Compendium of Multistakeholder Perspectives

Protecting the Healthcare Sector from Cyber Harm

About this Compendium

Throughout 2021 and 2022, the Government of the Czech Republic, the CyberPeace Institute, and Microsoft brought healthcare and cybersecurity communities together through the organization of multistakeholder workshops, each one addressing a critical topic related to the protection of healthcare sector from cyber harm. During these workshops, key recommendations, lessons learned, and good practices were collected from a diverse group of experts, practitioners, and stakeholders. Based on what we heard and learned in these discussions, we have developed this Compendium of Multistakeholder Perspectives on Protecting the Healthcare Sector from Cyber Harm that offers healthcare institutions, governments, international organizations, and other stakeholders a useful resource to support their efforts to safeguard the healthcare sector from cyber threats.

The insights and ideas captured in these discussions and reported in this compendium reflect the diverse perspectives and expertise of a broad multistakeholder group, not necessarily the views of any one individual participant or the co-chairs of this project.

Contents

Foreword

Attacks on healthcare are attacks on people. These attacks, whether perpetuated by cyber or kinetic means, are attacks on all of us. They hamper delivery and access to essential services with potentially devastating humanitarian consequences, as demonstrated in the context of the hybrid war in Ukraine. In the past, the healthcare sector has been severely impacted by major cyber incidents such as WannaCry, NotPetya, and countless others. Unfortunately, the volume of cyberattacks affecting the healthcare sector has increased dramatically since the start of the COVID-19 pandemic. Medical staff and healthcare facilities, already under immense pressure due to the enormous medical needs generated by the pandemic, had to also deal with a surge of sophisticated and opportunistic cyberattacks at a time when societies needed the sector the most. In a number of cases this had a direct impact on patients, whose treatments were delayed or postponed.

In our interconnected world, no one is safe until everyone is safe. Recognizing this, the multistakeholder community issued a Call to Governments during the COVID-19 pandemic to put an end to cyberattacks against healthcare. The need to protect this sector has also been highlighted by the United Nations (UN) where states unanimously agreed to increase protection of the healthcare sector from cyber harm by implementing norms of responsible state behavior in cyberspace. However, the global interdependence of the healthcare sector requires a decisive multistakeholder action, spanning diplomatic, operational, policy, and capacity-building initiatives, as well as ensuring accountability for perpetrators of cyberattacks.

Responding to this global Call for action, the Government of the Czech Republic, the CyberPeace Institute, and Microsoft partnered together to identify critical gaps that need to be addressed to protect the healthcare sector from cyber harm. Our organizations are committed to increasing the cyber resilience of the healthcare sector through a multistakeholder approach, whether at the practitioner, technology industry, or state and international levels. Our partnership reflects our shared commitment to advance the implementation of UN cyber norms through concrete action as well as our belief that a multistakeholder approach to protect the healthcare sector is the only way to meaningfully increase its resilience.

Through a series of thematic workshops, our project brought together healthcare practitioners, cybersecurity, policy, international law, and regulatory experts to identify lessons learned and good practices to protect this vital sector. Importantly, we recognized the differences and disparities in the healthcare systems around the world and the rich body of knowledge and expertise that already exists on this subject. As such, we did not reinvent the wheel but endeavored to build and expand on existing efforts. Key observations, proposals and good practices were developed as a concrete outcome of these workshops and formulated into a set of recommendations in this Compendium to support the global community engaged in the protection of the healthcare sector.

We believe that the recommendations contained in this *Compendium of Multistakeholder Perspectives: Protecting the Healthcare Sector from Cyber Harm* can inform discussions from the ambulance dispatch room to the UN General Assembly Hall. We also hope that this Compendium can inspire and strengthen a culture of cybersecurity and resilience in the healthcare sector, thereby protecting an area of vital importance for us all.

Ministry of Foreign Affairs of the Czech Republic

Jan Lipavský
Minister of Foreign Affairs
of the Czech Republic

Microsoft

Brad Smith
President and Vice Chair,
Microsoft Corporation

NÚKIB

Lukáš Kintr
Director of National Cyber and
Information Security Agency
of the Czech Republic

CyberPeace Institute

Stéphane Duguin
CEO,
CyberPeace Institute

Thematic Workshop 1
IT Practitioners Perspective

The importance of protecting the healthcare sector from cyberattacks is not and cannot be questioned. However, the steps needed to achieve this goal remain unclear whereas globally, the number of cyberattacks against medical facilities is rising. The COVID-19 pandemic put the healthcare sector under considerable strain due to a sharp rise in the need for urgent patient care, but also from the unprecedented increase in the number of cyber threats it faced.

The work of healthcare professionals is directly impacted by legal, technical, and political decisions, as well as high-level diplomatic discussions. Yet, when it comes to healthcare delivery, cybersecurity policy decisions, and normative protections of the sector, many of these discussions lack a general understanding of what the sector needs to address specific challenges and to increase its resilience against cyberattacks.

During the first thematic workshop, cybersecurity practitioners identified several key issues that need to be addressed. The importance of changes in the management culture of healthcare facilities was cited multiple times. For example, disagreements may arise between medical staff and the information technology (IT) experts supporting them, because the challenges they face in their respective roles are not mutually shared and may lead to competing priorities. This means the processes designed to increase cybersecurity are often perceived as obstructions, slowing down medical care delivery to patients. Other discrepancies appear between IT professionals and hospital management.

Oftentimes, cybersecurity (and IT in a broader sense) is considered as a secondary technical supportive function to medical care, mostly because the hospitals' top management consists of doctors with a limited understanding of the criticality of cybersecurity for the provision of care. Moreover, training lags behind the pace of developments in the field of Information and Communication Technology (ICT) and the overall dependence on ICTs. These are some of the reasons why cybersecurity measures are viewed as additional costs competing with the provision of care, rather than as an enabler of care. Also, funding – both for attracting and retaining IT and cybersecurity experts as well as for implementing specific solutions – often does not meet the needs of the sector. A shift in this mentality is key to ensure that all stakeholders, including the leadership within healthcare organizations, will take cybersecurity into careful consideration.

At the strategic level, the international community can advance the protections afforded to the sector by implementing and progressing the current UN normative framework for responsible state behavior in cyberspace, take concrete actions to operationalize national cybersecurity frameworks in the healthcare sector, and promote multistakeholder engagement at all levels to secure the sector.

Good practices, lessons learned, and recommendations identified by participants included:

- **Recognize cybersecurity as a priority at the leadership level** of hospitals. Resources are often allocated in a manner that prioritizes the provision of healthcare over cybersecurity measures. That might make sense at first glance but given the increasing reliance on technology in medical care today, it can be counterproductive as it may introduce vulnerabilities into the care system. For example, ransomware attacks could render medical devices useless, which could have a direct impact on the ability to provide care to patients.

- **Spread awareness about cybersecurity measures** at all organizational levels and hierarchies. Participants highlighted that the healthcare sector tends to be quite hierarchical, with the top management consisting predominantly of medical professionals, who tend to underestimate cybersecurity risks and rather prioritize other investments, such as the acquisition of new medical devices. An open culture needs to be encouraged and cultivated so that all staff, including IT professionals, feel empowered to speak up and communicate their cybersecurity concerns to management.

- It is essential that everyone involved in healthcare delivery sees **cybersecurity as an enabler and a continuous process, rather than as an obstacle and a compliance 'check-box' exercise.** One way to foster this view is for medical professionals and other staff to participate in cybersecurity related exercises, where they can experience (in a simulated environment) the impacts of a cyberattack on patients and their care.

- **Improve recruitment and retention of cybersecurity personnel** in healthcare facilities. There is currently a shortage of qualified IT experts in the sector, which weakens its cybersecurity capabilities and may result in rendering even existing security systems ineffective. One of the reasons is the disproportionately lower level of salaries for the IT professionals in contrast to other sectors. Considering the critical importance of delivering medical care, adequate remuneration should be the norm, not the exception.

- Enhance understanding between medical staff and IT experts on the sensitive and critical nature of **patient data** that is used in their work, ensuring that all data is **handled appropriately.** All staff must comply with legal regulations and IT restrictions regarding data use and processing and should cooperate with IT personnel to ensure it is sufficiently protected.

- **Procurement guidelines and cybersecurity measures for connected medical devices need to be put in place,** as the number of these devices used in healthcare facilities has increased dramatically in recent years. Connected medical devices, are usually insufficiently secured, and add a new vector of compromise to the sector. Considering the vast number of such devices in medical facilities and often inadequate personal capacities in their IT departments, innovative methods should be considered, such as solutions using machine learning.

- **Manufacturers should ensure frequent patching cycles of medical devices.** Currently, patches are often rare or even non-existent, which means medical devices do not benefit from new cybersecurity protective measures leaving these devices vulnerable to attacks. Available patches should be regularly and systematically implemented in medical facilities.

- **Understand the long and cascading supply chain in the sector which requires protection,** as was the case with the COVID-19 vaccine supply chain. From research and development to manufacturing and delivery, the supply chain consists of many entities (many of whom are small organizations), all of which need to implement adequate protections. The whole chain is only ever as secure as its weakest link.

- **Ensure the discussions about cybersecurity in healthcare are concrete and actionable.** For example, there are various debates at the international level that include the protection of the healthcare sector. Practitioners generally find these too abstract and often lacking in practical answers. One way of providing concrete guidance is **through a multistakeholder approach.** This means to include all relevant actors, such as relevant state officials, first responders, private sector representatives, and civil society organizations, in the discussion both at national and international levels to identify and address the gaps in the protection of the healthcare sector. These findings should be widely accessible to the public.

Recommended reading & resources shared by participants:

The Lancet and Financial Times Commission on governing health futures 2030: growing up in a digital world, Oct 2021; https://www.thelancet.com/commissions/governing-health-futures-2030

Hospital ransomware attack led to infant's death, lawsuit alleges, Healthcare IT News, Oct 2021; https://www.healthcareitnews.com/news/hospital-ransomware-attack-led-infants-death-lawsuit-alleges

Fears of hackers targeting hospitals, medical devices, ABC News, June 2017; https://www.youtube.com/watch?v=pU3NQ3GkC_0

Procurement Guidelines for Cybersecurity in Hospitals, European Union Agency for Cybersecurity (ENISA), Feb 2020; https://www.enisa.europa.eu/publications/good-practices-for-the-security-of-healthcare-services

Cloud Security for Healthcare Services, European Union Agency for Cybersecurity (ENISA), Jan 2021; https://www.enisa.europa.eu/publications/cloud-security-for-healthcare-services

'Provide Medical Care' is in Critical Condition: Analysis and Stakeholder Decision Support to Minimize Further Harm, Cybersecurity & Infrastructure Security Agency (CISA), July 2021; https://www.cisa.gov/publication/provide-medical-care-critical-condition-analysis-and-stakeholder-decision-support

Cybersecurity Perspectives: Healthcare and Public Health Response to COVID-19, Cybersecurity & Infrastructure Security Agency (CISA), January 2021; www.cisa.gov/sites/default/files/publications/CISA_01132021_HPH_Factsheet_508.pdf

The Second Oxford Statement on International Law Protections of the Healthcare Sector During Covid-19: Safeguarding Vaccine Research; The Second Oxford Statement - Oxford Institute for Ethics, Law and Armed Conflict

What happens in hospitals that have been hacked?

Rigorous evidence shows that connected medical devices and clinical systems save lives. Cyberattacks can, however, render those systems useless or actively work against clinical staff. What does a healthcare cyberattack look like from the inside?

At the CyberMed Summit,[1] physicians, hospital administrators, and cybersecurity researchers collaborated to create unique high-fidelity clinical simulations that reveal cybersecurity impacts on patient care. In these simulations, clinicians struggled to deal with devices that were unusable or actively working against them. These single patient encounters have been repeated hundreds of times in actual cybersecurity incidents.

First-of-its-kind analysis by the Cybersecurity and Infrastructure Security Agency (CISA) in 2021 confirmed that cyberattacks against healthcare providers or networks cause a statistically significant increase in mortality rates. Further, diverting patients to other facilities can trigger wider cascades of increased mortality rates at other providers if caseloads across the area are elevated.

At the same time, significant financial impacts can occur since billing workflows and systems can be disrupted. In the immediate term, cashflow shortages may result in reduced staffing or supplies, further degrading care delivery. In the longer term, the financial loss may drive some of the providers out of business, particularly among non-profit hospitals.

Beau Woods
Senior Advisor and Strategist
Cybersecurity and Infrastructure Security Agency

1 The CyberMed Summit is focused on protecting patients by ensuring medical devices and healthcare infrastructure are as safe and secure as possible. More here: www.cybermedsummit.org/homepage

Cybersecurity must be at the heart of healthcare provision

After years of cyberattacks disrupting critical health services and applying additional pressure to already stretched healthcare resources, it is clear that the healthcare sector must take steps to adopt better defenses.

This is hugely challenging when every dollar spent on cybersecurity is viewed as one not spent on patient care. We must translate cybersecurity dynamics to clinical environments, so security is no longer seen as an obstacle or check box exercise, but rather as an enabler to support continued patient care. Better security means more reliable availability of life-saving technology, and more integrity and confidentiality for patient data. Healthcare professionals must be part of the discussion so we can understand and respond to the specific dynamics that make healthcare unique and at risk. Working collaboratively creates more opportunities to build tailored solutions that support the unique needs of the health sector and helps to drive buy-in with healthcare professionals. Change will not come quickly though given the immense pressures and demands on healthcare.

Jen Ellis
Vice president of community and public affairs
Rapid7

Device security considerations in healthcare organizations

The healthcare sector is increasingly investing in connected medical devices, such as connected infusion pumps, x-ray machines, and MRI machines to improve patient care. Gartner Research predicts there will be over 1.3 billion connected medical devices in healthcare delivery organizations by 2030.[2]

The adoption of these devices, as well as Internet of Things devices generally, inadvertently expands the attack surface and introduces new management and security challenges to hospitals. These connected devices often lack built-in security controls, run unsupported operating systems, are difficult to patch, and lack encryption. Because the architecture of these devices differs from traditional IT, traditional security approaches such as endpoint protection do not work. The diversity of connected devices in healthcare organizations also makes them hard to secure. Devices are often connected to a network by medical staff, meaning they are unknown to the IT department. Finally, already-deployed legacy devices cannot be retroactively designed for security, posing a significant threat. In short, medical devices are a weak link in patient data protection and hospital continuity and can have a huge impact on patient safety.

Connected devices, like other IoT devices, are susceptible to cyberattacks including password and port attacks, worms, malware, botnets, and ransomware. Cyber criminals target these devices and use them as attack vectors to infiltrate hospital networks and sensitive patient data. Devices can be configured to send traffic to known bad destinations such as command and control (C2) servers or spread malware on a network. In 2020, Palo Alto Networks' review of the rapidly increasing use of IoT devices in healthcare found that over 98% of all IoT traffic was unencrypted; 51% of threats for healthcare organizations involve imaging devices, disrupting care, and allowing attackers to exfiltrate patient data; and 72% of healthcare networks mix IoT and IT, allowing malware to spread from computers to IoT devices[3]. Research in 2022 found that 75% of internet-connected infusion pumps had known security issues.[4]

For these reasons, when thinking of cybersecurity, healthcare organizations should also consider their growing number of connected devices. One way to manage related risks can be leveraging networks as a priority detection and enforcement point to prevent cyberattacks. Network-level IoT security at scale that leverages machine-learning (ML), automation, and the cloud can detect and stop anomalous behavior by devices regardless of the type of device or end-use. Solutions based on ML models bring an extensive, data-driven understanding of an IoT device's expected behavior, enabling ML to easily learn patterns in real time, ultimately to automate device identification at scale, proactively detect malicious deviations, and automatically prevent attacks. Last, but not least, letting the automated solutions do their work would unburden under-staffed and often overwhelmed IT specialists in the healthcare sector.

Dr. May Wang
Chief Technology Officer for IoT Security
Palo Alto Networks

2 Machina Research Forecast Database, https://machinaresearch.com/what-we-do/about-the-forecast-database

3 2020 Unit 42 IoT Threat Report, Palo Alto Networks, https://unit42.paloaltonetworks.com/iot-threat-report-2020

4 Know Your Infusion Pump Vulnerabilities and Secure Your Healthcare Organisation, Palo Alto Networks, https://unit42.paloaltonetworks.com/infusion-pump-vulnerabilities

Thematic Workshop 2
How do cybersecurity measures impact frontline healthcare practitioners?

One of the most worrying trends of recent years has been an exponential increase in cyberattacks targeting healthcare organizations. These have included, inter alia, attacks targeting Brno University Hospital in the Czech Republic,[5] Paris' hospital system,[6] the computer systems of Spain's hospitals,[7] Ireland's healthcare system,[8] and hospitals in Thailand[9] to name just a few.

While these attacks have rightly received a fair amount of attention in the press, the focus tends to be on "whodunnit" and the costs associated with the attacks. What often gets lost or unreported is the impact on patients, and on frontline healthcare practitioners. Modern hospitals are connected and increasingly rely on technology to provide care. This may make the practitioners' job easier, but it also means that they need to be ready and able to act even when their ability to do so is impacted by a cyberattack.

This also means that healthcare practitioners, such as doctors and nurses, must increasingly act as cybersecurity defenders. Hospital data has been an attractive target for malicious actors for some time, and the rise of ransomware has made medical facilities an even more attractive target. These facilities provide critical care where a continued ability to provide service must be assured. Practitioners need to learn how to leverage technology for better health outcomes, and to understand that cybersecurity is a vital part of that equation. As a result, they must be trained in cybersecurity good practices. Healthcare organizations must continuously test their readiness, leveraging simulations and exercises, and even test their resilience by using ethical hackers.

Good practices, lessons learned, and recommendations identified by participants included:

- **Cybersecurity must be viewed as an integral part of the delivery of patients' healthcare.** Traditionally, while IT teams emphasized cybersecurity, healthcare practitioners and the management of healthcare institutions tended to focus on patients' health. Such a strict divide is no longer tenable. On the contrary, investments into both medical care and cybersecurity need to be seen as mutually reinforcing, rather than as tradeoffs. The procurement of medical services that rely on technology needs to have cybersecurity at its heart, rather than be seen as an additional strain on stretched resources.

- Healthcare practitioners should **accept that healthcare institutions have become increasingly attractive targets for malicious actors.** They do not yet. Across the globe, many healthcare practitioners still believe that they will not be targeted by malicious actors. They harbor this misconception because a) they believe they are "doing good" and that therefore no one will be malevolent enough to attack them; and b) they do not see themselves as attractive targets, as they do not handle large amounts of money. This needs to change. Healthcare practitioners and management must realize that they are vulnerable to cyberattacks – and, importantly, that **cybersecurity can directly and significantly affect patient health.** Providing care is also about processing information. As such, if malware disables a vital computer system, this could potentially be just as dangerous to a patient's health as a biological virus.

5 Czech Republic's second-biggest hospital is hit by cyberattack, Cyber Scoop, www.cyberscoop.com/czech-hospital-cyberattack-coronavirus

6 Hackers steal Covid test data of 1.4 million people from Paris hospital system, Radio France International, www.rfi.fr/en/france/20210916-hackers-steal-covid-test-data-of-1-4-million-people-from-paris-hospital-system

7 Cyber-attack Threatens Spanish Hospital Computer Systems, Murcia Today, www.murciatoday.com/cyber_attack_threatens_spanish_hospital_computer_systems_1367723-a.html

8 Irish Hospitals Hit by Cyberattacks, Forcing an I.T. Shutdown, The New York Times, www.nytimes.com/2021/05/20/technology/ransomware-attack-ireland-hospitals.html

9 Thai hospitals and companies hit by ransomware attacks, Reuters, www.reuters.com/article/us-thailand-hospital-ransomware-idUSKBN2611WV

- Healthcare practitioners – including management – must be **trained in cybersecurity good practices,** including the fundamentals of cybersecurity hygiene, such as two-factor authentication. Training should be a regular, systematic, and continuous. Additionally, it should be conducted not solely through presentations, but also through immersive techniques such as simulations and prepardeness testing like ethical hacking/phishing.

    - Relatedly, it is important to realize that healthcare practitioners (and management) may not have the time to implement overly time-consuming cybersecurity measures. It is therefore important to develop "frictionless" cybersecurity practices where possible and appropriate. They should be easy to implement, including by relying on automation and security-by-design as much as feasible.

- Across the board, there is a need for all stakeholders to **improve their communication skills when communicating with representatives from other stakeholder groups.** This applies to medical professionals communicating with IT professionals and vice versa. It is essential, in order to reduce and, ideally, over time eliminate, the divide between the above mentioned "IT way of thinking" versus the "medical/management way of thinking". As such, participants called for skilling and training initiatives that could help build these capacities. They also recognized that such initiatives could not be one-off/ad-hoc events but would have to be part of a continuous and systematic training program.

- Healthcare entities should **incorporate resilience measures into their crisis planning** so that their overall systems keep working even when parts of the system fail. This should ensure access to critical data even if a network or parts thereof go down due to a cybersecurity incident.

- Healthcare organizations should **test their users' and infrastructure's cybersecurity readiness** by conducting exercises, phishing and ethical hacking. Notably, many healthcare institutions are building simulation centers for medical education. Participants strongly recommended **incorporating cybersecurity simulations into medical simulation centers.**

- Healthcare entities should **proactively reach out to and partner with the technology sector** to continuously improve their systems. This could include developing and implementing systems, including by **leveraging artificial intelligence that proactively monitors the threat landscape,** learns from patterns, and detects and provides early warnings about potential threats.

- Finally, practitioners must also **realize the importance of information-sharing across stakeholder groups** and organizations. Specifically, There should be a systematic sharing of cybersecurity best practices and, separately, health-related data, e.g., good practices on how to protect oneself from COVID-19. However, there was disagreement on whether a centralized or a decentralized option was best. A central organization, for example a universal healthcare information system for a given country, could help facilitate health-related data. Such centralization has several advantages over decentralization. For example, it is less complex, less expensive, reduces the points of vulnerability for the data being shared, and does not create interoperability concerns. However, centralization also has disadvantages. For example, using a central organization could reduce resilience – i.e., it could mean that if that one organization fails, the entire system of information-sharing fails. There is no easy answer to the choice between centralization and decentralization; the pros and cons must be carefully considered.

Recommended reading & resources shared by participants:

Good practices for the security of healthcare services (ENISA); https://www.enisa.europa.eu/topics/critical-information-infrastructures-and-services/health/good-practices-for-the-security-of-healthcare-services#/

Toolkits and Best Practices: Protecting Yourself is Protecting Others, The CyberPeace Institute, June 2021; https://cyberpeaceinstitute.org/news/toolkits-and-best-practices-protecting-yourself-is-protecting-others/.

Navigating cybersecurity: Guidance for (I)CSO professionals, The CyberPeace Institute, May 2022; https://cyberpeaceinstitute.org/news/navigating-cybersecurity-guidance-for-icso-professionals/.

Data is key in healthcare

Data is the new oil, and information is care. Care is enhanced by quality information and by the ability to share it meaningfully amongst the stakeholders in the healthcare and public health systems.

Beyond the implications for privacy of sensitive personal data, the conundrum, in the era of cybercrime, is to walk the fine line between enabling controlled cooperation of legitimate users to improve the quality, safety and efficiency of care, while minimizing the risk of exposing sensitive data to attacks by criminals. This requires a continuous investment by hospitals in IT security, including education of professionals as well as citizens on cybersecurity issues and practices.

Prof. Antoine Geissbuhler
MD, head of eHealth and telemedicine
Geneva University Hospitals

Divide the budget and master the training

Cybersecurity is often underestimated and neglected within the healthcare sector - until something serious happens. Experiencing a cyberattack always changes the views and approaches of those, who have had to face it. Unfortunately, that is often too late. What is the reason for this and how can we prevent it? How can we change the practitioners' minds before it is too late? These are the "one-million dollar" questions, but there are a few solutions available.

In many countries cybersecurity is paid from a health insurance budget, including in the Czech Republic. As a result, this ultimately means that it competes with the money for healthcare itself. No doctor or nurse will prioritize spending money on IT instead of improving patient care. To resolve this issue, cybersecurity should be funded from the "general" budget and not from the healthcare related funds.

Secondly, doctors and nurses are overloaded. They fight day and night for the health and life of their patients. Cybersecurity is seen as an additional burden. Instead, we need to ensure that healthcare professionals understand that a computer virus can be just as harmful to their patients as the biological virus or cancer. Healthcare professionals learn all their lives and the optimal way for medical training is experience. You always learn more, if you "live it", than if you "read it". The same might be true for cybersecurity. Furthermore, doctors and nurses are used to following guidelines. This could apply also to cybersecurity – instructions should be easy and straightforward though.

Our goal should be to minimize the perceived difference between a patients' health and cyber health. Both can jeopardize their lives. If we can motivate healthcare professionals this way, they will get on board and will do their best in both of these tasks, because they will do it for the good of their patients. And this is what they promised when taking the Hippocratic oath!

Jan Blatný
MD, PhD, Associate professor of pediatrics, medical director for pediatrics and consultant haematologist
University Hospital Brno

Médecins Sans Frontières:

Cyberattacks, regardless of the target or magnitude, can compromise relief to the populations that Médecins Sans Frontières (MSF) serves. Enforcement of appropriate data policies (including collection, use, storage, and disclosure) is further challenged by operations in difficult social environments and the inherently sensitive nature of humanitarian interventions.

A representative example of the high risk of human cost of cyberattacks is a small network of 20 laptops containing beneficiary information for food distribution in Niger during the food crisis of 2010. Had there been any kind of cyberattack or incident, 55,000 households would have been affected. MSF is also employing new technologies to support its work in the field. For example, the organization is increasing the use of connected devices both for population surveys and for medical data in our health centers. The vulnerabilities that the use of technology and ICTs introduces into the work of field teams with limited knowledge of cybersecurity best practices is a concern for them.

Franck Ale
Head of Epidemiology
Operational Directorate of MSF-West and Central Africa (WaCA)

Education, awareness, and capacity building are key to increasing awareness of the threat and the potential impact of cyber threats on our operations. In our assessment, awareness of basic cyber hygiene best practices and a resilience-driven mindset are key elements to respond to the growing threat.

Sonia Karkare
Director of Digital Transformation
MSF-WaCA

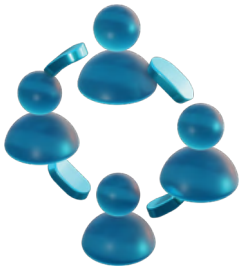
One of the key challenges for our IT teams is to ensure that systems are updated. Even such a simple cyber hygiene step can be challenging in an environment where MSF operates. The issue of personal data, especially the sensitivities of medical data and localization requirements requires training and constant review of data handling and security practices.

Tanguy Balima
Head of IT
MSF-WaCA

In our work respect for local norms, laws, standards, medical ethics and the need to meet the patient expectations have to be taken into consideration when deploying, using, and securing technology and data.

Douglas Nderitu
Data Protection Officer
MSF-WaCA

Thematic Workshop 3
Strengthening Resilience & Lessons Learned



Cyberattacks have quickly become a part of everyday life. Whether it is yet another story of an attack against a hospital in the news, or someone you know falling victim to a ransomware attack, one thing is clear: the number of cyberattacks is on the rise. As a result, increased cyber resilience is needed and should be recognized as a shared responsibility among stakeholders. From medical device manufacturers to governments participating in international discussions, every actor has a role to play in increasing cyber resilience of the healthcare sector.

The resilience of the sector can be improved by implementing good practices and lessons learned from previous attacks. One example of how these lessons could be learned, is through the PricewaterhouseCoopers' review of the "Conti cyberattack on the HSE",[10] a ransomware attack that infiltrated the Irish Health Service Executive (HSE) in 2021.

Strengthening cyber resilience of the healthcare sector is a monumental and continuous effort which requires sustainable changes and cultural shifts within the sector itself. As highlighted multiple times by various experts throughout this project, cybersecurity needs to be seen as something that enables the work of hospitals and care facilities, rather than a hindrance to their ability to deliver care. A shift in approach this significant requires consistent and relatable engagement on all levels within the healthcare sector, including medical staff, IT personnel, and government representatives. Communication and information sharing between and among these actors is essential to ensure that patient safety is not jeopardized because of cyber threats and that action can be taken before threats occur, rather than after a terrible event has taken place.

Good practices, lessons learned, and recommendations identified by participants included:

- There needs to be a **profound change of mindset** away from a compliance "box-ticking" to a continuous process aimed at raising resilience and preventing cyberattacks. Other recommended areas for improvement include:
    - Prioritization of cybersecurity spending by realizing that it is consistent with, and in fact supports, a patient-centric approach to healthcare.
    - Implementation of horizontal, not hierarchical, approaches to IT security teams within organizations. Otherwise, the layers of bureaucracy can become a problem when there is a need to escalate issues.
    - Integration of clear reporting structures that empower employees to highlight cybersecurity risks within their organization.
    - Promotion of the significance of cybersecurity across all levels of an organization.
    - Creation and implementation of training programs to improve cyber resilience.
- Protection of critical infrastructure requires a **joint effort from all relevant stakeholders.** Governments can help to prepare and execute training exercises in healthcare facilities (regardless of their ownership), and government and industry executives can substantively engage within the framework of public-private partnerships. Together, these efforts can help to assess the cybersecurity readiness of organizations.

10 Conti cyber attack on the HSE, Independent Post Incident Review, PwC, www.hse.ie/eng/services/publications/conti-cyber-attack-on-the-hse-full-report.pdf

- To strengthen the resilience of the healthcare sector, **collaboration** within and across organizations is key. This can be done through **communication and information-sharing** with other organizations – like the national cybersecurity authority – via systems that maintain an updated list of contacts for cybersecurity incidents. Communication also helps personnel to comprehensively understand the threat landscape in cyberspace.

- A **human-centric approach**, an integrated approach to cybersecurity that takes into consideration all the ways in which cyberspace impacts human life and conditions, **needs to be adopted** to ensure that the healthcare sector's ICT products and services are secured. This approach helps to make sure that the perspective of end-users is maintained throughout the security process so that they can be confident in the integrity, availability, and confidentiality of their own data. A human-centric approach also helps to empower end-users to take control of cybersecurity aspects that have a direct impact on lives.

- The interconnected nature of healthcare systems requires a **holistic approach to cybersecurity,** and so fragmentation within organizations needs to be reduced. Failure in any one part of the system can harm patients. It should be clear who is responsible for the management of which technology platform within organizations, and platforms should be regularly patched.

- **Legal and regulatory initiatives need to cover all relevant healthcare facilities.** This can be achieved by focusing on flexible criteria such as the unique types of care offered at particular facilities, rather than on quantitative criteria such as the number of beds a facility has.

- To help ensure the effectiveness of cybersecurity laws and policies, it is important to **provide policymakers with data regarding the effects of cybersecurity incidents** in a way that resonates with them.

- **Information** regarding cybersecurity incidents should be thoughtfully communicated to the public. This is important to maintain the public's confidence in the healthcare system, and their overall trust in technology.

Recommended reading & resources shared by participants:

Playing with Lives: Cyberattacks on Healthcare are Attacks on People, The CyberPeace Institute, March 2021, https://cyberpeaceinstitute.org/report/teaser/index.html

Addendum to the Strategic Analysis Report "Playing with Lives: Cyberattacks on Healthcare are Attacks on People," The CyberPeace Institute, October 2021, https://cyberpeaceinstitute.org/wp-content/uploads/Addendum-CITHEALTH.pdf

Cyber Incident Tracer, The CyberPeace Institute, https://cit.cyberpeaceinstitute.org/

The importance of cyber resilience

Cyberattacks on healthcare are increasing. In fact, healthcare today is one of the top industries being attacked. The top five threats against this sector represent ransomware deployments, spear-phishing, third-party breaches, data breaches and insider threats.

Cyber resiliency shows the preparedness of an organization to prevent cyber harm or to react to a cyber incident in a way that minimizes business impact and involves a number of different elements:

- Improving cyber resiliency should be the joint goal of a company's leadership. Safety, availability, and integrity of company data is in the interest of every executive. Clear communication about this joint goal and need for collaboration amongst all parts of the organization is vital for resiliency building success.
- One of the key components of resiliency is to ensure IT platforms are designed securely and kept up to date with patches. The majority of cyber threats are still based on older vulnerabilities. This goes hand in hand with efficacy and efficiency in terms of how to collect and store information about organizations' assets, ensuring security controls are in place and special due diligence for critical company assets.
- Resiliency also means assuming bad things will happen. Organizing tabletop exercises and adverse event simulations provides an excellent base for finding the gaps in the security architecture, security controls, processes, procedures, and awareness. Security processes and controls should be designed in a way to minimize impact on business and infrastructure should an incident occur.
- Ensuring company resiliency is also about resiliency of the company's supply chain, security language in the contracts, and bilateral collaboration on ensuring key processes in the supply chain are secure. Moreover, it is important to regularly check whether all these provisions are up to date, and to revise them regularly.
- To be able to effectively protect the company and industry we need to collaborate. Timely information sharing in the community, between industry peers, but also between the public and private sector is key.

Eva Telecka
Director, IT risk management and security
EMEA, MSD

Thematic Workshop 4
Capacity Building & Scenario-Based Resilience Planning

Capacity building is an essential part of improving the cyber resilience of individuals and organizations and is therefore key to managing threats.It is also a resource-intensive undertaking, which is hard to prioritize in an often under-resourced and overburdened healthcare sector.

To overcome these challenges, healthcare entities can learn from other fields with more experience in capacity building, such as development initiatives or the financial sector. They already offer skills training and resources to people around the world. The healthcare sector can leverage their knowledge and experience to build a contextualized approach that best addresses the needs in the healthcare sector. These needs could include good practices for protecting patient data or training programs specialized in securing medical devices.

A range of organizations and resources already exist and could support healthcare entities with cybersecurity capacity building efforts. Some examples include cybersecurity exercises led by national agencies, such as the National Cyber and Information Security Agency of the Czech Republic (NÚKIB),[11] which has created exercises tailored specifically to the needs and particularities of hospitals. Another example would be the CyberPeace Institute, a non-governmental organization running the CyberPeace Builders program[12] which provides cybersecurity assistance to humanitarian and healthcare organizations.

One thing is clear from these examples: a multistakeholder, whole-of-society approach is integral to strengthening the resilience of the healthcare sector. This workshop illustrated that positive will exists within the healthcare organizations to work on capacity building and scenario-based resilience planning initiatives. This represents an important step towards better protection of the healthcare sector from cyber harm.

Good practices, lessons learned, and recommendations identified by participants included:

- **Cybersecurity exercises help build capacity** and increase cyber resilience of an organization. Not only do they help to create and strengthen cybersecurity awareness, but they help to build the skills and muscle memory needed to effectively respond to cyberattacks. For ease of data collection and analysis, it is recommended that exercises focus on a particular issue, such as ransomware.
    - These exercises can be in the form of **tabletop or strategic decision-making exercises** and involve employees holding different roles across the organization. Primarily, these exercises should be designed for hospital management and a mix of both IT and non-IT staff. They are also an opportunity to test out the application of measures in real-time.
    - To facilitate trust building, the **exercises should ensure all participants feel that "there are no wrong answers"** and enable the free exchange of ideas and to learn from each other's practices and mistakes.

11 National Cyber and Information Security Agency of the Czech Republic (NUKIB), www.nukib.cz/en/

12 CyberPeace Builders, www.cyberpeaceinstitute.org/cyberpeacebuilders/

- It is important to **measure the success of cybersecurity exercises,** although this can be a challenge. Some potential indicators of success include interest from relevant stakeholders to participate in the exercise, and the prompting of a discussion outside the exercise, such as follow up conversations between participants on capacity-building and resilience measures.
- Focusing on the **purpose and spirit** of the exercise rather than on the technical details can also help address this issue.

- **Decision makers need better access to healthcare-specific threats and incident data** to help foster a better understanding of the cybersecurity capacity needs of today's healthcare sector. However, this increased access to data should not come at the cost of patient privacy; data protection and patient privacy should always be safeguarded.

- **Capacity building should use a whole-of-society approach** that brings together, as appropriate, stakeholders from government, the private sector, and civil society. This approach requires significant trust between the various stakeholders, and a clear demonstration from all sides that interests are aligned. It takes time to build trust between different actors and this therefore needs to be a continuous effort rather than a one-off attempt.

- **Capacity building should be discussed in regional and global forums.** These forums can include the World Health Organization (WHO), the World Bank, the UN more broadly, the Global Forum on Cyber Expertise (GFCE)[13] and the Global Fund,[14] among others. Discussions at this level can help facilitate information sharing across the globe and can also help to build each country's capacity and strengthen their resilience. These discussions can cover a range of issues from how to implement cybersecurity legislation, to cybersecurity good practices more broadly, and the nature of threats.

- Stakeholders in the healthcare sector should draw inspiration from other sectors, such as the banking sector, where investments in resilience have been growing significantly over the past years. However, **investing financial resources into cybersecurity is not enough; it is important to also invest in skills** development and recruitment of cybersecurity personnel. There is currently a high demand for, and low supply of, skilled workforce in the cybersecurity sector.

- Any **capacity-building effort must be tailored to the particular context** and capabilities of the institution at which the effort is targeted. This is based on the experiences of practitioners who have found that contexts and capabilities often vary widely in the healthcare sector including, for example, in the processes and awareness levels of hospital staff across different hospitals. One way to ensure that the capacity building effort is contextualized is to include input from individuals working in the sectors, regions and institutions where the exercises and scenarios are meant to take place.

- **Capacity-building and resilience measures need to be regularly adapted,** based on how the threat landscape is evolving. For example, a sudden surge of ransomware attacks represents new challenges for organizations in the healthcare sector. Nevertheless, recurring patterns and historical trends in the cyber threat landscape should also be taken into account.

- As previously mentioned, focus on **increasing the resilience of medical devices** is especially important, as they are particularly vulnerable to cyberattacks due to infrequent patching cycles. There is often a misconception that any update of medical device requires regulatory review, which can lead to irregular patching updates. Government and private sector actors can work together to help address this misperception.

13 Global Forum on Cyber Expertise, www.thegfce.org

14 The Global Fund, www.theglobalfund.org/en

Recommended reading & resources shared by participants:

Playing with Lives: Cyberattacks on Healthcare are Attacks on People, The CyberPeace Institute, March 9 2021, https://cyberpeaceinstitute.org/publications/sar001-healthcare/

Cyber Incident Tracer, The CyberPeace Institute, https://cit.cyberpeaceinstitute.org/

Crowdsourced Cyber Security | Sector Threat Intelligence | Shared Best Practices, Health-ISAC (Information Sharing and Analysis Center), https://h-isac.org/

Cyber Europe 2022 (former CE2020), European Union Agency for Cybersecurity (ENISA), https://www.enisa.europa.eu/topics/cyber-exercises/cyber-europe-programme/cyber-europe-2022

WeHeartHackers, https://wehearthackers.org/

Securing the IoT Threat in Healthcare, Palo Alto Networks, October 21, 2020, https://www.paloaltonetworks.com/resources/videos/securing-the-iot-threat-in-healthcare

2020 Unit 42 IoT Threat Report, Palo Alto Networks, https://start.paloaltonetworks.com/unit-42-iot-threat-report

Table-top exercises - benefits for healthcare: Health Czech 2021 example

The increasing number of cyberattacks against the Czech medical facilities before and during the COVID-19 pandemic fully exposed the gaps in their cybersecurity. One way NÚKIB has reacted was by carrying out a sectoral table-top exercise – Health Czech 2021.[15]

In general, table-top exercises are an effective tool for enhancing an entity's cyber resilience through raising cybersecurity awareness and preparedness. It allows participants to meet, sit at a table (hence its name) and go through the hypothetical crisis scenario and discuss it in a safe environment. It is an invaluable activity for bringing together a wide range of audiences: from technical experts, subject matter experts, to middle and top management.

Sectoral exercises offer added value in creating a platform for multiple organizations from the same sector, where they can discuss and share specific experiences, for example their cybersecurity measures (both pro- and re-active) and/or their approaches to media communication or employees' education. Speaking specifically about the healthcare sector, one needs to keep in mind several challenges.

- The first is the need to get completely different professionals (cybersecurity managers, law experts, IT specialists, doctors, spokespersons and data protection officers or crisis management experts) to the same place at the same time. This is challenging not just from the logistical perspective, but predominately because of their different perceptions of the importance of cybersecurity.
- The scenario needs to be authentic and realistic enough for each entity (Health Czech 2021 included 16 different hospitals) but still generic enough so only one scenario for the exercise is sufficient and there is no need to develop different and specific scenarios for every single entity in the sector.
- Last but not least, the exercise designer needs to deal with a lot of information related to highly specific medical technologies and devices. This requires research and support from medical professionals.

One of the main benefits of non-technical exercises is raising cybersecurity awareness throughout the organization. This was found especially crucial in the healthcare sector, where this can be utilized to bring the issue of cybersecurity closer to the leadership team, which oftentimes consists of medical personnel. In some cases, exercise scenarios revealed specific gaps to be filled and served as a catalyst to change cybersecurity processes and practices in individual entities.

15 First iteration took place in the fall 2021 and included the 16 largest hospitals in the Czech Republic that were by that time regulated by national cybersecurity legislation, Act. No. 181/2014 Coll., on Cyber Security (Cyber Security Act).

Thematic Workshop 5
International Law

The international community has repeatedly affirmed that international law applies to cyberspace, including at the United Nations.[16] However, cyberspace remains a relatively new field and many questions as to how existing international law applies to this domain are still open. Therefore, substantial work is still needed to reach agreement as to how international law applies in this context.

The healthcare sector, an area that everyone depends on, is protected by international law in both the kinetic and online environments. International law sets the rules and parameters of what is and what is not allowed or acceptable and outlines positive obligations of states to protect the sector and access to healthcare, which is a fundamental human right. Such rules are necessary to deal with perpetrators and work towards increased accountability in cyberspace.

Determining what these rules are in a new domain can be a complex challenge. Tackling it will include a discussion of various international law protections applicable to the healthcare sector, including protections under international human rights law, international humanitarian law (IHL), and international law more broadly. Both the positive and negative obligations of states need to be addressed, including measures that states should undertake, and activities that they should avoid doing.

Participants stressed the importance of interpreting and clarifying existing rules and identifying gaps but noted that new international law rules may be needed to effectively deal with current and future threats. Moreover, they underscored the need to translate rules into practical guidance for states and the importance of advancing a global geopolitical environment conducive to states abiding by international law. At the same time, it is important to remember that we do not need to start from scratch. For example, significant work has already been done by the International Committee of the Red Cross (ICRC) on the subject of how IHL protects medical facilities from cyber operations in the context of armed conflict,[17] or through the Oxford Process on International Law Protections in Cyberspace,[18] which looked to develop statements endorsed by the community of international law practitioners, including the Oxford Statement on cyber operations targeting the healthcare sector[19] and the Oxford Statement on vaccine research.[20]

Good practices, lessons learned, and recommendations identified by participants included:

- More research is needed to **better understand which rule of international law is breached by what kind of cyberattacks** on the healthcare sector. For example, participants stressed the importance of focusing not only on conventional attacks (e.g., data breaches) but also on "infodemics",[21] such as disinformation regarding the COVID-19 vaccine. It was noted that disinformation campaigns are increasingly becoming one of the key threats of our time and the legal community needs to pay more attention to them going forward.

16 See for example the 2013 Final Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, https://documents-dds-ny.un.org/doc/UNDOC/GEN/N13/371/66/PDF/N1337166.pdf?OpenElement

17 International Humanitarian Law and Cyber Operations during Armed Conflicts, ICRC, https://www.icrc.org/en/download/file/108983/icrc_ihl-and-cyber-operations-during-armed-conflicts.pdf

18 Oxford Process on International Law Protections in Cyberspace, www.elac.ox.ac.uk/research/the-oxford-process-on-international-law-protections-in-cyberspace

19 Oxford Statement on cyber operations targeting the healthcare sector, https://elac.web.ox.ac.uk/the-oxford-statement-on-cyber-operations-targeting-the-healthcare-sector

20 Oxford Statement on vaccine research, www.elac.ox.ac.uk/the-oxford-process/the-statements-overview/the-second-oxford-statement

21 World Health Organisation webpage on infodemics, www.who.int/health-topics/infodemic#tab=tab_1

- Assessment should be conducted not only in terms of how these activities fit within the rules of international law but also **what can be done about them.** A holistic approach is, therefore, essential. Nevertheless, it is necessary to recognize that these different activities are often linked and that international law, including international human rights law, can apply in ways that may have some commonalities but needs tailoring to the specific context.

- Participants called for **an in-depth thematic discussion among states on both active and passive precautions included under IHL.** For example, IHL discusses "active precautions" including that parties to an armed conflict must respect and protect – i.e., refrain from any behavior that would interfere with the functioning of medical facilities and medical personnel. More generally, civilian harm must be avoided during military operations. IHL also addresses "passive precautions" – e.g., recommendations that states should continuously build up and improve their cyber resilience.

- Participants reiterated the importance of **recognizing that international law's prohibition on the use of force** is relevant to protecting the healthcare sector from cyber harm. The 2021 Final Report of the Open-ended working group on developments in the field of information and telecommunications in the context of international security (OEWG)[22] reaffirmed the applicability of this point, which is also reflected in customary international law. However, what type of conduct is encompassed within the prohibition is contested – albeit not just in the cyber context but also more generally. As such, a clear recommendation is for states to clarify and publish their positions on this issue.

- The **rule of non-intervention should be leveraged** when seeking to regulate cyber activity in connection with the healthcare sector. However, more clarification as to the threshold for intervention is required. At a high level, that threshold is regulated by coercion. Though coercion is not defined by international law, it is generally considered to occur when one state effectively deprives another of its free will in relation to the exercise of its state powers. Delivering healthcare – and preventing another state from delivering it to its citizens – can be one such example. Participants called on the legal community to conduct more focused research into whether/how this situation can become even more complex, such as when private entities are delivering healthcare.

- **International human rights law can protect the healthcare sector from cyber harm** and may be particularly effective at doing so, compared to other branches of international law. This is because the interests of the individuals whose health is being harmed are at stake (rather than, for example, the state's interests). Human rights bodies have repeatedly reaffirmed a state's positive duty to protect its population subject to a due diligence standard. The right to life, for example, includes the proactive duty to combat the effects of infectious diseases – and so a state must act diligently to help its private healthcare entities to secure their networks and infrastructures. What is in doubt, however, is a state's positive duty towards people of other states – more research and clarity is required in this respect.

- Similarly, when assessing the harm one state inflicts on another state's population, **the issue of extraterritoriality warrants additional clarification** – i.e., to what extent international human rights law applies outside a state's own territory. That said, participants agreed that the only reasonable result seems that it should apply; it would be unconscionable to claim that from a human rights perspective, and in the context of healthcare, a state can take actions in other states that it cannot do in its own territory.

- Participants urged the **recognition of due diligence as an important positive obligation under international law** – including when dealing with cyber threats. At a high level, due diligence is essentially a state's obligation not to knowingly allow its territory to be used for acts contrary to other states' rights. Participants noted that the application of this principle requires that the state whose rights have been violated suffers sufficiently serious adverse consequences, and such adverse consequences are not limited to physical damage – but also noted that more discussions were needed to clarify this provision.

- Some states consider due diligence a binding legal obligation; others do not. In addition to understanding what the obligation is, it is important to translate that understanding into practical guidance for states. Relatedly, **it is important to bear in mind the no-harm rule:** a state's duty to prevent and remedy significant transboundary harm even if it is caused by lawful activity (injurious acts, not just of states but also of individuals). The breach of the rule derives after a state has

22 2021 Final Report of the Open-ended working group on developments in the field of information and telecommunications in the context of international security (OEWG), https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf

failed to compensate a victim for the damage caused. As the majority of cyberattacks against healthcare facilities are transboundary by nature, the due diligence obligation is crucial in this context.

- More **deliberations are needed to develop new rules as well as to clarify existing ones.** In particular, states should consider potentially developing new rules on specific issues such as, for example, sovereignty, extraterritoriality and the ban on the use of non-state actors for conducting cyber operations.

- In relation to IHL, participants noted that there is a **need to better interpret existing rules in the cyber context.** Participants also noted that as gaps in protection are identified, states may need to explore the development of additional rules to clarify how IHL applies in cyberspace.

- Participants stressed the **need to translate rules into practical guidance.** The importance of advancing a global environment conducive to states abiding by international law in cyberspace was also underlined. Even if and where international law is clear and (textually) effective, it may not serve to protect, if geopolitical considerations stand in the way.

- There is an urgent need to **build the capacity of states,** including via multistakeholder initiatives to better understand, comply and implement international law. Like all capacity building, this needs to be a continuous effort, rather than a one off/ad-hoc initiative. Multistakeholder partnerships can be particularly helpful and effective here and successful initiatives, such as the Oxford Process should be leveraged.

Recommended reading & resources shared by participants:

Protections Against Cyber Operations Targeting the Health Care Sector, https://www.elac.ox.ac.uk/the-oxford-statement-on-cyber-operations-targeting-the-healthcare-sector

Safeguarding Vaccine Research, https://www.elac.ox.ac.uk/article/the-second-oxford-statement The potential human cost of cyber operations, ICRC, 29 May 2019, https://www.icrc.org/en/document/potential-human-cost-cyber-operations

Provide medical care is in critical condition: analysis and stakeholder decision support to minimize further harm, https://www.cisa.gov/publication/provide-medical-care-critical-condition-analysis-and-stakeholder-decision-support

Signaling legal protection in a digitalizing world: a new era for the distinctive emblems?, Humanitarian Law and Policy, Sep 16, 2021, https://blogs.icrc.org/law-and-policy/2021/09/16/legal-protection-digital-emblem/

Avoiding civilian harm from military cyber operations during armed conflicts, ICRC, 26 May 2021, https://www.icrc.org/en/document/avoiding-civilian-harm-from-military-cyber-operations

International Humanitarian Law and Cyber Operations during Armed Conflicts, ICRC, November 2019, https://www.icrc.org/en/download/file/108983/icrc_ihl-and-cyber-operations-during-armed-conflicts.pdf

Cyber Attacks and Cyber (Mis)information Operations during a Pandemic, Marko Milanovic and Michael N Schmitt, Journal of National Security Law & Policy, Vol. 11, 2020, pp. 247–284, https://jnslp.com/wp-content/uploads/2020/12/Cyber-Attacks-and-Cyber-Misinformation-Operations-During-a-Pandemic_2.pdf

Scenario 20: Cyber operations against medical facilities, Tilman Rodenhäuser & Kubo Mačák, Cyber Law Toolkit, 15 February 2022, https://cyberlaw.ccdcoe.org/wiki/Scenario_20:_Cyber_operations_against_medical_facilities

International law protects the healthcare sector

International law has a crucial protective role to play, ensuring predictability and stability of interactions, and building confidence between states and other actors. The protection of the healthcare sector, established through a system of binding rules, is comprehensive: international law contains obligations applicable in both peacetime and armed conflict, binding both states and non-state actors, guaranteeing the interests of states, groups and individuals, requiring addressees to abstain from particular forms of conduct and to take certain positive protective steps. When properly internalized, implemented and enforced, these obligations can reduce vulnerabilities, prevent harmful cyber incidents, or mitigate their effects, and ensure accountability.

Both the Open-Ended Working Group and the Group of Governmental Experts underscored the role of international law as an essential framework for regulating the online environment.[23] As the discussion on how international law applies to ICTs is becoming more granular and sophisticated, two important aspects must be highlighted. First, we must not lose sight of the human cost of cyber operations. A human-centric approach must be mainstreamed in the consideration of international legal rules. Second, states and other stakeholders should work towards strengthening the system of positive obligations under, inter alia, international human rights law, international humanitarian law, the Corfu Channel Case[24] and no-harm rules by specifying concrete and effective legal, administrative, and technical steps capable of discharging these obligations. Implementing a robust set of positive measures to prevent, mitigate and redress the effects of cyber intrusions can substantially reduce the risk of cyber harm.

The international legal framework protecting the healthcare sector is both extensive and complex. A range of capacity-building measures seek to assist states and other stakeholders in navigating existing protections under international law. The Oxford Process on International Law Protections in Cyberspace,[25] an initiative of the Oxford Institute for Ethics, Law and Armed Conflict is a collaborative effort between international legal experts from across the globe aimed at the identification and clarification of rules of international law applicable to cyber operations across a variety of contexts. The first two Statements of the Oxford Process identified a wide range of international legal rules protecting the healthcare sector and affirmed the central role that international law has to play in ensuring its safety and resilience.

Tsvetelina Van Benthem
The Oxford Process on International Law Protections in Cyberspace

23 2021 Final Report of the UN Open-ended working group on developments in the field of information and telecommunications in the context of international security, https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf and 2021 Final Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security, https://documents-dds-ny.un.org/doc/UNDOC/GEN/N21/075/86/PDF/N2107586.pdf?OpenElement

24 The Corfu Channel case was the first public international law case heard before the International Court of Justice (ICJ) between 1947 and 1949 concerning state responsibility for damages. For more details, see www.icj-cij.org/en/case/1

25 Oxford Process on International Law Protections in Cyberspace, www.elac.ox.ac.uk/research/the-oxford-process-on-international-law-protections-in-cyberspace

Protecting the healthcare sector from cyber harm during armed conflicts

International humanitarian law (IHL) imposes limits on the conduct of cyber operations during armed conflicts, including in relation to the protection of the healthcare sector. The relevant rules of IHL are very clear: belligerents must at all times respect and protect medical facilities and medical personnel, including when carrying out cyber operations. These obligations derive from specific treaty rules in the Geneva Conventions and their Additional Protocols.[26] Today, they are also part of customary international law and apply equally in international and non-international armed conflicts.

The obligation to respect requires parties to the conflict to refrain from any behavior that would interfere with the functioning of medical facilities or with the work of medical personnel. First and foremost, this means refraining from directing attacks against such facilities. However, it is immaterial if the interference leads to death or injury or merely slows down the functioning of a hospital. Any kind of interference violates the duty to respect medical facilities.

In the physical world, such prohibited conduct includes, for example, preventing medical supplies from getting through or conducting inspections of a medical facility that would result in the patients no longer being able to receive the necessary medical treatment. In the cyber context, a cyber operation that, for instance, freezes a hospital's computers or that deletes or encrypts its data also interferes with the hospital's functioning and would be prohibited by IHL.

The obligation to protect requires the parties to the conflict to take positive steps to protect medical facilities and personnel from harm, including from harm caused through digital means. In the physical world, belligerents must ensure that medical establishments are not harmed by third parties such as looters or rioters, and if such persons are already impeding the functioning of a hospital, then the belligerent concerned must take feasible steps to protect the hospital. Similarly, in the cyber context, if a party to an armed conflict learns of the existence of a serious cyber threat to a medical facility – or an ongoing harmful cyber operation – and if it is in its power to address that situation, it is obliged to do so.

The importance of this legal framework is underscored by a number of recent public calls and documents issued by States,[27] the ICRC,[28] global leaders,[29] and academic experts,[30] which have been aimed at reaffirming these rules and at ensuring that medical facilities are respected and protected from harmful cyber operations, both during armed conflicts and in peacetime.

Kubo Mačák
Legal adviser
International Committee of the Red Cross (ICRC)

26 The Geneva Conventions of 1949 and their Additional Protocols, www.icrc.org/en/doc/war-and-law/treaties-customary-law/geneva-conventions/overview-geneva-conventions.htm

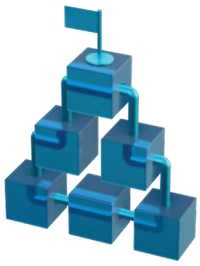
27 2021 Final Report of the UN Open-ended working group on developments in the field of information and telecommunications in the context of international security, https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf

28 International Humanitarian Law and Cyber Operations during Armed Conflicts, ICRC, November 2019, https://www.icrc.org/en/download/file/108983/icrc_ihl-and-cyber-operations-during-armed-conflicts.pdf

29 A Call to Governments: Work Together Now to Stop Cyberattacks on the Healthcare Sector, https://cyberpeaceinstitute.org/wp-content/uploads/engcyberpeace-institute-letter.pdf

30 Oxford Statement on cyber operations targeting the healthcare sector, https://elac.web.ox.ac.uk/the-oxford-statement-on-cyber-operations-targeting-the-healthcare-sector

Thematic Workshop 6
Diplomatic Measures



The international community has agreed repeatedly on the importance of protecting critical infrastructure from cyber harm. In the 2015 report of the UN Group of Government Experts (GGE) on developments in the field of information and telecommunications in the context of international security states committed to protect critical infrastructure from cyber threats and agreed not to conduct or knowingly support cyber activity contrary to international law that damages or otherwise impairs infrastructure providing essential services.[31]

Despite political commitment at the international level, recent years have seen a disturbing increase in cyberattacks targeting various organizations providing essential services, including in the healthcare sector. Between June 2020 and December 2021 alone, the CyberPeace Institute recorded a total of 235 cyber incidents affecting 35 countries around the world.[32] Recognizing the global scope of the problem, the multistakeholder community issued a Call to Governments in the midst of the COVID-19 pandemic to draw attention to the rise of cyberattacks on the healthcare sector and to stop such attacks.[33] Concurrently, the Governments of Australia and the Czech Republic successfully pushed for the UN GGE[34] and the first Open Ended Working Group (OEWG)[35] to recognize the healthcare sector as critical infrastructure under applicable cyber norms.

However, achieving additional progress on the diplomatic front will depend on the ability of the international community to harness the convening power of the UN to translate existing commitments into practical action. Participants of the workshop called on states to "walk the talk" and take responsibility for implementing their commitments. They also highlighted the need to pursue multistakeholder diplomacy in this space and encouraged stakeholders to combine their resources to support the implementation of the UN framework of responsible state behavior in cyberspace. Participants stressed that the diplomatic community can play a key role in bringing stakeholders together by setting up a permanent and action-oriented UN body to support information-sharing, thematic technical exchanges on best practices, and capacity building initiatives related to critical infrastructure protection.

Good practices, lessons learned, and recommendations identified by participants included:

- Participants recognized that the protection of critical infrastructure, including in the healthcare sector, is a shared responsibility among all stakeholder groups and urged states to **allow for meaningful stakeholder participation in both current and future UN cyber processes.** Specifically:
    - The current OEWG[36] for the years 2021-2025 should open its doors to participation and input from a wider range of relevant stakeholders than those currently accredited to participate in UN meetings, whilst respecting decision-making prerogatives of states.

31 2015 Final Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, www.un.org/ga/search/view_doc.asp?symbol=A/70/174

32 Cyber Incident Tracer #HEALTH, CyberPeace Institute, https://cit.cyberpeaceinstitute.org/explore

33 A Call to Governments: Work Together Now to Stop Cyberattacks on the Healthcare Sector, https://cyberpeaceinstitute.org/wp-content/uploads/engcyberpeace-institute-letter.pdf

34 2021 Final Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security, https://documents-dds-ny.un.org/doc/UNDOC/GEN/N21/075/86/PDF/N2107586.pdf?OpenElement

35 2021 Final Report of the UN Open-ended working group on developments in the field of information and telecommunications in the context of international security, https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf

36 Open-ended Working Group on security of and in the use of information and communications technologies 2021–2025, https://meetings.unoda.org/meeting/oewg-ict-2021/

- UN cyber processes could organize thematic interactive meetings with stakeholders dedicated to protecting critical infrastructure in different sectors to identify both general and sector-specific measures and best practices. These thematic areas could include – at minimum - health, water, energy, and the "public core of the Internet."[37]
- A dedicated UN funding mechanism could be established to support participation of subject-matter experts, particularly from developing countries, to allow for formal and informal exchanges among relevant technical experts from all stakeholder groups.
- Hybrid meetings should be preferred whenever possible to ensure the broadest possible participation of technical experts from Computer Emergency Response Teams and relevant subject-matter experts, particularly from developing countries.

- Participants agreed on the need to **connect the dots between UN discussions related to cybersecurity, digitalization, development and healthcare** in different UN bodies and technical agencies. Specifically:
  - Greater mainstreaming of cybersecurity into the UN digital development agenda should be considered. This would allow cyber capacity building programs to leverage UN development funds to ensure cyber-resilient digital transformation for everyone.
  - Holding a dedicated OEWG session with World Health Organization (WHO) and International Telecommunication Union (ITU) officials was proposed to identify synergies and opportunities for joint action in protecting the healthcare sector from cyber harm, including in ongoing and upcoming development projects. The WHO-ITU joint project Digital Health for Africa was referenced as an example of good practice.[38]
- Establishing a multistakeholder mechanism at the UN level to relay information pertaining to cyber incidents and existing vulnerabilities involving critical infrastructure, including in the healthcare sector.
  - Establishing a UN network of Points of Contacts at diplomatic, policy and technical levels was recommended to facilitate global information-sharing on rapidly evolving cyber threats directed against critical infrastructure.
  - A proposal was also made for the OEWG to develop regional arrangements with relevant infrastructure owners and operations within the health sector to help detect and mitigate cyber incidents affecting the sector globally.
- Participants urged states to **amplify a human-centric approach to cybersecurity and the human costs of cyberattacks against critical infrastructure in their messaging** to generate political will to increase investment into healthcare sector cyber-resilience. Specifically, systematically mapping the global impact of cyberattacks against the healthcare sector was highlighted as a means to empower the wider multistakeholder community with evidence to progress in their respective work and advocacy.

- Support the proposal to **establish a UN Programme of Action for Responsible State Behavior in Cyberspace (PoA)** as an inclusive, action-oriented, and permanent UN body to strenghten states' capacity to implement existing cyber norms, including through practical support for cyber capacity building in the area of critical infrastructure protection. The PoA could specifically:
  - Be used to launch multistakeholder capacity building projects designed to protect the healthcare sector from cyber harm and to strengthen synergies between security and development pillars of the UN system.
  - Establish a UN clearing house for matching capacity building needs with existing resources in close collaboration with succesful capacity building initiatives, including the Global Forum on Cyber Expertise (GFCE).[39]
  - Create a dedicated fund to support cyber capacity building related to critical infrastructure protection, with particular emphasis on meeting the specific needs of developing countries on both the digital development and cybersecurity fronts.

37 Global Commission on the Stability of Cyberspace Call to Protect the Public Core of the Internet, https://cyberstability.org/news/global-commission-proposes-definition-of-the-public-core-of-the-internet

38 Digital Health from Africa project website, www.itu.int/en/ITU-D/ICT-Applications/Pages/about-digital-health.aspx

39 Global Forum on Cyber Expertise, https://thegfce.org

- Governments, industry, and civil society stakeholders can **form multistakeholder partnerships to drive implementation of specific critical infrastructure commitments** in line with their priorities.
    - The "Adopt a Cyber CBM (Confidence Building Measures)" approach used by the Organization for Security and Cooperation in Europe (OSCE) was mentioned as a specific example of good practice, which could be translated to an "Adopt a Cyber Norm" approach in the OEWG context.

Recommended reading & resources shared by participants:

Final Report of the Group of Government Experts 2015, https://www.un.org/ga/search/view_doc.asp?symbol=A/70/174

Final Report of the Group of Government Experts 2021, https://daccess-ods.un.org/access.nsf/Get?OpenAgent&DS=A/76/135&Lang=E

Final Report of the UN Open-ended working group on developments in the field of information and telecommunications in the context of international security, https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf

General Assembly resolution 58/199 on the creation of a global culture of cybersecurity and the protection of critical information infrastructures, https://documents-dds-ny.un.org/doc/UNDOC/GEN/N03/506/52/PDF/N0350652.pdf?OpenElement

Cyber Incident Tracer, The CyberPeace Institute, https://cit.cyberpeaceinstitute.org/

Call to All Governments: Work Together Now to Stop Cyberattacks on the Healthcare Sector, https://cyberpeaceinstitute.org/wp-content/uploads/engcyberpeace-institute-letter.pdf

UN Secretary General Call to Protect Medical Facilities from Cyber-Attacks, https://www.un.org/sg/en/content/sg/speeches/2020-05-27/protection-of-civilians-armed-conflict-remarks-security-council-debate

Protecting the healthcare sector through multistakeholder engagement

The healthcare sector has over the years become a major target for malicious cyber activities. These activities range from ransomware and phishing emails to data theft and loss of connected medical devices that can impact the safety of patients. The COVID-19 crisis demonstrated the devastating effect malicious cyber operations can have. The fact that cyberattacks increased dramatically during the pandemic, including against the healthcare sector, is an urgent concern for the international community, as highlighted in the Final Reports of the 2019-2021 OEWG and GGE.[40]

At the OEWG in December 2021, the Czech Republic organized a side event on the multistakeholder approach to protecting critical infrastructure, particularly the healthcare sector, from cyber harm.[41] The Dutch Ambassador-at-Large for Security Policy and Cyber, Nathalie Jaarsma, joined the expert panel and referred back to an event that the Netherlands organized with Switzerland on the margins of the WHO General Assembly in May 2021. This event stressed the importance of connecting the ongoing discussions on health and cyber and concluded that addressing cyber threats facing the healthcare sector requires a collective, coordinated, and multistakeholder answer.

The CyberPeace Institute also underlined the urgency of a joint and coordinated response in its March 2021 report "Cyberattacks on Healthcare" while citing the Ryuk ransomware attack that affected hundreds of hospitals across the UK and the US in September 2020.[42] These attacks forced medical staff to revert to pen and paper, ambulances to redirect, and surgery patients to be relocated. This increased the risk of complications and in the worst case, death. Combining our efforts will increase our preparedness in such situations.

This is to an extent, already happening. The ITU and the WHO are working together to strengthen the healthcare sector through capacity building. As a multistakeholder platform for the coordination of capacity building the Global Forum on Cyber Expertise can also play a key role in increasing cyber resilience of the healthcare sector globally. Moreover, the 2021-2025 OEWG can enhance capacity building by developing regional arrangements with relevant infrastructure owners and operators within the healthcare sector to help detect and mitigate ICT incidents affecting the healthcare sector.

One of the priorities for the Netherlands in the 2021-2025 OEWG process lies with strengthening protection of critical infrastructure, including the public core of the internet, democratic electoral processes, and the healthcare sector. These three forms of critical infrastructure have been universally recognized by all UN Member States and should therefore enjoy the highest level of protection. The Netherlands is of the opinion that we must seek to strengthen the norms protecting these types of critical infrastructure, all the while avoiding over-regulation of the public core. We look forward to continuing our work on this in the years to come.

Kingdom of the Netherlands

40 2021 Final Report of the UN Open-ended working group on developments in the field of information and telecommunications in the context of international security, https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf and 2021 Final Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security, https://documents-dds-ny.un.org/doc/UNDOC/GEN/N21/075/86/PDF/N2107586.pdf?OpenElement

41 OEWG 2021-2025 website, side-events, https://documents.unoda.org/wp-content/uploads/2021/11/Concept-Note-Multi-stakeholder-OEWG-Event-Dec.15-Czech-Republic.docx39.pdf

42 Playing with Lives: Cyberattacks on Healthcare are Attacks on People, 2021 Report of the Cyber Peace Institute, https://cyberpeaceinstitute.org/report/2021-03-CyberPeaceInstitute-SAR001-Healthcare.pdf

Ministry of Foreign Affairs of the Czech Republic
Microsoft
NÚKIB
CyberPeace Institute