Cybersecurity in the Humanitarian Sector: New Challenges and Solutions

Mouhamed Ali Al Hamoud Al-Arab
Plant protection, Teacher in Orient University
Aleppo University, Syria
Email:*m.aliarab978@gmail.com*

DOI: 10.23918/ICABEP2023p57

Abstract:

Non-governmental organizations (NGOs) provide essential support and services to over 1 billion people worldwide, leveraging technology to carry out their activities and manage sensitive data, leveraging technology to carry out their activities and manage sensitive data. For example, social media, messaging apps, and collaboration platforms help humanitarian organizations to communicate and coordinate with their teams, partners, and beneficiaries in real-time. NGOs use mobile data collection tools and geographic information system (GIS) mapping to gain insights into community needs. Drones and remote monitoring technologies aid humanitarian organisations in responding to crises and disasters, especially in hard-to-reach areas. Digital payment systems increase aid distribution efficiency and stimulate local economies. Unfortunately, cyberattacks and information operations aimed at humanitarian and development NGOs are on the rise, with malicious actors relentlessly attacking NGOs in the cyberspace because of the data they hold. In fact, the non-governmental sector is the second most targeted one after IT. In the last three years, cybercriminals and state-sponsored actors have accessed systems and personal records, stolen millions of dollars in donations, conducted surveillance operations, and carried out disinformation campaigns against NGOs - even large organisations like Save the Children, Mercy Corps, and Roots of Peace. These attacks not only endanger lives, but also compromise the trust that is critical to the work of NGOs.

Keyword: Cybersecurity - Humanitarian organizations - Challenges – Solutions-NGOs-Cybercriminals

Commentary

Humanitarian organizations need to collect and process huge quantities of personal data. While digitalization improves the effectiveness of responses and operations, it also raises concerns about the risk of cyberattacks on sensitive information. Earlier this year, a group of unknown hackers breached the systems of the International Committee of the Red Cross (ICRC) and accessed the personal data of vulnerable populations across the world. This high-profile case is a stark reminder that humanitarian organizations face cyber threats.

The sector needs to assess current approaches and find robust solutions to safeguard digital assets. The sector is now exploring the use of digital emblems – digital markers or signals to identify protected assets in cyberspace – to enhance protection measures in adapting to the new realities of working in the digital space (Chen, Christopher, and Alistair, 2020)

As discussed above, an organization like the ICRC establishes its presence and work on the basis of acceptance and the trust that derives from its neutrality, impartiality, and independence, its exclusively humanitarian objectives, and its confidential approach. In this sense, being able to establish bilateral, confidential dialogue with all stakeholders, irrespective of whether they are state or non-state actors, or whether they are accepted as lawful groups or not, is an essential requirement to carrying out a humanitarian mandate. These are the features that shape the dialogue a humanitarian organization needs to have, fundamental and foundational principles that should extend naturally to activities in the cyber realm (Marelli, 2020).

Challenge

Most humanitarian organizations lack the expertise and technical skills to build a resilient digital infrastructure. The leadership of some of the world's more important organizations are so focused on responding to crises that they overlook the need to conduct risk assessments before their data is the target of a breach. In most humanitarian organizations, there is often little to no funding for cybersecurity (Rishi, 2021)

What Can Be Done?

While cybersecurity practices are very common in the private sector, their adoption is not widespread among humanitarian organizations. To build a sustainable resilient digital infrastructure, the following points should not be overlooked.

- **Risk Assessment:** Understanding the spectrum of potential data breaches is very critical to the security of a system. While building a new application or a system, a threat model should be created where each identified threat is matched with mitigation measures.
- **Security Audit:** Security audits should be conducted at regular intervals. An annual security audit is recommended by an external party not associated with the development team.
- **Build Internal Capacity:** Have at least one information security officer within the organization who can monitor the system and call in the external security provider when needed.

- **Secure Security Funding:** It is important to ensure the financing of security of any project, so make sure to include the security budget in the proposal to the donors. Make a comprehensive presentation to the donors on the potential threats and necessary mitigation measures.

- **Contingency Plan:** It is lifesaving if the organization has a contingency plan ready to go for when an incident or breach occurs. All staff within the organization must know who to contact once they detect a security compromise. The security officer or team must have an outlined plan on what to do with the affected infrastructure and what external organization can be contacted for assistance.

- **Improve Communication with Partners:** All the partner organizations must follow the same security protocols. Clear communication between partners can help flag any potential threat that can then be timely solved.

- **Consistent Data Policy:** A consistent and highly secure data protection policy must be adhered at all stages of the project. (Rishi, 2021)

Cybersecurity in the Humanitarian Sector:

Humanitarian organizations have been increasingly using and storing large quantities of data and communications within their digital infrastructure. This quick transformation of information and communication technology (ICT) in the humanitarian landscape has made it a new potential target for cyber-attacks by criminals, terrorists, and authoritative regimes. (Rishi, 2021)

In recent times, coordinated attacks on humanitarian organizations have raised questions about the preparedness of the aid sector in responding to and mitigating risks in cyberspace. In January 2022, a cybersecurity company hired by the ICRC discovered that a server containing information related to the International Red Cross and Red Crescent Movement's Restoring Family Links service was compromised by an unknown group of hackers. This exposed the personal data and information of over 500,000 vulnerable individuals, many of whom were separated from their families due to armed conflict, disasters, and migration. The exposed data included names, locations, and contact information collected by at least 60 National Red Cross and Red Crescent Societies around the world.

This was by no means a unique and isolated incident. In June 2021, hackers launched a phishing attack on humanitarian and development organisations by mimicking the email account of the US Agency for International Development (USAID). Hackers also infiltrated the computer networks of the United Nations in 2019 and in 2021. The main issue is that cybersecurity remains underfunded

and under-prioritised in the aid sector. While demand increases for data-driven approaches, investment in data protection has not kept pace. Large international NGOs have started to invest in inhouse cybersecurity experts and access to technical know-how; however, many of the smaller organizations have less resources and capacities to secure their data (Chen, Christopher, and Alistair, 2020) Developing a cybersecurity strategy. Once a humanitarian organization carries out an in-depth analysis of its cyber-perimeter, based on its status, mandate, and working modalities, it needs to formulate a clear cybersecurity strategy informing its stance in cyberspace as well as its decisions to prioritize investment areas and allocate resources. Such a strategy should set out: 1) the legal protections it needs to seek out; 2) the technical protection to which it is entitled for its data; and 3) the operational dialogue to employ and the stakeholders with whom it needs to engage (Marelli, 2020).

Digital Emblems: Opportunities and Challenges

Under International Humanitarian Law (IHL), the Red Cross, Red Crescent, and the Red Crystal emblems are used to identify and legally protect personnel, units, establishments, and transports in times of armed conflict. Generally, the emblems aim to protect medical services of the armed forces and civilian hospitals in war time. They are used by the National Red Cross and National Red Crescent Societies, the International Federation, and the ICRC.

Cyber-attacks are now a reality in armed conflict. The ICRC is exploring how the red cross, red crescent, and red crystal emblems can be digitalised and used in the cyber realm to cope with this new dynamic. In practice, digital emblems can be used to mark out protected digital assets – for instance, the personal data files of vulnerable populations found on the ICRC servers – to help avoid erroneous targeting, as well as to signify that they enjoy protection under IHL. While there is definite protective value in the use of digital emblems, challenges remain in implementation and doubts exist regarding their effectiveness. At an ICRC Expert Meeting in 2020, it was highlighted that marking an asset with a digital emblem runs the risk of identifying it as a ‘soft target’ to malicious actors, which ironically makes the asset more easily and systematically targeted.

As IHL is only applicable during times of armed conflict, situating digital emblems under its ambit might not necessarily increase its protective value in times of peace and normalcy. Furthermore, the physical emblems were created specifically to protect medical assets; transferring this protection to non-medical assets is problematic as it requires the restructuring of current humanitarian legal frameworks (Chen, Christopher, and Alistair, 2020). **Tackling Challenges in Cyberspace: Lessons from Singapore**

The use of digital emblems shows how the humanitarian sector is trying to enhance its security by adapting to new threats in the digital space. But, more than such piecemeal initiatives, what is required is system-wide investment and reform, specifically with regard to cybersecurity and resilience. To tackle challenges in the digital space, the aid sector can learn from national governments and the private sector that have demonstrated experience in cybersecurity. The Global Cybersecurity Index 2020 ranks Singapore fourth globally and first in the Asia-Pacific region when it comes to cybersecurity. Singapore's Cybersecurity Strategy 2021 lays out key pillars and enablers to strengthen the security and resilience of the nation's digital infrastructure.

There are a few strategies which can be adopted by the humanitarian sector.

Firstly, humanitarian organizations need to build resilient infrastructure. This will require stakeholders to support investment in cybersecurity.

Secondly, humanitarian organizations need to improve in-house capacity to assess, respond to, and mitigate cyber threats. This requires sustained investment in capacity development to help build up a pool of cybersecurity talent and to ensure that research and ideas translate into new cybersecurity products and services.

Thirdly, the sector needs to enhance cyber cooperation with different sectors to create more relevant and effective legal instruments. The idea of a Digital Geneva Convention has been brewing since 2017. The premise is that the Digital Geneva Convention would commit governments to adopt and implement norms to protect civilians on the internet, without introducing restrictions on online content, in times of peace. It aims to protect the humanitarian system through modified legal frameworks that can cope with existing and future realities that will include digital protection. It also pushes for increased collaboration with technology companies. Just as the Fourth Geneva Convention recognized that civilian protection required the active involvement of the Red Cross, protection against cyberattacks requires the active assistance of technology companies(Chen, Christopher, and Alistair , 2020).

An innovative solution - The Cyber Peace Builders Program:

To help them rise to cyberthreats, the CyberPeace Institute, an independent and neutral nongovernmental organization dedicated to ensuring the rights of people to security, dignity and equity in cyberspace, launched the CyberPeace Builders program in July 2021.

The CyberPeace Builders is a network of corporate cybersecurity volunteers supporting NGOs to enhance their cybersecurity posture. Volunteers interact with NGOs via a job board hosted on a

secure platform operated by the Institute. Jobs are co-defined with NGOs and broken down into hourly units. By design, jobs are neither time-sensitive nor time-consuming. They last between 1 and 4 hours. Volunteers can choose the jobs they want to do based on their skills, availability and interest.

Their diverse backgrounds – some have cybersecurity and IT skills, others have legal, communication or training experience – allow tailoring their responses to the NGOs' needs, with services provided to NGOs including:

Pre-incident: awareness training, security planning, vulnerability scanning, etc.

Post-incident services: attack notification, spyware detection, remediation, etc.

Support: legal advice, data protection, awareness comms, IT investments, etc.

This program has ultimately made it easier for many companies to engage their employees in volunteering activities, and it has even been proven to support retention rates (Francesca, 2023).

Whilst the ever-evolving technological landscape poses new challenges to the humanitarian sector, it also provides unprecedented opportunities to improve the efficiency and efficacy of aid delivery. As highlighted by the Cyberpeace Builders Program, digital solutions paired with expert support and knowledge can enhance crisis preparedness and disaster response. Looking ahead, it will be crucial to strengthen collaborative approaches and partnerships to safeguard humanitarian organisations from cyberattacks and allow them to continue harnessing digital tools and solutions to deliver on their important missions (Francesca, 2023).

Humanitarian organizations need to constantly innovate and invest in new solutions to stay ahead of the curve.

Reference

Chen, Christopher, and Alistair DB Cook. "Humanitarian assistance in the Asia-Pacific during COVID-19." (2020).

Francesca, B. (2023). Senior Advisor-Cyberplaces Institute, *A collaborative approach to reinforce cybersecurity among humanitarian NGOs*. The forum Network. https: 13, 2023, Switzerland

Marelli, M. (2020). Hacking humanitarians: moving towards a humanitarian cybersecurity strategy. *ICRC Humanitarian Law and Policy Blog (16 January 2020), available at:*

https://blogs. icrc. org/law-and-policy/2020/01/16/hackinghumanitarians-cybersecurity-strategy/(accessed 1 March 2021).

Rishi, J. (2021). Communications & Partnerships -Data Friendly Space. *Humanitarian Organizations and Cyber Security Challenges*, https://medium.com/geekculture/humanitarian-organizations-and-cyber-security-challenges-7e581ef99b77, Jul 13, 2021.