Kenya Red Cross | LUXEMBOURG AID & DEVELOPMENT | REPUBLIC OF KENYA | OFFICE OF THE DATA PROTECTION COMMISSIONER | ICRC

SAFEGUARDING HUMANITARIAN ORGANIZATIONS FROM DIGITAL THREATS

OBJECTIVES OF THE WORKING SESSION

- Understand the types of digital threats humanitarian organizations face, with a particular focus on the African region.
- Discuss ways in which humanitarian organizations can better protect themselves, their actions, and the people they serve from digital threats.

BACKGROUND INFORMATION

Humanitarian organizations operate in a context of increasingly digitalizing armed conflicts and in contested information environments, where state and non-state actors seek to exert control over the digital space. To operate securely, safely, and effectively – to fulfil their mandate – humanitarian organizations need to communicate, coordinate, and collaborate with communities, governments, non-state actors, and amongst themselves. They are, therefore, increasingly reliant on digital technologies to deliver aid and conduct their operations efficiently and effectively, complementing physical proximity with digital accessibility. These technologies allow humanitarian organizations to collect, process, and store personal data from vulnerable people, data which is entrusted to them for exclusively humanitarian purposes.

While this digital transformation has expanded the reach and impact of humanitarian action, it has also exposed organizations and the people they serve to a growing array of rapidly evolving digital threats.[1] In early 2022, an unprecedented cyber-attack on the International Committee of the Red Cross (ICRC) resulted in the unauthorized access of personal data entrusted to the ICRC.[2] The frequency and sophistication of cyber operations targeting humanitarian organizations are on the rise, potentially disrupting humanitarian operations, compromising sensitive data, eroding public trust, and exacerbating the vulnerabilities of affected people. This working session will focus on the digital threats facing humanitarian organizations and their operations in conflicts and crises. It will explore ways to safeguard these humanitarian organizations and their actions.

DIGITAL THREATS

Humanitarian organizations face digital threats that include **cyber operations** that disrupt digital infrastructure and communication systems or access or exfiltrate data, and **information operations** aimed at sowing confusion and mistrust and undermining reputations.[3] These threats can manifest in various forms: disruptions of information

[1] Global Interagency Security Forum (GISF), *Humanitarian Security in an Age of Uncertainty: the intersection of digital and physical risks*, January 2024, available at: https://gisf.ngo/wp-content/uploads/2024/01/Digital-Security-Final-Design-for-Publication.pdf (all internet references were accessed in October 2024).

[2] International Committee of the Red Cross (ICRC), *Cyber-attack on ICRC: What we know*, 24 June 2024, available at: https://www.icrc.org/en/document/cyber-attack-icrc-what-we-know; Kristin Bergtora Sandvik, "The centralisation of vulnerability in humanitarian cyberspace: the ICRC hack revisited", in Kristin Bergtora Sandvik, *Humanitarian extractivism*, Manchester University Press, October 2023, available at: https://manchesteruniversitypress.co.uk/9781526173355/

[3] International Committee of the Red Cross (ICRC), *International Humanitarian Law and the Challenges of Contemporary Armed Conflicts*, 2024, available at: https://shop.icrc.org/international-humanitarian-law-and-

communication technology (ICT) systems through DDoS attacks and the spread of malware, data breaches with the aim of either leaking sensitive data or extorting money through ransomware attacks, and disinformation campaigns aimed at undermining the reputation and trust of humanitarian organizations.[4]

The number and frequency of cyber operations targeting the humanitarian aid community have sharply risen in recent years.[5] This is also true for the African context, where several reports highlight the rise of cyber threats.[6] Essential civilian services and infrastructure have become prime targets in Africa, as exemplified with the large-scale cyber operation on the South African National Health Laboratory Service (NHLS) in June 2024 [7] and the distributed denial-of-service (DDoS) operation against Kenyan government websites in 2023.[8] Furthermore, internet shutdowns have become a frequent occurrence in conflicts and crises on the African continent,[9] leading to significant negative impact for the safety, dignity and resilience of affected people, financial losses, and for humanitarian operations. Information operations against the humanitarian community have equally risen in frequency. Across many active conflict contexts in the Eastern African Region, social-media-driven disinformation campaigns have consistently spread allegations that aid agencies are supportive of conflict parties, such as in Sudan,[10] Ethiopia,[11] and the DRC.[12] These campaigns have compounded safety and security risks for humanitarian organizations and sowed distrust among the public, undermining their ability to operate safely and effectively.

Several vulnerabilities within humanitarian organizations can be exploited by threat actors such as infrastructure flaws, including outdated systems, lack of robust security protocols and adequate data protection, and reliance on shared infrastructure with potential vulnerabilities. Additionally, inadequate cybersecurity preparedness often arises from insufficient cybersecurity budgets, a lack of skilled personnel, and limited cybersecurity awareness and training.[13] Human error also plays a significant role, with

the-challenges-of-contemporary-armed-conflicts-building-a-culture-of-compliance-for-ihl-to-protect-humanity-in-today-s-and-future-conflicts-pdf-en.html

[4] International Committee of the Red Cross (ICRC), *International Humanitarian Law and the Challenges of Contemporary Armed Conflicts*, 2024, available at: https://shop.icrc.org/international-humanitarian-law-and-the-challenges-of-contemporary-armed-conflicts-building-a-culture-of-compliance-for-ihl-to-protect-humanity-in-today-s-and-future-conflicts-pdf-en.html; International Council of Voluntary Agencies NGO Humanitarian Hub (ICVA), *Professional Standards for Protection Work*, 4th edition, 29 August 2024, available at: https://www.icvanetwork.org/resource/professional-standards-for-protection-work-4th-edition/

[5] United Nations International Computing Centre (UNICC), *Cyber Threat Landscape Report*, 2023, available at: https://www.unicc.org/wp-content/uploads/2024/07/2023-Cyber-Threat-Landscape-Report.pdf; NetHope, *2024 State of Humanitarian and Development Cybersecurity Report*, 2024, available at: https://nethope.org/toolkits/2024-state-of-humanitarian-and-development-cybersecurity-report/

[6] Check Point Software Technologies, "Unmasking cyberthreats in Africa", Techcentral, 26 August 2024, available at: https://techcentral.co.za/unmasking-cyberthreats-in-africa/250309/

[7] Tshwane, "National Health Lab Now Fully Operational After Cyber Attack", SA News, 22 August 2024, available at: https://www.sanews.gov.za/south-africa/national-health-lab-now-fully-operational-after-cyber-attack

[8] Abraham Augustine, "Pro-Sudan hackers attack digital services in Kenya", Techcabal, 27 July 2023, available at: https://techcabal.com/2023/07/27/pro-sudan-hackers-attack-digital-services-in-kenya/

[9] Eleanor Marchant, Nicole Stremlau, "The Changing Landscape of Internet Shutdowns in Africa", International Journal of Communication, Vol. 14, 2020, pp. 4216-4223, available at: https://ora.ox.ac.uk/objects/uuid:6a760859-7b23-44e1-b6c2-e73a335024e1

[10] Maram Mahdi, Kyle Hiebert, "Soudan's conflict is being fuelled by a digital propaganda war", Middle East Eye, 6 June 2023, available at: https://www.middleeasteye.net/opinion/sudan-civil-war-digital-propaganda-campaigns-fuelling

[11] Muna Shifa, Fabio Andrés Díaz Pabón, "The Interaction of Mass Media and Social Media in Fuelling Ethnic Violence in Ethiopia", Accord, 15 March 2022, available at: https://www.accord.org.za/conflict-trends/the-interaction-of-mass-media-and-social-media-in-fuelling-ethnic-violence-in-ethiopia/

[12] Insecurity Insight, *Online Negative Sentiment Towards International Community Further Underlines Reputational Risks*

to Humanitarian Agencies in the DRC, February 2024, available at: https://insecurityinsight.org/wp-content/uploads/2024/02/Online-Negative-Sentiment-DRC.pdf

[13] International Committee of the Red Cross (ICRC), *International Humanitarian Law and the Challenges of Contemporary Armed Conflicts*, 2024, available at: https://shop.icrc.org/international-humanitarian-law-and-the-challenges-of-contemporary-armed-conflicts-building-a-culture-of-compliance-for-ihl-to-protect-

staff falling victim to phishing scams, practicing poor password hygiene, and contributing to accidental data leaks.[14] Prioritizing cybersecurity investment can be challenging due to competing funding priorities within the humanitarian sector and pressure to allocate resources towards immediate aid delivery rather than long-term cybersecurity measures.[15] Taking a closer look at the African context, despite persistent differences in cybersecurity maturity between countries, the African region has made significant advancements on cybersecurity in the past years. Several countries – including Kenya, Mauritius, Rwanda, Ghana, and Tanzania – have reached "role-model" status according to the ITU's 2024 Global Cybersecurity Index.[16] Nevertheless, the rapid digitalization and numerous new infrastructure projects in Africa increase the exposure to cyber incidents that could severely disrupt essential services and put humanitarian organizations in a vulnerable position.[17]

HARM CAUSED BY DIGITAL THREATS

The harms and impact to humanitarian action are just as varied as the digital threats that cause them. Digital threats pose significant harms to humanitarian organizations, disrupting their vital work and endangering those they aim to assist. Cyberattacks, including denial-of-service attacks, malware, and ransomware, can cripple digital infrastructure and communication systems, hindering assistance delivery and potentially putting lives at risk.[18] Data breaches can expose sensitive information about both staff and aid recipients, violating privacy and leading to targeting, persecution, and identity theft.[19] Disinformation campaigns can erode trust in humanitarian organizations, damaging their reputation and impeding their ability to operate effectively.[20] The spread of misinformation can also directly threaten the safety of humanitarian staff, creating an environment of hostility and increasing the risk of physical harm.[21] Finally, cyber threats present unique challenges to the fundamental humanitarian principles of neutrality, impartiality, and independence. For instance, reliance on digital infrastructure owned by private companies affiliated with specific

humanity-in-today-s-and-future-conflicts-pdf-en.html; NetHope, *2024 State of Humanitarian and Development Cybersecurity Report*, 2024, available at: https://nethope.org/toolkits/2024-state-of-humanitarian-and-development-cybersecurity-report/

[14] OCHA Centre for Humanitarian Data, Guidance Note on The Implications of Cyber Threats for Humanitarians, March 2023, available at: https://centre.humdata.org/guidance-note-on-the-implications-of-cyber-threats-for-humanitarians/https://data.humdata.org/dataset/2048a947-5714-4220-905b-e662cbcd14c8/resource/848a05e7-38e8-4d30-a93a-065b07ac5805/download/guidance-note-on-the-implications-of-cyber-threats-for-humanitarians.pdf?_gl=1*1u07tuq*_ga*MTIzNzE4NzQ5OS4xNzI4Mzk5Mzg5*_ga_E60ZNX2F68*MTczMDIxMzQ3My43LjAuMTczMDIxMzQ3My42MC4wLjA; NetHope, *2024 State of Humanitarian and Development Cybersecurity Report*, 2024, available at: https://nethope.org/toolkits/2024-state-of-humanitarian-and-development-cybersecurity-report/

[15] Global Interagency Security Forum (GISF), *Humanitarian Security in an Age of Uncertainty: the intersection of digital and physical risks*, January 2024, Ch. 3.2.3, available at: https://gisf.ngo/wp-content/uploads/2024/01/Digital-Security-Final-Design-for-Publication.pdf

[16] UN International Telecommunications Union (ITU), *Global Cybersecurity Index 2024,* 5th Edition, 2024, available at: https://www.itu.int/hub/publication/d-hdb-gci-01-2024/

[17] Noëlle van der Waag-Crowling, "Living below the cyber poverty line: strategic challenges for Africa", ICRC Humanitarian Law & Policy Blog, 11 June 202, available at: https://blogs.icrc.org/law-and-policy/2020/06/11/cyber-poverty-line-africa/

[18] OCHA Centre for Humanitarian Data, Guidance Note on The Implications of Cyber Threats for Humanitarians, March 2023, available at: https://centre.humdata.org/guidance-note-on-the-implications-of-cyber-threats-for-humanitarians/; International Committee of the Red Cross (ICRC), *Global Advisory Board on digital threats during conflict*, 9 October 2023, available at: https://www.icrc.org/en/document/global-advisory-board-digital-threats https://www.icrc.org/en/document/global-advisory-board-digital-threats

[19] OCHA Centre for Humanitarian Data, Guidance Note on The Implications of Cyber Threats for Humanitarians, March 2023, available at: https://centre.humdata.org/guidance-note-on-the-implications-of-cyber-threats-for-humanitarians/; Global Interagency Security Forum (GISF), *Humanitarian Security in an Age of Uncertainty: the intersection of digital and physical risks*, January 2024, available at: https://gisf.ngo/wp-content/uploads/2024/01/Digital-Security-Final-Design-for-Publication.pdf

[20] International Committee of the Red Cross (ICRC), *International Humanitarian Law and the Challenges of Contemporary Armed Conflicts*, 2024, available at: https://shop.icrc.org/international-humanitarian-law-and-the-challenges-of-contemporary-armed-conflicts-building-a-culture-of-compliance-for-ihl-to-protect-humanity-in-today-s-and-future-conflicts-pdf-en.html

[21] *Humanitarian Security in an Age of Uncertainty: the intersection of digital and physical risks*, January 2024, available at: https://gisf.ngo/wp-content/uploads/2024/01/Digital-Security-Final-Design-for-Publication.pdf

states or parties to conflict can create (perceived) conflicts of interest and put adherence to the principles of neutrality and independence in question. These digital threats, combined with broader geopolitical developments and the modernization of warfare, create a complex and challenging landscape for humanitarian organizations. Addressing these issues requires a multifaceted approach involving increased investment in cybersecurity, improved digital literacy, and robust data protection measures.

ENHANCING CYBERSECURITY AND DATA PROTECTION IN THE HUMANITARIAN SECTOR

To mitigate the risks posed by cyber threats, humanitarian organizations must prioritize cybersecurity and data protection as integral components of their operations. Several useful frameworks and approaches have been created specifically for humanitarian action. The 2024 third edition of the ICRC Handbook on Data Protection in Humanitarian Action offers specific guidance on interpreting data protection principles in humanitarian context, particularly when new technologies are employed.[22] The 2023 Guidance Note on the implications of cyber threats for humanitarians by the OCHA Centre for Humanitarian Data details various cyber threats and vulnerabilities of humanitarian organizations. The note proposes a four-pronged approach to bolstering cybersecurity for the humanitarian sector, encompassing enhanced funding, institutional preparedness, increased digital literacy among staff, and a culture of collaboration and information exchange between organizations.[23] The 2024 Professional Standards for Protection Work by the ICRC emphasizes a principled approach to using digital technologies in humanitarian work, ensuring that protection work enabled or mediated by digital technologies should ensure the principles of humanity, impartiality and non-discrimination, independence, and neutrality.[24] Finally, the 2024 ICRC Global Advisory Board Report on Digital Threats Against Civilians in Armed Conflict recommends several steps humanitarian organizations should take to increase their cybersecurity posture. The report also emphasizes the need for humanitarian organizations to work together with other organizations as well as states and tech companies to better safeguard themselves from digital threats.[25]

GUIDING QUESTIONS

- How can humanitarian actors better assess and integrate digital threats in their situational awareness and response?
- How can humanitarian actors better protect themselves, the people they serve, and the sensitive data they hold from digital threats?
- How can humanitarian organizations build up higher resilience when faced with digital threats?

ADDITIONAL MATERIAL

- ICRC, 2024, “Challenges Report”, https://www.icrc.org/en/report/2024-icrc-report-ihl-challenges

[22] International Committee of the Red Cross (ICRC), *Handbook on Data Protection in Humanitarian* Action, 3rd Edition, October 2024, available at: https://www.cambridge.org/core/books/handbook-on-data-protection-in-humanitarian-action/025CE3DFD1FAD908DD1412C20E49F955

[23] OCHA Centre for Humanitarian Data, Guidance Note on The Implications of Cyber Threats for Humanitarians, March 2023, available at: https://centre.humdata.org/guidance-note-on-the-implications-of-cyber-threats-for-humanitarians/

[24] International Council of Voluntary Agencies NGO Humanitarian Hub (ICVA), *Professional Standards for Protection Work*, 4th edition, 29 August 2024, available at: https://www.icvanetwork.org/resource/professional-standards-for-protection-work-4th-edition/

[25] International Committee of the Red Cross (ICRC), *Global Advisory Board on digital threats during conflict*, 9 October 2023, available at: https://www.icrc.org/en/document/global-advisory-board-digital-threats

- ICRC, 2024, “Professional Standards for Protection Work 4th Edition”, https://www.icvanetwork.org/resource/professional-standards-for-protection-work-4th-edition/
- Rodenhäuser, Staehelin, and Marelli, 2022, “Safeguarding humanitarian organizations from digital threats”, ICRC Humanitarian Law and Policy Blog
- Gourdain, 2023, “Safeguarding Humanitarian Data and Protecting Humanitarian Organizations from Digital Threats”, RCRC Conference Blog
- GISF, 2024, “Humanitarian Security in an Age of Uncertainty”, https://gisf.ngo/wp-content/uploads/2024/01/Digital-Security-Final-Design-for-Publication.pdf
- Nethope, 2024, “2024 State of Humanitarian and Development Cybersecurity Report” https://nethope.org/toolkits/2024-state-of-humanitarian-and-development-cybersecurity-report/
- OCHA and Centre for Humdata, 2023, “Guidance Note on the Implications of Cyber Threats for Humanitarians”, https://centre.humdata.org/guidance-note-on-the-implications-of-cyber-threats-for-humanitarians/
- OCHA, UN Foundation, 2021, “The Humanitarian Implications of Cyber Threats”, https://reliefweb.int/report/world/humanitarian-implications-cyber-threats
- ICRC, 2023, “Global Advisory Board on digital threats during conflict”, https://www.icrc.org/en/document/global-advisory-board-digital-threats
- ITU, 2024, “Global Cybersecurity Index”, https://www.itu.int/hub/publication/d-hdb-gci-01-2024/