March 2021

Playing with Lives: Cyberattacks on Healthcare are Attacks on People

The CyberPeace Institute

Disclaimer

The opinions, findings, and conclusions and recommendations in this Report reflect the views and opinions of the CyberPeace Institute alone, based on independent and discrete analysis, and do not indicate endorsement by any other national, regional or international entity.

The designations employed and the presentation of the material in this publication do not express any opinion whatsoever on the part of the CyberPeace Institute concerning the legal status of any country, territory, city or area of its authorities, or concerning the delimitation of its frontiers or boundaries.

Copyright Notice

Foreword

Marietje Schaake

President, the CyberPeace Institute

The intensification of cyberattacks on healthcare is one of the untold stories of the COVID-19 pandemic. It is hard to overstate the harm to people that these attacks cause: Doctors are unable to treat patients, appointments are postponed, valuable time and resources are wasted.

Medical data is sensitive, highly personal, and exceedingly valuable for threat actors. Mikko Hyppönen, Chief Research Officer of cybersecurity firm F-Secure said, in response to a ransomware attack on psychotherapy clinics in Finland: “This is a very sad case for the victims, some of which are underage. The attacker has no shame.” We need to make sure that even if criminals and foreign intelligence agencies have no shame, they do face the consequences.

Beyond the harm inflicted on people and healthcare organizations, public trust in government and law enforcement, and in their ability to ensure security and protection, is eroded with every successful attack. For perpetrators, this means the winner takes all. For the CyberPeace Institute, their growing boldness is our call to action. In this Report, Playing with Lives: Cyberattacks on Healthcare are Attacks on People, we offer concrete policy recommendations to governments, corporations, civil society and experts with the aim of collectively ensuring security and resilience.

We track and analyse the methods used by criminals and nation states as they cynically seek to exploit the growing attack surface resulting from our time spent working, studying and accessing culture online from home. For a variety of goals, from espionage to financial gain, vulnerabilities in software or supply chains are exploited. On top of that, systematic disinformation is a weapon of choice. It is essential to end impunity and see more offenders held to account.

At the CyberPeace Institute, it is our conviction that a more thorough understanding of individual attacks and their collective impact on people is essential to effect positive change. In this Report, we probe how cyberattacks work, and the harm they cause to people. We hope that agreement will soon be reached that the status quo is unacceptable and that each of us can do more to prevent attacks, protect their victims and hold the perpetrators to account.

Stéphane Duguin

Chief Executive Officer, the CyberPeace Institute

When we drafted the first outline of this Report, we saw it as a story about cyberattacks on healthcare. We researched compromised infrastructure, phishing campaigns, ransomware, zero-days... But as we were interviewing healthcare professionals who became targets and patients who became victims, something new came to light. While documenting hospitals and vaccine laboratories being impacted, hearing how healthcare professionals and patients are suffering physically and mentally, seeing how attackers are immune to accountability, the true story imposed itself. It is a story about people – people whose health is at stake.

Since the 1948 Universal Declaration of Human Rights, numerous international instruments have recognized the human right to health. In a connected world, we need instruments to recognize cyberpeace for healthcare. Healthcare is a network. Not only does it connect professionals who have sworn to save lives, it interlinks global infrastructures. In this context, there is no isolated incident. Each attack impacts the overall construct; each attack is a threat to global health. We have all understood this about viruses by now: online or offline, they don’t stop at borders.

This very first Report of the CyberPeace Institute is the work of a coalition. Colleagues, partners, volunteers: everyone has given their best to analyse the immense threat confronting healthcare. The conclusion is clear: we need technical and regulatory actions from nation states to lead the way, to protect the human right to health and pave the way for cyberpeace. Nurses, doctors, researchers and other healthcare professionals are under attack. As they take care of our lives, their security is our collective responsibility.

Acknowledgements

The CyberPeace Institute would like to express its sincere gratitude to its Executive and Advisory Board members for their invaluable insights and continuous support of the Institute's activities.

Executive Board

Alejandro Becerra Gonzalez; Khoo Boon Hui; Merle Maigre;
Alexander Niejelow; Kate O'Sullivan; Anne-Marie Slaughter; Eli Sugarman;
Martin Vetterli

Advisory Board

Sunil Abraham; Cheryl Carolus; Ron Deibert; Niva Elkin-Koren; Jen Ellis;
Camille François; Vasu Gounden; Fergus Hansen; Chung Min Lee;
Joseph S. Nye Jr.; Luisa Parraguez Kobek; Michael Schmitt; Jamie Shea;
Danny Skriskandarajah; Luis Videgaray Caso

External partners and experts whose guidance and review of the Report are highly appreciated:

Alejandro Becerra Gonzalez; Khoo Boon Hui; Sung Choi Yoo;
François Delerue; Lilian Dolgolenko; Ben Edelman; Jen Ellis; Duncan Hollis;
Rebekah Lewis; Maria Mikryukova; Sarah Powazek; Dmitry Samartsev;
Michael Schmitt; Dmitriy Volkov; Beau Woods

The Institute is indebted to all the contributors to this publication for their generous dedication and tremendous collaboration.

Part 1:
Setting the Scene

Part 1: Setting the Scene

Introduction

The COVID-19 pandemic has reminded us that nurses, doctors, researchers and other healthcare professionals play an essential role in keeping us safe, healthy and alive. It also reminds us that they are facing simultaneous threats: on the one hand, they fight the pandemic, putting their own health at risk, and on the other they are targeted by repeated campaigns of cyberattacks, cyberespionage and disinformation at such speed and scale that they create a direct threat to life – the lives of healthcare professionals and the lives of their patients. **Healthcare needs cyberpeace**.[1] It must be free of any threat and must benefit from de-escalation of the number and magnitude of cyberattacks, the enforcement of responsibility and accountability of all actors, including via attribution of attacks, and the recognition that victims need a voice and have a right to redress.

Online threat to healthcare is not a new phenomenon, and part of the problem is that the international community is still lagging behind the reality of threat evolution and impact. The wake-up calls of WannaCry and NotPetya, two of the most destructive cyberattacks that have affected healthcare, did prompt responses, but did not allow for any scalable and sustainable solutions. In addition, the flood of COVID-19-related disinformation in the context of the so-called 'infodemic' has compounded and accelerated the threat potential.

Healthcare provision suffers from a myriad of broad and longstanding challenges: diversity in the types of cyberattacks it faces, an endemic lack of resources and lack of consistency in how national and international law is applied and enforced. Most importantly, the sector suffers from a growing accountability gap, seemingly making attacking healthcare a risk-free crime, with impunity for criminal groups and state-sponsored actors alike.

A holistic program to protect healthcare

Ensuring peace for healthcare in cyberspace requires a paradigm shift. At the CyberPeace Institute, our mission is to address such global challenges to critical civilian infrastructures. In 2020, we launched the **Cyber 4 Healthcare program to assist healthcare professionals**, **analyse attacks and advance policies to protect the sector**. We notably coordinated a Call to Governments (The CyberPeace Institute, 2020a) to promote cyberpeace in the sector while delivering direct operational support to healthcare (The CyberPeace Institute, 2020d). Through the Cyber 4 Healthcare program, we provide a global hub of expertise, connecting professionals in cybersecurity, healthcare, international law, forensic investigation and open-source intelligence to collect the pieces

[1] Cyberpeace exists when human security, dignity, and equity are ensured in digital ecosystems (The CyberPeace Institute).

of a multi-dimensional puzzle, gain an understanding of what is really happening to victims of attacks and facilitate a collective response. Thanks to the program, we offer resilience to cyberattack targets and assistance to victims, address information gaps and analyse systemic challenges in tackling the challenges, and design and propose technical and policy solutions.

How is this Report different?

This Report focuses on the impact of cyberattacks on people and society. As a cornerstone of the Cyber 4 Healthcare program, the Report consolidates scattered information for the first time, demonstrating the complexity, magnitude and scope of the cyber threat to healthcare, from ransomware through disinformation to COVID-19-related cyberespionage. It breaks down the silos of research and investigation to connect victims' testimonials, cybersecurity reporting, volunteer initiatives and academic findings. It analyses the technical innovation of *modus operandi,* the diversity of threat actors and their incentives, the difficult implementation of domestic and international norms and laws, the under-resourcing of the healthcare sector despite a vibrant ecosystem of assistance initiatives. Finally, it shows how accountability is critical to any systemic resolution in the current context where incidents are under-reported, attacks are seldomly attributed and threat actors evade punishment.

What do we want to achieve?

Online or offline, **attacking healthcare is attacking people**. Throughout our Cyber 4 Healthcare program, we aim to show that while healthcare professionals and patients are facing a significant, evolving and compounding threat, **collective action is possible**. The Report shows the overarching responsibilities of nation states in leading the way for attacks to decrease globally and threat actors to be held accountable. To achieve these goals, the Report maps existing initiatives and provides actionable recommendations to governments and policy makers to engage with civil society, industry and academia and design collective solutions.

To support these recommendations, the CyberPeace Institute will continue its efforts to campaign globally and engage all stakeholders around a simple goal – that every healthcare professional, patient and person across the globe has the right to benefit from healthcare without fear or harm, both during times of conflict and during times of peace.

Signposting – How to read the Report

The Report comprises two core parts to provide, first, an understanding of the threat landscape for healthcare organizations and second, toolkits that can play a pivotal role in tackling the threats they face today (see Figure 1).

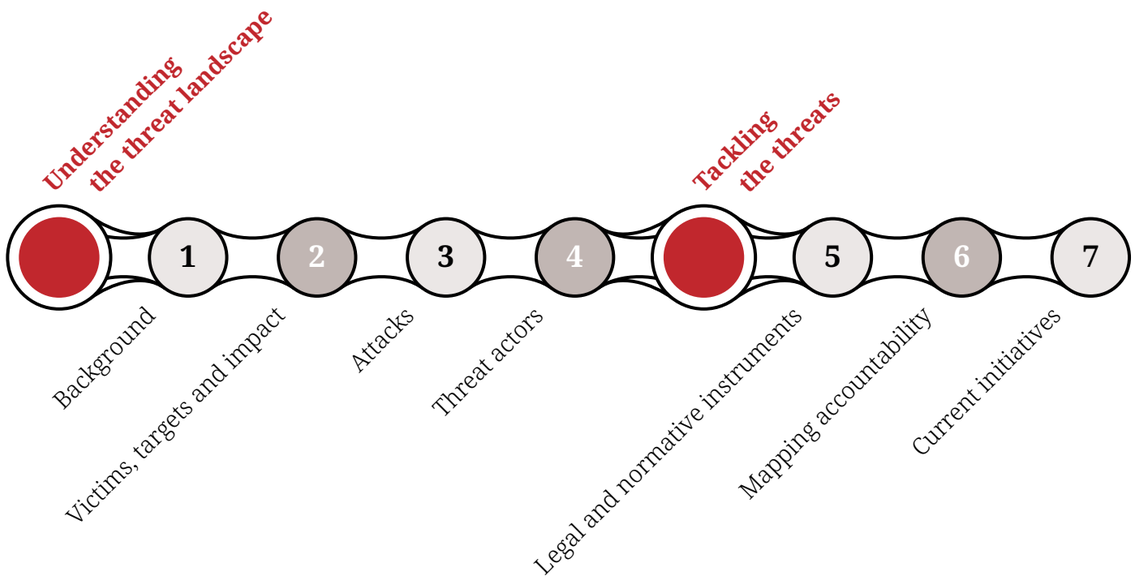


Figure 1: Report structure
Source: The CyberPeace Institute 2021

By answering a series of questions through dedicated but interconnected chapters we aim to bring the various research angles together to describe all dimensions of the threat:

1 Why is the healthcare sector under attack?

2 What is the true impact of attacks on healthcare?

3 How are attacks unfolding and evolving?

4 Who are the prevalent threat actors?

5 What instruments are available to protect healthcare from attacks?

6 Could a strong accountability framework increase responsible behavior in cyberspace?

7 How are different stakeholders joining forces in support of the healthcare sector?

Scope

The research and analysis focuses on attacks against the healthcare sector around the world; generally speaking, it does not seek to make a comparison against the context of other sectors. The Report covers three categories of cyberattacks against healthcare: disruptive attacks such as ransomware, data breaches and disinformation operations. Other than in Chapter 1, the Report focuses on the most recent cyber threats (primarily in 2020) and encompasses issues surrounding the global COVID-19 pandemic. Inasmuch as their respective impact and arguable severity may vary, the Report outlines the predominant threats that have affected the healthcare sector as a whole.

Consultations have taken place with cybersecurity professionals, chief information security officers (CISOs), hospital staff, legal experts, reporters, volunteers, and victims of attacks on healthcare as part of the drafting and review process to encourage transparency and ensure that findings are corroborated by those working directly with or in the healthcare sector. For further details of the methodology and the research limitations, we invite you to consult the Report Methodology appendix.

Terminology

To facilitate the reading of the Report, several key terms are defined from the outset to align the reader's understanding with the CyberPeace Institute's intended meaning and scope.

- **Accountability**: The degree to which a threat actor or stakeholder can be held to account for their actions, or lack thereof, that may contribute to an increased threat.

- **Attack or Cyberattack**: A disruptive cyber incident, data breach or a disinformation operation conducted by a threat actor using a computer network or system with malicious intention to cause damage (technical, financial, reputational or other) or extract / steal data without consent. The term 'attack' is used throughout the Report as an agglomeration of the three aforementioned attack types, whether the attacks are targeted or untargeted.

  — **Targeted attack**: When the target is deliberately singled out by the threat actor.
  — **Untargeted attack**: When the threat actor indiscriminately targets organizations, devices or vulnerabilities.

- **Attribution**: The process of identifying and tracking down which threat actor is responsible for an attack. The attribution may take place at a technical, political or legal level.

- **Healthcare / healthcare sector**: All healthcare organizations or entities, whether public, private or non-profit, providing healthcare-related goods, products or services.

- **Instruments**: Any legal, normative or regulatory mechanism, proposed or established, binding or non-binding, that governs responsible behavior in cyberspace to protect all users online, and more specifically victims and targets of attacks on healthcare.

- **Responsible behavior**: Behavior that conforms to justice, security and peace in cyberspace, and is enforcing human security, dignity and equity in digital ecosystems.

- **Stakeholder**: Any person, group, sector or entity in a position to play an active role in changing the attack threat landscape across the healthcare sector.

- **Target**: A healthcare organization that undergoes or may undergo in the future an attack, e.g. a hospital, a vaccine research laboratory or a country's ministry of health.

- **Threat actor**: An individual or a group, acting independently or on behalf of a nation state, or a nation state itself that attacks the healthcare sector.

  — **State actor**: A threat actor directly or indirectly colluding with a nation state, e.g. state actor or state-sponsored actor (see Section 4.2 for more details)
  — **Cybercriminal**: A threat actor operating independently from a nation state, e.g. non-state ransomware operators or groups.

- **Toolkits**: A set of instruments, frameworks and initiatives, existing or put forward, that provide opportunities for protecting and securing healthcare, holding threat actors to account and / or supporting victims of attacks.

- **Victim**: A person who is impacted, either directly or indirectly, following an attack on healthcare. E.g. a doctor, nurse or patient.

These terms will be expanded upon and contextualized in greater detail throughout the Report along with additional terms and acronyms of a technical, medical or ambiguous nature featured in the Glossary.

Spotlights

Throughout the Report a series of eight Spotlights highlight incidents of cyberattacks on healthcare. Each Spotlight includes:

- A description of the case, victims, targets and impact of the attack
- An overview of the attack method
- Information relating to the attribution of threat actor(s)
- Where relevant, details of responses (enforcement or otherwise) following the attack

Related topics

These sections contain insights into a topic that is related to the chapter or section in which they appear but can be read independently from the rest of the text. These related topics aim to complete, albeit briefly, the healthcare threat landscape profile.

Key Findings

Key Finding 1:

Attacks on healthcare are causing direct harm to people and are a threat to health, globally.

- **When healthcare providers are attacked**, **clearly it is people who suffer the consequences**. Whereas the targets of attacks are most often portrayed as the healthcare organizations or service providers whose data or infrastructure was compromised, the direct victims of attacks are healthcare professionals and patients. In addition to the disruption of medical services and IT systems that have an immediate impact on the process of patient care, healthcare professionals and patients also suffer less visible impact including acute stress from their being in an incident response situation or psychological trauma and a sensation of powerlessness from having private information stolen by criminals.

- **Attacking healthcare in a connected world is having a societal impact**, **globally**. The multiplication of attacks on healthcare, especially during the COVID-19 pandemic, is creating a global threat to health and human life. Considering that the phenomenon is under-researched, the documented impacts of converging threats raise immediate concern: disruption in patient care, loss of confidence in the sector's cybersecurity, notably with an erosion in trust in the sector's ability to protect patient data, while disinformation operations instill fear and distrust in the sector, causing confusion and harm throughout society.

Key Finding 2:

Attacks are increasing and evolving as they continue to exploit vulnerabilities in the healthcare sector's fragile digital infrastructure and weaknesses in its cybersecurity regime.

- **Attacks are increasing as the arsenal of weapons used to target healthcare is evolving**. Attacks on healthcare are not a new phenomenon but the COVID-19 pandemic is giving rise to an alarming convergence of malicious and irresponsible behaviors: vaccine research centers are targets of cyberespionage; hospitals are held to ransom with little choice but to pay to maintain operations; healthcare professionals and international health organizations are targeted with a blend of disinformation and cyberattacks aimed at undermining their credibility. As national statistics have shown, data breaches against healthcare in 2020 have increased significantly.

- **Ransomware creates both an immediate risk to patient care and long-lasting impact on healthcare organizations**. The escalation of ransomware attacks are particularly dangerous as they put both patient care and healthcare sector capability in jeopardy. The ransomware business model is in constant evolution, notably via the double extortion tactic. It is characterized by increased cooperation among cybercriminals, who have sought to maximize reach and increase profits. As a result, healthcare organizations suffer from costly and time-consuming disruption, requiring funding to recover and improve their systems, re-train staff, and manage reputational damage. Losing access to medical records and life-saving medical devices obstructs the healthcare professionals' ability to effectively care for their patients immediately and in the long run.

- **Healthcare has a fragile digital infrastructure**. Threat actors are exploiting the complex, vulnerable, and sometimes outdated healthcare digital environments including medical devices and IT infrastructure. Security-by-design does not apply to legacy systems and is difficult to achieve with the multiplication of connected endpoints. The healthcare security perimeter is widening, and as such calls for a closer look into the resilience of the supply chain.

- **Healthcare cybersecurity is under-financed**. Although a minority of large healthcare actors have deployed major cybersecurity programs, the vast majority of the sector suffers from a systemic lack of resources to secure its infrastructure, train its personnel, and hire and retain cybersecurity staff. The growing threat landscape exacerbates this resource gap, as attacks generate loss of revenue, new risks introduce higher cybersecurity costs to secure medical devices, hardware and software, including the rapidly expanding telehealthcare supply chain.

- **Technical and human resource limitations are preventing a healthy information-sharing environment within the healthcare sector**. Beyond the lack of financing in cybersecurity, the healthcare sector lacks technical and human resource capacities to send, receive and use threat-related information (i.e. indicators of compromises, e-evidence, threat intelligence). Sharing this information is critical to improving resilience and enabling rapid recovery. Best practices garnered from more mature sectors are not implemented at scale in healthcare (e.g. financial sector).

Key Finding 3:

Attacks on healthcare are low-risk, high-reward crimes. Acting with near impunity, criminals and state actors are joining forces against healthcare with varying motives and agendas.

- **Attacking healthcare is a lucrative and global business**. Attacks on healthcare are a global phenomenon, regardless of whether the intent is to hold healthcare providers to ransom, steal medical records and intellectual property, or erode public trust. As healthcare organizations are gatekeepers of sensitive information, the data they hold makes the sector a highly profitable target for both cybercriminals, state actors and state-sponsored actors.

- **Attacking healthcare serves geopolitical interests**. Not only does attacking healthcare provide state or state-sponsored threat actors with an attractive target for data theft regarding vaccine research and private medical records, but cyberattacks also weaken geopolitical rivals.

- **Attacks on healthcare are widely under-reported**. When targeted, many organizations don't know what to report and how to do so, notably because they don't have the necessary cybersecurity capability. Moreover,the fear of facing liabilities or reputational loss is hampering reporting as is a lack of faith that reporting will lead to prosecution. This underreporting prevents a comprehensive evaluation of the true scale of the threat.

- **Threat actors enjoy near impunity, as attribution and prosecution lag behind**. The law enforcement and prosecution rate of perpetrators of cyberattacks on healthcare is extremely low. This stems notably

from the under-reporting of attacks, from the lack of resources in law enforcement and the judiciary, and from shortfalls in attribution. In addition, opportunities available by means of legal instruments, such as investigative cooperation, and enforcement mechanisms, such as sanctions, are rarely used systematically in the case of attacks against healthcare and are rendered still more complex by geopolitical agendas in the case of state or state-sponsored attacks.

- **There are today no transparent and independent mechanisms to track accountability in cyberspace**. Various actors bear responsibilities to protect healthcare. When analysing an attack, there is no standard process to track who is responsible for what action or to hold them to account, let alone any systematic documentation or transparency on how malicious behaviors are violating laws, norms and principles.

Key Finding 4:

Healthcare professionals and patients do not benefit fully from legal instruments and existing assistance initiatives designed to protect them.

- **States are not availing themselves of the full extent of norms and laws available to protect healthcare**. State actors have a variety of opportunities at their disposal to protect the healthcare sector. It is a nation state's duty to ensure that its rule of law is respected and enforced within its jurisdiction. Nation states also have a duty to respect international law, including in cases of attacks performed by cyber means. Cooperation mechanisms also remain quite limited, despite the transnational nature of cyberspace. States have notably tread with caution in legal condemnation or prosecution of cyberattacks on healthcare or in conveying their interpretation of how international law applies, too often relying on political and technical attributions as a means of taking a stand against attacks.

- **Assistance initiatives lack visibility**, **scale and sustainability**. As criminals and threat actors join forces to attack healthcare, numerous coalitions have been established to provide fast and free support to healthcare professionals. Be it civil society, industry or individuals, from professionals to volunteers from all parts of the world, they operate with an agile and targeted assistance model. Regrettably, these initiatives lack adequate visibility, scale and sustainability. The Cyber 4 Healthcare initiative has identified that healthcare professionals were found to have limited visibility of the assistance resources available to support them and may lack the technical know-how to request the most relevant support and/or apply the recommendations.

Recommendations

These recommendations are intended for governments, industry, the healthcare sector, academia and civil society for the purpose of addressing the key findings and enabling their lasting impact by reducing cyberattacks on healthcare. It is important to note that although these recommendations are generic in nature, their implementation ought to take into account regional and local reality. The CyberPeace Institute will support this contextualization within its Cyber 4 Healthcare program, notably through the recruitment and deployment of regional advisors and volunteers with specific cyber expertise (CyberPeace Builders).

Recommendation 1:

Document attacks and analyse their human and societal impact

- **Academia and civil society**: Identify and connect existing initiatives aiming at assessing the impact of attacks (i.e. existing research, documented victims stories, healthcare community led initiatives, cybersecurity analytics).

- **Civil society**: Document attacks in a continuous and transparent way, with a focus on societal impact and victim testimonials.

- **Academia and civil society**: Perform empirical research on the short and long-term impacts of attacks on people, healthcare organizations and society, notably on healthcare professionals, patient care and trust in healthcare.

The CyberPeace Institute will support these recommendations by continuing to collect testimonials and by developing a publicly available database on attacks, notably to enhance transparency of human and societal impacts.

Recommendation 2:

Improve healthcare preparedness and resilience[2]

2.1 Improve the cybersecurity of healthcare infrastructure

- **Healthcare organizations and governments**: Develop certification and labeling schemes across the sector to enhance trust and security in products and services thereby protecting the complex healthcare supply chain which relies heavily on third-party vendors for its day-to-day operations.

- **Healthcare organizations**: Implement cybersecurity best practices and hygiene, such as patching vulnerabilities and updating systems. Assistance within civil society is available to support this resource-intensive activity (see below).

- **Governments**: Adopt stringent healthcare regulations, including procurement guidelines, to tighten healthcare cybersecurity requirements. Such regulations should apply regardless of whether healthcare is provided via a public or private entity, and across its supply chain. This should notably provide for standards to ensure state-of-the-art security and accountability criteria when healthcare providers write tenders.

- **Governments**: Adopt procurement regulations to facilitate efficient and cost-effective access to cybersecurity resources. **Industry**: Implement security-by-design and security-by-default models for healthcare product development across the supply chain. These designs and models should align with the previous recommendation about standards for operations and procurement in healthcare.

- **Industry**: Adapt pricing models according to the diversity of resources in healthcare, taking inspiration from pricing models facilitating the work in the not-for-profit sector (also recognizing that some not-for-profit entities are providing healthcare). This should prevent discrepancy from arising between those that can afford cybersecurity and those that can't.

2.2 Improve healthcare capacity and capabilities

- **Civil society**, **CERTs (Computer Emergency Response Teams) and volunteer networks**: Increase the visibility of available assistance initiatives, notably those offering pro bono support. Beyond availability, care should be given to making such initiatives understandable and adaptable to the reality of healthcare practitioners, recognizing that most lack baseline support resources to request and process the help received (tools, training, data).

- **Governments**, **philanthropy and industry**: Investigate how existing healthcare funding models should prioritize cybersecurity, design new cybersecurity-centric funding schemes, and inform healthcare decision makers about fundraising strategies and equipment acquisition.

- **Governments and industry**: Sponsor research in technical solutions such as zero-trust networks, behavioral authentication and monitoring to improve the protection of hospitals from vulnerabilities in their supply chain.

2.3 Improve healthcare preparedness against attacks

- **Governments**, **in close collaboration with CERTs**, **industry and healthcare**: Coordinate stress tests and awareness campaigns, and establish mandatory security audits and minimum compliance requirements to reinforce prevention against attacks and help healthcare organizations respond effectively in case of an incident.

- In parallel, **healthcare organizations** should build and maintain the level of cybersecurity capacity required, including by means of security exercises, IT stress-test training for staff, tabletop exercises and penetration testing to reduce human and technical vulnerabilities to prevent attacks and protect their patients. These cost-intensive activities should be supported by the community, and especially **pro bono assistance initiatives**.

- **Healthcare organizations**: Commit to due-diligence and standard rules of incident handling, notably via safely disclosing incidents and admitting compromises across the healthcare supply chain. This decreases the risk of potential lateral threats or further impact to victims.

The CyberPeace Institute will continue to promote the activities of volunteers, not-for-profit and industry stakeholders already providing assistance to the healthcare sector, supporting linkage between those in need and those with the capacity to help. Furthermore, the CyberPeace Institute is ready to cooperate with governments, industry and the healthcare sector to conduct vulnerability analysis and risk assessments so as to precisely define and evaluate shortfall in the human, financial, government, technical and insurance resources needed to secure the complex and critical healthcare infrastructure.

[2] Note: These recommendations are to be considered in the context of an endemic shortage of resources in the healthcare sector and that different countries and regions may also be at different levels of cyber maturity. In this regard, the use of available resources and know-how should be given priority, and collaboration with existing pro bono assistance initiatives should help to bridge the resource gap, and inform sustainable investment for capacity building.

Recommendation 3:

Activate technical and legal instruments to protect healthcare

These recommendations specify the opportunities available to various stakeholders seeking to better protect the healthcare sector from cyberattacks and hold threat actors to account. By systematically making use of legal instruments and available initiatives, along with developing a strong accountability framework, multisectoral stakeholders, with governments leading by example, can pave the way to cyberpeace.

3.1 Reinforce the legal and normative ecosystem

- **Governments**: State unanimously within the UN-mandated processes (UN GGE and UN OEWG) and multistakeholder initiatives (i.e. Paris Call) that medical and healthcare facilities must never be targeted and consistently protected against cyberattacks. Possible approaches include pledging to protect and 'do no harm', including public declarations of positions banning any type of state-sponsored cyberattacks on healthcare and cyberespionage against research centers and the vaccine industry.

- **Governments**: Publicly commit and, most importantly, take proactive steps to implement norms to secure effective protection of the healthcare sector. Said implementation of norms should complement the application of international law and create a baseline for responsible behavior. To this end, the healthcare supply chain shall be designated as critical infrastructure.

- **Governments**: Raise the capacity of their national law enforcement agencies and judiciary to act in the event of extraterritorial cases. This can be supported by reinforced and improved extradition processes and mutual legal assistance, notably through the systematic commitment to international cooperation mechanisms (e.g. the Budapest Convention, Mutual Legal Assistance Treaties, the Cloud Act).

- **Governments and international organizations**: Review the effectiveness of international cooperation mechanisms: First, by evaluating and supporting the development of cybersecurity capabilities and capacity across law enforcement and judicial entities globally, to allow for compelling investigations and the prosecution of threat actors. Second, by providing victims with a platform for their voices to be heard, enabling their access to information and securing compensation for the harm and damages they have suffered.

The CyberPeace Institute will support these recommendations by monitoring the application of international law and norms, and by advancing the protection of victims. These efforts will focus specifically on violations of human security, dignity and equity so as to understand the potential gaps in legal and regulatory frameworks, and will be available for public use.

3.2 Improve information sharing and reporting standards

Secure and effective information sharing is critical to the collective resilience of the healthcare sector and calls for diverse mechanisms to share highly diverse datasets (i.e. best practices, indicators of compromise, *modus operandi*, electronic evidence, threat intelligence). Various stakeholders have come together to this end but they need stronger support and coordination to ensure their sustainability and optimal efficiency.

- **Healthcare organizations**: Work with industry-specific organizations and associations to develop technological solutions that promote privacy-enhancing information-sharing. Engaging with established or emerging initiatives in other sectors can shed light on innovative methodologies and technologies for secure collaboration (financial sector).

- **Governments**: Develop cyber incident reporting schemes for the healthcare sector at the national level, or improve schemes in operation to support faster information sharing and richer research. The systematic reporting of incidents contributes to understanding the impact of full-scale cyberattacks against the sector, the associated risks, emerging trends and best practices.

- **Governments**: Sponsor specialized national, regional or sectoral communities in the form of a Computer Emergency Response Team (CERT) to enable an efficient incident-response platform for healthcare organizations.

The CyberPeace Institute will work with its partners to document and promote the many active information-sharing initiatives. The Institute will inform governments and industry of any findings likely to reinforce capacity building in the healthcare sector.

Recommendation 4:

Hold threat actors to account

- **Governments**: Ensure that the rule of law is strictly respected and applied, notably through enforcement, prosecution, sanctioning and extradition of accused or convicted threat actors. In the case of ransomware, law enforcement and the judiciary should investigate the money flow stemming from any extortion scheme (with a focus on cryptocurrencies), and opportunities for asset tracking and freezing to hinder the activities of threat actors.

- **Governments**: Work towards the systematic attribution of all types of cyberattacks on healthcare. Beyond geopolitical dimensions, said attribution shall provide a strong evidence base supported by technical and legal attribution.

- **Governments**: Specify which rule of international law or norm of responsible state behavior has been violated following an attack. Civil society and academia to support government efforts by systematically establishing any links between cyberattacks, human rights violations, and breach of international laws or norms of responsible state behavior.

- **Governments**, **CERTs and civil society**: Remind the healthcare sector that paying ransom is tantamount to direct financing of organized crime and invites threat actors to perpetrate more cyberattacks. Paying ransom may be seen as a fast-track solution, but it is no silver bullet. Civil society and governments should support the healthcare sector in setting up a playbook to cyberattacks, so that it is in a strong enough position to refuse payment by extortion and limit any ransom payment to critical cases only.

The CyberPeace Institute will increase efforts to document, track and analyse attacks and subsequent accountability, notably by applying its accountability framework. This will contribute to publicly establishing any links between malicious behavior, human rights violations, and violation of domestic or international rule. The Institute will document whether or not perpetrators are brought to justice, to ensure the right of victims to justice and redress. The CyberPeace Institute will ensure that this information is actionable by both policy makers and victims.

Part 2: Understanding the Threat Landscape

1 Why is the healthcare sector under attack?

"We are most concerned with ransomware attacks which have the potential to disrupt patient care operations and risk patient safety [...] We believe any cyberattack against any hospital or health system is a threat-to-life crime and should be responded to and pursued as such by the government."

A senior cybersecurity adviser to the American Hospital Association speaks out after the ransomware attack on Universal Health Services, USA, September 2020 *(CBS News, 2020)*.

1.1 A convergence of threats to healthcare

In 1989, a scientist at a World Health Organization AIDS conference knowingly distributed 20,000 floppy disks containing the so-called AIDS trojan. As the perpetrator promised a decryption key in exchange for money, this incident not only became known as the first documented ransomware attack but also one of the first cyberattacks on healthcare. Since then, the threat landscape of the sector has evolved with a growing number of threat actors and in terms of the sophistication and diversification of attack vectors.

Early threats to healthcare organizations often came from the inside and related primarily to the breach of select medical records (Coventry and Branley-Bell, 2018). With their increasing digitalization and growing value in the underground economy, however, medical records soon evolved into an attractive target for external threat actors (Coventry and Branley-Bell, 2018). The number of HIPAA-reported[3] healthcare data breaches in the United States (US) steadily grew from 199 in 2010 to 505 in 2019. While cyberattacks made up only 4.6% of reported healthcare data breaches in 2010, they accounted for an estimated 58% of breaches in 2019. (Seh *et al.*, 2020)

[3] HIPAA: The United States Health Insurance Portability and Accountability Act

More recently, the COVID-19 pandemic has given rise to a concerning convergence of malicious activities as well as an exacerbation of its existent threat landscape. Healthcare is increasingly under attack owing to a combination of three factors:

- Healthcare services are critical to maintain as patient health depends on them. This has made hospitals a target of choice for digital extortion.

- Healthcare is the custodian of valuable and sensitive information, such as medical records and vaccine research, making it an attractive target for data theft and cyberespionage.

- Healthcare has found itself at the center of strategic inter-state rivalries due to the pandemic, which have spilled into malicious activities such as disinformation campaigns against the sector.

These three incentives are accelerated by an endemic asymmetry in resources. Threat actors from criminal groups to state actors are well resourced, whereas the healthcare sector operates within an often complex, vulnerable, under-resourced, and outdated digital infrastructure.

1.2 Healthcare as a target of choice

For the responsibility it bears

As healthcare services have a direct impact on public trust and human lives, the sector suffers from additional risks associated with its disruption and breach of its data. Medical facilities **need to maintain business continuity makes healthcare a particularly lucrative target for ransomware** (Al Qartah, 2020). Ransomware attacks have proven capable of disrupting healthcare services, thereby threatening the health and lives of patients.

For its lucrative data

Due to the digitalization and associated increase in digitized data (i-SCOOP, no date), **healthcare organizations are gatekeepers of a trove of valuable and sensitive information**. This information needs to be readily accessible across an often complex network of heterogeneous digital infrastructures, making it a susceptible and lucrative target for various threat actors.

Financial Gain – The healthcare sector represents a financial opportunity in the eyes of threat actors. Healthcare data has a monetary value. While prices fluctuate, **a medical record of a single individual can be sold for an average of USD 250 on underground markets** (Trustwave, 2018). The value of medical records is determined by its suitability to be exploited for various fraudulent purposes. Unlike other personally identifiable information (PII), medical records contain information that never expires.

This data can be used to file false insurance claims, request credit cards, and for identity theft (Malwarebytes, 2020).

Information Acquisition – As the pandemic has highlighted, the valuable data available in the healthcare sector is not confined to medical records alone but includes **data relating to public health activities**, **research**, **and intellectual property**. State actors are especially targeting COVID-19-related research and development – including data on vaccines and treatments – in an attempt to gain a competitive edge (Burt, 2020). In the process, they risk jeopardizing the security and effectiveness of the response efforts around the globe (FBI & CISA, 2020). During the pandemic, the heightened level of distrust between governments is said to have led to "**intelligence collection** on a scale that rivals armed conflict" (Henderson et al., 2020). In addition, healthcare organizations hold a wealth of information on nation state leaders and government employees that may be of value to state actors seeking to exploit this information through cyberespionage operations. For example, in 2018, following the SingHealth data breach by a state actor, the data of the Prime Minister of Singapore was "specifically and repeatedly targeted" (MOH, 2018).

For its strategic positioning

The COVID-19 pandemic has elevated the importance of the already vital healthcare sector. A state's public health response is linked to its ability to recover economically (Correia, Luck and Verner, 2020) and is dependent on and a contributing factor to the trust of its population (Devine *et al.*, 2020). This has placed healthcare at the center of strategic rivalries of competing states, which have sought to undermine their rival's pandemic response through a combination of cyberattacks, data breaches and disinformation operations that target healthcare and the trust that people place in it.

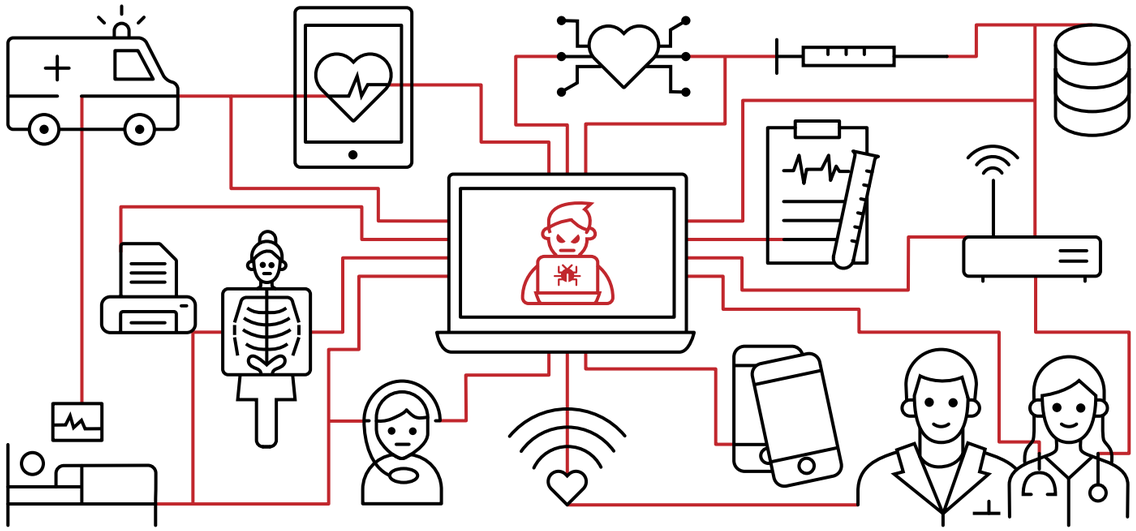


Figure 2: The healthcare digital ecosystem
Source: The CyberPeace Institute 2021

1.3 Cybersecurity in the healthcare sector

A fragile digital infrastructure

The global healthcare sector encompasses a plethora of public and private organizations that provide a broad range of products and services. It goes without saying that the digital infrastructure of healthcare organizations differs considerably from one organization to another and across geographies (see Figure 2). Nonetheless, healthcare organizations, especially hospitals and medical service providers, have suffered from a **rapid and disjointed digitalization** of their infrastructure. The COVID-19 pandemic has only accelerated these processes.

Processes like the adoption of telehealthcare and bring your own device practices (BYOD) have increased the number of devices and endpoints that are connected to a network[4] (Rossi, 2015). Despite this **growing attack surface** of healthcare organizations, **cybersecurity** has often been **only a secondary concern** (Randy, 2019). This has made them an easy target for threat actors. It is estimated that 83% of medical imaging devices are running on **unsupported operating systems** (OS) (Unit 42, 2020).

[4] 88% of questioned healthcare organizations allow the use of personal devices.

As many hospitals have **failed to properly segment their networks**, such unsecured devices have often been left connected to the wider hospital networks or directly to the internet, making them searchable on search engines for connected devices (Beek, 2018). Researchers demonstrated these vulnerabilities by penetrating a hospital network, intercepting medical images, and then altering them by removing evidence of medical conditions (Mirsky *et al.*, 2019). Additionally, healthcare is to be seen as part of a complex supply chain, where its security perimeters depend upon third-party technologies, security providers, and partners (Bisson, 2020). Lateral movement of security threats are becoming increasingly predominant (ManageEngine, no date).

Underinvestment in cybersecurity

Together with the broad attack surface, healthcare cybersecurity also suffers from a **general lack of human resources and budget allocation**. According to a recent survey, 87% of healthcare IT security leaders stated that they do not have enough cybersecurity personnel (Davis, 2020a). In 2017, three out of four US healthcare organizations did not even employ a designated cybersecurity professional (Health Care Industry Cybersecurity Task Force, 2017). Although numbers will differ across geographies and the size of organizations, this lack of cybersecurity personnel is in part due to what has been described as a “chronic underinvestment” in healthcare cybersecurity, partially due to the need to recognize the significance of cybersecurity vis-a-vis patient care and safety (The CyberPeace Institute, 2020c). An estimated 6% of US hospitals’ IT budget is allocated to cybersecurity (HIMSS, 2020). In comparison, financial institutions invest an average of 12% of their IT budgets into cybersecurity (Edelman and Dinesh, 2018).

Spotlight 1

WannaCry ransomware disrupts National Health Service (NHS)

Date: May 12, 2017 | **Location**: United Kingdom | **Target Type**: Hospitals and Medical Facilities

Victims, **Targets and Impact**: In May 2017, the self-propagating WannaCry ransomware affected systems across 150 countries, including those of the UK's NHS. At least 80 of 236 (34%) of the NHS trusts were disrupted, leading to over **19,000 cancelled appointments and operations**.[5] In five of these trusts, **patients had to be diverted** to more distant accident and emergency departments (Morse, 2018). The direct financial cost to the NHS was estimated at **GBP 92 million** (Cyber Security Policy, 2018). According to a 2019 report, 40% of healthcare organizations suffered from WannaCry in the six months prior to its writing (Armis, 2019). WannaCry continues to impact devices to this today (ANY.RUN, 2021).

Attack Method: The WannaCry ransomware was used to encrypt and lockdown computers, demanding a ransom payment in bitcoin to decrypt them. The ransomware was propagated via a communication protocol used to share files and printers across local networks (NHS, 2020). WannaCry exploited a vulnerability in Windows OS.

The majority of infected NHS devices were **running a supported OS for which a Microsoft patch and CareCERT alert had been issued but not applied** in the months leading up to the attack. Some trusts were running older, no longer supported OS. Issues were also reported with medical devices, such as MRI scanners, which had embedded unsupported OS that are generally managed by the system vendors. This left trusts unable to apply updates themselves (Morse, 2018).

Attribution and Response: The WannaCry Attack has been attributed (technical attribution) to the Lazarus Group based on commonalities in tools, code, obfuscation methods and other techniques (Johnson, 2017).

In July 2020, the EU imposed sanctions as part of its cyber diplomacy toolbox. The sanctions included travel bans and asset freezes of a legal entity from another nation state believed to be involved in the attacks (European Union, 2020). This followed the 2018 unsealing of a criminal complaint by the United States Department of Justice (DoJ) charging an individual from that same nation state for his involvement (U.S. DoJ, 2018). Most recently, in February 2021 the US DoJ unsealed an expansion of this indictment by adding two new defendants and recent global schemes to steal money and cryptocurrency from banks and businesses by a nation state (U.S. DoJ, 2021).

WannaCry was built around a vulnerability for which a national security agency developed the EternalBlue exploit. The exploit had previously been stolen from the national security agency and leaked by an unidentified threat actor (Fruhlinger, 2018). The vulnerability was shared with Microsoft only after the theft, raising concerns about the responsibility of states to effectively share vulnerability and cyber threat intelligence to prevent harm and protect people (Smith, 2017).

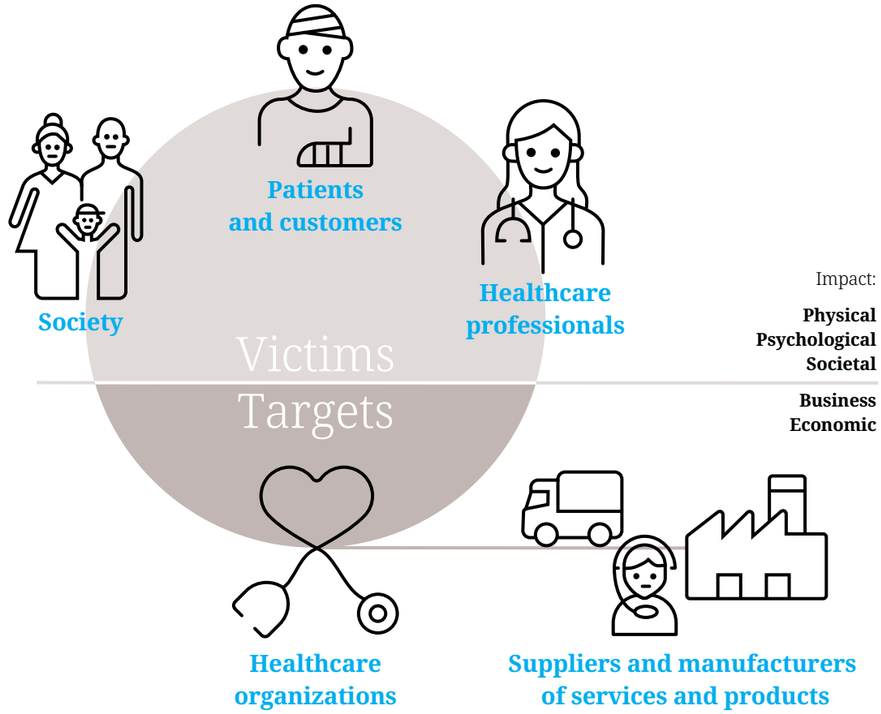
[5] A further 603 primary care and other NHS organizations, including 595 General Practitioner practices were affected.

2 What is the real impact of attacks on healthcare?

"The fact that someone, somewhere knows about my emotions and can read my intimate files is disturbing, but this also affects my wife and children [...] While I do not have long left in my life, what happens if someone uses my personal data after my death? There's nothing I can do about it."

A patient expresses concerns after the public announcement of the data breach at the Vastaamo Psychotherapy Center, Finland, September 2020 (Name Anonymised, 2020).

Figure 3: Victims and targets of attacks on healthcare
Source: The CyberPeace Institute 2021



2.1 A diversity of victims – the people

The victims of attacks are most often referred to as the target healthcare facilities, organizations, companies or services whose data or infrastructure was compromised. The reality is that the long-term victims of attacks are much broader in range than the original target and the impact of attacks is far reaching (see Figure 3). The direct impact of attacks on all entities within healthcare is often reported in numbers and figures but the indirect impact of these attacks on those affected by the theft of data or downtime of systems is best captured by those individuals on the front line.

> "All of our cathlabs[6] except for one are down and our sister hospital has no cathlabs. They are transferring patients to our facility. No anesthesia services. It took out the outpatient offices as well. I'm here trying to figure out how to find out what's going on with my patients."
>
> In the immediate aftermath of a ransomware attack on Universal Health Services, USA, 29 September 2020 (Name Anonymised, 2020).

Healthcare professionals are direct victims of disruptive attacks that impact their capacity to provide patient care – Not only are they held to ransom by the need to maintain operational capacity to save lives but they also suffer from the physical and psychological burdens of being in an incident response situation following an attack. Those on the frontline also suffer from the torrent of disinformation that undermines the public's trust in their efforts to provide healthcare.

Patients suffer directly and indirectly from attacks on the services designed to care for them – First and foremost, there is a direct threat to patient safety that results from any system downtime that causes a delay in their receiving medical care and treatment, notably when hospitals are targeted in ransomware attacks. Second, patients are victims of the theft and unlawful disclosure of their personal health information following a data breach, the indirect impacts of which are often long-standing.

[6] Catheterization laboratory

Spotlight 2

Psychotherapy center victim of major data breach

Date: November 2018 | March 2019	**Location**: Finland	**Target Type**: Medical Service Provider

Victims, **Targets and Impact**: In September 2020, the Vastaamo Psychotherapy Center was extorted by a threat actor with data that had been stolen in November 2018 and March 2019. Vastaamo runs 25 therapy centers across Finland. The records of approximately **36,000 patients**, **including juveniles**, **were stolen** (Kirp, 2020). These records contained highly sensitive personal health information, including information on therapy sessions of vulnerable patients (Yle, 2020), as well as the healthcare professionals who had treated them. As of November 2020, **over 25,000 victims had filed criminal complaints** (Rikosuhripäivystys, 2021).

Attack Method: The details of the data breaches have not been publicly disclosed but Vastaamo has admitted to vulnerabilities and data security shortcomings resulting in the data breach (Psykoterapiakeskus Vastaamo, 2021). The threat actor did not contact Vastaamo until September 2020, when they demanded a ransom payment of 40 Bitcoins (est. EUR 450,000).

On October 21, after Vastaamo had refused to pay the ransom, the threat actor began publishing batches of 100 patient records per day on underground forums, requesting patients to pay EUR 500 to have their records removed (Kärkkäinen, 2020). On October 24, Vastaamo reported that patients and employees were receiving extortion emails, requesting payment to prevent data from being published online (Psykoterapiakeskus Vastaamo, 2021).

Attribution and Response: As of this writing, no public attribution has been made. It remains unclear whether the threat actor(s) who breached Vastaamo and requested ransom payment from Vastaamo and/or patients are the same.

In Finland, discussions have emerged in relation to the securing of Vastaamo's systems following the breaches in 2018 and 2019. Public concerns were also raised about the one-month delay in Vastaamo reporting the breach to police, and to the breach becoming known to victims only after their data had been published. Following the attack, Vastaamo dismissed its CEO in October 2020 (Teivainen, 2020). This is a first step in the accountability process, while criminal (Muurman, 2020) and data protection (Råman, 2020) investigations currently underway could help to close the remaining accountability gap. In the wake of the attack, the Finnish Government has tabled laws and measures to secure databases and sensitive information held by organizations offering social and healthcare services (O'Dwyer, 2020).

Beyond the healthcare professionals and patients who are direct victims of attacks on healthcare, the accumulation and escalation of these attacks casts a much wider net in which society as a whole becomes their victim.

For every attack on healthcare there is an impact on society – Society globally is an indirect victim of attacks on healthcare as everyone at some point in their lives seeks medical treatment. An attack on healthcare is thus an attack on society as a whole, and more specifically on vulnerable persons in need of medical treatment. Ultimately, society as a whole suffers the consequences of an erosion in the security and credibility of the healthcare sector. This creates risks to life and public health, notably through inequitable access to care, and a digital divide between those who can access/finance safe and secure healthcare and those who cannot.

2.2 A typology of targets – healthcare organizations

> "We are attacked every day, it varies between twenty and a hundred times [...]. We even have days with 400 attacks. Yet we are a small establishment."
>
> The scale of the problem is described by the head of IT following a cyberattack on the Centre Hospitalier de Narbonne, France, 10 December 2020 *(Lherbette, Hélène; Centre Hospitalier de Narbonne in Causit, 2021).*

Targets come from highly diverse environments ranging from hospitals and medical service providers, biomedical research institutes, universities, government health ministries, international organizations, manufacturing, pharmaceutical companies including vaccine makers, health insurance entities, and civil society around the world (see Figure 4). It goes without saying that healthcare systems around the world differ significantly in terms of resources, business models and their stage of digitalization. A recent report by the CTI League specific to healthcare (see Section 7.2) reported that "nearly two-thirds of healthcare cybercrime victims were in North America and Europe, with **victims in every populated continent**" (Zaidenberg, 2021)**.**

The impact on healthcare targets is often the most visible in the form of financial costs, system downtime and volume of data losses as they are more easily measurable. Other facilities may be impacted indirectly as they assist during an incident response to provide the necessary services during operational downtime.

Suppliers, manufacturers and vendors of healthcare products and services have played and continue to play a critical role in the healthcare sector's degree of resilience to cyberattacks. This was demonstrated through the recent attacks on COVID-19 vaccine makers and testers. Vulnerabilities in their own products or software may also lead to compromises among healthcare service providers through a supply chain attack.Depending on the typology of the threat actor and their motive(s), the direct impact on these targets and the wider community they service also varies. By grouping healthcare into sub-sectors, it becomes clear that all entities are at risk of attack by various threat actors and the impact cannot be underestimated. The following table shows a small number of attacks grouped by sub-sector to illustrate the impact of different attack types, conducted by different threat actors, on the healthcare sector.

Figure 4: A sample of attacks on healthcare in 2020
Source: The CyberPeace Institute 2021

Jan-20
USA
1 **Moderna**
Cyberespionage

Mar-20
United Kingdom
2 **Hammersmith Medicines Research**
Ransomware

Mar-20
Switzerland
3 **World Health Organization**
Spear-phishing

Apr-20
China
4 **Huiying Medical Company**
Data Breach

Apr-20
China
5 **Ministry of Emergency Management**
Spear-phishing

Jun-20
South Africa
6 **Life Healthcare**
Disruptive Attack

Jul-20
Brazil
7 **Hapvida**
Data Breach

Aug-20
USA
8 **Northern Light Health Foundation**
Data Breach

Sep-20
USA
9 **Universal Health Services**
Ransomware

Sep-20
Georgia
10 **Health Ministry, The Richard Lugar Centre**
Disinformation Operation

Oct-20
India
11 **Dr Reddy's Laboratories**
Ransomware

Dec-20
Netherlands
12 **European Medicines Agency**
Disinformation Operation

Sub-sector	Attack target	Direct impact	Attack type | Threat actor typology
Hospitals and Medical Service Providers	2020 | USA Universal Health Services	All systems were disconnected and networks shut down to prevent propagation at **250 care sites and hospitals** (see Spotlight 6)	Ransomware | Cybercriminal
	2020 | South Africa Life Healthcare	**Disrupted company operations in southern Africa for over a month** including patient billing, aid claims submissions, invoice processing	Disruptive Attack | Unidentified Threat Actor
	2018 | Singapore SingHealth	Exfiltration of **1.5 million patient records** (The Committee of Inquiry, 2019) (Symantec, 2019)	Cyberespionage | State Actor
	2018 & 2019 | Finland Vastaamo Psychotherapy Center	Theft and circulation online of **36,000 patient records** containing extremely sensitive and confidential information (see Spotlight 2)	Data Breach | Cybercriminal
Bio-medical Research Institutes, Universities	2020 | United Kingdom Hammersmith Medicines Research	IT systems and emails disrupted for one day and the theft and leakage of sensitive data of **2,300 former patients** (Jay, 2020)	Ransomware | Cybercriminal
Government Health Ministries	2020 | Georgia Health Ministry, The Richard Lugar Centre	Theft, leak and **falsification of documents** and important information on the management of the COVID-19 pandemic (IDFI, 2020)	Disinformation Operation | Unidentified Threat Actor
	2020 | China Ministry of Emergency Management	**Intelligence gathering** during the early stage of crisis management following the pandemic (see Spotlight 7)	Spear-phishing | State Actor
International Organizations and Regulatory Bodies	2020 | Switzerland World Health Organization	Attempt to steal **the credentials of WHO employees** (Ferguson and Venkat, 2020)	Spear-phishing | Unidentified Threat Actor
	2020 | Netherlands European Medicines Agency	Theft and **manipulation of confidential data** relating to agency's approval of a COVID-19 vaccine that was later leaked and disseminated on underground forums (Var Group, 2021) (see Spotlight 5)	Disinformation Operation | Unidentified Threat Actor
Manufacturing[7]	2020 | China Huiying Medical Company	Theft and leak of **source code** for AI-assisted COVID-19 detection and experimental data (Paganini, 2020)	Data Breach | Cybercriminal
Pharmaceutical Companies[8]	2020 | India Dr Reddy's Laboratories (vaccine developer)	Forced to **temporarily shut operations at its key plants in the USA**, **UK**, **Brazil**, **India**, **and Russia** following ransomware attack with suspected data leakage shortly after approval of COVID-19 vaccine trial (Jay, 2020)	Ransomware | Cybercriminal
	2020 | USA Moderna (vaccine developer)	Victim of **information reconnaissance** activities potentially linked to the development of the COVID-19 vaccine (Bing and Taylor, 2020)	Cyberespionage | State Actor
Health Insurance	2015 | USA Anthem Blue Cross	**78.8 million patient records** stolen (Johnson *et al.*, 2017)	Data Breach | State Actor
	2020 | Brazil Hapvida	Potential **unauthorized access to customer registration data** such as name, address and taxpayer identification number (HAPVIDA, 2020).	Data Breach | Unidentified Threat Actor
Civil Society	2020 | USA Northern Light Health Foundation	Theft of personal data from over **657,000 donors** / **patients** following a compromise of Blackbaud's servers (database host) (Davis, 2020b)	Data Breach | Cybercriminal

2.3 A variety of impacts on victims and targets

> "We need governments to consider the damage to civilians that comes from hoarding these vulnerabilities and the use of these exploits."
>
> Microsoft's president addressing accountability following the WannaCry Attack on the National Health Service, United Kingdom, 12 May 2017 *(Smith, Brad; President of Microsoft in The Guardian, 2017).*

There is a tendency today to measure the impact of cyberattacks in terms of the economic cost suffered by the direct target. Ransomware payments, regulatory penalties, reputational damage and digital forensic investigation costs are measurable impacts of cyberattacks. The impact on people, both physical and psychological, as well as on organizations and society is not always immediately obvious and it is often the less visible impacts that cause long-standing harm. Any progress towards attaining cyberpeace

[7] Including: Medical Equipment and Supplies Manufacturing; Electromedical, Electrotherapeutic and X-Ray Apparatus Manufacturing; and Healthcare Product Manufacturing

[8] Including: Biopharmaceuticals & Biotherapeutics Manufacturing and Pharmaceutical Manufacturing

requires a focus on the well-being of human beings to ensure that human security, dignity and equity are respected in the digital ecosystem of the healthcare sector.

The direct and indirect human impact of attacks on healthcare

Patients	Healthcare professionals	Society
Delay in patient care Endangering lives Reduced patient safety Redirection to other facilities Inaccessibility of medical records and tests results	Stress and anxiety associated with incidence response Lack of access to medical devices and records Revert to pen and paper	Erosion of trust in the healthcare sector – from hospitals to regulatory bodies and vaccine developers to public health authorities – associated with: • handling of data confidentiality • vulnerabilities exploited in code, software and hardware • spread of disinformation • low rate of prosecution
Fear and sense of lack of control Public release of personal information > risk of identity theft Loss of trust in the security of personal information		

Physical impact on people

"We found that hospitals that had been breached, post-breach, over the next two, three years, saw increases in the 30 day mortality rate for their patients. And also that the time that it required to get an EKG increased in some cases by more than two minutes. And two minutes is a big deal when you're suffering a heart attack."

Vanderbilt University research findings on relationship breach remediation efforts and hospital care quality in 2019 *(Johnson, Eric; Dean at Vanderbilt Owen Graduate School of Management in BitSight, no date).*

Disruptive attacks on healthcare service providers cause delays and interruption to patient care that endanger lives.

Patient care is affected as services and appointments are delayed (CNBC, 2020), suspended, postponed or cancelled (McMillan and Evans, 2020), and patients are redirected and ambulances re-routed to other facilities (Silomon, 2020) For example, following an attack on the Brno University Hospital, Czech Republic in 2020, several patients had to be transferred to other hospitals and surgeries had to be cancelled (Khalili, 2020).

Thus far during the COVID-19 pandemic, anecdotal evidence of network disruptions linked to cyberattacks on healthcare facilities indicates that any downtime slows care services and affects not only the medical staff and patients but also their families.[9] For example, when a COVID-19 testing center or laboratory is under attack, having to repeat the test for accuracy places a psychological and potentially life-threatening burden for victims at a vulnerable time.

A study by Vanderbilt University found that hospitals that had been breached required more time – sometimes years after the breach – to provide a patient suffering from chest pain with an electrocardiogram (EKG) after their arrival. The study also reported that the mortality rate for those patients at those hospitals also increased (Choi, Johnson and Lehmann, 2019).

In cases of ransomware attacks on hospitals, their ability to secure patient safety and care may be jeopardized if computer networks go down. Losing access to medical records and life-saving medical devices affects the ability of healthcare professionals to effectively care for their patients and administer medicine in times of need (Snair and Henry, 2013).

Attacks can also impact society when healthcare providers are forced to close their doors permanently in their aftermath. For example, Wood Ranch Medical clinic in the USA closed its doors in December 2019 after a ransomware attack led to the loss of all its patients' records (Drees, 2020). The closure of one facility will inevitably shift patients to other facilities. Such an immediate shortage of hospital beds can have a detrimental effect on the capacity to provide adequate healthcare, especially during a crisis such as the COVID-19 pandemic (Zhou *et al.*, 2020).

Patient safety is compromised when medical devices and data are inaccessible or altered as a result of disruptive attacks.

"All possible cancellations have been done. We have problems with radiotherapy sessions and oncology [...] because of the problem with knowing the patient's file. [These] will also be redirected to all the hospitals in the region or nearby."

A plea for assistance from the chairman of the hospital supervisory board the day after a ransomware attack on Dax Hospital, France, 9 February 2021 *(Translated from French – Dubois, Julien; Chairman of the Supervisory Board of Dax Hospital in Mayer, 2021).*

[9] Little research is available on the psychological impact of cyberattacks on patients and society.

An attack on hospitals and medical service providers can cause the obstruction of access to patient files or imaging records (CNBC, 2020). This poses challenges to healthcare professionals in administering treatment and seeking to provide the best care possible to patients (WSJ, no date).

Depending on the threat actors' intentions, access to sensitive and personal patient records could result in data exfiltration and unlawful sharing / sale, or alteration of the data, which could result in serious effects to patient health and safety (Riggi, 2020). With an increasing attack surface, notably from connected medical devices and Internet-of-Things devices (see Section 1.3), concerns arise with regard to the impact on patient safety in the cases where critical medical devices (e.g. infusion pumps and CT scanners) would be directly targeted in an attack (Slabodkin, 2020).

Psychological impact

Perhaps the most challenging impact to measure is the psychological impact on those affected directly or indirectly by an attack and it should not be underestimated. Research, although not always specific to attacks in healthcare, is starting to emerge but has a long way to go before it becomes a mainstream consideration in the analysis of cyberattacks on healthcare.

Healthcare professionals experience increased levels of stress and anxiety in the current cyber threat landscape.

Research has demonstrated that an unexpected shutdown of a hospital information system imposes significant stress upon healthcare professionals providing trauma patient care and noted that those who are digital natives in particular lack the adaptability to handle a paper-based workflow (Zhao *et al.*, 2018). The study recommends that with cybersecurity threats on the rise in healthcare, "preparedness should be included in the graduate medical education curriculum."

Stress and anxiety linked to cybersecurity issues

Studies of the impact of attacks on non-healthcare organizations also shed light on the stress and anxiety borne by professionals. (Sungard Availability Services, 2019) "[...] research has identified a new resilience imperative, which is the personal impact on the individuals involved. Many business leaders suffer from stress-related illness or damage to their mental wellbeing when disruption [from cyber attacks, IT outages and network failures] happens, which also affects their family and friends." (Schneider, Kathy; CMO at Sungard Availability Services, 2019). In addition, constantly working in a state of high alert to secure full operational activities against cyber threats may result in long-term effects on a person's mental health and well-being as stress, anxiety and eventually burnout accumulate. This has the potential to impact the way an organization responds to incidents ('The Impact of Cyberattacks – Podcast', no date).

Fear and a sense of coercion, lack of control and powerlessness prevail when ransom demands are made of healthcare professionals and patients.

> "People felt a loss of control [...] as the threat was so pervasive and the only option for recovery – assuming no recent backups were made – was to pay the ransom."
>
> *(Bada and Nurse, 2019)*

Ransomware attacks on healthcare, in which a target organization or its patients / customers are coerced into paying a ransom to decrypt their files, unblock their systems or destroy stolen data, are crimes that are psychological in nature. Threat actors prey on the fear and vulnerabilities of their target to extort payment. As explained in Section 3.1, ransomware is constantly evolving but fear remains at the heart of its success (TrendMicro, 2016b).

Victims of identity theft can experience feelings of violation, betrayal, vulnerability, anger and powerlessness (Kirwan and Power, 2011). When ransomware operators leak sensitive information, cybercriminals find opportunities to engage in identity theft leading the re-victimisation of those whose data was originally stolen. Also of great concern are the implications of the theft of highly sensitive data such as medical records relating to HIV and substance abuse, which if leaked online can have significant adverse consequences for the patients. For example, a significant leak of confidential data of 14,200 people with HIV from Singapore's HIV registry in 2019 led to the fear of losing employment, being ostracised or receiving messages of hate (ET CISO, 2019).

An erosion of trust in the healthcare sector arises when patients' data is breached.

Data stolen from healthcare organizations often contain personal medical information, clinical trial data, and other private details. Thus, healthcare data breaches may result in distrust towards the healthcare provider's ability to protect the privacy of patient data as the exposure of such data can have long-term consequences for the victims (Snair and Henry, 2013). Likewise, it can lead to distrust of the sector as a whole. In an online survey conducted by the CyberPeace Institute in 2020 in Kenya, Namibia and Botswana, 82% of participants reported that they did not feel confident sharing personal data with their hospital. A special risk is posed by medical devices that have become increasingly networked and connected to patient data, thus jeopardizing confidentiality if the devices were breached (Snair and Henry, 2013).

Attacks impacting supply chains destabilize confidence in the healthcare sector's technical environment.

"Failure to protect the ability to trust software could cripple the benefits gained from it."

(Herr et al., 2020)

Cyberattacks against the healthcare supply chain can magnify the scale and impact of attacks on healthcare by disguising malicious code as trusted products to reach a wider array of targets. Although not specific to healthcare, the 2020 supply chain attack using malicious SolarWinds files potentially gave threat actors access to target networks. The attack highlights the reach of such attacks as it affected over 18,000 potential customers of which many were US government agencies (SEC, 2020). There is an underlying expectation of trust in the software or hardware that organizations acquire; threat actors abuse this trust. Thus, supply chain attacks sow distrust among organizations but also distrust in widely used open-source projects. They also destabilize the confidence in the core of an organization's technology stack as components are compromised (Herr *et al.*, 2020).

Societal impact

"I think through COVID we've understood much more how various actors may be using the opportunity with more people online, more people fearful, to erode trust in experts, in institutions, in people between themselves."

(Schaake, Marietje; President of the CyberPeace Institute in Schaake, 2020)

Attacks on healthcare erode trust in and within the sector and among the authorities meant to protect it.

"Underreporting cybercrime – even when disclosure is legally mandated – appears to be the norm."

(Touhill, Gregory J.; Board Director of ISACA in BusinessWire, 2019)

Cyberattacks against healthcare lead to a plethora of indirect impacts, but first and foremost they fuel digital distrust not just at an individual level but sector-wide and in society. In Cyber 4 Healthcare, the CyberPeace Institute's match-making initiative between cybersecurity companies and organizations in the fight against COVID-19, most beneficiaries handling clinical trial data shared deep concerns for their ability to protect such data, over the negative impact of personal data breaches for those they work with, and for their operating model.

The various tactics and techniques used to target the healthcare sector have a common motif, to "erode trust and to undermine liberal democracy" (Schaake, 2020). The difficulty in attribution of cyberattacks and a general lack of prosecution (NCA, 2018) of threat actors has an impact on the likelihood of victims reporting incidents to law enforcement (Swinhoe, 2019). With a loss of trust and skepticism in the ability of authorities to assist victims and the associated under-reporting of attacks (Europol, 2020), the actual scale of attacks against the healthcare sector is unknown. This hinders the assessment of the real impact of cyberattacks and the proportionate investment of resources to tackle the challenges at a technical, ethical, judicial and normative level.

Disinformation operations instill fear and cause confusion and harm.

"Part of the authentic documentation obtained as a result of illegal access into the computer system has been uploaded on a foreign website and is available to the public. However, the website has also uploaded obviously falsified documents, which are deliberately falsified in order to intimidate and confuse the public."

The Ministry of Internal Affairs of Georgia describing the motives behind a disinformation campaign against the Richard Lugar Public Health Research Center, Georgia, 1 September 2020 *(Georgian Ministry of Internal Affairs in Agenda.ge, 2020).*

The climate of fear and uncertainty that cyberattacks and digital distrust create are fertile ground for disinformation and misinformation campaigns that further undermine the trust that people place in organizations. The impact of such campaigns, especially during a global pandemic, can have significant consequences on society including mistrust in government responses, the perpetuation of transmission of the virus, violence against healthcare professionals and false about the origin of the disease which in turn can affect the public's decision to seek treatment (Bernard *et al.*, 2020). Other consequences for society include undermining the local and global responses to the COVID-19 pandemic and public health crises in future, and the politicization of scientific institutions, practitioners and researchers (Hunt, 2020).

"With the ice and snow storm at hand, coupled with one of the worst flu seasons in memory, we wanted to recover our systems in the quickest way possible and avoid extending the burden toward other hospitals of diverting patients. Restoring from backup was considered, though we made the deliberate decision to pay the ransom to expedite our return to full operations."

Chief Executive Officer of Hancock Regional Hospital on the rationale for paying ransom following the ransomware attack on the hospital, USA, 11 January 2018 *(Long, Steve; CEO of Hancock Regional Hospital in Campus Safety Magazine, 2018).*

The economic cost of cyberattacks on healthcare is staggering and continues to rise. In their 2020 report, IBM reported that healthcare companies continued to incur the highest average breach costs at USD 7.13 million – an increase of over 10% compared to 2019 (IBM, 2020).

For years after an attack, targets and victims will endure significant yet less tangible costs that are complex to measure.

Despite the availability of some estimations regarding the economic costs of breaches in the sector – GBP 92 million to the National Health Service in the United Kingdom following the WannaCry Attack in 2017 – the true financial impact and cost of cyberattacks across the sector globally are unknown.

A study by IBM Security and Ponemon Institute in 2019 examined the financial consequences of a data breach and reported an average of 67% of data breach costs were realized within the first year after a breach, 22% accrued in the second year and another 11% accumulated more than two years after (IBM, 2019). In a separate study that showed similar long-term impact trends (see Figure 5), Deloitte mapped the costs incurred by a US technology manufacturer at various phases of response to a data breach in which intellectual property was stolen by a nation state (Deloitte, 2016).

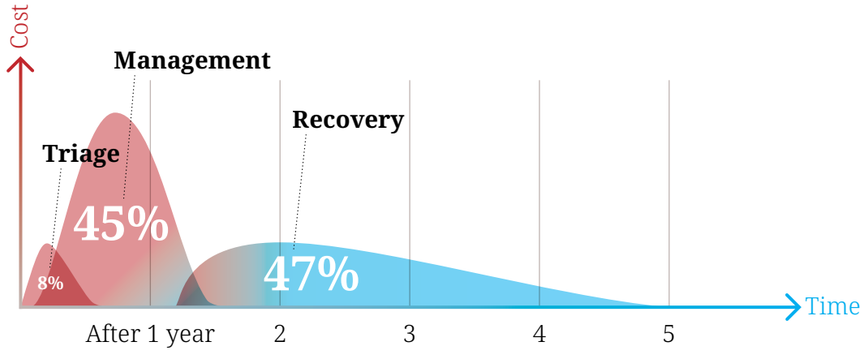


Figure 5: The long-term costs of a cyberattack
Source: (Deloitte, 2016)

The events that took place in this scenario are not dissimilar to the events and economic impact that would follow the theft of intellectual property relating to a vaccine or other sensitive medical research data. Below is a snapshot of some of the visible and less visible costs of an attack on healthcare of which only some may be applicable, depending on the type of attack and target.

Visible costs	Less visible costs
• Ransom payment	• Operational disruption
• External technical and digital forensics support	• Loss of business contracts
• Cyber risk assessment	• Loss of intellectual property
• Cybersecurity improvements	• Reduced growth
• Public relations	• Reputational damage leading to brand devaluation
• Legal fees and litigation	• Loss of value of customer / patient relationships
• Regulatory compliance (fines / penalties)	• Erosion of trust in the organization
• Patient / customer protection	• Insurance premium increases
• Patient / customer notification	• Loss of competitive advantage

Ransom demands following a ransomware attack on the healthcare sector in the US are anywhere between USD 1,000 and USD 14 million but beyond this immediate cost if the ransom is paid, the majority of hospitals attacked with ransomware will also suffer some downtime ranging from a matter of hours to weeks on end (Bischoff, 2020).

Following a disruptive attack in August 2020, Life Healthcare – the second-largest private hospital operator in South Africa – described how the attack impacted the business: "the manual backup processes, brought into effect as a result of the attack, impacted the ability of the southern African operations during the month of June and part of July 2020 to complete patient billing, submit claims to medical aids, process supplier invoices and produce financial results." (Mungadze, 2020)

The business and economic impact of attacks on healthcare plays out for several years after the attack itself. Following an attack, in addition to suffering from costly and time-consuming disruption, an organization must invest in repairing and improving its systems, but also re-train employees and manage damage to its reputation (TEC, 2018).

To pay or not to pay – weighing the impact of ransom payments.

In the immediate aftermath of a disruptive ransomware attack, the priority of critical services such as hospitals is to ensure patient care. Unlike in other sectors, this brings about additional considerations in the decision making process when trying to return operations to normal levels if backups are not available or have also been encrypted in the attack. The CEO of the Hollywood Presbyterian Medical Center best illustrates this when he said the "quickest and most efficient way to restore our systems and administrative functions" was by paying a ransom of USD 17,000 (see Spotlight 4). In a 2020 study on ransomware attacks in the healthcare sector, RiskIQ found that 16%of targeted organizations disclosed paying the ransom (RiskIQ, 2020).

A USadvisory highlights the sanction risks associated with ransomware payments – "companies that facilitate ransomware payments to cyber actors on behalf of victims, including financial institutions, cyber insurance firms, and companies involved in digital forensics and incident response, not only encourage future ransomware payment demands but also may risk violating OFAC[10] regulations" (U.S. DoT, 2020). Notwithstanding the legal repercussions associated with paying a ransom, research indicates that encryption keys may not be released by the threat actor (FBI, 2016), further ransoms may be requested or data leaked despite the ransom being paid (Coveware, 2020).

[10] U.S. Department of the Treasury's Office of Foreign Assets Control

3 How are attacks unfolding and evolving?

On account of the vital responsibility that it bears, the data that it holds, and its strategic positioning in recent years, notably during the COVID-19 pandemic, the healthcare sector is the target of three main types of attacks:

- **Disruptive attacks**: Healthcare organizations have been hit by both targeted and indiscriminate disruptive attacks. Botnets, DDoS and remote code execution have all been used against healthcare facilities (Bracken, 2021) but ransomware is the most disruptive. By encrypting systems and files and holding healthcare professionals to ransom, ransomware attacks have a significant impact on healthcare professionals' capacity to deliver vital services.

- **Data breaches**: Healthcare data such as medical records have long been monetized through their sale on underground markets, extortion, and other fraudulent activities. The COVID-19 pandemic has elevated the strategic value of healthcare data related to the pandemic response and associated medical research.

- **Disinformation operations**: Healthcare organizations have been at the center of cyber-enabled information operations, which comprise the exfiltration, manipulation, and dissemination of information. Such attacks, be it deliberately or as collateral damage, undermine the public trust in healthcare and the pandemic response.

While this typology of attacks can be broadly linked to specific threat actors, they are not exclusively so linked. Cybercriminal and state actors adopt and adapt attack types that are most suited to accomplish their monetary and strategic objectives.

Spotlight 3

Medical center pays ransom after computers go offline for a week

Date: February 5, 2016

Location: USA

Target Type: Hospitals and Medical Facilities

Victims, **Targets and Impact**: Following a ransomware attack in February 2016 at the Hollywood Presbyterian Medical Center (HPMC), the president and CEO at the time reported that the attack did not affect the delivery and quality of patient care. Nevertheless, the media reported several stories of patients having to travel long distances to other facilities and employees resorting to pen and paper. The computers were offline for 10 days and HPMC ended up paying a ransom of 40 bitcoins (USD 17,000 at the time) to obtain the decryption key and restore normal operations indicating that the organization suffered both business and economic impact as a result of the attack (Barrett, 2016).

Attack Method: The hospital's computer system was accessed without authorization and the SamSam ransomware was deployed leading to the encryption of the computers (U.S. District Court, 2018).

Attribution and Response: On November 28, 2018 two individuals were indicted for their involvement in the conspiracy to commit fraud, conspiracy to commit wire fraud, cause intentional damage to a protected computer and other offences against 200 victims (corporations, hospitals including Hollywood Presbyterian Medical Center (HPMC), universities, and government agencies) (U.S. District Court, 2018).

In parallel, the US Treasury Department took action against two other individuals who helped exchange bitcoin ransom payments into fiat currency on behalf of the aforementioned threat actors (U.S. DoT, 2018). This was the first time the Office of Foreign Assets Control publicly attributed digital currency addresses to designated individuals and imposed compliance requirements with the aim of limiting future transactions. This case highlights the important role that financial analysis plays in the attribution of ransomware attacks.

Information provided by the United Kingdom (notably digital forensic evidence) was instrumental in the charges. As stated by Mark Stirling, of the National Crime Agency's National Cyber Crime Unit "It demonstrates once again that this form of crime does not recognise international borders, so it takes an international law enforcement response to bring the perpetrators to justice" (NCA, 2018).

3.1 Disruptive attacks – ransomware's evolving threat to healthcare

Ransomware (see Figure 6) has become the weapon-of-choice against healthcare organizations (Bracken, 2021). In October 2020 alone, ransomware attacks against US healthcare facilities increased by 71% (Check Point Software, 2020), underscoring both the profitability of ransomware attacks against healthcare targets (Al Qartah, 2020), and the sector's vulnerability towards them. Attacks against the healthcare sector rose by 45% from November 2020 until January 2021 – almost double the increase recorded in other sectors (Check Point Software, 2021); ransomware accounts for a majority of these attacks.

Double extortion

Since November 2019, ransomware operators have adopted a new tactic in their attacks. Double extortion attacks (see Figure 6) do not merely encrypt a target's files and demand a ransom in exchange for a decryption key, they also exfiltrate sensitive data. An additional element of extortion may be introduced when a threat actor leaks this data on a public site. Likewise, double extortion **enables the extortion of targets even if they are able to recover their systems** through data backup (Coveware, 2020). An estimated **50% of ransomware attacks on all sectors use elements of double extortion** (Coveware, 2020). From November 2019 to February 2021, five known ransomware operators used double extortion tactics and leaked data of at least 35 healthcare organizations, including urgent care facilities, pharmaceutical companies, and hospitals.

Cybersecurity researchers asked various ransomware operators whether they would continue targeting the healthcare sector throughout the pandemic (Abrams, 2020a). Even though some ransomware operators vowed not to target hospitals, all of those contacted have attacked healthcare organizations involved in the COVID-19 response (Abrams, 2020a). This may partially be due to their definition of legitimate targets. For example, certain ransomware operators justified targeting pharmaceutical companies with the reasoning that they "benefit from the current pandemic" (Abrams, 2020a).

The stolen data market

When attack targets fail to pay ransom demands, the ransomware operator will publish the stolen data on a dedicated dumpsite as punishment for "non cooperation." In 2020, at least **20 major ransomware operators hosted their own dumpsites** (Cimpanu, 2020a), of which nearly half have targeted healthcare. Such healthcare dumps can contain up to **600 GB of data**, **including sensitive information such as medical records**. To raise the potential stakes of double extortion, threat actors sometimes advertise the leaks on the surface web through social media accounts and advertisements (Krebs, 2020) as well as dedicated websites. Some healthcare dumps have had over 25,000 views in a matter of months (CyberPeace Institute research, 2020)**.**

While the data of some healthcare organizations is available in their entirety and for free, some ransomware operators publish only a portion of the data. The rest is then often sold or auctioned separately. The sale and auction of data is not the only data monetization method. In some cases, targets that had already paid were re-extorted or had their data leaked nevertheless (Coveware, 2020). Even when targets were provided with "proof of deletion," these files were fake, hinting at a **retainment of the data for future monetization** (Coveware, 2020).

Ransomware attack

The threat actor

Enters the network through a phishing email or RDP compromise

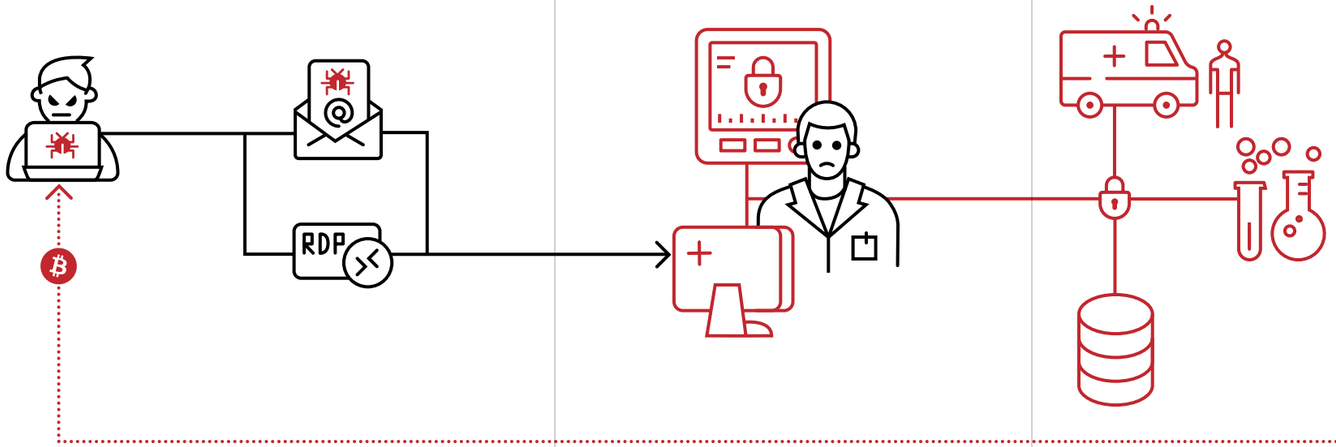
The victim

A simple click or point of vulnerability can substantially disrupt entire healthcare services

The impact

The ransomware encrypts files, preventing access to medical records and applications.

A ransom demand is made in exchange for a decryption key



Recovery

The attack is mitigated.

Backup storage allows files to be restored

Ransom payment

A ransom is paid.

There is no guarantee the victim will receive a decryption key or not be re-victimized

Double extortion

The criminal ecosystem

Ransomware operators and affiliates collude under a RaaS business model

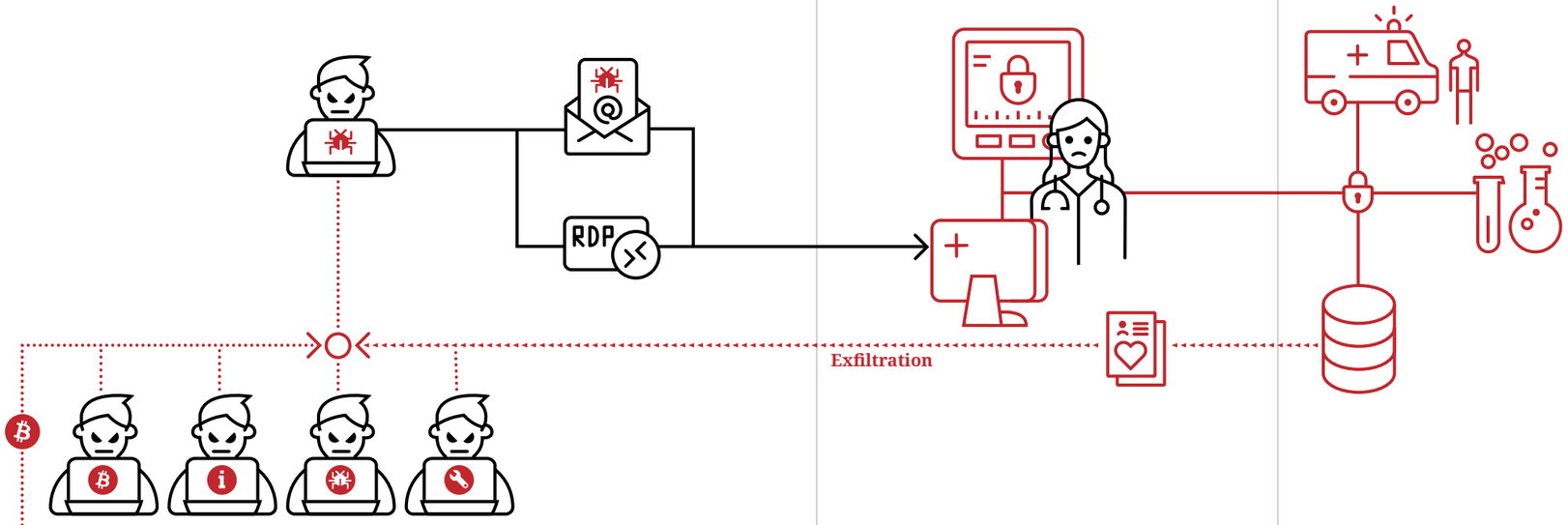
The victim

Using double extortion tactics, data is exfiltrated before the ransomware is deployed

The impact

The ransomware encrypts files, preventing access to medical records and applications.

The threat actor demands money in exchange for a decryption key and threatens to leak the data



Recovery

Backup storage allows files to be restored but the threat remains

Ransom payment

A ransom is paid. There is no guarantee the victim will get a decryption key or not be re-victimized

Data leak

The data is posted on a dumpsite.

The data can later be monetized through further exploitation

Figure 6: Ransomware attack and double extortion
Source: The CyberPeace Institute 2021

The criminal ecosystem

The widespread adoption of the Ransomware-as-a-Service (RaaS) business model has enabled the purchase of ransomware packages on the darknet for as low as USD 40 and up to thousands of USD (zvelo, 2020). Thereby, RaaS has allowed less capable threat actors to conduct ransomware attacks (TrendMicro, 2016a). Likewise, threat actors have been selling access to compromised systems on the darknet including Remote Desktop Protocol (RDP) endpoints of healthcare organizations (Nuspire, 2020). In 2020, ransomware operators constituted the majority of clients of these so-called RDP shops, with some even working exclusively for them (Cimpanu, 2020b).

Major ransomware operators have established so-called affiliate programs, which have been identified as a particular threat to healthcare organizations (Microsoft 365 Defender Threat Intelligence Team, 2020). To join these programs, potential affiliates often have to undergo strict vetting processes, which can include interviews and showing of previous work and payments (Abrams, 2020b). Affiliates are responsible for carrying out the attack (e.g. infiltration and data exfiltration) for 70-80% of the ransom payout (Gatlan, 2020a); the ransomware operator conducts the negotiations, maintains the ransomware, and provides the data extortion infrastructure (Seals, 2020). According to a prominent ransomware operator, this model has enabled one of its affiliates to increase its earnings from approximately USD 25,000 per target to about USD 7.5 million in only six months (Intel 471, 2020a).

Triple extortion – a potential evolution targeting victims

While not a ransomware attack, the attack on the Vastaamo Psychotherapy Center nonetheless provides an example of a potential evolution of double extortion tactics, or what could be referred to as a sort of triple extortion (Ransomware 3.0). After Vastaamo refused to pay 40 Bitcoins (est. EUR 450,000), the attacker began to both leak the data on the darknet and **directly extort the data subjects**, namely the patients themselves. While some patients were prompted to pay EUR 500 to have the leak removed, others were extorted to not have their data published in the first place. A similar evolution of ransomware attacks could include the amplification of double extortion by combining ransomware with other attack types such as DDoS attacks (Vijayan, 2021).

Primary Attack Vectors for Ransomware Attacks

Email phishing and Remote Desktop Protocol (RDP) compromise constitute the two primary infiltration vectors for ransomware attacks. Their respective use depends both on the ransomware strain and on the size of the target organization. Whereas smaller organizations across all sectors were predominantly infiltrated via RDP compromise, larger organizations were mainly targeted via email phishing in Q4 2020 (Coveware, 2021).

Phishing Attacks

> "That's all it takes – one employee out of 14,000 clicking on the wrong link and your whole IT system can be paralyzed."
>
> *(Dickson, Eric; President and CEO of UMass Memorial Health Care in Bartlett, 2020)*

Phishing is the most commonly used social engineering tactic against healthcare targets, with nearly 60% of healthcare organizations reporting such attacks in 2020 (HIMSS, 2020). Threat actors have capitalized on the pandemic-induced fear by using COVID-19-themed lures in their phishing attacks (Recorded Future, 2020). To lend further credibility to these emails, threat actors have imitated organizations involved in the national and international pandemic responses (Kaspersky, 2020). The FBI has explicitly warned of such lures being used against healthcare targets (Gatlan, 2020b).

RDP Compromise

Whereas phishing attacks rely on human error and interaction, attackers may also access a healthcare target's networks via network misconfigurations. RDP enables connecting to a remote device over the internet (e.g. for maintenance), thereby often leaving it exposed and vulnerable to attacks. RDP compromise represents one of the most common infiltration vectors for ransomware attacks against healthcare (Microsoft 365 Defender Threat Intelligence Team, 2020) and remains a primary attack vector for specific ransomware operators that have been known to target healthcare (Coveware, 2021).

3.2 Data breaches – from theft to cyberespionage

The pandemic has been accompanied not only by an acceleration of ransomware attacks against healthcare but also by an increase in healthcare data breaches. According to the US Department of Health and Human Services (HHS), **healthcare providers experienced a total of 348 "hacking/IT incident" related data breaches in 2020 – a 39% increase from 2019** – with over 18 million individuals affected (U.S. DoHHS, no date).[11] In 2019, the HHS registered 250 such incidents, with 26 million individuals affected (see Figure 7). This trend is also reflected in the identifiable surge of advertised healthcare data on underground criminal markets, where the data is sold for immediate financial gain or as a potential access point for more lucrative victims (Zaidenberg, 2021).

[11] The data relates to breaches affecting 500 or more individuals. Filters were applied to select only 'hacking / IT Incidents' targeting healthcare providers, either under investigation or archived.

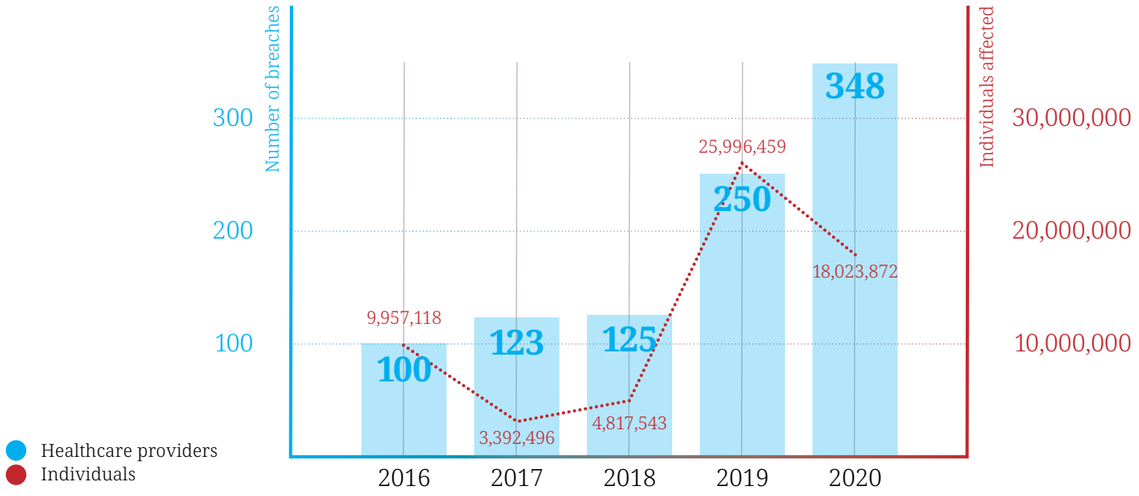


Figure 7: Breaches of protected health information, USA (2016–2020)
Source: The CyberPeace Institute 2021 sourced from data (U.S. DoHHS, no date)

While the increase in healthcare data breaches could be linked to the increase in remote work and a surge in telehealthcare due to social distancing measures, the pandemic has greatly amplified the value of COVID-19 related data. In April 2020, a threat actor was selling the source code of a COVID-19 detection technology from the Beijing-based Huiying Medical Technology firm (Cyble Inc, 2020). The offer included over 1GB of data and was being sold for 4 Bitcoins. One month earlier, Huiying Medical Technology claimed that its technology could detect COVID-19 from CT scans with 96% accuracy (Wiggers, 2020).

Just as the pandemic has increased the financial profitability of selling COVID-19-related data, it has also elevated its strategic value for state actors. Numerous state or state-sponsored actors have conducted cyberespionage over the course of the pandemic to fill information gaps (see an example in Spotlight 7). More recently, state sponsored threat actors were accused of targeting vaccine research data as part of the global vaccine race (Burt, 2020) such as the political attribution following the attack on Pfizer, the pharmaceutical company behind the Comirnaty vaccine (Shin, 2021).

Cyberespionage attacks have also been conducted against international organizations, notably the World Health Organization (WHO), which was targeted in a spear-phishing attack in 2020 whereby a malicious site disguised as the WHO internal email system was used to steal credentials of targeted staff (Ferguson and Venkat, 2020).

Spotlight 4

Suspected state-sponsored actors target COVID-19 drugmaker

Date: April, 2020

Location: USA

Target Type: Pharmaceutical Company

Victims, Targets and Impact: In April 2020, Reuters and cybersecurity researchers discovered a targeted campaign against Gilead Sciences (Stubbs and Bing, 2020). The pharmaceutical firm, producer of the antiviral drug Remdesivir, had just been authorized for emergency use against COVID-19. The impact of the campaign has not been publicly disclosed.

Attack Method: Through an analysis of internet archives, the researchers were able to identify fake email login pages that were targeted to steal the login credentials of top legal and corporate executives at Gilead Sciences (Stubbs and Bing, 2020). Other attack vectors included spear-phishing messages that impersonated journalists as well as password spraying attacks (Ajaz, 2020).

Attribution: Researchers claim to have linked the web domains and servers that were used in the attack to a nation state (Stubbs and Bing, 2020) while cybersecurity firms specifically attributed the infrastructure to Charming Kitten (APT35), a cyberespionage group from said nation state (ClearSky Security Ltd., 2020).

Supply chain attacks

With the increased digitalization of the healthcare sector, many of its services have been outsourced and the sector has become reliant on third-party vendors for software, cloud-based solutions, and medical devices (Rosario Fuentes and Huq, 2018). As such, **healthcare organizations have not only become dependent on their own cybersecurity practices but also on those of their suppliers**. As healthcare organizations often do not host their data but rely on co-shared Electronic Health Record (EHR) systems (TrendMicro, 2018), supply chain attacks offer an infiltration vector for data breaches (Rosario Fuentes and Huq, 2018). An estimated 32% of reported US healthcare data breaches were the result of compromises of business associates and third-party vendors (U.S. DoHHS, no date).

3.3 Disinformation operations – an erosion of trust

The COVID-19 pandemic has been accompanied by a so-called Infodemic, which refers to the ever-increasing volume of accurate and inaccurate information that is confronting society on a daily basis (WHO, 2020). With the healthcare sector already under significant strain, the proliferation of false and misleading information amid facts further threatens healthcare services and the pandemic response. Such virulent information environments have been linked to a heightened death toll during the 2014 Ebola Outbreak in West Africa (Allgaier and Svalastog, 2015) as well as to a wave of methanol poisonings across Iran (Islamic Republic of) with over 500 confirmed deaths (Shokoohi *et al.*, 2020).

While the unintentional spread of misinformation has contributed to the COVID-19 Infodemic (Zeng and Chan, 2021), some nation states have further exploited the information ambiguity by spreading disinformation on the virus and its origin, by amplifying voices against public health measures, or by undermining the efficiency of certain vaccines (EU

vs DiSiNFO, 2020). One common method of lending credibility to such disinformation narratives has been to construct them around a "kernel of truth," for example in the form of leaked documents and correspondence. Data breaches have thus become an integral part of many disinformation operations, or so-called cyber-enabled information operations.

Cyber-enabled information operations have also been used to spread COVID-19 disinformation. In September 2020, documents of the Tbilisi-based Richard Lugar Research Center were stolen and leaked online together with inauthentic documents. The attack led to the political but uncorroborated public attribution of the attack to a state actor (IDFI, 2020). Similarly, in January 2020, attackers compromised the content management system of a Lithuanian news site and planted a falsified story of foreign military spreading COVID-19 in the Baltics (The Baltic Times, 2020).

The impact of such cyber-enabled information operations against healthcare organizations is twofold. First, they directly undermine the trust that people place in the breached and defamed organization. Second, the resulting disinformation narratives negatively impact the already oversaturated information environment of the COVID-19 Infodemic. In conjunction, these direct and indirect attacks against healthcare threaten to weaken the trust that people place in it by adding to a climate of fear, distrust, and uncertainty. In turn, this undermines the local and global responses to the COVID-19 pandemic and public health crises to come.

Opportunistic actors exploit the crisis

Threat actors will often exploit the information ambiguity of crises or events – the COVID-19 pandemic is no exception (Ray, Marshall and Coderre, 2019). Just as COVID-19 has been used as a lure in phishing emails, threat actors have created COVID-19-themed domains to host malware or for command and control purposes (Szurdi *et al.*, 2020). Furthermore, scammers have created webshops that advertise counterfeit products, such as masks, hand sanitizers, and other medical products (Szurdi *et al.*, 2020). Similar products were also sold on underground marketplaces, often from vendors that had previously sold illegal drugs (Zaidenberg, 2021).

Spotlight 5

European Medicines Agency (EMA) targeted in apparent cyber-enabled information operation

Date: December 9, 2020	**Location**: The Netherlands	**Target Type**: Regulatory Body

Victims, **Targets and Impact**:: In early December 2020, the EMA – a regulatory body that facilitates the development and access to medicines – announced that it had been the target of a data breach. The breach occurred weeks before the first COVID-19 vaccines of BioNTech-Pfizer and Moderna were authorized by EMA. The data relating to the authorization of their vaccines was later leaked online in a manipulated format, "in a way which could undermine trust in vaccines" (EMA, 2021). By undermining the trust in vaccines and in EU public health institutions, this attack threatened to perpetuate, if not exacerbate, the COVID-19 pandemic.

Attack Method: The attack targeted a single IT application and selected documents and correspondence relating to COVID-19 medicines and vaccines (EMA, 2020). A zip file, containing confidential data relating to the EMA's approval of the BioNTech-Pfizer vaccine – Comirnaty, was later leaked and disseminated on an online forum on 30 December 2020 (Var Group, 2021). The EMA confirmed the leak, adding that some of the correspondence had been "manipulated by the perpetrators."

Attribution: The targeted nature of the attack and manipulated leak hints towards a state-sponsored cyber-enabled information operation that could potentially undermine the reputation of Comirnaty, both globally and regionally. In turn, this could give rival vaccines a competitive edge in states' soft power bid of "vaccine diplomacy" as well as impede the pandemic response in the EU as part of a greater Infodemic.

4 Who are the prevalent threat actors?

In the context of cyberattacks on the healthcare sector, two types of threat actors are deemed to pose the greatest threat: cybercriminals and state actors. Other actors, such as insiders and ideological actors, also pose different kinds of threats to the sector but are not covered within the scope of this Report.

The challenge of attribution

The attribution of attacks is widely reported to be one of the biggest challenges in the cyber threat landscape. Attribution is a key element in preventing cybercriminals and state actors from acting maliciously with near impunity (Maglaras *et al.*, 2019) and ensuring that they are held to account.

There are several types of attribution possible, each with their own challenges, though together they would form a full process and work to advance accountability in cyberspace:

- **Political attribution** often lacks transparency and non circumstantial evidence in support of claims (Aravindakshan, 2020). The use of evidentially-weak public attribution as a political tool induces higher levels of uncertainty and distrust in these attribution statements (Egloff, 2020).

- **Technical attribution** can be as specific as identifying individuals involved in the attack and as general as detecting the tools used in the attack. The challenge in technical attribution lies in the need to produce data and processes that can be peer reviewed (Tsagourias and Farrell, 2020), used in legal procedures and are independent of commercial incentive (Egloff, 2020). The lack of physical evidence and the opacity surrounding the capabilities of various threat actors may constitute further obstacles.

- **Legal attribution** is instrumental to holding to account a state actor under domestic and international law. "For a state to take legal action against another state in an international legal forum for harm caused to it by a malicious cyber activity, it will necessarily have to meet the required evidentiary standards of proof in international law" (Aravindakshan, 2020).

Another complexity in the attribution of attacks is the sensitive distinction between state and non-state actors, and in understanding who acted in which regard. When a cyberattack is committed by a cybercriminal or by organs of a nation state (e.g intelligence services), attribution is clearer than when it is committed by non-state actors such as private entities acting on the instruction of a nation state or controlled by a state. Moreover, if one threat actor did not necessarily carry out the whole of an attack, this further complicates attribution. Without concrete and evidence-based attribution, the application of the relevant law is limited.

4.1 Cybercriminals and criminal groups

These terms refer to individuals or groups of individuals whose main objective is to draw **financial gain** through the theft and subsequent monetization of sensitive data (e.g. medical records, vaccine development research or healthcare-specific intellectual property) or the disruption of business continuity in exchange for payment by the target or victim (CIS, no date). Cybercriminals use technology to unlawfully access healthcare computer systems and networks with **malicious intent** (TrendMicro, no date)**.** In the evolution of ransomware attacks, cybercriminals are increasingly using underground marketplaces to trade both malicious services and stolen data. This type of actor is assessed to pose **a high-impact and high-frequency threat to the healthcare sector** (FireEye, 2019).

While not an extensive list, Intel471 has identified 25 ransomware operators, which it has categorized into three tiers. In its first "Most Wanted" tier, it has placed five ransomware operators (Intel 471, 2020b), of which each has targeted healthcare organizations on multiple occasions. However, ransomware attacks are not always the only malicious activities these operators conduct. The threat actors behind these operations have often engaged in other malicious cyber activities long before the ransomware operations that have been attributed to them.

Spotlight 6

Ryuk ransomware attack affects hundreds of hospitals

Date: September 27, 2020 | **Location**: UK, USA | **Target Type**: Hospitals and Medical Facilities

"As of right now we have no access to any patient files, history, nothing [...] Doctors aren't able to access any type of X-rays, CT scans."

(CBS News, 2020)

Victims, **Targets and Impact**: On September 29, 2020 Universal Health Services (UHS) announced that it had been the victim of an attack, largely claimed to be by Ryuk ransomware (UHS, 2020b). UHS is one of the largest providers of hospital and healthcare services with over 400 facilities across the US and UK that treat an estimated 3.5 million patients per year. The attack affected all 250 of the organization's hospitals in the US (Bajak, 2020), leaving its staff without computer access and phone systems (Gatlan, 2020c).

The attack occurred at a time when the US and UK were already struggling and burdened in their COVID-19 response. With systems and medical reports offline, staff were forced to revert to pen and paper. Likewise, affected hospitals had to redirect ambulances and relocate surgery patients, increasing the risk of complications and in the worst case, death (Mitnick Security, 2020). While not officially confirmed, online discussions between alleged UHS staff linked the attack to the death of patients (Name Anonymised, 2020). Exactly one month after UHS reported the attack, the organization claimed to have recovered its systems at its acute care and behavioral health hospitals (UHS, 2020a).

Attack Method: The attackers launched the ransomware attack in the early hours of September 27 to avoid detection before they encrypted and locked all compromised systems (Gatlan, 2020c). Ryuk is known to be deployed as the final step of the so-called loader-ransomware-banking trifecta (Schwartz, 2020). After an initial infiltration through Emotet[12] via phishing or RDP attacks, TrickBot is loaded onto the victim's systems, which in turn facilitates the lateral movement and privilege escalation for the Ryuk ransomware to be deployed (Intel 471, 2020c).

Attribution: Cybersecurity experts and media outlets have widely attributed the attack to the Ryuk ransomware operator, commonly referred to as Wizard Spider or UNC1878. This assessment was made on a number of indicators: first, a UHS employee reported that the attacker used the .ryk file extension and left a ransom note that resembled that of Ryuk (Gatlan, 2020c). Second, according to a cyber threat intelligence firm, Emotet and TrickBot had been detected on UHS systems in September 2020 (Gatlan, 2020d).

The case, nonetheless, highlights the issues of uncorroborated public attribution based on technical or political information alone. First, while many of the Ryuk ransomware attacks may be conducted by Wizard Spider, there are other groups that use Ryuk as a part of RaaS (Intel 471, 2020b). Second, Wizard Spider began using a different malware (other than TrickBot) to load Ryuk on target systems around the time of the attack (Intel 471, 2020b). Third, much of the publicized evidence is from secondary sources that reference individuals who are allegedly familiar with the case. Finally, Wizard Spider itself has been publicly attributed to both a nation state actor and cybercriminals from a different nation state (Hanel, 2019).

[12] Emotet is a Trojan that is primarily spread through spam emails (malspam).

4.2 State and state-sponsored actors

States may have government bodies whose mission is to conduct cyberespionage, cyberattacks and disinformation operations; targets of these attacks include organizations within the healthcare sector. In recent years, the cyber threat landscape has seen an emergence of state-sponsored or funded proxies who act on behalf of states, which has complexified the attribution of attacks and subsequent accountability (van der Meer, 2020). For this reason, the Report uses the term state actors to include both state bodies and state-sponsored entities that target the healthcare sector. Nevertheless, regardless of whether a state actor is a state entity or a state-sponsored entity, they commit attacks with a **geopolitical motive to compromise**, **steal**, **change or destroy information** (CIS, no date).

State actors are frequently referred to as the most sophisticated threat actors due to their significant resources and ability to coordinate attacks over long periods of time while avoiding detection (Canadian Centre for Cyber Security, 2018). Several state actors have been accused of targeting the healthcare sector, mainly in cyberespionage. However, if state actors were to engage in **disruptive attacks against the healthcare sector,** such action could result in "a potential for **significant to catastrophic impacts**" (FireEye, 2019).

The COVID-19 pandemic has been not only a major boon for cybercriminals but has also provided an opportunity for states to shift the realities of global geopolitics. One primary platform of doing so has been through the so-called COVID-19 vaccine race, which has directly translated into an escalation of state actor activity in cyberspace. Since March 2020, state-sponsored cyberespionage groups have targeted vaccine research, development, and testing facilities in an attempt to gain a competitive edge. State actors have also been involved in disinformation operations impacting other states' response efforts during the COVID-19 pandemic (see Section 3.3).

Spotlight 7

Suspected nation state actor targets Chinese public health organizations involved in COVID-19 response

Date: January to April 2020	**Location**: China	**Target Type**: Government (Health) Ministries

Victims, **Targets and Impact**:: As governments were sent scrambling for an appropriate response in the early months of the COVID-19 pandemic, the threat actor OceanLotus was accused of targeting Chinese public health organizations and officials in an alleged bid to gather intelligence on the crisis (Henderson *et al.*, 2020). The first identified intrusion attempt occurred on January 6, 2020 against China's Ministry of Emergency Management (Henderson *et al.*, 2020). The campaign also targeted the government of Wuhan, from where COVID-19 originated.

Attack Method: OceanLotus targeted organizations with spear phishing emails that were tailored to internal processes, such as "office equipment bid[s]." (Henderson et al., 2020) The group also used COVID-19-themed phishing lures that shared malicious attachments relating to travel restrictions in Hubei Province, of which Wuhan is the capital.

Attribution: The cyberespionage campaign was attributed (technical attribution) to the OceanLotus threat actor (APT32) on the basis of the domains in embedded links that had been used for command and control purposes in previous OceanLotus phishing campaigns against targets in Southeast Asia (Carr, 2017). OceanLotus has been broadly attributed to a state actor and specifically to an IT company within that state (Stubbs and Pearson, 2020). This is not the first time that the group has targeted healthcare organizations; its tactics had been identified in UK healthcare organizations in previous incidents. (FireEye, 2019)

Part 3:
Tackling the Threats

5 What instruments are available to protect healthcare from attacks?

This section explores the opportunities and protections that legal and normative instruments make available to state and industry actors in relation to the healthcare sector. Some derive from legal obligations in effect under domestic and international law (Delerue, 2020), while others are voluntary commitments and normative efforts to foster responsible behavior. Influential work such as the Tallinn Manual on the International Law Applicable to Cyber Warfare (Schmitt, 2013, 2017) clarifies how international law applies in cyberspace. The recent Oxford Statements re-assert the specific rules and principles of international law that apply to secure healthcare facilities from cyberattacks and interference (Akande, Coco, *et al.*, 2020; Akande, Hollis, *et al.*, 2020). We start by mapping the current tools and opportunities available for protecting healthcare, in order to understand how an accountability framework can fill the gaps and drive action.

5.1 Opportunities for state actors to protect the healthcare sector

To ensure rule of law and enforce the law in their jurisdiction

Domestic law and jurisdiction are first avenues to consider when discussing the healthcare context and attacks against hospitals and medical facilities. All states exercise jurisdiction over their own territory and some are also explicit about covering harmful effects in their territory that originate abroad (UNODC, 2019), as is often the case with attacks against healthcare.

Criminal law specifically proscribes conduct endangering health and threatening life, but other bodies of law, such as data protection, are also relevant for ensuring that the rights of patients and medical personnel are protected in case of data breaches (European Parliament and Council of the European Union, 2016). Naturally, the protection of personal information is integral to the healthcare sector as it deals with high volumes of such data. It is also important to note that legal jurisdictions have different levels of maturity in terms of the level of protection that is granted to personal data,

the penalties for breaching the law and the related reputational damage that the victims of a data breach will suffer.

Beyond the lack of harmonization, there are numerous other challenges to the adequate protection of the healthcare sector at the domestic level: states might have low capacity for law enforcement within their own territory and their laws might have limited scope for pursuing attacks originating outside their borders, as is often the case with attacks on healthcare. Certain pre-conditions must be met in order to proceed: the consent of the foreign state where the suspected criminal or evidence is located, and the availability of robust forms of transnational law enforcement cooperation, whether for extradition or mutual legal assistance. In addition to territorial constraints on enforcement, foreign states and international organizations will often have certain immunities (e.g., sovereign immunity) that preclude their being subject to domestic criminal law directly (Yang, 2016).

Some challenges to these instruments to take into consideration include the extraterritorial application of domestic law, which is more limited in scope in the cyber domain, and is especially more complicated when it involves international organizations such as the WHO, foreign nationals, or cases of cyberespionage. In July 2020, the US Department of Justice filed an indictment against two foreign nationals for corporate espionage of COVID-19 vaccine facilities and included counts such as "Conspiracy to Access Without Authorization and Damage Computers" and "Conspiracy to Commit Theft of Trade Secrets" (Hyslop, Goeke and McCulloch, 2020). However, since the USA and China do not have an extradition treaty in place it is likely that nothing more will become of these charges.

To refrain from violating state sovereignty and intervening, including by cyber means, in the internal or external affairs of another state

International law generally prohibits states from violating the sovereignty principle, which grants them supreme authority within their territory, the plenitude of internal jurisdiction and immunity from other states' own jurisdiction[13] (Besson, 2011). Sovereignty is also a prerequisite for prohibiting intervention, including by cyber means, in the internal or external affairs of another state, based on the principle of non-intervention. Attacks during the pandemic can amount to a violation of these two principles, as follows:

Violation of sovereignty

The prohibition of unauthorized exercise of authority by one state in another state's territory applies not only to the territorial integrity of the victim state, but also to harmful impact in the absence of physical effects, for example by interfering with governmental functions using cyber means (Schmitt, 2017). Affecting the health of citizens in a direct manner or causing the loss of functionality of critical infrastructure (e.g. rendering medical equipment inoperable) would constitute valid grounds for an internationally wrongful act if attributed to a state (Milanovic and Schmitt, 2020). The French Ministry of the Armies makes this explicit in its Position Paper:

"[a]ny cyberattack against French digital systems or any effects produced on French territory by digital means by a state organ, a person or an entity exercising elements of governmental authority or by a person or persons acting on the instructions of or under the direction or control of a state constitutes a breach of sovereignty" (DICoD, 2019).

Violation of the principle of non-intervention

The principle of non-intervention prohibits a state from intervening by coercive means in matters within the sovereign competence of a target state, often dubbed *domaine réservé*. How a state decides to handle a health crisis such as the COVID-19 pandemic, involving both public and private essential services, would qualify as *domaine réservé* (Milanovic and Schmitt, 2020). The prohibition of non-intervention also applies if a state actor intentionally obstructs another state's activities but remains below the threshold of use of force, for example in order to purposefully inhibit the ability of the other state to control the crisis. Additionally, when non-state actors act on behalf of a state, and these actions can be attributed as such, this principle can be violated and international law can be invoked. In the work of the UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (UN GGE), a voluntary, non-binding norm of responsible state behavior specifically reinforces this principle:

UN GGE Norm F: "A State should not conduct or knowingly support ICT[14] activity contrary to its obligations under international law that intentionally damages critical infrastructure or otherwise impairs the use and operation of critical infrastructure to provide services to the public" (United Nations, 2015).

There is emerging consensus in intergovernmental processes about the designation of health and medical facilities as critical infrastructure, though this has not yet reached universal recognition. Given the vulnerability of the healthcare infrastructure, states including Australia, Czech Republic, Estonia, Japan, Kazakhstan and the USA came forward in a joint proposal recommending that healthcare and medical facilities be explicitly included under critical infrastructure in the upcoming United Nations Open-ended Working Group on developments in the field of information and telecommunications in the context of international security (UN OEWG) report (Australia et al., 2020). Though there is no unequivocal global agreement on what is included under the definition of

[13] Pursuant to Art 2 (4) and (7) of the UN Charter (United Nations, 1945)

[14] Information and Communications Technology

critical infrastructure, steps are being taken by states and regional bodies to specify this. In the EU, a proposed directive under discussion since 2020 aims to designate sectors that provide essential functions as critical infrastructure in order to better protect them from disruption caused by natural disasters and man-made threats (European Commission, no date).

What remains to be discussed and debated, and as such a challenge to implementing these principles, is the understanding of what constitutes 'use of force' under international law. With cyber capabilities continuously evolving in sophistication, they can less and less often be mapped against a kinetic counterpart despite their destabilizing effects, thereby obliging states to decide on which meet or fall below the threshold. Due to this ongoing debate, particular types of attacks, such as large-scale disinformation campaigns during health crises, fall through the cracks as states need to determine whether such campaigns violate the principles of sovereignty or non-intervention.

To respond to and stop internationally wrongful acts that emanate from their jurisdiction

Under the principle of due diligence, a state must take all feasible measures to prevent or stop an attack that emanates from its territory or infrastructure under its jurisdiction or control, as long as they are aware of it (Schmitt, 2015). This also applies to the activities of cybercriminals and non-state actors. If due diligence applies, it is an obligation of effort, not result (Schmitt, 2017), such that a state is not responsible solely because an attack impacting another state's healthcare sector originated in its territory. Rather, obligation emerges where a state knows or should know of the conduct, in which case it must employ "all means reasonably available" to redress it (Schmitt, 2017). The UN GGE reinforces this opportunity under Norm C: "States should not knowingly allow their territory to be used for internationally wrongful acts using ICTs" (United Nations, 2015)All states have endorsed this voluntary, non-binding norm of responsible behavior in the UN General Assembly.

A key challenge to the application of this principle of international law is for states to recognize, in a timely manner, that their territory is being used for malicious purposes and from where the malicious actor is acting. In the recent case of the attack against Universal Health Services medical facilities (USA), the private cybersecurity firm CrowdStrike attributed the attack to the criminal group Wizard Spider, which likely operates out of Russia (Hanel, 2019). In this scenario, the burden of due diligence would fall on Russia. For this to happen, the US Government would have to independently confirm these allegations and call on Russia to hold the suspected criminals to account. This in itself is also a challenge for reasons of geopolitical relationships and political considerations, which oftentimes impact a state's actions following an attack.

To respect and ensure the right to life, the right to health, and the right to seek and receive information

International human rights law requires states to respect and protect the right to life and the right to health (OHCHR, 1966a, 1966b) of all persons within their jurisdiction, including by taking measures to prevent third parties from interfering with these rights by cyber means. It addresses the harm caused by attacks on both human life and health, and offers a practical and symbolic means of analysing attacks beyond the victim as state and focuses on the victim as an individual (Milanovic and Schmitt, 2020, pp. 261–266).

International human rights law also provides for the right to seek and receive information, a crucial right in times of crisis, such as a pandemic. The UN Committee on Economic, Social, and Cultural Rights affirms that the "deliberate withholding or misrepresentation of information vital to health protection or treatment" violates a state's duty to respect the right to health (United Nations, 2000). Having access to truthful information about the pandemic and the measures one should take to protect themselves and others from its spread falls under this right (Kaye, Désir and Lanza, 2020).

The question of complexity surfaces again with respect to human rights law, as it has not been universally agreed upon whether a state must respect the human rights of individuals located outside its territory.[15] During a health crisis, resourcing represents another important challenge to the application of human rights and the protection of life, health and access to information. Resourcing also has an impact on the already challenging task of measuring harm, and especially how much harm can be linked to an attack and what remedy is owed to the victim.

If party to an armed conflict, to ensure that medical units, transport and personnel are protected at all times

In accordance with international humanitarian law (IHL), both state and non-state parties to armed conflicts: must not disrupt the functioning of healthcare facilities through cyber operations; must take all feasible precautions to avoid incidental harm caused by cyber operations, and; must take all feasible measures to facilitate the functioning of healthcare facilities and to prevent them being harmed, including by cyberattacks (Iaria, 2020).

IHL provides for the explicit protection of medical and healthcare facilities during times of conflict. Building on the advances of IHL, a new norm proposed by the International Committee of the Red Cross (ICRC) in the UN ambit specifically calls for the protection of medical facilities and services

[15] A broader interpretation of this territorial limitation is offered by the UN Human Rights Committee in its General Comment No. 36 on the right to life and is understood to encompass state control over a victim's enjoyment of their rights, rather than state control over the victim themselves (UNHCR, 2018).

at all times (Mačák, Rodenhäuser and Gisel, 2020). In more extreme cases, attacks against medical facilities may amount to international crimes and could, provided specific conditions are met, trigger indictments on grounds of war crimes and crimes against humanity (Akande, Hollis, *et al.*, 2020). As support grows for the consideration of health and medical facilities as critical infrastructure, the question remains whether this would be enough to protect the healthcare sector, including its workers, from the harms of potential attacks.

To make best use of cross-border cooperation mechanisms

In line with the transnational nature of cyberattacks, there is an opportunity to apply cross-border policing mechanisms. Law enforcement cooperation bodies such as AFRIPOL, ASEANAPOL, EUROPOL and INTERPOL help to facilitate communication, sharing of information and evidence, and to conduct joint investigations. Treaties such as the 2001 Council of Europe Convention on Cybercrime (Budapest Convention), signed by 65 states, criminalize certain cyber activities including illegal access (Article 2), data interference (Article 4), and system interference (Article 5) (Council of Europe, 2001). When it comes to non-legally binding mechanisms, confidence-building measures such as those proposed by the Organization for Security and Co-operation in Europe (OSCE) in 2013 and 2016, enhance transparency and facilitate exchanges between states by encouraging direct communication, the sharing of good practices and the voluntary reporting of vulnerabilities in the ICT systems (OSCE, 2013, 2016).

Such efforts complement more formal frameworks set out by agencies such as INTERPOL, yet information exchange among states remains limited, despite the urgency imposed by the COVID-19 threat landscape. Several states have repeatedly cited the importance of multilateral agreements (MLATs) and international cooperation during investigations. For example, due to limited resources, Malta and Georgia rely on international cooperation for more effective investigations (Secretariat of the Cybercrime Convention Committee, 2020) and Sri Lanka has recognized the benefits of gathering and sharing electronic evidence, which has also encouraged spontaneous information-sharing between states (Secretariat of the Cybercrime Convention Committee, 2020).

To impose punitive measures on threat actors and intermediaries

The legal instruments previously referred to also include the possibility of imposing punitive measures against attackers. There is growing recognition of the violations triggered by attacks targeting the healthcare sector:

> "The Netherlands is appalled by the abuse of the COVID-19 crisis by States to conduct or effectively control non-state actors in launching cyber operations, including the disruption of the healthcare sector, and cyber enabled information operations to interfere with the crisis response in times of urgent crisis. Not only are these operations highly deplorable examples of irresponsible state behavior; in many instances, they constitute violations of international law."
>
> *(Kingdom of the Netherlands, 2020)*

Diplomatic tools and restrictive measures are available to states confronted with this situation. In the European context, the EU Cyber Diplomacy Toolbox aims to facilitate cooperation amongst parties and to mitigate threats from malicious actors, including by imposing targeted sanctions, as in the case of the WannaCry Attack (Council of the European Union, 2017). Other regional bodies, such as the African Union, have also envisioned such mechanisms. The proposed African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention) outlines the evolution of thinking on sanctions, specifically relating to attacks on critical infrastructure (African Union, 2014).[16]

The opportunity to take punitive measures is a road less travelled by most states, for a variety of political, legal, and technical reasons. Few states make public attribution statements following investigations of cyberattacks, and when they do, legal and normative obligations are rarely invoked.[17] Those that have publicly attributed attacks and followed through with indictment measures face the challenge of extradition of the foreign national concerned. Since there are no extradition treaties between some key states, little to no action can in fact be taken against individuals found guilty of attacks. Along with extradition treaties, the challenges

[16] The Malabo Convention was proposed in 2014 but has not yet entered into force as it requires 15 ratifications. To date, 18 states have signed it, but only 8 have ratified it (Angola, Ghana, Guinea, Mauritius, Mozambique, Namibia, Rwanda and Senegal).

[17] For more on this topic, see Martha Finnemore and Duncan B. Hollis: *Beyond Naming and Shaming: Accusations and International Law in Cybersecurity (2020).*

related to territorial constraints already mentioned may specifically affect the protection of human rights and questions around cyberespionage. Cyberespionage campaigns, specifically those related to COVID-19 vaccine research, are commonly found to be state-sponsored. They also rely upon the use of offensive tactics, techniques and procedures (TTPs) to exploit vulnerabilities in order to capture information and surveil (Schmitt, 2017), which impacts the security of all internet users. To render these TTPs ineffective, industry actors have a key role to play in the prevention and handling of the attacks.

5.2 Opportunities for industry actors to protect the healthcare sector

Industry stakeholders have several instruments with which to better protect the healthcare sector. Though bound by international standards, domestic legislation and regulatory frameworks, a number of multistakeholder norms have been created and adopted by members of the industrial community to clarify their role in protecting the healthcare sector.

To produce secure products and services (security-by-design)

Designing and producing secure products and services from the start is integral to protecting users and protecting the healthcare sector. By strengthening the design of products, the impact of attacks such as ransomware, malware, or even cyberespionage, can be significantly reduced. This is captured under Principle 6, Lifecycle Security, of the Paris Call (Paris Call, 2018b). This Call has been signed by over 680 companies which demonstrates the level of multistakeholder agreement on this point (Paris Call, 2018a).

The challenge alongside this opportunity is that without strong regulations in place, the user is left to trust that the products and services that they use are designed in the most secure way possible. This trust can be eroded by actors who gain access to hospitals, medical and manufacturing facilities via backdoor vulnerabilities to cause damage that spreads across networks. The impact of supply chain infiltration, for example, in the ongoing Orangeworm campaign (see Spotlight 8), is little known, but ultimately, this should not be a question of trust but a question of obligation. Securely designed products and services will ultimately reinforce supply chain protection.

Spotlight 8

Unidentified threat actor targets healthcare supply chains for years

Date: Ongoing since 2015	**Location**: Asia, Europe, North America	**Target Type**: Hospitals and Medical Facilities, Manufacturing

Victims, **Targets and Impact**: First identified by Symantec in 2015, Orangeworm is a threat actor that is known for targeted attacks against healthcare organizations in Asia, Europe, and the United States (Symantec, 2018). Nearly 40% of Orangeworm's confirmed victims were in the healthcare sector, such as hospitals and international healthcare and pharmaceutical companies (FBI, 2020). The group's secondary targets, including manufacturing and software vendors, often exhibited "multiple links" to the healthcare sector through their products and services (Symantec, 2018).

Attack Method: Orangeworm's primary infiltration vector into a healthcare target is to infect its vendor software (Symantec, 2018) and hardware supply chain with the group's custom backdoor RAT – Kwampirs (Hulsebos, 2020). As it inflicts no damage, Kwampirs can remain undetected for a long period, during which it can spread via updates, software co-development, as well as software and devices installed in a customer's infrastructure (FBI, 2020). Kwampirs has been found on medical imaging devices, such as X-Ray and MRI machines (Symantec, 2018).

Attribution: To date, no attribution has been made for this campaign. Symantec's 2018 analysis states that there are no "technical or operational indicators to ascertain the origin of the group" but they "do not believe that the group bears any hallmarks of a state-sponsored actor" (Symantec, 2018). In early 2020, law enforcement authorities issued a warning of the ongoing Advanced Persistent Threat (APT) campaign using Kwampirs against the healthcare supply chain, which noted code-based similarities between Kwampirs and Shamoon, a data-wiping malware (FBI, 2020). The extent of these similarities has been challenged (Infosec Resources, 2020) as has the attribution of Shamoon to a specific nation state (Perlroth, 2012) shedding light once again on the need for transparent and evidence-based attribution.

To comply with regulatory requirements

Regulatory requirements are another instrument presenting an opportunity to better protect the healthcare sector, both for their legally binding nature and what they stand for. These requirements work to improve and protect the quality of medical devices, but also increase transparency about the products and services for the consumer. The EU has been working towards new regulations on medical devices and in-vitro medical devices, which will come into force in May 2021 and May 2022 respectively (European Commission, 2020a). The US Department of the Treasury has also issued a warning that companies that, "facilitate ransomware payments to cyber actors on behalf of victims, including financial institutions, cyber insurance firms… not only encourage future ransomware payment demands but also may risk violating OFAC [the Office of Foreign Assets Controls] regulations" (U.S. DoT, 2020).

Requirements such as those put forth by the EU and OFAC are important steps towards the regulation of specifically medical devices and associated hardware and software, which in turn protect patient health and safety as well as their access to effective legal recourse. The distinction between what is considered to be a medical device and an ICT product is

continuously blurring with the rapid advancement of technology, such that regulatory requirements for healthcare devices are struggling to keep pace.

Product Vulnerability Standards

New standards have been introduced in some countries to reduce product vulnerabilities in connected medical devices – examples include the European Union Regulation 2017/745 on Medical Devices (European Commission, 2020a) and pre- and post-market guidance in the United States (FDA, 2020) – although these can refer to connected technologies introduced after the requirements came into force. Legacy systems that would require major overhaul or may have no appropriate updating mechanism for hospital deployment may not be covered by such instruments. Additionally, these instruments do not always apply to healthcare technologies that do not require regulatory approval, such as electronic health record systems, networking equipment, technologies manufactured and deployed in countries that do not have such standards for product security of connected medical devices (Beardsley, 2018).

Broader coverage of vulnerabilities and supply chain responsibilities are negotiated in the European Union in two directive proposals, aiming to protect new sectors based on their criticality for the economy and for society. In line with the proposal for a directive on the resilience of critical entities, the revised Directive on Security of Network and Information Systems (NIS2) puts forward new frameworks for critical supplier relationships risk management and coordinated vulnerability disclosure. Alongside a European vulnerability registry, stricter supervisory and sanctioning regimes across member states are proposed for essential and important entities (European Commission, 2020b).

To inform about vulnerabilities, especially those in critical infrastructure

Vulnerabilities in digital products and services used in critical infrastructure contexts pose a threat to human health and security. Based on multistakeholder norms such as the Paris Call and Cybersecurity Tech Accord, there is general agreement by signatories that vulnerabilities should be disclosed.

While said agreement is heartening, there is no real framework in place to effectively make this a best practice. Such a framework could include guidelines on issues such as the importance of disclosing vulnerabilities in a timely manner and how to encourage users to update their systems as required. Enhancing communication between the industry stakeholders who have designed, built, and possibly used the products, and public and private stakeholders who also use the product would help to ensure the protection of users. As previously mentioned, there are several instances where threat actors have exploited the vulnerabilities of the healthcare sector's digital landscape for their own gain. In the case of the WannaCry Attack (see Spotlight 1), a vulnerability in the operating system of (UK) National Health Service computers led to widespread disruption of healthcare services.

To protect users

The protection of users, specifically users of critical infrastructure in this case, should be at the core of industry action. This is an opportunity to always place people at the focal point of intention and purpose, which ultimately helps to better protect them. Voluntary commitment frameworks emphasize the importance of user protection: both the Paris Call (Paris Call, 2018b) and the Cybersecurity Tech Accord (Cybersecurity Tech Accord, no date) place user protection as their first principles, and the Charter of Trust (Charter of Trust, 2018) as its fourth.

The challenge here is to advance user protection through tangible action. The principles set forth in multistakeholder initiatives are a good first step to foster agreement. The time has come to apply them on a larger scale, for companies large and small, so that they may ultimately become standard behavior. Without a binding framework to ensure users are protected, the risk of missteps will always remain.

The key opportunities presented here for states and industry can, when applied, work to protect the healthcare sector. These instruments have their respective challenges and complexities, leaving the targets and victims of attacks with little possible legal recourse, and threat actors free to act with impunity. Through a human-centric approach and by focusing efforts on the protection of users and victims, the case for a targeted accountability framework can be made.

Mapping Accountability

6 Could a strong accountability framework increase responsible behavior in cyberspace?

6.1 The accountability gap

The growing weaponization of the internet reflects the current threat landscape, where state and non-state actors are perpetrating attacks with little risk of being held accountable. These attacks at times have a very direct, real and visible impact. Many of them, however, such as cyberespionage or reconnaissance campaigns, are stealthy, have limited visible impact and remain undiscovered. This does not mean that they are acceptable. Too often, the lack of thorough investigation after major attacks leaves people desensitized, disillusioned, and disempowered, consequently crippling their trust in institutions and governments.

Not closing the accountability gap means widening the digital divide between those who have the capability to react to attacks, and those who do not. More importantly, not addressing and closing the accountability gap will exacerbate the void between victims, targets and threat actors.

Closing the accountability gap goes beyond the basics of identifying the origin of an attack or determining which was the weak spot. It is all about understanding and specifying who is responsible for security, dignity and equity in cyberspace and how these stakeholders may act to attain cyberpeace.

6.2 Taking responsibility – the CyberPeace accountability framework

The CyberPeace Institute has developed a proposal for an accountability framework with the goal of mapping accountability to help make responsible behavior the norm among all stakeholders of the digital world. The framework has four key goals:

- Identify clear and common **expectations** of what constitutes responsible behavior in cyberspace
- Establish stakeholder **commitment** to uphold expectations
- Track stakeholder **adherence** to commitments
- Implement the **consequences** for failure to uphold commitments and reward or incentivize upholding commitments.

With this framework to guide its actions and serving as a neutral and independent source of information on the practices of stakeholders active in cyberspace, the CyberPeace Institute seeks to effect change and promote responsible behavior in cyberspace through:

- Identifying the weakest links and vulnerabilities in the cybersecurity chain
- Identifying the interactions, or lack thereof, and communication deficiencies between the different stakeholders
- Identifying the practical actions that make a real difference – what works and what doesn't
- Providing insights and information on the obligations of all stakeholders, including state and non-state entities.

6.3 Mapping accountability in the healthcare sector

The healthcare sector encompasses a large number of various types of companies, institutions and facilities that make them targets of threat actors for different reasons. Each attack has its own threat actors, methods and motivations contributing to the degree of its success.

To illustrate how the framework is used, one may consider the fictitious case of a hospital being the target of ransomware. The attack starts with a vulnerability on one of the hospital's devices that exposes a remote access service to the internet. Patient data is made unavailable and the hospital's IT infrastructure is temporarily out of order. An investigation conducted by security professionals and law enforcement agencies shows that the attack succeeded because a patch was not applied on time, due to a lack of IT resources delaying the patch campaign. The investigation also reveals that the vendor took six months after the vulnerability was discovered to apply the patch. The threat actor is identified as an international criminal group, but no punitive measures are taken at the government level. Another attack with identical *modus operandi* is perpetrated a couple of months later against another hospital.

The first step of the methodology consists in determining who are the relevant stakeholders in the case, and may include for example:

- The target hospital, which may comprise three subgroups of actors:
- The senior management, responsible for strategic decisions
- The IT department, managing the IT infrastructure
- The healthcare professionals (medical and administrative staff), end-users of the IT infrastructure
- The vendors and manufacturers of medical devices, IT equipment and software
- The patients (victims impacted by the attack)
- The government, through the investigation that has followed the attack and also in its capacity of regulator and protector of the healthcare system.

This list is not exhaustive and many more relevant stakeholders may be involved, notably the threat actors themselves, depending on the complexity of the case.

Threat actor impunity – the enforcement gap

It is estimated that in the United States "the enforcement rate for reported incidents of the IC3[18] database is 0.3%. Taking into account that cybercrime victims often do not report cases, the effective enforcement rate estimate may be closer to 0.05%."

(Eoyang et al., 2018)

The challenges of attributing attacks to specific threat actors (see Chapter 4) have played a major role in the accountability gap. Given the low incidence of credible attribution events and subsequent enforcement, **threat actors have been able to act with near impunity**. The challenges of attribution and enforcement have been exacerbated by a number of interrelated factors:

1. **Lack of available data** has been associated with the underreporting of attacks, due to the perceived repercussions on side of the victims[19] as well as inconsistency in how and to whom to report attacks (Eoyang *et al.*, 2018).
2. Low reporting incidence has been a contributing factor to the **inadequate allocation of resources** into investigative and enforcement capabilities (Swinhoe, 2019).
3. **Different levels of maturity** around the world **in the technical expertise and capabilities** of those officially responsible for the investigation and analysis of attacks. (Peters and Jordan, 2020).
4. While the value of capacity building and cooperation has been acknowledged on a global level, it has "**not been matched by sufficient resources and political will**." (Peters and Jordan, 2020).

The attribution and enforcement of state and state-sponsored threat actors poses additional challenges due to their high degree of sophistication, obfuscation and the geopolitical agendas at play.

Cyberpeace exists when human security, dignity and equity are ensured in digital ecosystems.

Considering the Institute's definition of cyberpeace, the questions that must be answered are:

- What can one expect in terms of security, dignity and equity from each of the stakeholders?

[18] Internet Crime Complaint Center. The IC3 provides a reporting mechanism to submit information to the Federal Bureau of Investigation concerning suspected Internet-facilitated criminal activity.

[19] European law enforcement authorities have often had to rely on media reports to identify ransomware victims and commence a criminal investigation (Europol, 2020). To avoid reputational damage or re-victimization, many target organizations have preferred to engage with private security firms, which often have trusted relationships with ransomware operators (Europol, 2020).

- In the context of the digital world and the attack in particular, did stakeholders commit to these expectations and in what way?

- Are they a model or is there any way to improve their adherence to their commitment with respect to the expectations?

For the sake of simplicity, only stakeholders 1a, 1b, 1c, 2 and 4 (above) are taken into account in the methodology at this stage (see Figure 8).

Expectations: The hospital is a place where trust is absolutely essential. A patient will not entrust healthcare professionals with his/her life when he/she does not feel safe, that is when the professional is not deemed competent and benevolent. Expectations should be defined as to how this sense of trust can be guaranteed in the context of an attack.

Commitments: Commitments are concrete decisions taken by a stakeholder and which fulfill the expectations (e.g. decision by senior management to push for a cybersecurity policy). Sometimes, a stakeholder may have 'implicitly' committed to upholding expectations by virtue of their role or status. It may be important to identify where stakeholder commitment is unclear and/or deviates from the established expectation and to analyse why so (e.g. absence of awareness regarding the confidentiality of patient recordings).

Adherence: Decisions are followed by actions. One way to measure the adherence of a stakeholder is to determine which follow-up actions have actually been undertaken or not and what was the timeline. Are these actions recurrent (e.g. awareness training)? Is there any evolution in time (e.g. updates of a cybersecurity policy)?

Consequences: In evaluating consequences and incentives, the primary consideration from a human-centric standpoint should be the effectiveness in decreasing the impact of cyberattacks on the population; in the case of an attack on a hospital, the protection and safety of the hospital staff and patients are the priority.

Expectations regarding security, dignity, equity are defined for each of the actors. Commitments that have been communicated or publicly announced in the past are arranged according to the expectations and adherence to these is measured through the number of initiatives and their efficiency at reducing the impact of attacks on the population. The number of commitments and corresponding initiatives may be used as a metric to estimate the potential for each actor to make change happen. In this fictitious case, the government has the capability to make a real difference, through many initiatives that may have been proposed but not necessarily implemented or lack the necessary resources or impulse to be successful.

The weakest and most promising initiatives are identified (e.g.: digital education in schools that is not seen as a real discipline, lack of security-by-design at the vendor level), but programs that had a positive impact in the past should be considered as well (ex: awareness program by IT at hospital level). The consequences may take the shape of a public call to action, a push for new projects by associations, or simply praise and a reminder of actionable initiatives that work (see Figure 9).

This example has been reduced to a few actors for the sake of comprehension. The methodology can be applied to the non-exhaustive list of stakeholders that follows. Many of these stakeholders exist across various sectors, whereas some are not directly involved in the digital world:

- patients and customers
- hosting companies
- hosted services (e.g. compromised websites distributing malware unintentionally)
- software vendors
- free open-source software developers
- journalists
- general public
- civil society and human rights groups
- threat actors, most pressingly when they are state actors.

Each of these stakeholders has a role to play in achieving and sustaining cyberpeace, and the Institute considers it important to identify expectations for responsible behavior in terms of these various stakeholder groups. This framework applies beyond technical experts as investigations from journalists or public outcry, for example, may also contribute positively or negatively to the evolution of the threat landscape.

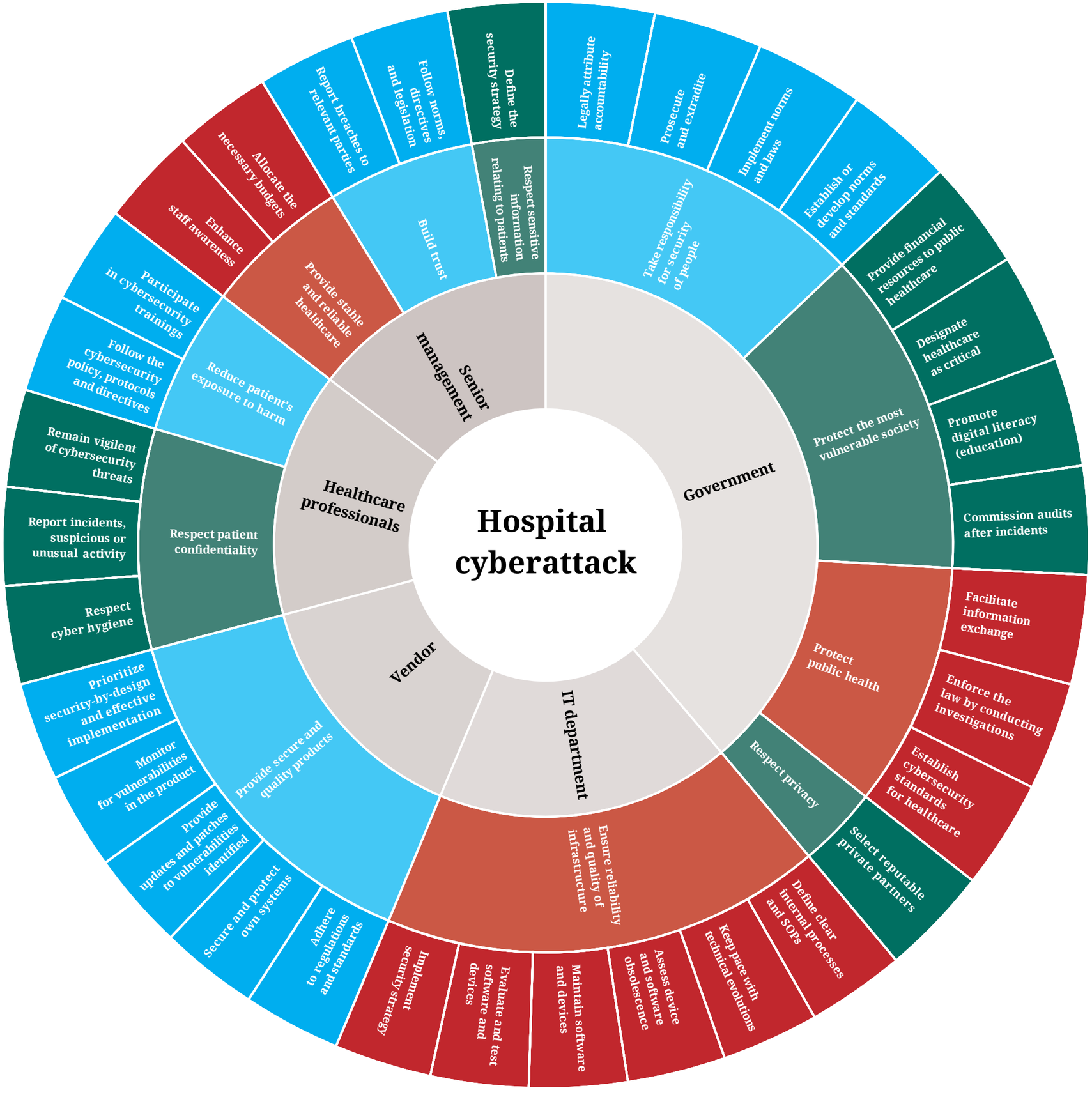


Figure 8: Expectations and commitments of stakeholders
Source: The CyberPeace Institute 2021

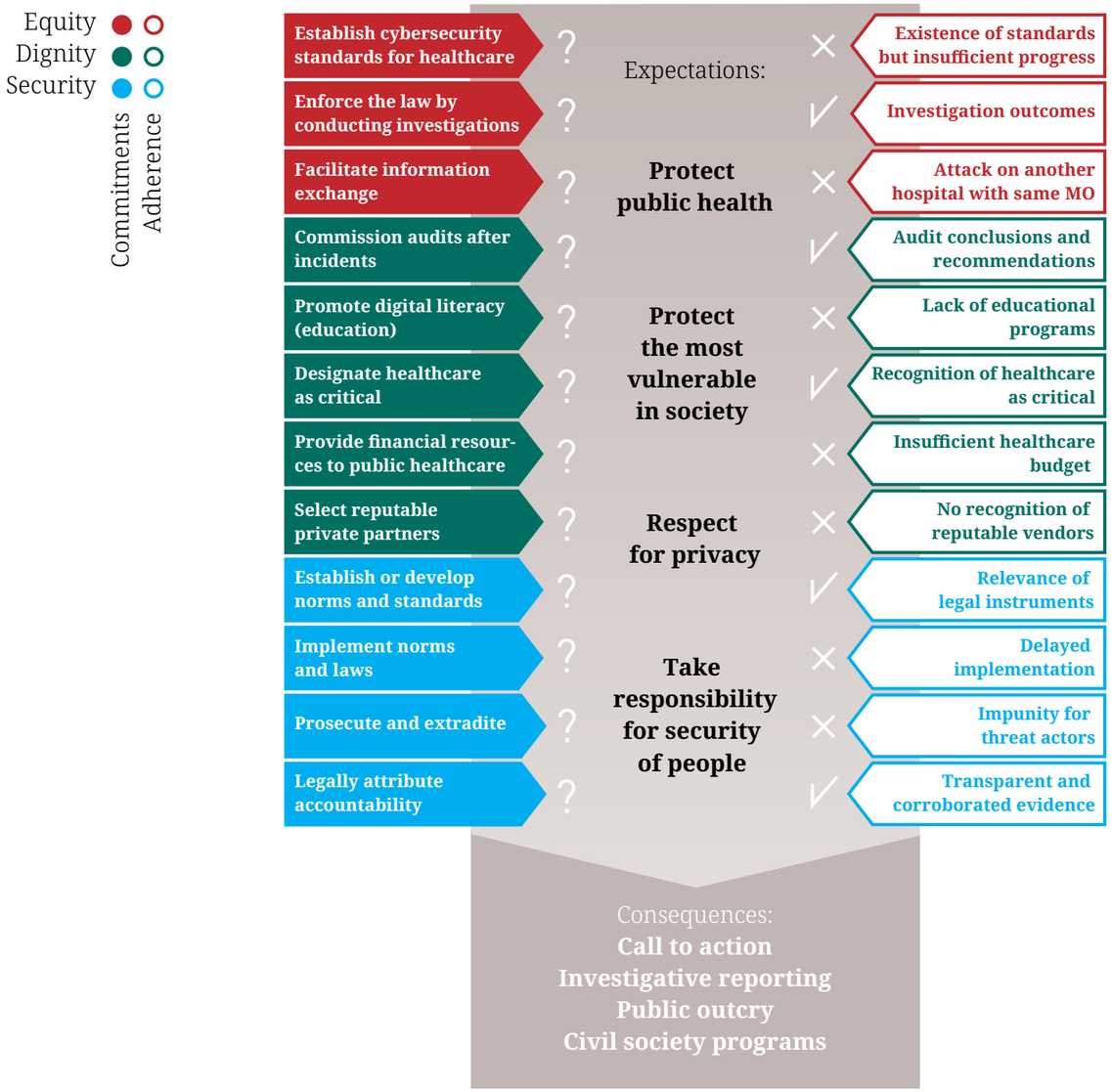


Figure 9: Mapping commitments to adherence, and consequences
Source: The CyberPeace Institute 2021

6.4 Putting the framework into practice

The Institute believes that applying the accountability framework has the potential to deepen understanding of the current cybersecurity landscape in an innovative way, by shedding light on the weak spots in cybersecurity that have a direct impact on people as well as systems and infrastructure.

Applying the framework as often as possible will allow for more effective filling of the gaps in cybersecurity, by revealing which of them have the most impact on the victims as people. Applying the methodology to a case also exposes aspects that may not be related to IT and cybersecurity *stricto sensu* but are systemic in nature, e.g. a lack of policy or investment regarding cybersecurity in general, inadequate laws, a lack of education about digital devices or recurrent problems with financing.

As an initial proposal, the framework is a work-in-progress and as such, necessarily limited at this stage. There might be insurmountable obstacles in relation to existing standards, norms and laws. Cybersecurity is often considered an impediment to efficiency and ease of use, which are also components of well-being to some extent. But the goal is very much about pushing back these limits and making every stakeholder conscious of their power, responsibilities and duties, at all levels.

The Institute is therefore calling for collaboration with healthcare partners who have been victims of an attack to testrun the methodology with as many cases as possible. It is also prepared to collaborate with entities concerned with policy making, cybersecurity and human well-being, to improve the framework. No single entity – individuals, industries or government – is above the law. The CyberPeace Institute is a driving force for accountability in cyberspace, for everyone, everywhere.

Current Initiatives

7 How are different stakeholders joining forces in support of the healthcare sector?

When analysing the threat landscape in which healthcare professionals and patients are victims of attacks, it is easy to paint a dark picture. But this would not do justice to the multiplicity of national and international initiatives available to help the healthcare sector face these threats more robustly:

- Resilience initiatives – to help healthcare organizations prevent and defend against attacks
- Response initiatives – to provide cybersecurity and technical expertise in times of crisis
- Victim-support initiatives – to provide assistance to victims following a cyberattack

Such initiatives have existed for years, but the exponential growth of COVID-19-related attacks has led many in healthcare and cybersecurity to launch new efforts to assist those most in need, volunteering their time, expertise and resources. The founders of the CTI League, a "Global Volunteer Emergency Response Community, defending and neutralizing cyber-security threats and vulnerabilities to the life-saving sectors related to the current COVID-19 pandemic" (Zaidenberg, 2020), were recently featured in Wired's list of 25 people who made things better in 2020 (Hacia, 2020). Many other groups of people, tightly or loosely organized (see Figure 10), also made things better in 2020 in healthcare cybersecurity. Below are a few examples, not an exhaustive selection, of these initiatives; we encourage the reader to contact the CyberPeace institute in our efforts to map these kinds of initiatives.

Figure 10: Joining forces in support of the healthcare sector
Source: TheCyberPeace Institute 2021

7.1 Resilience initiatives

Resilience initiatives in support of the healthcare sector can be categorized into three subsets:

Initiatives driven by information-sharing and partnership-building to improve cybersecurity in the healthcare sector.

"As long as we make sure that everyone at every skill level knows that they are welcome, and we make sure they get value out of volunteering, such efforts will never slow down."

(Galinkin, Erick; Cyber Threat Coalition in The CyberPeace Institute, 2020b)

Information-sharing and partnerships across sectors are crucial to accurate understanding of the threat landscape, developing new mechanisms to improve resilience and for widely-communicating emerging issues across the healthcare sector.

Informal organizations have seen the light, mostly based on individual volunteering like the COVID-19 Cyber Threat Coalition, which rallied experts in their first months of operation, exchanging indicators of compromise, taking down botnets and malicious domains notably. Long-

standing volunteer-based organizations active in medical cybersecurity like I Am The Cavalry, have also seen many experts join their ranks in hopes to be able to help.

Active assistance and information-sharing, public-private communities like Health-ISAC or Medical ISAC Japan continue to play a crucial role during the pandemic while some private-sector companies have put competition aside and collaborated to provide free cybersecurity support to the healthcare sector, like the Cyber Alliance to Defend Our Healthcare. Healthcare professionals can also benefit from threat-centric initiatives, such as No More Ransom! or the recently created Ransomware Task Force.

In Academia, the University of Sheffield put together the SEC3R platform, a diverse repository of tools and other resources for security professionals to help them respond to COVID-19-related threats.

Lead sector	Lead organization	Initiative	Description
Academia	Sheffield Hallam University	Sec3R[20]	A platform that converges the capabilities of the security research community to support efforts to combat COVID-19 and provide knowledge and resources for public authorities, blue light services and researchers worldwide.
International organization	ITU[21]	CYB4COVID	Encourages the sharing of information about initiatives, actions, resources and projects on cybersecurity.
	EUROPOL	No More Ransom!	Law enforcement and cybersecurity companies join forces to help victims of ransomware retrieve encrypted data without having to pay the ransom and educate users about ransomware and countermeasures to prevent infection.
Private- Sector Partnership		Cyber Alliance to Defend our Healthcare	An alliance of cyber professionals who focus on the cyber defence of healthcare systems and providers.
Public-Private Partnership	H-ISAC HEALTH-ISAC	Health Information Sharing and Analysis Center	A trusted community of critical infrastructure owners and operators within the Health Care and Public Health sector primarily focused on sharing information.
	医療ISAC	Medical ISAC Japan	Raises awareness of the importance of information security in the medical field and provides specific services to solve information security-related problems.
	IST[22]	Ransomware Task Force	The taskforce will develop a comprehensive framework of actionable solutions to mitigate the threat presented by ransomware through extensive engagement.
Volunteers	COVID-19 CYBER THREAT COALITION	COVID-19 Cyber Threat Coalition	A global volunteer community focused on stopping cybercriminals from attacking critical institutions through intelligence-sharing.
	I AM THE Cavalry	Hippocratic Oath for Connected Medical Devices	A volunteer organization devoted to improving the security of four main focus areas: medical devices, transportation, connected homes, and infrastructure.

Initiatives that provide tools and services to help targets protect themselves from cyberattacks.

Private companies, on their own initiative, have adapted their commercial offering to better support healthcare organizations, sometimes for free, as the latter integrated remote-working operations and faced heightened risks.

Lead sector	Private company	Initiative	Description
Private sector	Microsoft	AccountGuard for Healthcare	A security service offered at no cost designed to help highly targeted healthcare customers protect themselves from cybersecurity threats.
	kaspersky	B2B product availability	Free availability of endpoint security products for healthcare organizations, to help them stay protected from cyberthreats during the pandemic.

Initiatives aimed at raising awareness, both within the healthcare sector and the general public, to improve cyber hygiene and help defend against cyberattacks in the future.

Established national or regional cybersecurity organizations and law enforcement agencies have naturally increased their focus on healthcare and warned (Henriquez, 2020) of upcoming threats targeting hospitals

[20] Security Research Rapid Response to COVID-19

[21] International Telecommunication Union: United Nations specialized agency for information and communication technologies

[22] Institute for Security and Technology

and vaccine research centers, and helped defend against or recover from attacks.

International organizations have launched specific information pages, like the European Union Agency for Cybersecurity, the United Nations or the World Health Organization. Health associations have taken on similar initiatives such as the American Health Association (AHA) or the Healthcare Information and Management Systems Society (HIMSS, 2019).

Lead sector	Lead organization	Initiative	Description
Government	CISA	Information and updates on COVID-19	Brings partners in industry and the federal government together to improve American cyber and infrastructure security.
	incibe_ [23]	#CiberCOVID19	A campaign whose objective is to help citizens and organizations improve their cybersecurity, providing advice and solutions.
	Basque Cybersecurity Centre	Awareness kit against COVID-19	Awareness kit for citizens with tips to help avoid risks in the face of the increase in cyberattacks arising from COVID-19.
International organization	enisa [24]	COVID-19 Awareness Raising Campaign	Awareness campaign and sharing of cybersecurity recommendations on a variety of topics as well as updates on security advice to affected sectors.
	INTERPOL	COVID-19 Cyber Threats Campaign	Public awareness campaign and prevention tips.
	World Health Organization	COVID-19 Awareness Raising	Public awareness raising in the context of the COVID-19 pandemic.

[23] Instituto Nacional de Ciberseguridad, Spain

[24] EU Agency for Cybersecurity

7.2 Incident-response initiatives

Initiatives providing incident response and support to healthcare targets following a cyberattack to help in investigating the threat and secure infrastructure to return or maintain operational activity.

The cybersecurity support ecosystem benefits from a multitude of **CERTs** (**Computer Emergency Response Teams**) created with varying focal points: national, sectorial, commercial, organizational or educational. Although CERTs are primarily involved in incident-response activities and information-sharing initiatives, they operate in a intertwined network cooperation scheme that exchanges threat and remediation information to improve responses during a cyber incident. Since 1990, the FIRST community has coordinated CERT memberships to improve coordination and trust-building among members. (FIRST, no date). During the COVID-19 pandemic, CERTs, spearheaded initiatives to bring volunteers together in support of the healthcare sector.

Public-private cooperation have evolved with new initiatives emerging such as We Help Our Hospitals in Belgium, Wijhelpenziekenhuizen in the Netherlands, the COVID-19 Cyber Defence Force in Canada or the CTI League, which brought cybersecurity experts together for free to help national hospitals facing critical cyberattacks.

Lead sector	Lead organization	Initiative	Description
Public-Private Partnership	WEHELPOURHOSPITALS.BE		A group of security experts who are on call to ensure critical healthcare providers in Belgium can remain up and running in times of need.
Private-Sector Partnership	Z CERT	We Helpen Hospitals coalition	The coalition offers free of charge support to healthcare organizations in urgent need of cybersecurity expertise and services.
Volunteers	CTI [25]	CTI League	The CTI League is the first Open Global Volunteer Emergency Response Center aiming to create a safer cyberspace for healthcare organizations worldwide.
	SecDev	COVID-19 Cyber Defence Force	A volunteer-based program calling on Canada's top cybersecurity and IT professionals to join forces to protect key services and critical infrastructure from cyberattacks by developing strategies and enhancing cybersecurity.
	CV19	CV19-RO	An operational initiative through CERT.RO with 180 volunteers coming together to focus on prevention, identification and response services to possible computer vulnerabilities in the Romanian medical system.

7.3 Victim-support initiatives

Initiatives providing practical assistance and psychological support to victims of cyberattacks.

Civil society has launched a number of initiatives to support victims impacted by cyberattacks on healthcare. The Finnish Red Cross provided a helpline following the attack on the Vastaamo Psychotherapy Center publicly disclosed in 2020, while CyberHelpLine in the United Kingdom helps individuals avoid COVID-19-related scams.

[25] Cyber Threat Intelligence League

Lead sector	Lead organizations	Initiative	Description
Civil Society	The Cyber Helpline	The Cyber Helpline	A free, confidential helpline for individuals who have been a victim of cybercrime and helps them understand, contain, recover and learn from cyberattacks by linking them with cybersecurity technology and experts.
	Punainen Risti	HelpLine of the Finnish Red Cross	The helpline provides free crisis assistance to victims of the Vastaamo Psychotherapy Center data breach. Finnish Red Cross volunteers trained in psychological support answer calls to the helpline (Valtioneuvosto, 2020).
Hybrid	CyberPeace Institute	Cyber 4 Healthcare	A designated service for healthcare organizations fighting COVID-19 to find, in one click, trusted, free cybersecurity assistance provided by qualified and reputable companies.

The CyberPeace Institute's initiative, Cyber 4 Healthcare, is led by civil society, leverages volunteers and connects any organization in the fight against COVID-19 with renowned cybersecurity companies that have agreed to provide their help for free. From pentests to audits and network security hardening, for NGOs in India to social entrepreneurs in Latin America and vaccine research organizations in Europe, Cyber 4 Healthcare brings a highly tailored assistance to organizations whose only fight right now should be against the pandemic.

Most beneficiaries that the Institute helped in Cyber 4 Healthcare handle patient or clinical data. As such, data protection is always a key concern, followed by remote-working issues. In our experience, the level of cybersecurity maturity is generally very low even for large beneficiaries (100+ staff), and so assistance services provided thus far revolve around basic cybersecurity measures: website pentest, first-level security audit, awareness training to staff, support to implement two-factor authentication, etc.

Another key finding of Cyber 4 Healthcare concerns the trust capital required to provide cybersecurity assistance in a sector that is so critical to human life. Due to common misconceptions around cybersecurity arising from limited digital literacy, only highly targeted and specialized initiatives have a chance of success. As such, more so than in other verticals, contextual efforts through local partners in healthcare, are critical to building the trust capital just to be in a position to help.

Appendices

Report Methodology

The Report is based on desktop research of open-source information with reliance on trusted primary and secondary sources including cybersecurity firms, academia, technology companies, government agencies, international organizations and civil society. A review was undertaken of international law and regulatory frameworks, and applied to cases in the healthcare sector. A wide literature review was also conducted to support our work.

Media and news outlets as well as social media platforms have been used to a lesser degree to better understand the public perception of attacks or to direct the researcher towards the primary source of information. Research was conducted on underground forums and marketplaces on topics such as the publication, marketing and sale of data following a breach to complement information retrieved from other sources.

Consultations have taken place with healthcare cybersecurity researchers, hospital staff, legal experts, reporters and victims of cyberattacks in healthcare as part of the drafting and review process for this Report to encourage transparency and ensure findings are corroborated by those working directly with or in the healthcare sector. Information was also gathered through expert panels and CyberPeace Labs organized or attended by the CyberPeace Institute.

Limitations

The Report is not exhaustive and acknowledges that there are other threat actors, stakeholders, techniques, and instruments that come into play aside from those mentioned herein. For example, Chapter 5 on international law and norms is not exhaustive, but rather presents a condensed overview with a specific application to protection of the healthcare sector. The focus is on those most prominent threats to healthcare and for which a global response would be most relevant. The Report attempts to cover a global scope but recognizes there are methodological and data limitations.

The research was conducted primarily in English with a reliance on a select set of search engines. This is likely to result in an unintentional filtering of information published in the English language and thus inadvertently limiting access to information from certain regions or countries. This may lead the global picture to be skewed towards a western perception of the threat. Collaboration with global partners on future reports will ensure greater diversity in the representation of regional information.

There is no global and concrete set of data relating to attacks on the healthcare sector. Data may be collected at a national level, though this is not always the case, and aggregated with data from other sectors and across attack types making it difficult to break down the problem into its constituent parts. There is no set methodology or international reporting / recording standards for attacks on healthcare. A significant proportion of the research and analysis currently available is focused on threat actors and their tactics, techniques and procedures (TTPs) with very limited information on victims, targets and the societal impact of attacks. This Report advocates systematic and standardized collection, analysis and sharing of information to provide ever-better responses and facilitate international collaboration.

Glossary

A	**Advanced Persistent Threat (APT)**	Highly sophisticated and systematic cyberattack campaigns or programs.
	Attack and Cyberattack	A disruptive cyber incident, data breach or a disinformation operation conducted by a threat actor using a computer network or system with malicious intent to cause damage (technical, financial, reputational or other) or extract / steal data without consent.
	Attack Vector	Technique or technology leveraged to execute an attack, sometimes using well-known or undisclosed vulnerabilities.
B	**Backdoor**	Hidden mechanism used to access a computer system or data without authorized access credentials.
	Backup	Copy of computer data that is kept in a safe environment, to be used in case of infrastructure failure to restore a system to a working condition.
	Bitcoin	A type of virtual or cryptocurrency.
	Botnet	Stemming from the words robot and network, a network of devices infected with malware and controlled by a threat actor. Used to automate and increase the magnitude of attacks.
	Breach	See Data breach.
	BYOD	Bring Your Own Device. A policy allowing or encouraging employees to use their own computer or smartphone for professional activity.
C	**CERTs**	Computer Emergency Response Teams are expert groups that handle cybersecurity incidents.
	CISO	Chief Information Security Officer. Senior-level executive responsible for establishing and maintaining the security of data and information within an entity.
	Cryptocurrency	Digital asset designed to be used as a trustworthy and non-forgeable means of monetary exchange.
	Cybercriminal	Individuals or teams of people who use technology with malicious intent to harm or otherwise obstruct activities on digital systems or networks.
	Cyberespionage	Espionage activities conducted in cyberspace, usually through the surveillance of systems and exfiltration of data.
	Cyber Operation	The employment of cyber capabilities to achieve objectives in or through cyberspace.
	Cyberpeace	Cyberpeace exists when human security, dignity and equity are ensured in digital ecosystems.
	Cybersecurity	The practice of protecting computer systems and networks from unauthorized information disclosure, theft of or damage to their hardware, software, or electronic data. Through the application of technologies, processes and controls cybersecurity serves to reduce the risk of cyberattack and protect systems, networks and technologies.
	Cyberspace	Refers to the online world and digital systems, accessible through computer networks and the internet.
	Cyber Threat	A threat in cyberspace.
D	**Darknet**	In computer security, the darknet generally refers to websites that are specifically used for criminal purposes and cannot be accessed through the regular World Wide Web. The darknet is part of the deep web.
	Data Breach	Exposure of files containing confidential, sensitive, or protected information to an unauthorized person.
	Data Dump	When breached data is transferred from the victim's network to another location. Subsequently data can be published online for example on underground forums / marketplaces.
	Distributed Denial-of-Service (DDoS)	Distributed Denial-of-Service is an attack technique consisting of flooding a network, service or server with excessive traffic to prevent it from functioning normally. It is said to be distributed when the source of the attack is composed of several computer systems.
	Decryption	Decoding of encrypted data. See also encryption.
	Decryption Key	Piece of information needed for the decryption process.
	Deep Web	The part of the World Wide Web that is not indexed by search engines, and therefore not straightforward to access.
	Digital Forensics	Analysis of digital evidence in a criminal investigation.
	Disinformation	A type of information created to confuse and intentionally mislead. Disinformation is spread further by innocent and often well-meaning individuals, unbeknownst to them.
	Domain	On a computer network, a domain is the name given to a computer resource or set of computer resources administered by one given entity.
	Double Extortion	A.k.a. Ransomware 2.0. A type of ransomware activity whereby the victim's data is both encrypted and exfiltrated. If the victim can recover from the encryption, the attacker can threaten to make the data publicly available.
	Dump	See data dump.
	Dumpsite	A dedicated website to publish stolen data for extortion or monetization purposes.
E	**Encryption**	Encoding of data in such a way that it cannot be understood, but still conveys the same information. See also decryption.

I	**Ideological Actors**	In the context of cybercrime, cybercriminals operating in the name of a system of ideas and ideals, especially concerning economic or political theory and policy.
	Infodemic	Denotes the ever- increasing volume of both true and false information circulating in society, making it particularly challenging to distinguish the true from the false.
	IoT	Internet of Things. Describes smart devices that are connected to the internet but are not personal computers or smartphones.
	IP address	In the information technology context, Internet Protocol address.
K	**Keylogger**	A computer program designed to steal everything that is typed on the keyboard.
L	**Lateral Movement**	Denotes the way cyberattackers progressively make their way inside a network when searching for critical assets and ultimately reach their target.
	Log (file)	A log or log file is a collection of information that is gathered by a computer system during normal operation and aimed at an easier diagnostic in case of failure.
M	**Malspam**	Malware delivered as malicious attachments in spam email.
	Malware	Intrusive or malicious software designed to damage or destroy computer systems. e.g. viruses, trojans, ransomware and spyware.
P	**Password Spraying**	Technique applied to acquire user credentials by trying a few known or common passwords with a lot of different computer accounts.
	Patch	A piece of software whose purpose is to fix a software bug or vulnerability.
	Pentest	Short for Penetration Testing. Activity consists in trying to find as many vulnerabilities or weaknesses as possible in a computer system.
	Phishing	A fraudulent communication, purporting to be from a reputable source, with the aim to trick the recipient into giving away sensitive data or installing malware.
	Privilege Escalation	In a computer system, getting access to a higher level of privilege, that is, to a greater number of abilities.

R	**Ransomware**	A type of malware designed to extort money by encrypting / blocking access to files or the computer system until a ransom is paid.
	Ransomware-as-a-Service (RaaS)	Ransomware-as-a-Service (RaaS) functions as a form of Software-as-a-Service (SaaS) model. RaaS are used by cybercriminals to facilitate the processes of launching ransomware attacks. This malicious model allows anyone to become an 'affiliate' of an established RaaS package or service.
	Remote Desktop Protocol (RDP)	RDP allows users to connect to and use computers or servers remotely over the internet. Machines offering RDP may be abused to access an organization's systems and install malware.
	RDP Shop	A website where lists of RDP credentials for compromised computers and systems can be found.
S	**Social Engineering**	Psychological manipulation of a person to make him/her perform an action or give away some information.
	Software Co-Development	A model of software development involving the collaboration of several entities on the same software project.
	Source Code	Description of the behavior of a computer software written in a programming language by a developer.
	Spear-Phishing	Targeted phishing, exploiting real information about the victim in order to make the source of the attack even more credible.
	Spyware	Software designed to spy on the activity of a computer user.
	Supply Chain Attack	A supply chain attack is a cyberattack that aims at damaging an organization by targeting less secure elements in its supply chain.
T	**Tactics, Techniques, and Procedures (TTPs)**	The various steps, methods and tools that a threat actor uses to conduct a cyberattack from the tactical to the operational level.
	Triple Extortion	Double extortion supplemented with threatening people whose personal data has been stolen, also known as Ransomware 3.0.
	Trojan	Software that hides its true purpose from the user. Derived from the Trojan Horse, a subterfuge used by the ancient Greeks to enter the independent city of Troy.
V	**VB Script**	Visual Basic scripts are small programs that can be run in Microsoft Windows and Microsoft Office, often incorrectly referred to as 'Word macros'.
	Virus	Software designed to replicate itself and propagate in a computer infrastructure.
	Vulnerability (Vuln)	A vulnerability is an error in a piece of software that may be exploited to compromise a computer system.
Z	**Zip file**	A type of file containing data in a more compact form.

References

Abrams, L. (2020a) *Ransomware Gangs to Stop Attacking Health Orgs During Pandemic*, *BleepingComputer*. Available at: https://www.bleepingcomputer.com/news/security/ransomware-gangs-to-stop-attacking-health-orgs-during-pandemic/ (Accessed: 16 February 2021).

Abrams, L. (2020b) 'Ransomware recruits affiliates with huge payouts, automated leaks', *BleepingComputer*, 15 May. Available at: https://www.bleepingcomputer.com/news/security/ransomware-recruits-affiliates-with-huge-payouts-automated-leaks/ (Accessed: 12 January 2021).

African Union (2014) 'African Union Convention on Cyber Security and Personal Data Protection'. Available at: https://www.opennetafrica.org/?wpfb_dl=4 (Accessed: 15 February 2021).

Agenda.ge (2020) *Documents stolen from Lugar Lab following foreign cyber attack*, *Agenda.ge*. Available at: https://agenda.ge/en/news/2020/2725 (Accessed: 11 January 2021).

Ajaz, S. (2020) 'Coronavirus Drugmaker Gilead A Target Of Iranian Hackers.', *PrivacySpoof*, 5 August. Available at: https://privacyspoof.com/infosec-news-blogs/coronavirus-drugmaker-gilead-hackers/ (Accessed: 8 February 2021).

Akande, D., Hollis, D., *et al.* (2020) *The Oxford Statement on the International Law Protections Against Cyber Operations Targeting the Health Care Sector*. Available at: https://www.ejiltalk.org/oxford-statement-on-the-international-law-protections-against-cyber-operations-targeting-the-health-care-sector/ (Accessed: 7 January 2021).

Akande, D., Coco, A., *et al.* (2020) *The Second Oxford Statement on International Law Protections of the Healthcare Sector During Covid-19: Safeguarding Vaccine Research*. Available at: https://www.ejiltalk.org/the-second-oxford-statement-on-international-law-protections-of-the-healthcare-sector-during-covid-19-safeguarding-vaccine-research/ (Accessed: 15 February 2021).

Al Qartah, A. (2020) *Evolving Ransomware Attacks on Healthcare Providers*. Utica College. Available at: http://rgdoi.net/10.13140/RG.2.2.23202.45765 (Accessed: 11 January 2021).

Allgaier, J. and Svalastog, A. L. (2015) 'The communication aspects of the Ebola virus disease outbreak in Western Africa – do we need to counter one, two, or many epidemics?', *Croatian Medical Journal*, 56(5), pp. 496–499. doi: 10.3325/cmj.2015.56.496.

ANY.RUN (2021) *WannaCry*, *Malware Trends Tracker*. Available at: https://any.run/malware-trends/wannacry (Accessed: 10 February 2021).

Aravindakshan, S. (2020) 'Cyberattacks: a look at evidentiary thresholds in International Law', *Indian Journal of International Law*, pp. 1–15. doi: 10.1007/s40901-020-00113-0.

Armis (2019) *Two Years In and WannaCry is Still Unmanageable*, *Armis*. Available at: https://www.armis.com/resources/iot-security-blog/wannacry/ (Accessed: 10 February 2021).

Australia *et al.* (2020) 'Malicious cyber activity against healthcare services and facilities. Joint OEWG Report Proposal from Australia, Czech Republic, Estonia, Japan, Kazakhstan and United States of America'. Available at: https://front.un-arm.org/wp-content/uploads/2020/05/final-joint-oewg-proposal-protection-of-health-infrastructure.pdf (Accessed: 2 January 2021).

Bada, M. and Nurse, J. R. C. (2019) 'The Social and Psychological Impact of Cyber-Attacks', in Benson, V. and McAlaney, J. (eds) *Emerging cyber threats and cognitive vulnerabilities*. 1st edn. San Diego: Elsevier, pp. 73–92.

Bajak, F. (2020) 'Hacked hospital chain says all 250 US facilities affected', *AP NEWS*, 10 January. Available at: https://apnews.com/article/virus-outbreak-malware-software-1d76456be-a2036b97d3a83f81e43dabe (Accessed: 17 February 2021).

Barrett, B. (2016) 'Hack Brief: Hackers Are Holding an LA Hospital's Computers Hostage', *Wired*, 26 February. Available at: https://www.wired.com/2016/02/hack-brief-hackers-are-holding-an-la-hospitals-computers-hostage/ (Accessed: 1 February 2021).

Bartlett, J. (2020) 'Massachusetts hospitals on high alert after phishing emails target execs – Boston Business Journal', *Boston Business Journal*, 11 April. Available at: https://www.bizjournals.com/boston/news/2020/11/04/cyber-attack-on-ma-hospitals-leads-to-high-alert.html (Accessed: 28 January 2021).

Beardsley, T. (2018) 'R7-2018-01 (CVE-2018-5551, CVE-2018-5552): DocuTrac Office Therapy Installer Hard-Coded Credentials and Cryptographic Salt', *Rapid7*, 14 March. Available at: https://blog.rapid7.com/2018/03/14/r7-2018-01-cve-2018-5551-cve-2018-5552-docutrac-office-therapy-installer-hard-coded-credentials-and-cryptographic-salt/ (Accessed: 26 February 2021).

Beek, C. (2018) 'McAfee Researchers Find Poor Security Exposes Medical Data to Cybercriminals', *McAfee Blogs*, 3 November. Available at: https://www.mcafee.com/blogs/other-blogs/mcafee-labs/mcafee-researchers-find-poor-security-exposes-medical-data-to-cybercriminals/ (Accessed: 11 January 2021).

Bernard, R. *et al.* (2020) 'Disinformation and Epidemics: Anticipating the Next Phase of Biowarfare', *Health Security*. doi: 10.1089/hs.2020.0038.

Besson, S. (2011) 'Sovereignty', *Max Planck Encyclopedias of International Law*. Available at: https://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e1472?prd=OPIL (Accessed: 15 February 2021).

Bing, C. and Taylor, M. (2020) 'Exclusive: China-backed hackers "targeted COVID-19 vaccine firm Moderna"', *Reuters*, 30 July. Available at: https://www.reuters.com/article/us-health-coronavirus-moderna-cyber-excl-idUSKCN24V38M (Accessed: 8 February 2021).

Bischoff, P. (2020) '172 ransomware attacks on US healthcare organizations since 2016 (costing over $157 million)', 11 February. Available at: https://www.comparitech.com/blog/information-security/ransomware-attacks-hospitals-data/ (Accessed: 17 February 2021).

Bisson, D. (2020) 'Supply Chain Risks in Health Care: Time to Increase Security', *Security Intelligence*. Available at: https://securityintelligence.com/articles/supply-chain-risks-healthcare-opportunity-to-increase-security/ (Accessed: 17 February 2021).

BitSight (no date) 'Do hospital data breaches reduce patient care quality?' (BitSight Risk Review). Available at: https://info.bitsight.com/bitsight-risk-review-episode-16 (Accessed: 8 February 2021).

Bracken, B. (2021) 'Cyberattacks on Healthcare Spike 45% Since November', *Threat Post*, 1 May. Available at: https://threatpost.com/cyberattacks-healthcare-spike-ransomware/162770/ (Accessed: 16 February 2021).

Burt, T. (2020) 'Cyberattacks targeting health care must stop', *Microsoft On the Issues*, 13 November. Available at: https://blogs.microsoft.com/on-the-issues/2020/11/13/health-care-cyberattacks-covid-19-paris-peace-forum/ (Accessed: 11 January 2021).

BusinessWire (2019) 'New Study Reveals Cybercrime May Be Widely Underreported—Even When Laws Mandate Disclosure', *BusinessWire*, 6 March. Available at: https://www.businesswire.com/news/home/20190603005858/en/New-Study-Reveals-Cybercrime-May-Be-Widely-Underreported%E2%80%94Even-When-Laws-Mandate-Disclosure (Accessed: 31 January 2021).

Campus Safety Magazine (2018) 'Indiana Hospital Pays Bitcoin Ransom After Computer System Hacked', *Campus Safety Magazine*, January/February 2018, p. 12.

Canadian Centre for Cyber Security (2018) *Canadian Centre for Cyber Security*, *Canadian Centre for Cyber Security*. Available at: https://cyber.gc.ca/en/ (Accessed: 17 February 2021).

Carr, N. (2017) *Cyber Espionage is Alive and Well: APT32 and the Threat to Global Corporations*, *FireEye Inc*. Available at: https://www.fireeye.com/blog/threat-research/2017/05/cyber-espionage-apt32.html (Accessed: 17 February 2021).

Causit, C. (2021) 'Covid-19 : Comment les cybercriminels cherchent à profiter de la pandémie', *FranceInfo*, 2 May. Available at: https://www.francetvinfo.fr/sante/maladie/coronavirus/covid-19-comment-les-cybercriminels-cherchent-a-profiter-de-la-pandemie_4246923.html (Accessed: 8 February 2021).

CBS News (2020) 'Cyberattack hobbles hospital chain Universal Health Services', *CBS News*, 29 September. Available at: https://www.cbsnews.com/news/cyberattack-universal-health-services-hospital-chain-united-states/ (Accessed: 17 February 2021).

Charter of Trust (2018) *Charter of Trust*, *Charter of Trust*. Available at: https://www.charteroftrust.com/about/ (Accessed: 15 February 2021).

Check Point Software (2020) 'Hospitals Targeted in Rising Wave of Ryuk Ransomware Attacks', *Check Point Software*, 29 October. Available at: https://blog.checkpoint.com/2020/10/29/hospitals-targeted-in-rising-wave-of-ryuk-ransomware-attacks/ (Accessed: 12 January 2021).

Check Point Software (2021) 'Attacks targeting healthcare organizations spike globally as COVID-19 cases rise again', *Check Point Software*, 1 May. Available at: https://blog.checkpoint.com/2021/01/05/attacks-targeting-healthcare-organizations-spike-globally-as-covid-19-cases-rise-again/ (Accessed: 12 January 2021).

Choi, S. J., Johnson, M. E. and Lehmann, C. U. (2019) 'Data breach remediation efforts and their implications for hospital quality', *Health Services Research*, 54(5), pp. 971–980. doi: 10.1111/1475-6773.13203.

Cimpanu, C. (2020a) 'Here's a list of all the ransomware gangs who will steal and leak your data if you don't pay', *ZDNet*, 21 April. Available at: https://www.zdnet.com/article/heres-a-list-of-all-the-ransomware-gangs-who-will-steal-and-leak-your-data-if-you-dont-pay/ (Accessed: 25 January 2021).

Cimpanu, C. (2020b) 'Top exploits used by ransomware gangs are VPN bugs, but RDP still reigns supreme', *ZDNet*, 24 August. Available at: https://www.zdnet.com/article/top-exploits-used-by-ransomware-gangs-are-vpn-bugs-but-rdp-still-reigns-supreme/ (Accessed: 28 January 2021).

CIS (no date) *Cybersecurity Spotlight – Cyber Threat Actors*, *Center for Internet Security*. Available at: https://www.cisecurity.org/spotlight/cybersecurity-spotlight-cyber-threat-actors/ (Accessed: 17 February 2021).

ClearSky Security Ltd. (2020) *The Kittens Are Back in Town 3*. ClearSky Security Ltd. Available at: https://www.clearskysec.com/wp-content/uploads/2020/08/The-Kittens-are-Back-in-Town-3.pdf.

CNBC (2020) 'Cyberattack hobbles major hospital chain's U.S. facilities', *CNBC*, 29 September. Available at: https://www.cnbc.com/2020/09/29/cyberattack-hobbles-major-hospital-chains-us-facilities.html (Accessed: 31 January 2021).

Correia, S., Luck, S. and Verner, E. (2020) *Pandemics Depress the Economy, Public Health Interventions Do Not: Evidence from the 1918 Flu*. SSRN Scholarly Paper ID 3561560. Rochester, NY: Social Science Research Network. doi: 10.2139/ssrn.3561560.

Council of Europe (2001) *Convention on Cybercrime*. Brussels, BE: Council of Europe, pp. 1–22. Available at: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680081561 (Accessed: 20 December 2020).

Council of the European Union (2017) *Cyber attacks: EU ready to respond with a range of measures, including sanctions*, *Council of the European Union*. Available at: https://www.consilium.europa.eu/en/press/press-releases/2017/06/19/cyber-diplomacy-toolbox/ (Accessed: 15 February 2021).

Coventry, L. and Branley-Bell, D. (2018) 'Cybersecurity in healthcare: A narrative review of trends, threats and ways forward', *Maturitas*, 113. doi: 10.1016/j.maturitas.2018.04.008.

Coveware (2020) *Ransomware Demands continue to rise as Data Exfiltration becomes common, and Maze subdues*, *Coveware: Ransomware Recovery First Responders*. Available at: https://www.coveware.com/blog/q3-2020-ransomware-marketplace-report (Accessed: 12 January 2021).

Coveware (2021) *Ransomware Payments Fall as Fewer Companies Pay Data Exfiltration Extortion Demands*, *Coveware: Ransomware Recovery First Responders*. Available at: https://www.coveware.com/blog/ransomware-marketplace-report-q4-2020 (Accessed: 16 February 2021).

Cyber Security Policy (2018) *Securing cyber resilience in health and care*. London, UK: Department of Health & Social Care. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/747464/securing-cyber-resilience-in-health-and-care-september-2018-update.pdf (Accessed: 17 February 2021).

Cybersecurity Tech Accord (no date) *Cybersecurity Tech Accord*, *Cybersecurity Tech Accord*. Available at: https://cybertechaccord.org/accord/ (Accessed: 15 February 2021).

Cyble Inc (2020) 'Huiying Medical Breached; Source Code for AI-assisted COVID-19 Detection, and Experimental Data of COVID-19 on Sale', *Cyble Inc.*, 25 April. Available at: https://cybleinc.com/2020/04/25/huiying-medical-breached-source-code-for-ai-assisted-covid-19-detection-and-experimental-data-of-covid-19-on-sale/ (Accessed: 31 January 2021).

Davis, J. (2020a) *87% Health Orgs Lack Security Personnel for Effective Cyber Posture*, *Health IT Security*. Available at: https://healthitsecurity.com/news/87-health-orgs-lack-security-personnel-for-effective-cyber-posture (Accessed: 11 January 2021).

Davis, J. (2020b) *Blackbaud Ransomware Hack Affects 657K Maine Health System Donors*, *HealthITSecurity*. Available at: https://healthitsecurity.com/news/blackbaud-ransomware-hack-affects-657k-maine-health-system-donors (Accessed: 8 February 2021).

Delerue, F. (2020) *Cyber Operations and International Law*. Cambridge: Cambridge University Press (Cambridge Studies in International and Comparative Law). doi: 10.1017/9781108780605.

Deloitte (2016) *Beneath The Surface – A deeper look at business impacts*, *Deloitte United States*. Available at: https://www2.deloitte.com/us/en/pages/risk/articles/hidden-business-impact-of-cyberattack.html (Accessed: 16 February 2021).

Devine, D. *et al.* (2020) 'Trust and the Coronavirus Pandemic: What are the Consequences of and for Trust? An Early Review of the Literature', *Political Studies Review*, p. 1478929920948684. doi: 10.1177/1478929920948684.

DICoD (2019) *International Law Applied to Operations in Cyberspace*. Délégation à l'information et à la communication de la défense, p. 20. Available at: https://www.defense.gouv.fr/content/download/567648/9770527/file/international+law+applied+to+operations+in+cyberspace.pdf.

Drees, J. (2020) *What 4 facilities did after ransomware attacks: Permanent closures, temporary service suspensions & more*, *Beckers Hospital Review*. Available at: https://www.beckershospitalreview.com/cybersecurity/4-hospitals-that-closed-after-ransomware-attacks.html (Accessed: 9 February 2021).

Edelman, K. and Dinesh, A. (2018) *The state of cybersecurity at financial institutions*. Deloitte, p. 16. Available at: https://www2.deloitte.com/content/dam/Deloitte/de/Documents/risk/Deloitte-Risk-Cybersecurity-Financial-Institutions.pdf (Accessed: 17 February 2021).

Egloff, F. J. (2020) 'Contested public attributions of cyber incidents and the role of academia', *Contemporary Security Policy*, 41(1), pp. 55–81. doi: 10.1080/13523260.2019.1677324.

EMA (2020) *Cyberattack on EMA – update 3*, *European Medicines Agency*. Available at: https://www.ema.europa.eu/en/news/cyberattack-ema-update-3 (Accessed: 9 February 2021).

EMA (2021) *Cyberattack on EMA – update 5*, *European Medicines Agency*. Available at: https://www.ema.europa.eu/en/news/cyberattack-ema-update-5 (Accessed: 2 February 2021).

Eoyang, M. *et al.* (2018) *To Catch a Hacker: Toward a comprehensive strategy to identify, pursue, and punish malicious cyber actors*. Third Way, pp. 1–37. Available at: https://thirdway.imgix.net/pdfs/override/To_Catch_A_Hacker_Report.pdf.

ET CISO (2019) 'LGBT+ people in Singapore "more fearful" after HIV data leak', *The Economist Times CISO*, 30 January. Available at: https://ciso.economictimes.indiatimes.com/news/lgbt-people-in-singapore-more-fearful-after-hiv-data-leak/67749845 (Accessed: 26 February 2021).

EU vs DiSiNFO (2020) *EEAS SPECIAL REPORT UPDATE: Short Assessment of Narratives and Disinformation Around the COVID-19 Pandemic (UPDATE MAY – NOVEMBER)*, *EU vs DiSiNFO*. Available at: https://euvsdisinfo.eu/eeas-special-report-update-short-assessment-of-narratives-and-disinformation-around-the-covid-19-pandemic-update-may-november/ (Accessed: 17 February 2021).

European Commission (2020a) *Medical Devices – New regulations*, *Public Health – European Commission*. Available at: https://ec.europa.eu/health/md_newregulations/overview_en (Accessed: 15 February 2021).

European Commission (2020b) *Proposal for directive on measures for high common level of cybersecurity across the Union*, *Shaping Europe's digital future – European Commission*. Available at: https://ec.europa.eu/digital-single-market/en/news/proposal-directive-measures-high-common-level-cybersecurity-across-union (Accessed: 26 February 2021).

European Commission (no date) *Protecting critical infrastructure in the EU – new rules*, *European Commission*. Available at: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12462-Enhancement-of-European-policy-on-critical-infrastructure-protection (Accessed: 16 February 2021).

European Parliament and Council of the European Union (2016) 'Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)'. Official Journal of the European Union.

European Union (2020) *COUNCIL DECISION (CFSP) 2020/1127*, *Official Journal of the European Union*. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32020D1127&from=EN (Accessed: 17 February 2021).

Europol (2020) *Internet Organized Crime Threat Assessment 2020*. Den Haag, NL: European Union Agency for Law Enforcement Cooperation, p. 64. Available at: https://www.europol.europa.eu/sites/default/files/documents/internet_organised_crime_threat_assessment_iocta_2020.pdf.

FBI (2016) *Ransomware Victims Urged to Report Infections to Federal Law Enforcement*, *Internet Crime Complaint Center (IC3)*. Available at: https://www.ic3.gov/Media/Y2016/PSA160915 (Accessed: 17 February 2021).

FBI (2020) 'Kwampirs Malware Employed in Ongoing Cyber Supply Chain Campaign Targeting Global Industries, including Healthcare Sector', 20 March. Available at: https://isc.sans.edu/diaryimages/Kwampirs_PIN_20200330-001.pdf.

FBI & CISA (2020) 'People's Republic of China (PRC) Targeting of COVID-19 Research Organizations'. FBI & CISA. Available at: https://www.aha.org/system/files/media/file/2020/05/Joint_FBI-CISA_PSA_China_Cyber-COVID-19_05082020_FINAL4.pdf.

FDA (2020) *Cybersecurity*, *U.S. Food & Drug Administration*. FDA. Available at: https://www.fda.gov/medical-devices/digital-health-center-excellence/cybersecurity (Accessed: 26 February 2021).

Ferguson, S. and Venkat, A. (2020) 'Hackers Targeted World Health Organization', *BankInfoSecurity*, 24 March. Available at: https://www.bankinfosecurity.com/hackers-targeted-who-spear-phishing-attack-a-14003 (Accessed: 5 February 2021).

FireEye (2019) *Beyond Compliance: Cyber Threats and Healthcare*, p. 10. Available at: https://content.fireeye.com/cyber-security-for-healthcare/rpt-beyond-compliance-cyber-threats-and-healthcare (Accessed: 16 February 2021).

FIRST (no date) *Improving Security Together*, *FIRST — Forum of Incident Response and Security Teams*. Available at: https://www.first.org/ (Accessed: 19 February 2021).

Fruhlinger, J. (2018) *What is WannaCry ransomware, how does it infect, and who was responsible?*, *CSO Online*. Available at: https://www.csoonline.com/article/3227906/what-is-wannacry-ransomware-how-does-it-infect-and-who-was-responsible.html (Accessed: 9 February 2021).

Gatlan, S. (2020a) 'Dozens of ransomware gangs partner with hackers to extort victims', *BleepingComputer*, 16 November. Available at: https://www.bleepingcomputer.com/news/security/dozens-of-ransomware-gangs-partner-with-hackers-to-extort-victims/ (Accessed: 12 January 2021).

Gatlan, S. (2020b) 'FBI warns of COVID-19 phishing targeting US health providers', *BleepingComputer*, 21 April. Available at: https://www.bleepingcomputer.com/news/security/fbi-warns-of-covid-19-phishing-targeting-us-health-providers/ (Accessed: 12 January 2021).

Gatlan, S. (2020c) 'UHS hospitals hit by reported country-wide Ryuk ransomware attack', *BleepingComputer*, 28 September. Available at: https://www.bleepingcomputer.com/news/security/uhs-hospitals-hit-by-reported-country-wide-ryuk-ransomware-attack/ (Accessed: 1 February 2021).

Gatlan, S. (2020d) 'UHS restores hospital systems after Ryuk ransomware attack', *BleepingComputer*, 30 October. Available at: https://www.bleepingcomputer.com/news/security/uhs-restores-hospital-systems-after-ryuk-ransomware-attack/ (Accessed: 17 February 2021).

Hacia, G. (2020) 'Meet This Year's WIRED25: People Who Are Making Things Better', *Wired*, 9 September. Available at: https://www.wired.com/story/wired25-2020-people-making-things-better/ (Accessed: 16 February 2021).

Hanel, A. (2019) 'What is Ryuk Ransomware? The Complete Breakdown', *Crowdstrike*, 1 October. Available at: https://www.crowdstrike.com/blog/big-game-hunting-with-ryuk-another-lucrative-targeted-ransomware/ (Accessed: 17 February 2021).

HAPVIDA (2020) 'Notice to the market'. HAPVIDA PARTICIPAÇÕES E INVESTIMENTOS S.A. Available at: https://api.mziq.com/mzfilemanager/v2/d/6bbd1770-f9f4-44e8-a1b1-d26b7585eec1/587e9f65-cd9e-c418-5ab1-772536eb309d?origin=1 (Accessed: 17 February 2021).

Health Care Industry Cybersecurity Task Force (2017) *Report on improving cybersecurity in health care industry*. Health Care Industry Cybersecurity Task Force, p. 96.

Henderson, S. *et al.* (2020) *Vietnamese Threat Actors APT32 Targeting Wuhan Government and Chinese Ministry of Emergency Management in Latest Example of COVID-19 Related Espionage*, *FireEye Inc.* Available at: https://www.fireeye.com/blog/threat-research/2020/04/apt32-targeting-chinese-government-in-covid-19-related-espionage.html (Accessed: 11 January 2021).

Henriquez, M. (2020) 'CISA: Ransomware activity targeting the healthcare and public health sector', *Security Magazine*, 29 October. Available at: https://www.securitymagazine.com/articles/93774-cisa-ransomware-activity-targeting-the-healthcare-and-public-health-sector?v=preview (Accessed: 16 February 2021).

Herr, T. *et al.* (2020) *BREAKING TRUST: Shades of Crisis Across an Insecure Software Supply Chain*. Atlantic Council. Available at: https://www.atlanticcouncil.org/wp-content/uploads/2020/07/Breaking-trust-Shades-of-crisis-across-an-insecure-software-supply-chain.pdf.

HIMSS (2019) *What We Do Initiatives*, *Healthcare Information and Management Systems Society*. Available at: https://www.himss.org/what-we-do-initiatives (Accessed: 17 February 2021).

HIMSS (2020) *2020 HIMSS Cybersecurity Survey*. Survey. Chicago, IL: Healthcare Information and Management Systems Society, p. 32. Available at: https://www.himss.org/sites/hde/files/media/file/2020/11/16/2020_himss_cybersecurity_survey_final.pdf.

Hulsebos, R. (2020) 'How to Defend Your Network Against the Kwampirs Malware – Forescout', *Forescout*, 13 April. Available at: https://www.forescout.com/company/blog/how-to-defend-your-network-against-the-kwampirs-malware/?utm_campaign=everyonesocial&utm_source=everyonesocial&utm_medium=twitter&utm_term=262706&es_p=11560374 (Accessed: 8 February 2021).

Hunt, J. S. (2020) *The Covid-19 pandemic vs Post-Truth*. Global Health Security Network, p. 19. Available at: https://www.ghsn.org/resources/Documents/GHSN%20Policy%20Report%201.pdf.

Hyslop, W. D., Goeke, J. A. and McCulloch, S. K. (2020) *United States of America v. LI XIAOYU and DONG JIAZHI*. Available at: https://www.justice.gov/opa/press-release/file/1295981/download.

Iaria, A. (2020) 'Digital Emblems: The Protection of Health Care Facilities in the Cyber Domain in the Age of Pandemics', *Opinio Juris*, 28 October. Available at: http://opiniojuris.org/2020/10/28/digital-emblems-the-protection-of-health-care-facilities-in-the-cyber-domain-in-the-age-of-pandemics/ (Accessed: 16 February 2021).

IBM (2019) *IBM Study Shows Data Breach Costs on the Rise; Financial Impact Felt for Years*, *IBM News Room*. Available at: https://newsroom.ibm.com/2019-07-23-IBM-Study-Shows-Data-Breach-Costs-on-the-Rise-Financial-Impact-Felt-for-Years (Accessed: 9 February 2021).

IBM (2020) *Compromised Employee Accounts Led to Most Expensive Data Breaches Over Past Year*, *IBM News Room*. Available at: https://newsroom.ibm.com/2020-07-29-IBM-Report-Compromised-Employee-Accounts-Led-to-Most-Expensive-Data-Breaches-Over-Past-Year (Accessed: 16 February 2021).

IDFI (2020) *Cyberattack on the Ministry of Health and Russian Trace*, *Institute for Development of Freedom of Information*. Available at: https://idfi.ge:443/en/strategy_of_russian_cyber_operations (Accessed: 11 January 2021).

Infosec Resources (2020) *Kwampirs malware: what it is, how it works and how to prevent it | Malware spotlight*, *Infosec Resources*. Available at: https://resources.infosecinstitute.com/topic/kwampirs-malware-what-it-is-how-it-works-and-how-to-prevent-it-malware-spotlight/ (Accessed: 26 February 2021).

Intel 471 (2020a) *Alleged REvil member spills details on group's ransomware operations*, *Intel 471*. Available at: https://intel471.com/blog/revil-ransomware-interview-russian-osint-100-million/ (Accessed: 9 February 2021).

Intel 471 (2020b) 'Ransomware-as-a-service: The pandemic within a pandemic', *Intel 471*, 16 November. Available at: https://intel471.com/blog/ransomware-as-a-service-2020-ryuk-maze-revil-egregor-doppelpaymer/ (Accessed: 1 February 2021).

Intel 471 (2020c) *Understanding the relationship between Emotet, Ryuk and TrickBot*, *Intel 471*. Available at: https://intel471.com/blog/understanding-the-relationship-between-emotet-ryuk-and-trickbot/ (Accessed: 17 February 2021).

i-SCOOP (no date) 'Evolutions in healthcare and cybersecurity threats – beyond compliance', *i-SCOOP*. Available at: https://www.i-scoop.eu/cyber-security-cyber-risks-dx/healthcare-and-cybersecurity-beyond-compliance/ (Accessed: 11 January 2021).

Jay (2020) 'Indian drugmaker Dr. Reddy's Laboratories suffers major cyber attack', *teiss Cyber Brief*, 22 October. Available at: https://www.teiss.co.uk/dr-reddys-laboratories-cyber-attack/ (Accessed: 8 February 2021).

Johnson, A. L. (2017) 'Endpoint Protection – Symantec Enterprise', *Broadcom*, 22 May. Available at: https://community.broadcom.com/symantecenterprise/communities/community-home/librarydocuments/viewdocument?DocumentKey=b2b00f1b-e553-47df-920d-f79281a80269&CommunityKey=1ecf5f55-9545-44d6-b0f4-4e4a7f5f5e68&tab=librarydocuments (Accessed: 9 February 2021).

Johnson, D. L. *et al.* (2017) '2015 Anthem Data Breach', *Network Security News*, 4 April. Available at: https://asamborski.github.io/cs558_s17_blog/2017/04/04/anthem.html (Accessed: 8 February 2021).

Kärkkäinen, H. (2020) *Tämä Vastaamo-kiristyksestä tiedetään nyt – 9 avointa kysymystä*, *Ilta-Sanomat*. Available at: https://www.is.fi/digitoday/tietoturva/art-2000006697806.html (Accessed: 1 February 2021).

Kaspersky (2020) 'The year of social distancing or social engineering? Phishing goes targeted and diversifies during COVID-19 outbreak', *Kaspersky*, 8 July. Available at: https://www.kaspersky.com/about/press-releases/2020_the-year-of-social-distancing-or-social-engineering (Accessed: 31 January 2021).

Kaye, D., Désir, H. and Lanza, E. (2020) 'COVID-19: Governments must promote and protect access to and free flow of information during pandemic – International experts'. Available at: https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=25729&LangID=Eccess (Accessed: 31 January 2021).

Khalili, J. (2020) *Coronavirus hospital suspends activity over cyber-attack*, *TechRadar*. Available at: https://www.techradar.com/news/coronavirus-hospital-suspends-activity-over-cyberattack (Accessed: 11 February 2021).

Kingdom of the Netherlands (2020) *The Kingdom of the Netherlands' response to the pre-draft report of the OEWG*, pp. 1–6. Available at: https://front.un-arm.org/wp-content/uploads/2020/04/kingdom-of-the-netherlands-response-pre-draft-oewg.pdf (Accessed: 14 December 2020).

Kirp, D. (2020) 'The cyber attack that rocked the nation', 22 December. Available at: https://www.helsinkitimes.fi/columns/columns/331-david-kirp/18450-the-cyber-attack-that-rocked-the-nation.html (Accessed: 1 February 2021).

Kirwan, G. and Power, A. (2011) *The Psychology of Cyber Crime: Concepts and Principles*. IGI Global (Advances in Digital Crime, Forensics, and Cyber Terrorism). doi: 10.4018/978-1-61350-350-8.

Krebs, B. (2020) 'Ransomware Group Turns to Facebook Ads', *KrebsonSecurity*, 11 October. Available at: https://krebsonsecurity.com/2020/11/ransomware-group-turns-to-facebook-ads/ (Accessed: 25 January 2021).

Mačák, K., Rodenhäuser, T. and Gisel, L. (2020) *Cyber attacks against hospitals and the COVID-19 pandemic: How strong are international law protections?*, *Humanitarian Law & Policy Blog*. Available at: https://blogs.icrc.org/law-and-policy/2020/04/02/cyber-attacks-hospitals-covid-19/ (Accessed: 15 February 2021).

Maglaras, L. *et al.* (2019) 'Threats, Countermeasures and Attribution of Cyber Attacks on Critical Infrastructures', *ICST Transactions Preprint*, pp. 1–8.

Malwarebytes (2020) *What cybercriminals want from your healthcare organization*. Malwarebytes, p. 20. Available at: https://resources.malwarebytes.com/files/2020/06/FINAL_What-Cybercriminals-Want-Healthcare_eBook_FINAL.pdf (Accessed: 16 February 2021).

ManageEngine (no date) 'Traversing one step at a time: The lateral movement attack phase in a healthcare network.', *ManageEngine Log360*. Available at: https://www.manageengine.com/log-management/healthcare-security-compliance/the-lateral-movement-attack-phase-in-a-healthcare-network.html (Accessed: 17 February 2021).

Mayer, C. (2021) 'L'hôpital de Dax en partie paralysé par une attaque informatique', *Le Monde*, 2 October. Available at: https://www.lemonde.fr/pixels/article/2021/02/10/l-hopital-de-dax-en-partie-paralyse-par-une-attaque-informatique_6069430_4408996.html (Accessed: 16 February 2021).

McMillan, R. and Evans, M. (2020) 'Ransomware Attack Hits Universal Health Services', *Wall Street Journal*, 28 September. Available at: https://www.wsj.com/articles/ransomware-attack-hits-universal-health-services-11601341873 (Accessed: 31 January 2021).

van der Meer, S. (2020) *How states could respond to non-state cyber-attackers*. NL: Clingendael, Netherlands Institute of International Relations, p. 6. Available at: https://www.clingendael.org/sites/default/files/2020-06/Policy_Brief_Cyber_non-state_June_2020.pdf.

Microsoft 365 Defender Threat Intelligence Team (2020) *Ransomware groups continue to target healthcare, critical services; here's how to reduce risk*, *Microsoft Security*. Available at: https://www.microsoft.com/security/blog/2020/04/28/ransomware-groups-continue-to-target-healthcare-critical-services-heres-how-to-reduce-risk/ (Accessed: 8 February 2021).

Milanovic, M. and Schmitt, M. N. (2020) 'Cyber Attacks and Cyber (Mis)information Operations during a Pandemic', pp. 247–284. doi: 10.2139/ssrn.3612019.

Mirsky, Y. *et al.* (2019) 'CT-GAN: Malicious Tampering of 3D Medical Imagery using Deep Learning', *arXiv:1901.03597 [cs]*, p. 19.

Mitnick Security (2020) *An Overview of the 2020 UHS Ransomware Attack*, *Mitnick Security*. Available at: https://www.mitnicksecurity.com/blog/an-overview-of-the-2020-uhs-ransomware-attack (Accessed: 17 February 2021).

MOH (2018) *Singhealth's IT system target of cyberattack*, *Ministry of Health – Singapore*. Available at: https://www.moh.gov.sg/news-highlights/details/singhealth's-it-system-target-of-cyberattack (Accessed: 26 February 2021).

Morse, A. (2018) *Investigation: WannaCry cyber attack and the NHS*. National Audit Office, p. 35. Available at: https://www.nao.org.uk/wp-content/uploads/2017/10/Investigation-WannaCry-cyber-attack-and-the-NHS.pdf (Accessed: 16 February 2021).

Mungadze, S. (2020) 'Life Healthcare reveals damage caused by data breach', *ITWeb*, 31 August. Available at: https://www.itweb.co.za/content/rW1xLv59YPGvRk6m (Accessed: 17 February 2021).

Muurman, T. (2020) *NBI to continue criminal investigation into exceptionally large-scale hacking of psychotherapy customer files*, *Police*. Available at: https://poliisi.fi/en/-/nbi-to-continue-criminal-investigation-into-exceptionally-large-scale-hacking-of-psychotherapy-customer-files (Accessed: 1 February 2021).

Name Anonymised (2020) 'Cyberattack on UHS Hospitals Nationwide Last Night', *r/hacking*. Available at: http://www.reddit.com/r/hacking/comments/j17aj1/cyberattack_on_uhs_hospitals_nationwide_last_night/ (Accessed: 12 December 2020).

NCA (2018) *National Crime Agency – FBI & NCA investigation leads to charges against alleged cyber criminals*, *National Crime Agency*. Available at: https://web.archive.org/web/20181211020508/http://www.nationalcrimeagency.gov.uk/news/1512-fbi-nca-investigation-leads-to-charges-against-alleged-cyber-criminals (Accessed: 1 February 2021).

NHS (2020) *WannaCry Ransomware Using SMB Vulnerability*, *NHS Digital*. Available at: https://digital.nhs.uk/cyber-alerts/2017/cc-1411 (Accessed: 9 February 2021).

Nuspire (2020) 'TrueFighter: Remote Desktop Protocol Accounts Compromised', *Nuspire*, 17 August. Available at: https://www.nuspire.com/blog/truefighter-remote-desktop-protocol-accounts-compromised/ (Accessed: 31 January 2021).

O'Dwyer, G. (2020) 'In wake of horrific Vastaamo breach, Finnish government tables laws to protect data from cyber criminals', *DataBreaches.net*, 18 December. Available at: https://www.databreaches.net/in-wake-of-horrific-vastaamo-breach-finnish-government-tables-laws-to-protect-data-from-cyber-criminals/ (Accessed: 16 February 2021).

OHCHR (1966a) *International Covenant on Civil and Political Rights*, *OHCHR*. Available at: https://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx (Accessed: 11 December 2020).

OHCHR (1966b) *International Covenant on Economic, Social and Cultural Rights*, *OHCHR*. Available at: https://www.ohchr.org/en/professionalinterest/pages/cescr.aspx (Accessed: 11 December 2020).

OSCE (2013) 'Decision No. 1106 Initial Set of OSCE Confidence-Building Measures to Reduce the Risks of Conflict Stemming from the Use of Information and Communication Technologies'. Organization for Security and Co-operation in Europe Permanent Council. Available at: https://www.osce.org/files/f/documents/d/1/109168.pdf.

OSCE (2016) 'Decision No. 1202 OSCE Confidence-Building Measures to Reduce the Risks of Conflict Stemming from the Use of Information and Communication Technologies'. Organization for Security and Co-operation in Europe Permanent Council. Available at: https://www.osce.org/files/f/documents/d/a/227281.pdf.

Paganini, P. (2020) *Bad actor sells Huiying Medical Technology's source code for AI-assisted COVID-19 detection*, *Security Affairs*. Available at: https://securityaffairs.co/wordpress/102270/data-breach/huiying-medical-technology-data-breach.html (Accessed: 8 February 2021).

Paris Call (2018a) *Paris Call for Trust and Security in Cyberspace*, *Paris Call for Trust and Security in Cyberspace*. Available at: https://pariscall.international/en/ (Accessed: 15 February 2021).

Paris Call (2018b) *The 9 principles*, *Paris Call for Trust and Security in Cyberspace*. Available at: https://pariscall.international/en/principles (Accessed: 15 February 2021).

Perlroth, N. (2012) 'In Cyberattack on Saudi Firm, U.S. Sees Iran Firing Back', *The New York Times*, 24 October. Available at: https://www.nytimes.com/2012/10/24/business/global/cyberattack-on-saudi-oil-firm-disquiets-us.html (Accessed: 9 February 2021).

Peters, A. and Jordan, A. (2020) 'Countering the Cyber Enforcement Gap: Strengthening Global Capacity on Cybercrime', *Journal of National Security Law & Policy*, 10(487), p. 38.

Psykoterapiakeskus Vastaamo (2021) *Psychotherapy Center Vastaamo has become victim of a data system break-in and extortion., Psykoterapiakeskus Vastaamo*. Available at: https://vastaamo.fi/ajankohtaista/en.html (Accessed: 1 February 2021).

Råman, J. (2020) *The Office of the Data Protection Ombudsman is investigating the legality of the psychotherapy centre Vastaamo's operations*, *Office of the Data Protection Ombudsman*. Available at: https://tietosuoja.fi/en/-/the-office-of-the-data-protection-ombudsman-is-investigating-the-legality-of-the-psychotherapy-centre-vastaamo-s-operations (Accessed: 1 February 2021).

Randy, G. (2019) 'Is Cybersecurity A Priority In Healthcare?', *Healthcare IT Today*, 19 March. Available at: https://www.healthcareittoday.com/2019/03/19/is-cybersecurity-a-priority-in-healthcare/ (Accessed: 17 February 2021).

Ray, J., Marshall, H. and Coderre, R. (2019) *2019 Cyber Threatscape Report*. Accenture, p. 102. Available at: https://www.accenture.com/_acnmedia/pdf-107/accenture-security-cyber.pdf.

Recorded Future (2020) 'Capitalizing on Coronavirus Panic, Threat Actors Target Victims Worldwide', *Recorded Future*, 3 December. Available at: https://www.recordedfuture.com/coronavirus-panic-exploit/ (Accessed: 31 January 2021).

Riggi, J. (2020) 'The importance of cybersecurity in protecting patient safety', *AHA Center for Health Innovation*, 10 September. Available at: https://www.aha.org/center/cybersecurity-and-risk-advisory-services/importance-cybersecurity-protecting-patient-safety (Accessed: 31 January 2021).

Rikosuhripäivystys (2021) 'Vastaamo Case from the Victim Perspective', *Rikosuhripäivystys*, 1 April. Available at: https://www.riku.fi/en/vastaamo-case-from-the-victim-perspective-2/ (Accessed: 1 February 2021).

RiskIQ (2020) *Ransomware in Health Sector 2020: A Perfect Storm of New Targets and Methods*. Available at: https://www.riskiq.com/wp-content/uploads/2020/04/Ransomware-in-Health-Sector-Intelligence-Brief-RiskIQ.pdf (Accessed: 17 February 2021).

Rosario Fuentes, M. and Huq, N. (2018) *Securing Connected Hospitals: A Research on Exposed Medical Systems and Supply Chain Risks*. TrendMicro, p. 61. Available at: https://documents.trendmicro.com/assets/rpt/rpt-securing-connected-hospitals.pdf.

Rossi, B. (2015) 'Why the healthcare industry badly needs a cyber security health check', *Information Age*, 25 August. Available at: https://www.information-age.com/why-healthcare-industry-badly-needs-cyber-security-health-check-123460052/ (Accessed: 8 December 2020).

Schaake, M. (2020) 'Marietje Schaake is "very concerned about the future of democracy"'. Available at: https://cyberpeaceinstitute.org/news/marietje-schaake-is-very-concerned-about-the-future-of-democracy/ (Accessed: 31 January 2021).

Schmitt, M. N. (2013) *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge: Cambridge University Press. doi: 10.1017/CBO9781139169288.

Schmitt, M. N. (2015) 'In Defense of Due Diligence in Cyberspace', *The Yale Law Journal Forum*, 125, pp. 68–81.

Schmitt, M. N. (2017) *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. 2nd edn. Cambridge: Cambridge University Press. doi: 10.1017/9781316822524.

Schwartz, S. (2020) *Ryuk wakes from hibernation; FBI, DHS warn of healthcare attacks*, *Cybersecurity Dive*. Available at: https://www.cybersecuritydive.com/news/Ryuk-FBI-DHS-ransomware-healthcare/587961/ (Accessed: 17 February 2021).

Seals, T. (2020) 'REvil Gang Promises a Big Video-Game Hit; Maze Gang Shuts Down | Threatpost', *ThreatPost*, 29 October. Available at: https://threatpost.com/revil-video-game-hit-revenue/160743/ (Accessed: 12 January 2021).

SEC (2020) *SolarWinds Corporation – Form 8-K*. Washington, DC: U.S. Securities and Exchange Commission. Available at: https://www.sec.gov/ix?doc=/Archives/edgar/data/1739942/000162828020017451/swi-20201214.htm (Accessed: 31 January 2021).

Secretariat of the Cybercrime Convention Committee (2020) *The Budapest Convention on Cybercrime: benefits and impact in practice*. Council of Europe, pp. 1–45. Available at: https://rm.coe.int/t-cy-2020-16-bc-benefits-rep-provisional/16809ef6ac (Accessed: 23 January 2020).

Seh, A. H. *et al.* (2020) 'Healthcare Data Breaches: Insights and Implications', *Healthcare (Basel)*, 8(2), p. 133. doi: 10.3390/healthcare8020133.

Shin, S. C., Hyonhee (2021) 'North Korean hackers tried to steal Pfizer vaccine know-how, lawmaker says', *Reuters*, 16 February. Available at: https://www.reuters.com/article/us-northkorea-cybercrime-pfizer-idCAKBN2AG0NI (Accessed: 16 February 2021).

Shokoohi, M. *et al.* (2020) 'A syndemic of COVID-19 and methanol poisoning in Iran: Time for Iran to consider alcohol use as a public health challenge?', *Alcohol (Fayetteville, N.y.)*, 87, pp. 25–27. doi: 10.1016/j.alcohol.2020.05.006.

Silomon, J. (2020) 'The Düsseldorf Cyber Incident', *Institute for Peace Research and Security Policy*, 30 September. Available at: https://ifsh.de/en/news-detail/the-duesseldorf-cyber-incident (Accessed: 31 January 2021).

Slabodkin, G. (2020) 'Coronavirus chaos ripe for hackers to exploit medical device vulnerabilities', *MedTech Dive*, 4 August. Available at: https://www.medtechdive.com/news/coronavirus-chaos-ripe-for-hackers-to-exploit-medical-device-vulnerabilitie/575717/ (Accessed: 31 January 2021).

Smith, B. (2017) *The need for urgent collective action to keep people safe online: Lessons from last week's cyberattack*, *Microsoft On the Issues*. Available at: https://blogs.microsoft.com/on-the-issues/2017/05/14/need-urgent-collective-action-keep-people-safe-online-lessons-last-weeks-cyberattack/ (Accessed: 9 February 2021).

Snair, J. and Henry, D. G. (2013) 'Risks of Cyber Attacks on the Healthcare Sector Leave Public Health of Communities Vulnerable', *Naccho*, 24 October. Available at: https://www.naccho.org/blog/articles/risks-of-cyber-attacks-on-the-healthcare-sector-leave-public-health-of-communities-vulnerable (Accessed: 31 January 2021).

Stubbs, J. and Bing, C. (2020) 'Exclusive: Iran-linked hackers recently targeted coronavirus drugmaker Gilead', *Reuters*, 5 August. Available at: https://www.reuters.com/article/us-healthcare-coronavirus-gilead-iran-ex-idUSKBN22K2EV (Accessed: 31 January 2021).

Stubbs, J. and Pearson, J. (2020) 'Facebook tracks "OceanLotus" hackers to IT firm in Vietnam', *Reuters*, 12 November. Available at: https://www.reuters.com/article/facebook-vietnam-cyber-idCAKBN28L03Y (Accessed: 17 February 2021).

Sungard Availability Services (2019) *The Resilience Imperative*. Sungard Availability Services, p. 11. Available at: https://cdn2.hubspot.net/hubfs/6679661/sungardas-the-resilience-imperative.pdf.

Swinhoe, D. (2019) 'Why businesses don't report cybercrimes to law enforcement', *CSO Online*, 30 May. Available at: https://www.csoonline.com/article/3398700/why-businesses-don-t-report-cybercrimes-to-law-enforcement.html (Accessed: 31 January 2021).

Symantec (2018) 'New Orangeworm attack group targets the healthcare sector in the U.S., Europe, and Asia', *Symantec*, 23 April. Available at: https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/orangeworm-targets-healthcare-us-europe-asia (Accessed: 31 January 2021).

Symantec (2019) 'Whitefly: Espionage Group has Singapore in Its Sights', *Symantec*, 3 June. Available at: https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/whitefly-espionage-singapore (Accessed: 11 January 2021).

Szurdi, J. *et al.* (2020) 'Studying How Cybercriminals Prey on the COVID-19 Pandemic', *Palo Alto Networks – Unit42*, 22 April. Available at: https://unit42.paloaltonetworks.com/how-cybercriminals-prey-on-the-covid-19-pandemic/ (Accessed: 16 February 2021).

TEC (2018) 'The impact of cyber crime: Why cybersecurity should be your priority', *The Executive Connection*, 16 July. Available at: https://tec.com.au/the-impact-of-cyber-crime-why-cybersecurity-should-be-your-priority/ (Accessed: 16 February 2021).

Teivainen, A. (2020) *Vastaamo's ex-CEO and his parents have almost €10m in assets seized*. Available at: https://www.helsinkitimes.fi/finland/finland-news/domestic/18237-vastaamo-s-ex-ceo-and-his-parents-have-almost-10m-in-assets-seized.html (Accessed: 1 February 2021).

The Baltic Times (2020) 'Fake report about coronavirus-infected US soldier posted on Lithuanian news website', *The Baltic Times*, 31 January. Available at: https://www.baltictimes.com/vilnius__jan_31__bns___lithuania_s_law_on_state_language_needs_to_be_amended_and_adapted_to_the_existing_reality__linguists_say__adding_that_the_state_needs_to_learn_side-by-side_with_the_english_language____we_can_be_glad_with__the_existing___bns__law_bu/ (Accessed: 31 January 2021).

The Committee of Inquiry (2019) *Public Report of the Committee of Inquiry (COI) into the cyber attack on Singapore Health Services Private Limited Patient Database*. Singapore: Ministry of Communications and Information, p. 454. Available at: https://www.mci.gov.sg/-/media/mcicorp/doc/report-of-the-coi-into-the-cyber-attack-on-singhealth-10-jan-2019.ashx.

The CyberPeace Institute (2020a) 'Call to Governments', *The CyberPeace Institute*, 26 May. Available at: https://cyberpeaceinstitute.org/call-for-government/ (Accessed: 16 February 2021).

The CyberPeace Institute (2020b) *COVID-19 Infodemic: Cyber Volunteers and Healthcare – State of Play*. (CyberPeace Lab). Available at: https://cyberpeaceinstitute.org/event/cyberpeace-lab-covid-19-infodemic-cyber-volunteers-and-healthcare-state-of-play/ (Accessed: 16 February 2021).

The CyberPeace Institute (2020c) 'Cyber Volunteering during the COVID-19 Pandemic', *The CyberPeace Institute*, 6 May. Available at: https://cyberpeaceinstitute.org/news/2020-06-05-cyber-volunteering-during-covid19/ (Accessed: 17 February 2021).

The CyberPeace Institute (2020d) 'Cyber4Healthcare', *The CyberPeace Institute*, June. Available at: https://cyberpeaceinstitute.org/cyber4healthcare/ (Accessed: 16 February 2021).

The Guardian (2017) 'Ransomware attack "like having a Tomahawk missile stolen", says Microsoft boss', *The Guardian*. Available at: http://www.theguardian.com/technology/2017/may/15/ransomware-attack-like-having-a-tomahawk-missile-stolen-says-microsoft-boss (Accessed: 11 January 2021).

'The Impact of Cyberattacks – Podcast' (no date). (Resilient). Available at: https://www2.deloitte.com/us/en/pages/risk/articles/long-term-impact-of-cyber-attacks.html (Accessed: 31 January 2021).

TrendMicro (2016a) 'Ransomware-as-a-Service: Ransomware Operators Find Ways to Bring in Business', *TrendMicro*, 9 February. Available at: https://www.trendmicro.com/vinfo/es/security/news/cybercrime-and-digital-threats/ransomware-as-a-service-ransomware-operators-find-ways-to-bring-in-business (Accessed: 16 February 2021).

TrendMicro (2016b) 'Why Ransomware Works: The Psychology and Methods Used to Distribute, Infect, and Extort – Security News', *TrendMicro*, 16 June. Available at: https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/why-ransomware-works-psychology-and-methods-to-distribute-infect-and-extort (Accessed: 6 January 2021).

TrendMicro (2018) 'Exposed Devices and Supply Chain Attacks: Overlooked Risks in Healthcare Networks', *TrendMicro*, 4 May. Available at: https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/exposed-medical-devices-and-supply-chain-attacks-in-connected-hospitals (Accessed: 2 February 2021).

TrendMicro (no date) *Cybercriminals – Definition*, *TrendMicro*. Available at: https://www.trendmicro.com/vinfo/us/security/definition/cybercriminals (Accessed: 17 February 2021).

Trustwave (2018) *2018 Trustwave Global Security Report*. Trustwave. Available at: https://trustwave.azureedge.net/media/15350/2018-trustwave-global-security-report-prt.pdf?rnd=131992184400000000 (Accessed: 16 February 2021).

Tsagourias, N. and Farrell, M. (2020) 'Cyber Attribution: Technical and Legal Approaches and Challenges', *European Journal of International Law*, (chaa057), pp. 941–967. doi: 10.1093/ejil/chaa057.

UHS (2020a) 'Statement from Universal Health Services', *Universal Health Services*, 28 September. Available at: https://www.uhsinc.com/statement-from-universal-health-services/ (Accessed: 17 February 2021).

UHS (2020b) *Universal Health Services, Inc. Reports Information Technology Security Incident | Universal Health Services Inc.*, *Universal Health Services*. Available at: https://ir.uhsinc.com/news-releases/news-release-details/universal-health-services-inc-reports-information-technology (Accessed: 17 February 2021).

UNHCR (2018) 'General comment No. 36 (2018) on article 6 of the International Covenant on Civil and Political Rights, on the right to life'. United Nations Human Rights Committee. Available at: https://tbinternet.ohchr.org/Treaties/CCPR/Shared%20Documents/1_Global/CCPR_C_GC_36_8785_E.pdf (Accessed: 16 February 2021).

Unit 42 (2020) '2020 Unit 42 IoT Threat Report', *Palo Alto Unit42*, 3 October. Available at: https://unit42.paloaltonetworks.com/iot-threat-report-2020/ (Accessed: 31 January 2021).

United Nations (1945) *Charter of the United Nations: Chapter I*, *United Nations*. Available at: https://www.un.org/en/sections/un-charter/chapter-i/index.html (Accessed: 15 February 2021).

United Nations (2000) 'Committee on Economic, Social and Cultural Rights General Comment No. 14'. United Nations Committee on Economic, Social and Cultural Rights. Available at: http://docstore.ohchr.org/SelfServices/FilesHandler.ashx?enc=4slQ6QSmlBEDzFEovLCuW1AVC1NkPsgUedPlF1vfPMJ2c7ey6PAz2qaojTzDJmC0y%2B9t%2BsAtGDNzdEqA6SuP2r0w%2F6sVBGTpvTSCbiOr4XVFTqhQY65auTFbQRPWNDxL (Accessed: 16 February 2021).

United Nations (2015) *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*. A/70/174. United Nations, pp. 1–17. Available at: https://undocs.org/A/70/174 (Accessed: 14 December 2020).

UNODC (2019) *Cybercrime Module 3 Key Issues: The Role of Cybercrime Law*, *United Nations Office on Drugs and Crime*. Available at: https://www.unodc.org/e4j/en/cybercrime/module-3/key-issues/the-role-of-cybercrime-law.html (Accessed: 1 February 2021).

U.S. District Court (2018) *United States of America v. Faramarz Shahi Savandi and Mohammad Mehdi Shah Mansouri*. Available at: https://www.justice.gov/usao-nj/press-release/file/1114791/download.

U.S. DoHHS (no date) *Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information*, *U.S. Department of Health & Human Services – Office for Civil Rights*. Available at: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (Accessed: 17 February 2021).

U.S. DoJ (2018) *North Korean Regime-Backed Programmer Charged With Conspiracy to Conduct Multiple Cyber Attacks and Intrusions*, *Unites States Department of Justice*. Available at: https://www.justice.gov/opa/pr/north-korean-regime-backed-programmer-charged-conspiracy-conduct-multiple-cyber-attacks-and (Accessed: 9 February 2021).

U.S. DoJ (2021) *Three North Korean Military Hackers Indicted in Wide-Ranging Scheme to Commit Cyberattacks and Financial Crimes Across the Globe*, *Unites States Department of Justice*. Available at: https://www.justice.gov/opa/pr/three-north-korean-military-hackers-indicted-wide-ranging-scheme-commit-cyberattacks-and (Accessed: 18 February 2021).

U.S. DoT (2018) *Treasury Designates Iran-Based Financial Facilitators of Malicious Cyber Activity and for the First Time Identifies Associated Digital Currency Addresses | U.S. Department of the Treasury*, *U.S. Department of the Treasury*. Available at: https://home.treasury.gov/news/press-releases/sm556 (Accessed: 1 February 2021).

U.S. DoT (2020) 'Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments'. U.S. Department of the Treasury's Office of Foreign Assets Control. Available at: https://home.treasury.gov/system/files/126/ofac_ransomware_advisory_10012020_1.pdf (Accessed: 16 February 2021).

Valtioneuvosto (2020) *Where to get help for victims of recent data breach at Psychotherapy Centre Vastaamo — a list of key organisations providing help*, *Valtioneuvosto*. Available at: https://valtioneuvosto.fi/en/-/1271139/where-to-get-help-for-victims-of-recent-data-breach-at-psychotherapy-centre-vastaamo-a-list-of-key-organisations-providing-help (Accessed: 16 February 2021).

Var Group (2021) 'Documenti riservati di ema sul vaccino pfizer trovati nel dark web, grazie al team di cyber intelligence di yarix', *Var Group*, 1 November. Available at: https://www.var-group.it/comunicati-stampa/documenti-riservati-di-ema-sul-vaccino-pfizer-trovati-nel-dark-web-grazie-al-team-di-cyber-intelligence-di-yarix/ (Accessed: 9 February 2021).

Vijayan, J. (2021) 'Growing Collaboration Among Criminal Groups Heightens Ransomware Threat for Healthcare Sector', *Dark Reading*, 2 November. Available at: https://www.darkreading.com/attacks-breaches/growing-collaboration-among-criminal-groups-heightens-ransomware-threat-for-healthcare-sector/d/d-id/1340142 (Accessed: 16 February 2021).

WHO (2020) 'Managing the COVID-19 infodemic: Promoting healthy behaviours and mitigating the harm from misinformation and disinformation', *World Health Organization*, 23 September. Available at: https://www.who.int/news/item/23-09-2020-managing-the-covid-19-infodemic-promoting-healthy-behaviours-and-mitigating-the-harm-from-misinformation-and-disinformation (Accessed: 11 January 2021).

Wiggers (2020) 'Huiying Medical claims its AI can detect coronavirus from CT scans with 96% accuracy', *VentureBeat*, 27 March. Available at: https://venturebeat.com/2020/03/27/huiying-medical-claims-its-ai-can-detect-coronavirus-from-ct-scans-with-96-accuracy/ (Accessed: 16 February 2021).

WSJ (no date) 'Why Doctors Need More Help With Cybersecurity', *Wall Street Journal Custom Content*. Available at: https://partners.wsj.com/ama/charting-change/doctors-need-help-cybersecurity/ (Accessed: 16 February 2021).

Yang, X. (2016) *Sovereign Immunity*, *Oxford Bibliographies*. Available at: https://www.oxfordbibliographies.com/view/document/obo-9780199796953/obo-9780199796953-0018.xml (Accessed: 16 February 2021).

Yle (2020) *Extortionist publishes more sensitive data on psychotherapy centres' patients*, *Yle Uutiset*. Available at: https://yle.fi/uutiset/osasto/news/extortionist_publishes_more_sensitive_data_on_psychotherapy_centres_patients/11608960 (Accessed: 1 February 2021).

Zaidenberg, O. (2020) 'CTI-League makes this year's WIRED25!: People Who Are Making Things Better', *CTI League*, 9 November. Available at: https://cti-league.com/cti-league/cti-league-makes-this-years-wired25-people-who-are-making-things-better/ (Accessed: 16 February 2021).

Zaidenberg, O. (2021) 'CTIL Darknet Report – 2021', *CTI League*, 2 November. Available at: https://cti-league.com/blog/darknet-report-2021/ (Accessed: 16 February 2021).

Zeng, J. and Chan, C. (2021) 'A cross-national diagnosis of infodemics: comparing the topical and temporal features of misinformation around COVID-19 in China, India, the US, Germany and France', *Online Information Review*, ahead-of-print(ahead-of-print). doi: 10.1108/OIR-09-2020-0417.

Zhao, J. Y. *et al.* (2018) 'Impact of Trauma Hospital Ransomware Attack on Surgical Residency Training', *Journal of Surgical Research*, 232, pp. 389–397. doi: 10.1016/j.jss.2018.06.072.

Zhou, W. *et al.* (2020) 'Impact of Hospital Bed Shortages on the Containment of COVID-19 in Wuhan', *International Journal of Environmental Research and Public Health*, 17(22), p. 8560. doi: 10.3390/ijerph17228560.

zvelo (2020) 'Ransomware as a Service (RaaS) | The Business of Ransomware', *zvelo*, 21 April. Available at: https://zvelo.com/raas-ransomware-as-a-service/ (Accessed: 12 January 2021).