SUBMISSION ON THE PROTECTION OF HUMANITARIAN NGOs

to the Open-Ended Working Group on security of and in the use of information and communications technologies 2021-2025

In anticipation of the fourth substantive session of the Open-Ended Working Group on security of and in the use of information and communications technologies 2021-2025 (OEWG), and in line with our earlier recommendations\(^1\) and the statement on the protection of the humanitarian sector\(^2\), the CyberPeace Institute\(^3\) welcomes the opportunity to provide the following recommendations on the protection of humanitarian non-governmental organizations (NGOs). This contribution is evidence-based, forward-looking and action-oriented, and aims to inform the work of the OEWG across its priority areas. It outlines the cyber threat landscape for humanitarian action, the remaining gaps in the cyber preparedness of NGOs, and the need for a collective approach to cyber resilience in this vital sector.

Provision of critical services

Humanitarian organizations provide critical services to those most in need of assistance and protection, including those living in areas of armed conflict or natural disaster. For the past years, the humanitarian sector has been undergoing a rapid digital transformation, leveraging technologies to strengthen and scale up the reach and impact of their humanitarian responses, including informing and engaging with beneficiaries and connecting people to services.

At the same time, the digitization and digitalization of humanitarian organizations have increased the risks of cyberattacks.
The cyber threat landscape for humanitarian organizations

Technologies that allow humanitarian action to be more effective are being exploited against the organizations themselves and their beneficiaries. Malicious actors seek to steal funds, exfiltrate data, including highly sensitive data on people, or to disrupt the organizations’ ability to operate. Threat actors weaponize data, identify individuals or groups for persecution, conduct hack and leak operations, seek financial gain from organizations through demands for ransom, and/or spread disinformation about humanitarian organizations to undermine their credibility and the trust that they depend upon to help persons in need. Recent cyberattacks have affected both large international organizations such as the International Committee of the Red Cross (ICRC)\(^4\) and UN agencies\(^5\) and small NGOs such as Roots of Peace\(^6\) and Insecurity Insights\(^7\).

In addition, there is the risk that cyberattacks and operations lead to an increase in humanitarian needs, for example, if infrastructure essential for the survival of the population is targeted disrupting the provision of power supplies, health care, clean water, etc.\(^8\)

Humanitarian organizations often lack cybersecurity capabilities to both understand their threat landscape and to put in place adequate measures to prevent, respond to and recover from cyberattacks. They may not have the resources and expertise to properly secure their ICT infrastructure and digital assets or to develop an adequate incident response system that could minimize the impacts of cyberattacks.

A collective approach to cyber resilience in the humanitarian sector

Bolstering the cyber resilience of humanitarian organizations will require a collective effort to support cyber capacity building and provide resources to help better detect and respond to threats. A multistakeholder approach can enable sharing and exchanging of expertise, perspectives, lessons learned, good practices, and resources across the sector.

The CyberPeace Institute has been assisting humanitarian NGOs through the CyberPeace Builders
By identifying the vulnerabilities that attackers exploit and alerting NGOs to their risks and vulnerabilities, the Institute program helps to prevent future attacks. The Institute carries out a general security assessment of each NGO, and then tailors support to their needs: a recent cybersecurity assessment conducted on a number of NGOs found that the organizations’ average score was only 28 points out of 100.

Through facilitating this tailored-made and free of charge assistance, the CyberPeace Builders program actively contributes to closing the cybersecurity gap by empowering each organization’s adoption of cyber preparedness and resilience measures. The program currently supports over 110 humanitarian NGOs across the world, and this number is growing every week.

Recognizing the growing and diverse needs of this vital sector, the CyberPeace Institute launched the Humanitarian Cybersecurity Center (HCC) on 27 February 2023. The Centre provides tools, expert support, and free cyber assistance to NGOs, tailored to their needs, through partnerships and networks of dedicated professionals and volunteers. This evidence-based approach can contribute to increased understanding of the threats, harm and challenges of the malicious use of cyber against humanitarian NGOs, and recognition that such attacks are unacceptable and the need for better protection of humanitarian organizations.

Recommendations

The CyberPeace Institute provides the following recommendations for Member States consideration during the OEWG discussions based on our mission, expertise on the cyber threat landscape, and experience assisting humanitarian NGOs, and are in line with the areas of work of the OEWG and its overarching goal of maintaining international peace and security in cyberspace.

1. Protection of the humanitarian sector under the legal and normative frameworks

We call on States to affirm that humanitarian organizations, their staff and humanitarian data must not be the target of cyberattacks and to ensure that the international legal and normative frameworks provide adequate protection for humanitarian organizations online as well as offline. This includes acting in line with obligations under international law, as well as universally agreed-upon norms.
States should share their national positions on how and when international humanitarian law applies to cyber operations and the use of ICTs.

2. **Protection of humanitarian data**
States should affirm that humanitarian data is a civilian object and thus protected under international humanitarian law: it should not be breached, manipulated or destroyed including through cyberattacks or operations.

Humanitarian data must only be available for and used for the purpose for which it has been collected to avoid possible privacy violations and re-victimization.

States should also maximize the protection for the humanitarian sector under domestic legal frameworks and introduce safeguards that effectively protect humanitarian organizations, their data, and their operations. The critical and sensitive nature of humanitarian action should guide and inform the design of data protection frameworks and the legislative approaches to increase protection for the confidentiality of data gathered, managed, processed, and stored.

3. **Study of existing and potential threats**
States should study existing and potential threats that the humanitarian sector faces and facilitate gathering evidence that informs the understanding of the cyber threat landscape. Multistakeholder initiatives and expertise can be instrumental when building knowledge about cyberattacks and their harm and impact, for example, the CyberPeace Institute is collecting and analysing data about cyberattacks targeting the humanitarian sector as part of its programs and support to NGOs.

4. **Improved and transparent reporting**
Transparent reporting on cyberattacks against humanitarian NGOs should be supported and mainstreamed. Sharing of information can facilitate increased understanding of the threat landscape, including the vector, impact, means, and actors. This can also ensure that capacity building initiatives are needs-driven, increase cyber resilience, and inform and influence policy making. It is paramount to concurrently prevent further revictimization of NGOs, their staff, and beneficiaries. This will require robust
safeguards to guarantee the protection, confidentiality, and integrity of information. Reporting should be strictly limited to data necessary to understand the security and operational implications of the attack.

5. **Building cyber capacity and resilience**

States need to build capacity at all levels to create policies and initiatives that can support the protection of humanitarian NGOs and reduce the proliferation of cyberattacks targeting them. Efforts should be increased to build the capacity of humanitarian organizations to strengthen their resilience to cyber incidents.

States should engage in broad multistakeholder participation when building the cyber resilience of NGOs. Actors from diverse areas of humanitarian action, including managerial, operational, and technical, should be encouraged to participate in multistakeholder processes, alongside civil society, academia, and the private sector to share best practices and increase common understanding. The CyberPeace Institute can contribute its expertise and experience to such multistakeholder action, such as the establishment of the Humanitarian Cybersecurity Centre with the aim to support the capacities of humanitarian organizations and increase their cyber resilience.

**Conclusion**

The protection of humanitarian organizations is essential for the people who depend on them, our societies, and international peace and security as a whole, and should receive adequate protection in cyberspace. Humanitarian organizations make a vital contribution to humanity, assisting and protecting people. Malicious use of cyberattacks against humanitarian organizations demonstrates a clear disregard for lives. Such attacks – in peacetime and wartime – must stop. Protecting humanitarian action must be a collective goal and a collective effort.
Annex

**Humanitarian Cybersecurity Center (HCC)**

In the last 3 years, cybercriminals and Nation State actors have accessed systems and personal records, stolen millions of dollars of donations, carried out surveillance operations, or led disinformation campaigns against non-governmental organizations (NGOs).

Humanitarian and development NGOs are targeted by cyberattacks and information operations. They do not have the capacity to both be on the frontline of aid delivery and respond to cyber threats. Cyberattacks imperil lives and erode the trust in organizations that is essential for their work.

This is why the CyberPeace Institute launched the Humanitarian Cybersecurity Center (HCC) – developed and hosted in Switzerland, and operating globally. This is a partnership platform, scaling-up cybersecurity solutions for humanitarian NGOs.

More than 1 billion people across the world receive vital support and services from NGOs. These organizations leverage technologies to carry out their activities and are entrusted to hold vast troves of sensitive data on people. This has increased the cyberattack surface of these organizations.

There is an urgent need to help NGOs to protect themselves.

The Humanitarian Cybersecurity Center provides them with free tools, workforce and knowledge to face the threat.

The Center provides expert support and practical assistance to NGOs in the humanitarian and development sectors, tailored to their needs, and available anywhere in the world. The Center builds upon the CyberPeace Institutes key capabilities and develops programs of
activities and associated projects to support communities vulnerable to threats in cyberspace.

Providing assistance and advice adapted to the specific needs of each NGO and working to foster collaboration and strengthen resilience, the Center carries out activities in 4 key focus areas:

1. DETECT & INFORM: Equipping NGOs with guidance and cyber threat intelligence so that they can detect upcoming cyberattacks.
2. PREVENT: Providing hands-on assistance to NGOs to build cyber preparedness and resilience through risk assessments, simulation exercises and training.
3. ASSIST: Hands-on technical and forensic investigative support and assistance with incident and crisis management.
4. STRENGTHEN: Developing standards, fostering multi-stakeholder collaboration and advocating for protection of the humanitarian sector at international fora.

---


3 The CyberPeace Institute is an independent and neutral non-governmental organization that strives to reduce the frequency, impact and scale of cyberattacks, to advocate for responsible behaviour and respect for laws and norms in cyberspace, and to assist vulnerable communities.

4 The targeted cyberattack against the ICRC led to the compromise of personal data and confidential information on more than 515,000 vulnerable people, including those separated from their families due to conflict, migration and disaster, missing persons and their families, and people in detention. Because of the attack, the ICRC had to shut down the systems underpinning their Restoring Family Links work, affecting the Red Cross and Red Crescent Movement’s ability to locate missing people and reunite separated family members. See more information here: ICRC, “Cyber attack on ICRC: What we know,” February 16, 2022, available from: https://www.icrc.org/en/document/cyber-attack-icrc-what-we-know#:~:text=Update%3A%2024%20June%202022.,in%20a%20sophisticated%20cyber%20attack; ICRC, “Misinformation about ICRC activities for people affected by the armed conflict in Ukraine,” February 23, 2023, available from: https://www.icrc.org/en/document/false-information-about-icrc-ukraine


8 The ongoing international armed conflict between the Russian Federation and Ukraine has witnessed a prolific use of cyber, and the CyberPeace Institute has been monitoring and aggregating data in a publicly available platform with regard to cyberattacks and operations against critical infrastructure. Four types of cyberattacks have
been documented - Destructive, Disruptive, Disinformation and Data Weaponization - including incidents of attacks against humanitarian organizations. Access the Cyber Attacks in Times of Conflict Platform here: https://cyberconflicts.cyberpeaceinstitute.org/


10 The General Security Assessment (GSA) intends to provide an overview of some of the key cybersecurity elements of an organization. This assessment allows the organization to go deeper in the analysis of its cybersecurity infrastructure and implement specific measures to improve its overall cybersecurity measures in a well-structured manner. The main objective of this assessment is to provide a structured approach to observe the wide-ranging cybersecurity challenges/needs of humanitarian NGOs. The GSA is usually done at the beginning of collaboration with a humanitarian NGO that joins the CyberPeace Builders program, and then informs the creation of support to them missions/jobs.


12 From detection and analysis of cyberattacks to the sharing of actionable threat intelligence to hands-on technical support and the fostering of collaboration, standards and advocacy efforts for the protection of the sector, the Institute offers practical help while creating momentum for further multistakeholder progress.