RSIS | S. RAJARATNAM SCHOOL OF INTERNATIONAL STUDIES
Nanyang Technological University, Singapore

RSIS COMMENTARY

www.rsis.edu.sg

No. 118 – 18 November 2022

*RSIS Commentary is a platform to provide timely and, where appropriate, policy-relevant commentary and analysis of topical and contemporary issues. The authors' views are their own and do not represent the official position of the S. Rajaratnam School of International Studies (RSIS), NTU. These commentaries may be reproduced with prior permission from RSIS and due credit to the author(s) and RSIS. Please email to Editor RSIS Commentary at RSISPublications@ntu.edu.sg.*

# Cybersecurity in the Humanitarian Sector: New Challenges and Solutions

*By Christopher Chen*

## SYNOPSIS

*On 3 November 2022, the International Committee of the Red Cross released its report, "Digitalising the Red Cross, Red Crescent and Red Crystal Emblems: Benefits, Risks and Possible Solutions." It was in response to cyber intrusions the movement faces. As the humanitarian sector integrates digital technologies into its operations, it faces significant cyber risks. How should the sector navigate this increasingly complex space?*

## COMMENTARY

Humanitarian organisations need to collect and process huge quantities of personal data. While digitalisation 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 organisations 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.

### Cybersecurity in the Humanitarian Sector

In recent times, coordinated attacks on humanitarian organisations 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 in-house cybersecurity experts and access to technical know-how; however, many of the smaller organisations have less resources and capacities to secure their data.

## 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.

**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 organisations need to build resilient infrastructure. This will require stakeholders to support investment in cybersecurity.

Secondly, humanitarian organisations 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.

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

*Christopher Chen was, until recently, an Associate Research Fellow with the Humanitarian Assistance and Disaster Relief (HADR) Programme, Centre for Non-Traditional Security (NTS) Studies at the S. Rajaratnam School of International Studies (RSIS), Nanyang Technological University (NTU), Singapore.*