diaz, Security information and event management (SIEM): analysis, trends, and usage in critical infrastructures, Sensors 21 (14) (2021) 4759, https://doi.org/10.3390/s21144759.

[27] D.M. Kiambi, A. Shafer, Corporate crisis communication: examining the interplay of reputation and crisis response strategies, Mass Commun. Soc. 19 (2) (2016) 127–148, https://doi.org/10.1080/15205436.2015.1066013.

[28] O. Kulikova, R. Heil, J. Van Den Berg, W. Pieters, Cyber crisis management: a decision-support framework for disclosing security incident information, in: 2012 International Conference on Cyber Security, 2012, pp. 103–112, https://doi.org/10.1109/CyberSecurity.2012.20.

[29] G. Mott, J.R.C. Nurse, C. Baker-Beall, Preparing for future cyber crises: lessons from governance of the coronavirus pandemic, Policy Design and Practice 6 (2) (2023) 160–181, https://doi.org/10.1080/25741292.2023.2205764.

[30] J. Srinivas, A.K. Das, N. Kumar, Government regulations in cyber security: framework, standards and recommendations, Future Gener. Comput. Syst. 92 (2019) 178–188, https://doi.org/10.1016/j.future.2018.09.063.

[31] S. Chaudhary, V. Gkioulos, S. Katsikas, Developing metrics to assess the effectiveness of cybersecurity awareness program, Journal of Cybersecurity 8 (1) (2022), https://doi.org/10.1093/cybsec/tyac006 tyac006.

[32] G. Hatzivasilis, S. Ioannidis, M. Smyrlis, G. Spanoudakis, F. Frati, L. Goeke, T. Hildebrandt, G. Tsakirakis, F. Oikonomou, G. Leftheriotis, Modern aspects of cyber-security training and continuous adaptation of programmes to trainees, Applied Sciences 10 (16) (2020) 5702, https://doi.org/10.3390/app10165702.

[33] L. Li, W. He, L. Xu, I. Ash, M. Anwar, X. Yuan, Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior, Int. J. Inf. Manag. 45 (2019) 13–24, https://doi.org/10.1016/j.ijinfomgt.2018.10.017.

[34] J. Prümmer, T. van Steen, B. van den Berg, A systematic review of current cybersecurity training methods, Comput. Secur. 136 (2024) 103585, https://doi.org/10.1016/j.cose.2023.103585.

[35] K. Macnish, J. van der Ham, Ethics in cybersecurity research and practice, Technol. Soc. 63 (2020) 101382, https://doi.org/10.1016/j.techsoc.2020.101382.

[36] M.-J. Sule, M. Zennaro, G. Thomas, Cybersecurity through the lens of digital identity and data protection: issues and trends, Technol. Soc. 67 (2021) 101734, https://doi.org/10.1016/j.techsoc.2021.101734.

[37] A. Chidukwani, S. Zander, P. Koutsakis, A Survey on the cyber security of small-to-medium businesses: challenges, research focus and recommendations, IEEE Access 10 (2022) 85701–85719, https://doi.org/10.1109/ACCESS.2022.3197899.

[38] J.S. Hiller, R.S. Russell, The challenge and imperative of private sector cybersecurity: an international comparison, Computer Law & Security Review 29 (3) (2013) 236–245, https://doi.org/10.1016/j.clsr.2013.03.003.

[39] R. Knight, J.R.C. Nurse, A framework for effective corporate communication after cyber security incidents, Comput. Secur. 99 (2020) 102036, https://doi.org/10.1016/j.cose.2020.102036.

[40] G.R.T. White, R.A. Allen, A. Samuel, A. Abdullah, R.J. Thomas, Antecedents of cybersecurity implementation: a Study of the cyber-preparedness of U.K. social enterprises, IEEE Trans. Eng. Manag. 69 (6) (2022) 3826–3837, https://doi.org/10.1109/TEM.2020.2994981.

[41] * 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, ProQuest Dissertations Publishing, 2020 [Doctoral dissertation, Marymount University].

[42] * S. Mierzwa, J. Scott, Cybersecurity in Non-profit and Non-governmental Organizations, Institute for Critical Infrastructure Technology, 2017.

[43] * S. Powazek, S. Pierson, Cybercan: Cybersecurity for Cities and Nonprofits, CLTC, 2024, https://cltc.berkeley.edu/publication/cybercan-cybersecurity-for-cities-and-nonprofits/.

[44] * R. Vhikai, E. Mugoni, A.P. Mataka, F. Saruchera, Digitalisation and efficient humanitarian logistical operations in Zimbabwe, Cogent Soc. Sci. 10 (1) (2024) 2321725 https://doi.org/10.1080/23311886.2024.2321725.

[45] C. Droege, Get off my cloud: cyber warfare, international humanitarian law, and the protection of civilians, Int. Rev. Red Cross 94 (886) (2012) 533–578, https://doi.org/10.1017/S1816383113000246.

[46] L. Gisel, T. Rodenhäuser, K. Dörmann, Twenty years on: international humanitarian law and the protection of civilians against the effects of cyber operations during armed conflicts, Int. Rev. Red Cross 102 (913) (2020) 287–334, https://doi.org/10.1017/S1816383120000387.

[47] * K.B. Sandvik, M. Gabrielsen Jumbert, J. Karlsrud, M. Kaufmann, Humanitarian technology: a critical research agenda, Int. Rev. Red Cross 96 (893) (2014) 219–242, https://doi.org/10.1017/S1816383114000344.

[48] A.C. Tricco, E. Lillie, W. Zarin, K.K. O'Brien, H. Colquhoun, D. Levac, D. Moher, M.D. Peters, T. Horsley, L. Weeks, PRISMA extension for scoping reviews (PRISMA-ScR): checklist and explanation, Ann. Intern. Med. 169 (7) (2018) 467–473, https://doi.org/10.7326/M18-0850.

[49] H. Arksey, L. O'Malley, Scoping studies: towards a methodological framework, Int. J. Soc. Res. Methodol. 8 (1) (2005) 19–32, https://doi.org/10.1080/1364557032000119616.

[50] Z. Munn, M.D.J. Peters, C. Stern, C. Tufanaru, A. McArthur, E. Aromataris, Systematic review or scoping review? Guidance for authors when choosing between a systematic or scoping review approach, BMC Med. Res. Methodol. 18 (1) (2018) 143, https://doi.org/10.1186/s12874-018-0611-x.

[51] M.D.J. Peters, C. Marnie, H. Colquhoun, C.M. Garritty, S. Hempel, T. Horsley, E.V. Langlois, E. Lillie, K.K. O'Brien, Özge Tunçalp, M.G. Wilson, W. Zarin, A. C. Tricco, Scoping reviews: reinforcing and advancing the methodology and application, Syst. Rev. 10 (1) (2021) 263, https://doi.org/10.1186/s13643-021-01821-3.

[52] S. Mikki, Google Scholar Compared to Web of Science. A Literature Review. Nordic Journal *of Information Literacy in Higher Education*, vol. 1, 2009, https://doi.org/10.15845/noril.v1i1.10, 1.

[53] N.R. Haddaway, A.M. Collins, D. Coughlin, S. Kirk, The role of Google scholar in evidence reviews and its applicability to grey Literature searching, PLoS One 10 (9) (2015) e0138237, https://doi.org/10.1371/journal.pone.0138237.

[54] European Civil Protection and Humanitarian Aid Operations. (n.d.). Humanitarian aid. https://civil-protection-humanitarian-aid.ec.europa.eu/what/humanitarian-aid_en.

[55] ICRC, The Code of Conduct for the International Red Cross and Red Crescent Movement and Ngos in Disaster Relief, 1995.

[56] J.R. Landis, G.G. Koch, The measurement of observer agreement for categorical data, Biometrics 33 (1) (1977) 159–174, https://doi.org/10.2307/2529310.

[57] E.Y. Handri, P.A.W. Putro, D.I. Sensuse, Evaluating the people, process, and technology priorities for NIST cybersecurity framework implementation in E-Government, in: 2023 IEEE International Conference on Cryptography, Informatics, and Cybersecurity (Icocics), 2023, pp. 82–87, https://doi.org/10.1109/ICoCICs58778.2023.10277024.

[58] A. Taher, Stakeholders' opinions support the people-process-technology framework for implementing digital transformation in higher education, Technol. Pedagog. Educ. 32 (5) (2023) 555–567, https://doi.org/10.1080/1475939X.2023.2248134.

[59] * Z. Al Achkar, Digital Risk: how new technologies impact acceptance and raise new challenges for NGOs. Achieving Safe Operations Through Acceptance: Challenges and Opportunities for Security Risk Management, 2021.

[60] * K.B. Sandvik, M. Fujita, Y. Kanatani, W. Rogers, G. Chamales, M. Arii, K. Kurokawa, The risks of technological innovation, in: *In World Disasters Report 2013: Focus on Technology and the Future of Humanitarian Intervention*. International Federation of Red Cross and Red Crescent Societies, 2013.

[61] * CyberPeace Institute, Cyber resilience for NGOs: a collective intelligence effort, https://cyberpeaceinstitute.org/news/publications/cyber-resilience-ngos-collective-intelligence-effort/, 2024.
[62] * D. Vitaliev, Cyber Security for International Aid Agencies: a Primer, vol. 3, SMI Professional Development Brief, 2009.
[63] * D. Elshani, Are Non-governmental Organizations Prepared to Deal with Cyber Threats? an Analysis of Perceptions of Cybersecurity Capacities Among Ngos in Kosovo, Kosovar Centre for Security Studies, 2023.
[64] * A. Fitz-Gerald, J. Hennebry, Protecting civilians in a data-driven and digitalized battlespace: toward a baseline humanitarian technology infrastructure. Frontiers in Human Dynamics 6 (2025) 1465594 https://doi.org/10.3389/fhumd.2024.1465594.
[65] * B.D. Parmadi, K. Ramli, Transforming humanitarian response with IoT in conflict zones: field insights, ethical frameworks, and deployment challenges, International Journal of Electrical, Computer, and Biomedical Engineering 3 (1) (2025) 157–187, https://doi.org/10.62146/ijecbe.v3i1.112.
[66] * R. Byrne, Measures for mitigating cyber-security risks, in: Communications Technology and Humanitarian Delivery: Challenges and Opportunities for Security Risk Management, European Interagency Security Forum (EISF), 2014.
[67] * G. Loukas, D. Gan, T. Vuong, A review of cyber threats and defence approaches in emergency management, Future Internet 5 (2) (2013) 205–236, https://doi.org/10.3390/fi5020205.
[68] * N. Bell, X. Liu, Level of cybersecurity readiness of small and medium nonprofit organizations (NPOs) during COVID-19, Journal of Strategic Innovation & Sustainability 18 (2) (2023).
[69] * R. de Bruin, S. Von Solms, Humanitarian perspective of cybersecurity and cybersecurity governance, in: 2017 IST-Africa Week Conference (IST-Africa), IEEE, 2017, pp. 1–10.
[70] * K. Saeedi, M.A. Hassan, S. Alarifi, H. Almagwashi, An intuitive approach to cybersecurity risk assessment for non-governmental organizations, Transforming Gov. People, Process Policy 19 (1) (2024) 159–182, https://doi.org/10.1108/TG-08-2024-0201.
[71] * M. Marelli, The SolarWinds hack: lessons for international humanitarian organizations, Int. Rev. Red Cross 104 (919) (2022) 1267–1284, https://doi.org/10.1017/S1816383122000194.
[72] * D. Gilman, Humanitarianism in the Age of cyber-warfare: towards the Principled and Secure Use of Information in Humanitarian Emergencies, United Nations Office for the Coordination of Humanitarian Affairs, 2014.
[73] * D. Gilman, Cyber-Warfare and humanitarian space, in: Communications Technology and Humanitarian Delivery: Challenges and Opportunities for Security Risk Management, European Interagency Security Forum (EISF), 2014, pp. 8–12.
[74] * K.B. Sandvik, The centralization of vulnerability in humanitarian cyberspace: the ICRC hack revisited, in: Humanitarian Extractivism, Manchester University Press, 2023, pp. 38–56.
[75] * 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 102 (913) (2020) 367–387, https://doi.org/10.1017/S1816383121000151.
[76] H. Khalil, M.D.J. Peters, A.C. Tricco, D. Pollock, L. Alexander, P. McInerney, C.M. Godfrey, Z. Munn, Conducting high quality scoping reviews-challenges and solutions, J. Clin. Epidemiol. 130 (2021) 156–160, https://doi.org/10.1016/j.jclinepi.2020.10.009.
[77] D.K. Pollock, H. Khalil, C. Evans, C. Godfrey, D. Pieper, L. Alexander, A.C. Tricco, P. McInerney, M.D.J. Peters, M. Klugar, M. Falavigna, A.T. Stein, A. Qaseem, E.B. de Moraes, A. Saran, S. Ding, T.H. Barker, I.D. Florez, R.M. Jia, Z. Munn, The role of scoping reviews in guideline development, J. Clin. Epidemiol. 169 (2024) 111301, https://doi.org/10.1016/j.jclinepi.2024.111301.
[78] * B. Hayes, Migration and data protection: doing no harm in an age of mass displacement, mass surveillance and "big data.", Int. Rev. Red Cross 99 (904) (2017) 179–209, https://doi.org/10.1017/S1816383117000637.
[79] * A. Martin, G. Sharma, S. Peter De Souza, L. Taylor, B. Van Eerd, S.M. McDonald, M. Marelli, M. Cheesman, S. Scheel, H. Dijstelbloem, Digitisation and sovereignty in humanitarian space: technologies, territories and tensions, Geopolitics 28 (3) (2023) 1362–1397, https://doi.org/10.1080/14650045.2022.2047468.
[80] * S. Le Blond, A. Cuevas, J.R. Troncoso-Pastoriza, P. Jovanovic, B. Ford, J.-P. Hubaux, On enforcing the digital immunity of a large humanitarian organization, in: 2018 IEEE Symposium on Security and Privacy (SP), 2018, pp. 424–440, https://doi.org/10.1109/SP.2018.00019.
[81] * M. Duffield, The resilience of the ruins: towards a critique of digital humanitarianism, Resilience 4 (3) (2016) 147–165, https://doi.org/10.1080/21693293.2016.1153772.
[82] * K.B. Sandvik, K.L. Jacobsen, S.M. McDonald, Do no harm: a taxonomy of the challenges of humanitarian experimentation, Int. Rev. Red Cross 99 (904) (2017) 319–344, https://doi.org/10.1017/S181638311700042X.
[83] * J.P. Kalkman, Practices and consequences of using humanitarian technologies in volatile aid settings, Journal of International Humanitarian Action 3 (1) (2018) 1, https://doi.org/10.1186/s41018-018-0029-4.
[84] * K.B. Sandvik, The humanitarian cyberspace: shrinking space or an expanding frontier?, Third World Q. 37 (1) (2016) 17–32, https://doi.org/10.1080/01436597.2015.1043992.
[85] * P. Meier, New information technologies and their impact on the humanitarian sector, Int. Rev. Red Cross 93 (884) (2011) 1239–1263, https://doi.org/10.1017/S1816383112000318.
[86] * N. Ermicioi, M. Xiang Liu, Cybersecurity in nonprofits: factors affecting security readiness during Covid-19, in: SAIS 2022 Proceedings, 2022.
[87] International Organization for Migration (IOM), IOM Data Protection Manual, 2010. https://publications.iom.int/books/iom-data-protection-manual.
[88] Sphere. (n.d.). Sphere | for life with dignity. Retrieved July 12, 2024, from https://www.spherestandards.org/.
[89] Inter-Agency Standing Committee, Operational Guidance: Data Responsibility in Humanitarian Action, 2021.
[90] C. Kuner, M. Marelli, Handbook on Data Protection In Humanitarian Action, 2020.
[91] W.T. Coombs, Protecting Organization reputations during a crisis: the development and application of situational crisis communication theory, Corp. Reput. Rev. 10 (3) (2007) 163–176, https://doi.org/10.1057/palgrave.crr.1550049.
[92] J.Z.L. Covarrubias, Effective communication as A pillar of cybersecurity: managing incidents and crises in the digital era, Journal of Risk Analysis and Crisis Response 15 (2) (2025), 34-34.
[93] T. Wakolbinger, F. Toyasaki, Impacts of funding systems on humanitarian operations, in: Humanitarian Logistics: Meeting the Challenge of Preparing and Responding to Disasters and Complex Emergencies, Kogan Page Limited, 2014, pp. 21–24.
[94] Inter-Agency Standing Committee. Donor conditions and their implications for humanitarian response, 2016, May 18. https://reliefweb.int/report/world/donor-conditions-and-their-implications-humanitarian-response.
[95] GISF, Community acceptance: a cornerstone of humanitarian security risk management, Global Interagency Security Forum (2021). https://gisf.ngo/blogs/community-acceptance-a-cornerstone-of-humanitarian-security-risk-management/.
[96] GISF, Achieving Safe Operations through acceptance: challenges and opportunities for security risk management, Global Interagency Security Forum (2022). https://reliefweb.int/report/world/achieving-safe-operations-through-acceptance-challenges-and-opportunities-security-risk.
[97] H.S. Chen, T.M.C. Jai, Cyber alarm: Determining the impacts of hotel's data breach messages, Int. J. Hosp. Manage. 82 (2019) 326–334, https://doi.org/10.1016/j.ijhm.2018.10.002.
[98] T. Coombs, Situational theory of crisis: Situational crisis communication theory and corporate reputation. The Handbook of Communication and Corporate Reputation, John Wiley & Sons, Ltd., 2013, pp. 262–278. https://doi.org/10.1002/9781118335529.ch23.
[99] M.M. Al-Nassiri, I.A. Al-Balatah, Enhancing information security awareness model to advance human aspects in humanitarian organizations, in: 2024 1st International Conference on Emerging Technologies for Dependable Internet of Things (ICETI), IEEE, 2024, pp. 1–8, https://doi.org/10.1109/ICETI63946.2024.10777196.
[100] A. Othman, Z. Ahmad, Innovation adoption in humanitarian logistics: a framework for evaluating the implementation of cutting-edge technologies in relief operations, in: Supply Chain in Humanitarian Operations: Managing Disruption Through Intervention and Innovation, Springer Nature, Singapore, 2025, pp. 43–54.

[101] A. Pollini, T.C. Callari, A. Tedeschi, D. Ruscio, L. Save, F. Chiarugi, D. Guerri, Leveraging human factors in cybersecurity: an integrated methodological approach, Cognit. Technol. Work 24 (2) (2022) 371–390, https://doi.org/10.1007/s10111-021-00683-y.
[102] M. Eminağaoğlu, E. Uçar, Ş. Eren, The positive outcomes of information security awareness training in companies – a case study, Inf. Secur. Tech. Rep. 14 (4) (2009) 223–229, https://doi.org/10.1016/j.istr.2010.05.002.
[103] United Nations Office for Disaster Risk Reduction, Sendai framework for disaster risk reduction 2015—2030. https://www.undrr.org/publication/sendai-framework-disaster-risk-reduction-2015-2030, 2015.
[104] International Organization for Standardization, ISO 22301:2019. https://www.iso.org/standard/75106.html, 2019.