CyberPeace Institute

Addendum to the Strategic Analysis Report

"Playing with Lives: Cyberattacks on Healthcare are Attacks on People"

Geneva, October 2021

Foreword

Marietje Schaake

President, the CyberPeace Institute

Cyberattacks on healthcare have been on the rise since our strategic analysis report came out in March 2021. The harm to people that these attacks continue to cause is immense: access to medical services is at risk or delayed and valuable resources and time are wasted, with long-term consequences on the sector and on society as a whole.

In our report, Playing with Lives: Cyberattacks on Healthcare are Attacks on People, we offered concrete policy recommendations to governments, corporations, civil society and experts with the aim of collectively ensuring security and resilience. With the launch of the Cyber Incident Tracer, we are responding to the recommendation about data collection in relation to cyberattacks, as a first step towards evidence-informed policymaking.

The protection of the healthcare sector has made it to the top of the agenda for governments around the world, but the information remains scattered, insufficient and reported in various formats. To fight a global challenge, we need to pull resources and take a collective approach to attacks that affect our fundamental rights, such as access to health. The Cyber Incident Tracer (CIT) #HEALTH is part of the solution.

Stéphane Duguin

Chief Executive Officer, the CyberPeace Institute

Over the past two years, the story has remained the same: people's health is put even more at risk as cyberattacks against the healthcare sector are more and more common. Healthcare professionals are suffering physically and mentally as they try to manage and recover from these attacks, and patients' lives are put at risk despite them seeking care, which is a basic human right.

Since the establishment of the CyberPeace Institute, the protection of the healthcare sector from cyberattacks has been a key priority. We launched the Cyber 4 Healthcare program in May 2020 with the Call to Governments, immediately followed by our Cyber 4 Healthcare initiative, in an effort to actively assist vulnerable populations targeted by large-scale cyberattacks and to assist healthcare professionals, analyse attacks and advance policies to protect the sector. As a key step, the CyberPeace Institute team, along with the effort of partners and volunteers, analysed this complex issue in our Report on Cyberattacks on Healthcare. However, this was just the first step to understand the problem through the lens of cyberpeace, and what this means for the security of cyberspace. Now, with this foundational research, we have taken the next step and operationalised a key recommendation in the report: to document attacks and analyse their impact.

The CIT #HEALTH is the first of its kind platform to capture attack data in one place, and analyses the impact that these attacks have on people and society as a whole. With this data accessible to the public, our hope is that researchers, policymakers, and tech professionals alike will use it to better inform their work and practices. The responsibility to secure cyberspace falls on us all. We must each do our part to make sure that those who conduct reckless attacks on our healthcare system are held accountable for their actions, so that those in charge of saving our lives can focus on just that: saving lives. We invite you to contribute to this work if you are interested, and call on all stakeholders to think critically about what they can do to take action to better protect the healthcare sector from cyberattacks.

Introduction

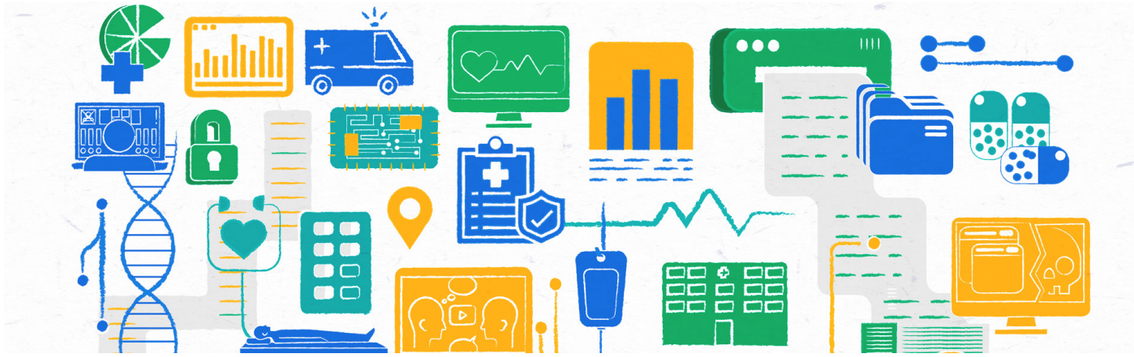
Cyberattacks on healthcare are attacks on people. Access to critical healthcare and cybersecurity are intertwined in the digital age. The right to health is a human right and safe, secure and stable cyberspace is a gateway to secure access to healthcare.

The wake-up call from the WannaCry malware infection in 2017 was short lived despite the fact that it affected many sectors including the National Health Service in the UK. With potentially tragic consequences, the healthcare sector remains under cyberattack. Today, we are not able to quantify the magnitude of the problem of cyberattacks on healthcare. For example, to determine the impact of cyberattacks on the sector and the operational disruption caused.

Cyberattacks against the healthcare sector are a threat and detrimental to achievement of the 2030 targets in the United Nations Sustainable Development Goals (SDG), and in particular SDG 3: Ensure healthy lives and promote well-being for all at all ages. To realize the 2030 goals of SDG 3, trust in, resilience of, and capacity of healthcare around the globe are essential. The CIT #HEALTH platform can support policy-makers and healthcare professionals in their decision making to achieve these goals. The platform provides an aggregation of reliable and publicly available data on cyberattacks against the healthcare sector. Better understanding of these attacks can contribute to preserving the potential of and trust in the technology used everyday in healthcare, and provide the necessary support so healthcare professionals can focus on achieving the goals outlined in the UN's 2030 vision.

It is important that we understand the true scale and impact of cyberattacks against healthcare in order to design better policies and rules to protect this sector in perpetuity. At the CyberPeace Institute, we believe that an evidence-based understanding of the impact of these attacks can help to raise political and social awareness. It is time that there is collective action to help uncover the gaps in prevention and mitigation of cybersecurity risks in the healthcare sector, and to inform the steps that all stakeholders must take for a safe, secure, and equitable cyberspace.

This addendum outlines information that the CyberPeace Institute gathered and analyzed through its the Cyber Incident Tracer (CIT) #HEALTH. The CIT #HEALTH is a platform that bridges the current information gap on cyberattacks on healthcare and their impact on people. The platform serves as a source of information for evidence-led operational, policy, and legal decision-making. Knowing and understanding more systematically what is happening is the first step to taking action for global change. We are convinced that data helps seemingly intractable problems become understandable.



Cyber Incident Tracer(CIT) #HEALTH

The Cyber Incident Tracer (CIT) #HEALTH is a platform that works to close the information gap related to cyberattacks on the healthcare sector on a global scale. Disruptive attacks affect the delivery of healthcare, compromise sensitive healthcare-related data, and have an impact on patients, healthcare professionals, facilities and organizations. The platform provides a data-driven approach to understanding the impact of cyberattacks on the sector. Thus far, limited visibility and data on the impact of cyberattacks has complicated policy making and the inability to understand the impact of cyberattacks on people and has resulted in a failure to develop suitable policies to ensure a safe and secure cyberspace. The CIT #HEALTH platform brings greater visibility to the problem and the disruptions caused to the provision of healthcare.

The information in the platform is updated on a weekly basis with new data on cyberattacks against the healthcare sector. One key finding that has already arisen from this work is the stark disparity in reporting and availability of data on cyberattacks across the world. To enable sustainable change on the policy level, the evidence needs to be made publicly available. There is an urgency to make data publicly available, as evidenced by the analysis of the data we have been able to collect.

Data captured on the platform provides details on 235 cyberattacks[1] against the healthcare sector across 33 countries between June 2020 and September 2021. This equates to an average of 3.5 incidents per week over the last 16 months. Table 1 provides a breakdown of the number of incidents by continent / sub-region by quarters.

[1] Data breaches are excluded from the statistics in this report due to data collection limitations explained in the CIT Methodology section. All CIT #HEALTH related statistics in this report represent data for the period June 2020 to September 2021 unless otherwise stated.

Table 1: Incidents by quarter across continents and regions.

Continent	Region	2020		2021		
		Qtr3	Qtr4	Qtr1	Qtr2	Qtr3
Africa	Sub-Saharan Africa					1
Americas	Latin America and the Caribbean		1	2	4	2
	Northern America	28	29	34	30	19
Asia	Eastern Asia				1	3
	South-eastern Asia	1				2
	Southern Asia		4		1	1
	Western Asia	1			2	1
Europe	Eastern Europe	1	1	3		1
	Northern Europe			1	2	2
	Southern Europe	1	1	4	7	1
	Western Europe	2	11	11	3	4
Oceania	Australia and New Zealand	2	1	1	2	

Source: CyberPeace Institute - CIT #HEALTH

Key findings: Across these incidents, the CIT #HEALTH seeks to report on the impact they've had on organizations and individuals:

- operational disruption to services lasted from a matter of hours to four months, averaging **19.3 days per incident**
- the number of records breached and / or patients impacted following an attack reached up to 2.4 million, averaging **155,000 records per incident**
- in 57% of incidents systems went offline, and
- in 73% of incidents data was leaked or exposed.

Disruptive cyberattacks hit **169 patient care services** in 26 countries resulting in:

- The diversion of ambulances or incoming patients in 15% of the incidents
- The cancellation of appointments or surgeries in 21% of the incidents

The healthcare sector must be protected from cyberattacks to ensure not only that people can access appropriate healthcare but also to safeguard trust in healthcare institutions that they can provide the care that people expect.

Framing this topic in the CyberPeace Institute's work

Since the establishment of the CyberPeace Institute, the protection of the healthcare sector from cyberattacks has been a key priority. The Institute's Cyber 4 Healthcare program was launched in 2020 in an effort to actively assist vulnerable populations targeted by large-scale cyberattacks and to assist healthcare professionals, analyse attacks and advance policies to protect the sector. In May 2020, we published a Call for Governments to take immediate and decisive action to prevent and stop cyberattacks that target hospitals, healthcare, research organizations, and international authorities providing critical care and guidance in the health sector - which was signed by more than 50 current and former world leaders.

The CyberPeace Institute developed the CIT #HEALTH following the publication of its Strategic Analysis Report in March 2021 that identified the gap in availability of information about cyberattacks on healthcare. The Report, entitled Playing with Lives: Cyberattacks on Healthcare are Attacks on People identifies the gaps in availability of information about cyberattacks on healthcare and outlines several key recommendations on how to improve the resiliency of the healthcare sector, in an effort to increase accountability in cyberspace. The first recommendation is of particular importance: it encourages stakeholders to document attacks and to analyse their human and societal impact. Under this recommendation, the CyberPeace Institute's goal was to develop a publicly available database of cyberattacks in an effort to enhance transparency and access to information. The Cyber Incident Tracer (CIT) #HEALTH is the response to this commitment.

Cyber Incident Tracer (CIT) #HEALTH: what the data tells us

The Cyber Incident Tracer (CIT) #HEALTH is a platform that works to close the information gap related to cyberattacks on the healthcare sector on a global scale. Disruptive attacks affect the delivery of healthcare, compromise sensitive healthcare-related data, and have an impact on patients, healthcare professionals, facilities and organizations.

The platform provides a data-driven approach to understanding the impact of cyberattacks on the sector. Thus far, limited visibility and data on the impact of cyberattacks has complicated policy making and the inability to understand the impact of cyberattacks on people and has resulted in a failure to develop suitable policies to ensure a safe and secure cyberspace. The CIT #HEALTH platform brings greater visibility to the problem and the disruptions caused to the provision of healthcare.

The information in the platform is updated on a weekly basis with new data on cyberattacks against the healthcare sector. One key finding that has already arisen from this work is the stark disparity in reporting and availability of data on cyberattacks across the world. To enable sustainable change on the policy level, the evidence needs to be made publicly available. There is an urgency to make data publicly available, as evidenced by the analysis of the data we have been able to collect.

The CIT #HEALTH illustrates that the cyberthreat landscape changes over time and the targeting of organizations changes as the socio-economic environment evolves. The volume of attacks continues to pose a significant threat to a critical sector already under pressure.. For example, in 2020, when research and production of the COVID-19 vaccine were in full swing, medical manufacturing and the pharmaceutical industry were targets of attacks. Analysis of available data shows that in the first half of 2021, there has been an increase in attacks against patient care services (including medical specificalists, care providers and hospitals) and a decrease in attacks on pharmaceuticals.

Table 2: Comparing the number of incidents in second half of 2020 to the first half of 2021

Sub-sector / Organization type	2nd half 2020	1st half 2021	Percentage Change
Patient care services	**54**	**84**	**56%**
medical specialist	13	24	85%
hospital	13	23	77%
healthcare network	15	11	-27%
care provider	4	11	175%
clinic	5	7	40%
mental health and substance abuse facility	4	5	25%
National Health System	0	3	-
Pharmaceuticals	**13**	**7**	**-46%**
pharmaceutical	10	6	-40%
pharmacy	3	0	-100%
biotech company	0	1	-
Medical Manufacturing & Development	**9**	**9**	**0%**
medical manufacturer	6	8	33%
medical research and developer	3	1	-67%
Other	**8**	**8**	**0%**
laboratories and diagnostics center	5	4	-20%
EHR / PM vendor	1	3	200%
ambulance services	2	1	-50%

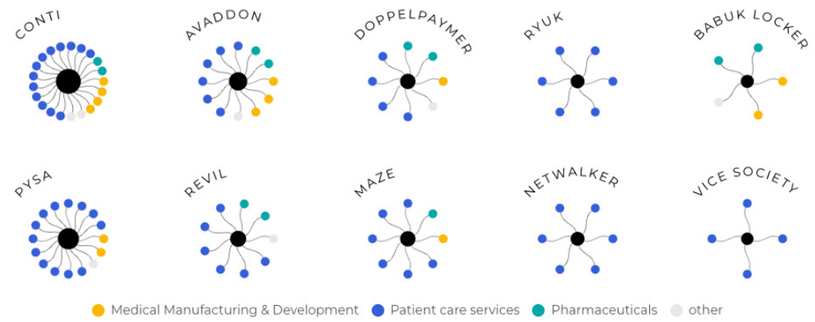
Source: CyberPeace Institute - CIT #HEALTH

The CIT #HEALTH has also begun the process of collecting publicly available information on the ransomware operators behind the attacks[2]. To date we have observed a total of 38 ransomware operators targeting the healthcare sector and have been able to collect this information across 66% of incidents.

[2] The CyberPeace Institute has not, at this stage, conducted its own corroboration analysis in order to link an ransomware strain / operator to an incident but is relying only on publicly available citations. Where more than one ransomware strain / operator has been listed to a single incident these are all included in the collection to allow for further research in the future.

The top 10 operators account for 68% of incidents for which this information is known with Conti and Pysa accounting for over a quarter (26%) of the incidents between them. Graph 1 provides an overview of the incidents within four sub-sectors of healthcare that the top 10 operators have targeted, noting that the majority, excluding Babuk Locker, all target patient care services such as hospitals, medical specialists and clinics.

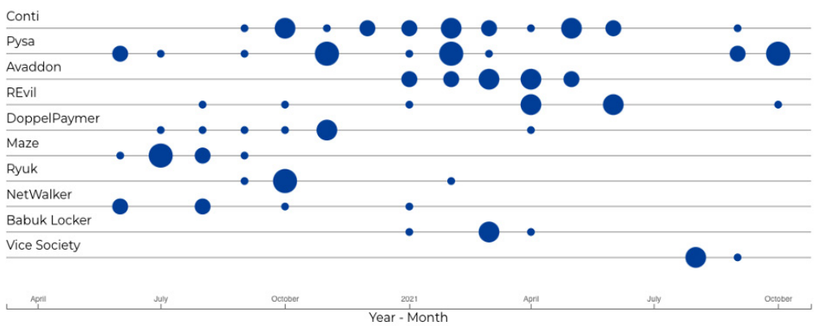
Graph 1: Incidents colored by sub-sector for top 10 ransomware operators



Source: CyberPeace Institute - CIT #HEALTH

The CIT #HEALTH also captures how the various operators' activity increases and decreases overtime providing a snapshot of which ransomware operator poses the greater threat at any given time. As we see from Graph 2 below, some operators are consistently active in targeting the sector. For example Conti have been systematically targeting the sector since September 2020 to date whilst Avaddon were very active from January to May 2021 until the moment they shut down and released decryption keys in early June[3]. On the other hand the targeting of Pysa is more sporadic with clusters of incidents taking place for example in June and November 2020, February 2021 and most recently increasing their attacks on the sector in September-October[4] 2021.

Graph 2: Incidents by top 10 ransomware operators by month



Source: CyberPeace Institute - CIT #HEALTH

The CyberPeace Institute endeavours to further its research on the subject of ransomware operators and to increase data collection to allow for better insights to be drawn in the future using the CIT #HEALTH platform.

[3] Source: www.bleepingcomputer.com/news/security/avaddon-ransomware-shuts-down-and-releases-decryption-keys/
[4] At the time of publishing, data for is only available up to 18th October inclusive.

The data in the CIT #HEALTH platform is collected from publicly available sources, and is cross-referenced to ensure accuracy. All data sources used in relation to a specific attack are listed in the incident details and impact card. On the platform itself, data sources are categorized as either primary sources, secondary sources, or tertiary sources and are classified based on the reliability of the information source. Data is collected on the basis of the following definition of a cyberattack: a cyberattack is a disruptive attack or data breach conducted by a threat actor using a computer network or system with the intention to cause damage (technical, financial, reputational or other) or extract or steal data without consent.

"Safeguarding healthcare organizations and the associated victims during data processing and publication of information in the CIT #HEALTH is important."

The CyberPeace Institute recognizes the sensitivity of information on cyberattacks and the importance of not re-victimizing the targeted organizations, and so were particularly careful not to provide the names of victim organizations. It is critical to raise awareness of the importance of the protection of data subjects whose data has been breached and may be accessible online.

The team has faced several limitations throughout this project, such as data completeness due to the differences in public reporting and disclosure of cyberattacks, as well as data delays and data validation. However, this project would not have been possible without the ongoing effort of four individuals and organizations who have helped to identify and track cyberattacks against the healthcare sector. They have provided data for the Institute to use and make publicly available in order to support the goal of creating a reliable data source for all to access.

From the end-user, to the industry CISO, to the diplomat at the UN, all stakeholders face their own obstacles in preventing and mitigating the impact of cyberattacks against their respective entity. With the CIT #HEALTH platform, the CyberPeace Institute is collecting, categorizing and visualizing data on cyberattacks against the healthcare sector in order to make the impact of these cyberattacks more understandable. This effort should support the recognition and development of solutions, norms and standards that work towards a safer cyberspace for all.

Achieving Accountability for Attacks on Healthcare

The general lack of accountability in cyberspace, meaning the lack of options to enforce a malicious actor to take responsibility for their actions and to deter this malicious behaviour in the first place, has dire consequences on the state of security of the healthcare sector.

Thus far, these gaps have resulted in a generalized sense of impunity for cybercriminals who take on essential services and critical infrastructure. At the CyberPeace Institute, we believe that accountability is crucial for a more secure cyberspace, and so we created an 'Accountability Framework' with the goal of mapping accountability in order to help make responsible behaviour in cyberspace the default among all stakeholders of the digital world.

Our aim with this framework is to increase engagement of all stakeholders on this issue and to build and refine a tool that will help to create sustainable accountability; not just one-off instances of it. This aim is rooted in the concept of responsible behaviour, which we believe should apply to all stakeholders. The idea of 'responsible behaviour in cyberspace' most notably came out of the UN GGE's 2015 report, where it states that, "Norms reflect the expectations of the international community, set standards for responsible State behaviour and allow the international community to assess the activities and intentions of States. Norms can help to prevent conflict in the ICT environment and contribute to its peaceful use to enable the full realization of ICTs to increase global social and economic development" (UN GGE, 2015, p. 7). We believe in a shared responsibility framework in which various stakeholders can advance accountability across governments, industry, academia, and civil society and work towards cyberpeace (see also initiatives such as the Paris Call for Trust and Security in Cyberspace, Cybersecurity Tech Accord, and Charter of Trust).

What it is and how it works

Below is our proposal for an Accountability Framework that can be applied specifically to cyberattacks. Based on our understanding of responsible behaviour as outlined above and rooted in human security, dignity, and equity, our three elements of cyberpeace, we propose the following four steps in order **to map accountability as it currently stands in cyberspace and to see the gaps where more action is required.**

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.

Collective responsibility: we all have a role to play

We need collective action to stop the attacks on the healthcare sector and on the people seeking healthcare. Despite the disparity in reporting and availability of data on cyberattacks across the world, the CIT #HEALTH is contributing to awareness raising. Aggregating available data and making it publicly accessible is a necessary contribution, and this is coupled with specific calls for action. The CyberPeace Institute, based on its report recommendations, believes that this is a key step to understand the scale of and overall societal impact of cyberattacks against the healthcare sector in order to lead to positive change. We do not know the boundaries that have to be crossed in order to make the relevant stakeholders act against cyberattacks on the healthcare sector. We believe that action must be taken before lives are lost and hope our call for action is answered.

The CyberPeace Institute Calls for Action

Call to Governments

The CyberPeace Institute calls on all governments to do their part to stop attacks on healthcare. Health is a fundamental human right and it is the responsibility of states to lead the way to protect this common good. Government entities must take meaningful action and enforce norms of responsible behavior and work to apply international law to cyberspace in relation to attacks against the healthcare sector. As agreed during the United Nations Open Ended Working Group (OEWB) process in 2021, healthcare is a critical infrastructure and is off-limits to attack by other state entities.

States must take measures, such as protection, detection, recovery, mitigation, and investigation of attacks, to protect the human rights of individuals within their jurisdiction from harmful operations on the healthcare sector. States must not allow their territory or infrastructure under their jurisdiction or control to be used by state or non-state actors to conduct operations on the healthcare sector.

States must not only act in a reactionary way, they must also look to the future and invest resources in cybersecurity to ensure that the healthcare sector is equipped to deal with cyber threats. Part of this forward-thinking approach is to contribute to initiatives that bring greater visibility as to how attacks on the healthcare sector impact people and the provision of care. It is also the responsibility of states to ensure accountability for cyberattacks on healthcare by arresting perpetrators of attacks and supporting a transparent and efficient judicial process to hold criminals to account.

Call to Healthcare Sector

The CyberPeace Institute calls on the healthcare sector to take the necessary steps to increase the resilience, response, and recovery of their IT infrastructure.

We encourage those working in and related to the healthcare sector to be aware of current cyber threats and implement defences that are proportionate to them. This includes conducting vulnerability scanning, security assessments, and the timely patching of systems. Securing potential attack vectors and endpoints is crucial to avoid the repercussions of a cyberattack.

If an organisation or professional comes across pertinent information, they are encouraged to share this information with all relevant stakeholders, e.g. relating to a software vulnerability.

It is important to report any incidents to the relevant authority, such as local or national law enforcement agencies to help to prevent the spread of an attack and limit the negative impact of the attack upon other organisations.

Call to Industry Actors

The CyberPeace Institute calls on industry actors to recognize the crucial role they play in the healthcare sector ecosystem, as often they are responsible for the creation, production, and maintenance of the tools used in the sector.

We encourage industry actors to implement security-by-design and security-by-default models for healthcare systems and product development across the supply chain.

We recommend to adapt pricing models according to the diversity of resources in healthcare to prevent discrepancies arising from those who can and cannot afford cybersecurity measures.

We encourage industry actors to sponsor research in technical solutions such as zero-trust networks, behavioural authentication and monitoring to improve the protection of hospitals and healthcare facilities from vulnerabilities in their supply chain.

The CyberPeace Institute Call for Contributions

The CIT #HEALTH is an ongoing initiative, and the CyberPeace Institute is continuing to collect data on cyberattacks and to further develop the platform. There are several areas where collaboration and support are essential to continue with this work. Some of these areas include:

- Strengthening data collection;
- Technical development and usability of the platform;
- Developing methodological expertise to measure the human and societal impact of cyber incidents and to track attribution and accountability;
- Refining the methodology.

If you have the capabilities to support this endeavour, or would like to have more information to understand the CIT #HEALTH, we would appreciate hearing from you. Please contact us at **cit@cyberpeaceinstitute.org**

How to support the CyberPeace Institute

If you are interested in our work, there are several ways you can support the CyberPeace Institute:

- Donations
  - If you believe in our mission and would like to see us continue our work to ensure a safer and more equitable cyberspace for all, we encourage you to make a donation. Your support will make a difference.
- Testimonials
  - If you have been a victim of a cyberattack, or have experienced the impact that a cyberattack can have, we would appreciate hearing your story. No matter how big or small you feel the incident may have been, please reach out to our assistance team at: **assistance@cyberpeaceinstitute.org** to discuss your experience.
- General Enquiries
  - If you have any questions, or other ideas of how we can work together, please don't hesitate to reach out to our team at: **info@cyberpeaceinstitute.org** to see how we can support each other in this process towards cyberpeace.

Mission Statement

The CyberPeace Institute is an independent and neutral non governmental organization whose mission is to ensure the rights of people to security, dignity and equity in cyberspace. The Institute works in close collaboration with relevant partners to reduce the harms from cyberattacks on people's lives worldwide, and provide assistance. By analyzing cyberattacks, the Institute exposes their societal impact, how international laws and norms are being violated, and advances responsible behaviour to enforce cyberpeace.

Contact details

For more information please contact: **info@cyberpeaceinstitute.org**

Access the full Strategic Analysis Report - Playing with Lives:Cyberattacks on Healthcare are Attacks on People

Access the CIT #HEALTH platform

Access the full Report