TOKAT, YASIN

Cyber Threats to Hospitals and Critical Infrastructure in Times of COVID-19 Pandemic

Introduction

Technological advancement is undoubtedly a cornerstone of the development of human civilization of this century. On the other hand, behind their tremendous benefits, there are also vulnerabilities in the malevolent use of these technologies. That being said, the malicious use of Information Communication Technologies by State and non-State actors towards critical services and infrastructure in times of calamities and disasters can further worsen the damages already incurred by the disaster. The recent COVID-19 pandemic has affected almost every country all around the globe and proved to be a global challenge in tackling the consequences of healthcare impact, patient safety, lockdown measures, economic and social impacts, and much more. Various countries have been affected with different severities, some having more death tolls, while others embraced an economic collapse. Recently, schools, businesses, government meetings, banking, shopping, entertainment, and non-essential functions rely on digitalization and networks to operate as undisturbed as possible. Nevertheless, the security of the networks, software, and hardware is questionable.

Even at the beginning of the Pandemic, the cyberattacks began to increase considerably. According to the April 2020 report of the US Department of Justice, the FBI's Internet Crime Complaint Center has received and reviewed more than 3,600 complaints about COVID-19 related scams, many of which originated from websites that advertised fake vaccines and cures, fraudulent charity campaigns, various types of malware and fraudulent activities. To attract traffic, these websites often utilized domain names that contained words such as 'covid19' or 'coronavirus'. In some cases, the fraudulent sites claimed to be run by or affiliated with public health organizations or agencies.[1] According to the 2020 Interpol report, there is an increase in cyber threats including malicious domains, malware, and ransomware, which are used to mislead users, steal sensitive data, or block access to a computer unless a ransom is paid. Furthermore, it is noted that it is especially the health service providers and essential product suppliers which are increasingly targeted and the

[1] The US Department of Justice: *Department of Justice Announces Disruption of Hundreds of Online COVID-19 Related Scams*. Press Release Number: 20-395. 04.22.2020. https://www.justice.gov/opa/pr/department-justice-announces-disruption-hundreds-online-covid-19-related-scams (30.05. 2021)

impact of such cyber attacks can be heavy as they are considered critical infrastructure. To make things worse, there are increased fake COVID-19 cures and tests via social media, encrypted apps, and the Darknet.

This paper will investigate the effects of COVID-19 on the digital landscape by going through cyber attacks on hospitals, critical infrastructure, and supply chain. As such attacks can result in damage to human wellbeing and life, their potential to revoke some of the EU and international laws will be analyzed. Recently, there has been a stimulus to overcome such issues at the EU and international levels. Nevertheless, comprehensive regulatory measures are quite difficult in a multinational world with different legal systems and borderless cyberspace. In an environment where international networks and online capacity grow, cyberattacks benefit from the anonymous nature of the internet, jurisdictional arbitrary issues, and difficulty of establishing international laws within the global cyberspace level. These can be some of the underlying causes of increasing cyber attacks as the attackers and organized cyber criminals often emerge from the States which have little to no laws concerning handling cybercrime. For instance, some states are lagging in cyber technologies and unable to detect cyber crimes stemming from their territories as the same socio-economic conditions further motivate some skilled individuals to take part in cyber attacks. Hence, cyberspace is like a huge jungle, led by the rules of the jungle with increasingly high stakes as the world depends more and more on internet technologies while some countries also try to gain strategic leverage on cyberspace through surveillance, intelligence, and cyber offensive operations. However, if a state infiltrates an ICT environment, it will not stick to its national borders due to the internet's global nature. If one capable state opens Pandora's box, there is no reason for others to lag. Consequently, the cyber arms race has already started.

Investigating such harmful trends is critical for the future of cybersecurity and security of critical operations as the rise of the Internet of Things, Artificial Intelligence, Big Data, Machine Learning, and 5G technology will further change and reshape our political, legal, economic, and social realm. The current effects of COVID-19 might be a lesson learned for the development of better cooperative, detective, and protective systems.

Literature Review

David Harries and Peter M. Yellowlees published an article[2] in the Telemedicine and e-Health Journal in early 2013 about the potential impact of cyber attacks on healthcare systems. In their article "Cyberterrorism: Is the US Healthcare System Safe?" they point out that, due to the advantages provided by the Internet, healthcare has become increasingly reliant on ICT-related activities. It is because of this dependence that malevolent individuals or organizations are more likely to engage in activities on the Internet that cause physical or psychological damage. The word "cyberterrorism" has been coined to describe these activities. Various attacks can target the healthcare sector, according to their report, such as shutting down a hospital computer system or releasing confidential medical records to the media, which can have huge public, political, security, and economic consequences if patient care is jeopardized.

---

[2] David HARRIES– Peter M. YELLOWLEES: Cyberterrorism: Is the U.S. Healthcare System Safe?. *Telemedicine and e-Health* Jan (2013) 61-66. https://doi.org/10.1089/tmj.2012.0022 (30.05.2021)

In 2017, an analysis[3] was published in the British Medical Journal by Martin Guy, Martin Paul, Hankin Chris, Darzi Ara, Kinross James with the title of "Cybersecurity and healthcare: how safe are we?" According to the writers, healthcare systems across the world have enormous potential for enhancing clinical outcomes and transforming care delivery. Nevertheless, increasing cybersecurity risks to healthcare necessitate policymakers addressing decentralized governance, developing and implementing security standards, and assisting organizations in improving their resilience. According to their results, healthcare faces far greater cyber threats than other industries due to inherent security flaws.

Also, another paper[4] released by IOS Press highlights new risks to vital healthcare industries hiding in the shadows. Researchers Clemens Scott Kruse, Benjamin Frederick, Taylor Jacobson, and Kyle D. Monticone investigate cybersecurity trends, including ransomware, and identify possible solutions by querying academic literature. According to their findings, the healthcare industry is falling behind in terms of security. Healthcare, like other sectors, needs well-defined cybersecurity procedures.

Lynne Coventry and Dawn Branley from the Northumbria University conducted further research[5] on modern trends and threats of Cyber Attacks on critical infrastructure. The International Journal of Midlife Health and Beyond published their article "Cybersecurity in Healthcare: A Narrative Analysis of Patterns, Challenges, and Ways Forward" in April 2018. Their research also shows that cyber attacks on healthcare systems can erode the trust of patients and raise security concerns. Individual medical equipment, electronic health records, and the healthcare system may all be targeted with awful consequences.

The analysis[6] of Steven Walker-Roberts, Mohammad Hammoudeh, and Ali Dehghantanha from the Manchester Metropolitan University examined the technological aspects of the attacks as well as potential countermeasures. Their analysis was published by the Institute of Electrical and Electronics Engineers under the title "A Systematic Review of the Availability and Efficacy of Countermeasures to Internal Threats in Healthcare Critical Infrastructure". Their findings indicate that, in addition to more efficient Intrusion Detection and Prevention Systems, a threat mitigation model that considers the unknown malicious insider is required. They also concluded that new policymaking is essential to successfully address the problem.

Oxford Analytica has released an expert briefing[7] on misinformation in the context of a global pandemic with the article "COVID-19 intensifies the cyber race on disinformation". According to their report, democratic governments are attempting to devise a fruitful formula for fighting disinformation operations, which are showing no signs of waning in the face of the pandemic. Since there is a fundamental asymmetry between the relative

---

[3] Martin GUY– Martin PAUL – Chris HANKIN – Ara DARZI – James KINROSS: Cybersecurity and healthcare: How safe are we? *BMJ* July 06 (2017) 358. https://doi.org/10.1136/bmj.j3179 (30.05.2021)

[4] Clemens Scout KRUSE – Benjamin FREDERICK – Taylor JACOBSON– D. Kyle MONTICONE: Cybersecurity in healthcare: A systematic review of modern threats and trends. *Technology and health care. Official journal of the European Society for Engineering and Medicine* 25(1) (2017) 1–10. https://doi.org/10.3233/THC-161263 (25.05.2021)

[5] Lynne COVEBTRY – Branley DAWN: Cybersecurity in healthcare: A narrative review of trends, threats, and ways forward. *The International Journal of Midlife Health and Beyond* April 21 (2018) https://www.maturitas.org/article/S0378-5122(18)30165-8/fulltext (30.05.2021)

[6] Steven WALKERS-ROBERTS – Mohammad HAMMOUDEH – Ali DEHGHANTANHA: A Systematic Review of the Availability and Efficacy of Countermeasures to Internal Threats in Healthcare Critical Infrastructure. *IEEE Access* vol. 6 (2018) 25167-25177 DOI: 10.1109/ACCESS.2018.2817560 (30.05.2021)

[7] OXFORD ANALYTICA: *COVID-19 intensifies the cyber race on disinformation*. Expert Reviews. 05.05.2020. https://www.emerald.com/insight/content/doi/10.1108/OXAN-DB252406/full/html (05.30.2021)

vulnerabilities of democratic and authoritarian states to disinformation campaigns, democratic policymakers have no easy policy options.

Furthermore, Dr. Brendan Flynn from the National University of Ireland, Galway has published the article[8] "The Inexorable Rise of the Pandemic State? Second-Guessing the long-term political repercussions of COVID 19". In his paper, he examines the impact of the pandemic on state political systems, concentrating on issues such as increasing authoritarianism in Western states, limiting freedom of movement, long-term health policies, re-nationalization policies, and emergency pandemic response policies, as well as the potential dominance of multinational tech behemoths in the online marketplace.

Another researc[9] was published by Petar Radanliev, David C. De Roure, and Max Van Kleek in the journals of the Institute of Electrical and Electronics Engineers. Their paper is titled "Digitalization of COVID-19 Pandemic Management and Cyber Risk from Connected Systems". They have also looked at the cyber threats associated with connected systems, which can be difficult to handle during a pandemic. According to their findings, there are significant risks associated with how states handle the pandemic via monitoring applications because they already have the systems in place, gathering and processing data autonomously.

The Cyber Attacks to the Hospitals and Critical Infrastructure

Vulnerabilities and Cyber Attack Types

Cyber-attacks tend to increase globally as internet technologies are more and more integrated into everyday life and our dependence on them increases day by day. Cyber operations might be also strategic for state actors to gain some sort of advantage against their opponents. Nevertheless, cyberattacks on critical infrastructure and healthcare might cause direct harm to people and threaten human lives on an international scale. What the COVID-19 has done is to increase the contrast between the underlying vulnerabilities and possible gains out of cyberattacks to critical institutions and infrastructure.

In general, there are vulnerabilities in the healthcare sector due to the weak digital infrastructure, limited human resources to tackle security issues, financial and resource limitations, and deficiencies in its cybersecurity management. A healthcare facility's main function is to serve people in healthcare-related matters. Therefore, the information technology part is often neglected or left behind. Naturally, the hospitals do not dedicate that much manpower nor resources to cyber defenses. These reasons lead the way to the vulnerabilities against cyber attacks. Moreover, the rule of thumb in cybersecurity is that the biggest weakness in security is the human factor. As that being said, the staff working in these critical sectors often lacks enough updates and training about security weaknesses, vulnerabilities, and cyber threat trends. Furthermore, the time pressure and stress factor of the healthcare-related professions mostly leave a weakness that can be exploited in the hands of master manipulators. For instance, an attacker with a good understanding of human psychology can exploit emergencies through urgent requests that will bypass the logical

[8] Brendan FLYNN: *The Inexorable Rise of the Pandemic State? Second-Guessing the long-term political repercussions of COVID 19*. March 18, 2020. https://politicalreform.ie/2020/03/18/the-inexorable-rise-of-the-pandemic-state-second-guessing-the-long-term-political-repercussions-of-covid-19/ (05.30.2021)

[9] Petar RADANLIEV – C. David DE ROURE – Max VAN KLEEK: Digitalization of COVID-19 Pandemic Management and Cyber Risk from Connected Systems. *IEEE Internet of things News*, SSRN. 2020. https://ssrn.com/abstract=3604825 (30.05.2021)

judgments of the staff. With these manipulative behaviors and technical knowledge, attackers can use various tactics like phishing, whaling to gain access to the hospital systems, steal sensitive healthcare or patient data or lock the hospital networks with ransomware.

Let us briefly outline the attack types and how they are performed beginning with phishing. Phishing is the deceitful act to acquire sensitive information like usernames, passwords, social security numbers, credit card numbers by imitating or impersonating a trustworthy entity or person in an information communication technology platform.[10] According to the Internet Crime Complaint Centre of the Federal Bureau of Investigation, phishing was the most prevalent attack type conducted by cyber-criminals as of the year 2020.[11] According to this report, phishing incidents were twice as prevalent as any other type of computer crime. Most of the phishing attacks take place on email platforms. If these phishing emails are sent in a batch to multiple recipients, they are not often personalized nor do they target a specific individual or company. This type of phishing is regarded as 'bulk phishing'.[12] A typical bulk phishing message can include financial services, fake bank claims, service provider notifications, and so forth. If the user is not attentive, they can click on the links or open the attachment that comes with the email. This leaves the victim's system vulnerable to attackers. Compromised accounts may be used to perform various attacks for a particular purpose during prolonging to various periods. Possible goals can be theft of restrictive information, the installation of malware, or the spread of more specifically crafted and complicated phishing emails which are called spear-phishing. Attackers can then utilize the credentials obtained to directly steal money from the victim's bank if any of these attacks yield a positive result for them.

More specifically, in spear phishing, the attacker has the knowledge of the organizational hierarchy to directly target a specific company or person with appropriately tailored phishing emails. Differing from bulk phishing, in order to perform spear phishing, attackers need to collect and utilize specific, personal information about their target to enhance their likelihood of carrying out a successful attack.[13] As the metaphorical naming might suggest, spear-phishing generally targets managers, administrators, or workers in important institutions and financial departments that have access to the organization's sensitive data and services.

Whaling is also related to spear-phishing but the attacks are directed towards bigger fishes. As it can be understood from the metaphorical description. This type of phishing specifically targets senior executives and high-profile targets.[14] Whaling entails the development of spoofed emails purporting to be from senior executives in order to persuade other workers at a company to take a particular action, such as the wiring of funds to an offshore account.[15] While such frauds have much lower success rates, offenders can attain very substantial amounts of money from those few attempts if they work.

---

[10] Zulfikar RAMZAN: *Phishing attacks and countermeasures.* In: Mark Stamp – Peter Stavroulakis (eds.): Handbook of Information and Communication Security. Springer, Berlin – Heidelberg, 2010.

[11] FEDERAL BUREAU OF INVESTIGATION: *Internet Crime Report 2020*. FBI Internet Crime Complaint Centre. 2020. https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf (30.05.2021)

[12] VERIZON: 2019 Data Breach Investigations Report. 2019. https://www.phishingbox.com/assets/files/images/Verizon-Data-Breach-Investigations-Report-DBIR-2019.pdf (30.05.2021)

[13] Debbie STEPHENSON: *Spear Phishing: Who's Getting Caught?* Firmex. 30.05.2013. https://www.firmex.com/resources/infographics/spear-phishing-whos-getting-caught/ (30.05.2021)

[14] Paul GIL: *What Is Whaling?* Lifewire. 05.04.2020. https://www.lifewire.com/what-is-whaling-2483605 (30.05.2021)

[15] Marianne JUNGER – Victoria WANG – Marleen SCHLÖMER: Fraud against businesses both online and offline: crime scripts, business characteristics, efforts, and benefits. *Crime Science* 9 (1) 13. December (2020)

Ransomware is a form of malware that uses encryption to permanently block access to the victim's data unless a ransom is paid. Although some ransomware locks the system in a way that is easy to undo for a savvy user, more sophisticated malware employs a tactic known as cryptoviral extortion. It encrypts the files of the victim, rendering them unavailable until a form of payment to the offenders has been done.[16] Recovery of encrypted files without the decryption key is an obstinate problem in a properly executed ransomware attack and the attackers often ask the payment to be made in a form of cryptocurrency which is difficult to trace and prosecute the perpetrators. When a Trojan is disguised as a legitimate file and sent as an email attachment, the user is tricked into installing or opening it, resulting in a ransomware attack. Just like other forms of cyber attacks, the use of ransomware has grown internationally. According to the July 2018 news of Help Net Security,[17] there were 181.5 million ransomware attacks in the first six months of 2018. This represents a 229 percent raise over the same period in 2017. There were particularly successful ransomware attacks in recent years. Before being shut down by authorities, CryptoLocker was especially successful in 2014, causing an estimated 3 million dollar impact.[18] Another infamous and more impactful attack was carried out by CryptoWall which was estimated to have accumulated over 18 million dollars by June 2015.[19] Moreover, one recent high-profile example, the WannaCry worm, traveled automatically between computers without user interaction. According to Europol, WannaCry infected 200,000 machines around the world, causing interruptions in hospitals, post offices, car plants, and government offices.[20]

As a result, attacks are on the rise while they are constantly evolving in the hands of various actors with various technical and hardware capacities. These attacks directed towards healthcare and critical facilities are low-risk for the attacks which promise high rewards. Operating with their position and attraction of such rewards, criminals and state actors are joining forces against healthcare with varying motives and agendas. These motives can be seizing valuable and sensitive data to gain financial benefit, impede competitive businesses, geopolitical agenda, or overall ideological and political reasons.

Some Cyber Attacks That Took Place in 2020 During the Pandemic

Due to the increased digitization of daily activities, the COVID-19 pandemic also provided an incentive for malicious activities to take advantage of people's sense of insecurity, information need, anxieties, and lack of security knowledge. When it comes to someone's well being, the need for information can be quickly intensified, particularly when the concerns are about preventive strategies, medical procedures, vaccines, or alleged

---

[16] A. YOUNG –Moti A. YUNG: *Cryptovirology: extortion-based security threats and countermeasures.* Proceedings 1996 IEEE Symposium on Security and Privacy. Oakland, CA, USA, 1996. 129-140.

[17] HELP NET SECURITY: Ransomware back in big way, 181.5 million attacks since January. *Online News.* 11.07.2018. https://www.helpnetsecurity.com/2018/07/11/2018-sonicwall-cyber-threat-report/ (30.05.2021)

[18] Mark WARD: Cryptolocker victims to get files back for free. *BBC News.* 06.08.2014. https://www.bbc.com/news/technology-28661463 (14.04.2021)

[19] Sean GALLAGHER: FBI says crypto ransomware has raked in >$18 million for cybercriminals. *Ars Technica.* 25.06.2015. https://arstechnica.com/information-technology/2015/06/fbi-says-crypto-ransomware-has-raked-in-18-million-for-cybercriminals/ (30.05.2021)

[20] Phil MCCAUSLAND – Sam PETULLA – Alastair JAMIESON: Global Cyberattack Hits 150 Countries, Europol Chief Says. *NBCNews.* 14.05.2017. https://www.nbcnews.com/tech/internet/after-huge-global-cyberattack-countries-scramble-halt-spread-ransomware-n759121 (14.04.2021)

government information.[21] As a result, internet users become vulnerable to ransomware and social engineering attacks. According to the information security firm Fireeye, criminal phishing campaigns linked to the coronavirus have increased sharply since January 2020.[22]

Numerous COVID-19 related attacks took place in 2020. Below are some of the cyber incidents that took place in Europe. The German Federal Office for Information Security (BSI), which is in charge of IT security, warned of a "rising amount of corona virus-related cyber attacks on companies and civilians" in early April 2020.[23] Criminals are mainly involved in extracting demographic and financial records from hospitals while conducting a cyber attack to profit from digital identity data.[24] In March 2020, a ransomware attack struck the Brno University Hospital in Czechia, which was one of the country's COVID19 research labs, forcing it to shut down the entire IT network.[25] In the same month, the Maze ransomware group leaked the confidential and medical information of thousands of former COVID19 screening patients from a London-based medical research company.[26] During the same month, the networks of several hospitals in Paris that play a vital role in tackling the COVID19 crisis in the capital were targeted by DDoS attacks, which interrupted server and email access.[27] Phishing emails were sent to senior executives at a German organization that provides personal protective equipment in June 2020. The phishing links were created with the aim of redirecting executives to bogus Microsoft login pages in order to capture their credentials.

There have also been similar attacks that took place outside of Europe. In March 2020, a DDoS attack was launched against the US Department of Health and Human Services, which is heavily involved in the COVID19 crisis in the nation.[28] In June 2020, the University of California San Francisco (UCSF), which was conducting research on a COVID19 vaccine, was the victim of a ransomware attack and was forced to pay cybercriminals, a group called Netwalker 1.14 million US dollars.[29] There have also been reports of websites and an Android app that offer to provide users with real-time updates on the spread of the virus,

---

[21] Johannes WIGGEN: *Impact of COVID-19 on cyber crime and state-sponsored cyber activities*. Konrad Adenauer Stiftung, Germany. 2020. https://www.jstor.org/stable/pdf/resrep25300.pdf?acceptTC=true&coverpage=false (03.05. 2021)

[22] Patrick Howell O'NEILL: Chinese hackers and others are exploiting coronavirus fears for cyber espionage. *MIT Technology Review*. 12 March 2020. https://www.technologyreview.com/2020/03/12/916670/ chinese-hackers-and-others-are-exploiting-coronavirus-fears-for-cyberespionage/ (03.05.2021)

[23] Id. Ref.21.

[24] Caroline BROOKS – Xuefeng JIANG: Types of Information Compromised in Breaches of Protected Health Information. *Annals of Internal Medicine* 21.01.2020. https://www.acpjournals.org/doi/10.7326/M19-1759 (03.05.2021)

[25] Catalin CIMPANU: Czech hospital hit by cyberattack while in the midst of a COVID-19 outbreak. *ZDNet*. 03.03.2020. https://www.zdnet.com/article/czech-hospital-hit-by-cyber-attack-while-in-the-midst-of-a-covid-19-outbreak/ (03.05.2021)

[26] Dan GOODIN: The Internet is drowning in COVID-19-related malware and phishing scams. *Ars Technica* 16.03.2020. https://arstechnica.com/information-technology/2020/03/the-internet-is-drowning-in-covid-19-related-malware-and-phishing-scams/ (03.05.2021)

[27] Bernardi PRANGGONO – Abdullahi ARABO: COVID-19 pandemic cybersecurity issues. *Internet Technology Letters. Wiley Online Library* 4(2) (2021) 247. https://onlinelibrary.wiley.com/doi/full/10.1002/itl2.247 (03.05.2021)

[28] Shira STEIN – Jennifer JACOBS: Cyber-Attack Hits U.S. Health Agency Amid Covid-19 Outbreak. *Cybersecurity. Bloomberg* 16.03.2020. https://www.bloomberg.com/news/articles/2020-03-16/u-s-health-agency-suffers-cyber-attack-during-covid-19-response (03.05.2021)

[29] Id. Ref.27.

similar to the popular Johns Hopkins University map, but actually corrupted them with malware.[30]

How Attacks Happen?

Ransomware attacks are usually launched by a threat actor. To infiltrate the network, they use phishing emails and remote desktop control. Due to stress, exhaustion, an emergency, or other emotional factors, the victim doesn't always pay attention and click on the malicious email or links, leaving the device vulnerable to the attackers. As a result, entire healthcare systems can come to a chokepoint. As a consequence, entire healthcare networks can experience slowdowns if the malware encrypts the network's sensitive data, making it impossible to access critical medical information or apps. Due to its anonymity, the payment is often requested in the form of a cryptocurrency. However, there is no assurance that the perpetrator will ever send the decryption key. It is also a question of whether the victim can be revictimized in the future. The fate of the victims is hence in the hands of the offenders. Moreover, attackers can steal sensitive data from the hospital network even if they decrypt the hard drives. This compromised data will later be used for a profit.

Cyber espionage is another form of attack that is more of a hidden threat. They are carried out for a variety of reasons, including harming reputation, intelligence operations, and intellectual property theft. Infiltration occurs when a hacker gains access to a device by spear-phishing or leveraging internal vulnerabilities. After that, the attackers must keep access to the target system. They use Remote Access Trojans, or RATs, for this reason. As a result, they try to hide their tracks by deleting system and security logs. They often use memory-resident malware that self-destructs. Service delays, eroding patient confidence, intellectual property theft, compromising information for a reputational assault, data manipulation, and discrediting the victim's credibility are all possible consequences of this sort of attack.

Another kind of assault is disinformation or propaganda, which is used to propagate infodemics. During the COVID-19 pandemic, inaccurate and deceptive facts were widely disseminated. Some nation-states took advantage of the uncertainties and gaps in the data by promoting misinformation about the virus and its sources. Data manipulation in a target network can also be accomplished in a cyber process. This could cause a shift in decision-making, jeopardizing local and global responses to the COVID-19 pandemic. Online rolling and conspiracy theories on social media sites are examples of such techniques.

The Impact

The consequences of cyber attacks and cyber operations can be divided into several categories. They mostly endanger the human life and well-being of people who have little to do with political or financial affiliations. In such a sensitive time, such attacks will cause delays or suspend patient treatment. These attacks endanger lives and compromise patient safety amid a worldwide pandemic. If the primary facility is under attack, critical patients can miss the vital time when being redirected to other facilities. Such circumstances will prevent medical practitioners from providing quality care and leaving them blind without access to medical records.

---

[30] Id. Ref.26.

Furthermore, both patients and care practitioners are affected psychologically and emotionally. The currently tense healthcare situation will be exacerbated by such assaults. Operational processes can get even more distressed as a result of this. Additional problems can arise as a result of incident management and remediation efforts. The whole chain of events can ruin the already weary morale and stamina of the people in the forefront fighting the COVID-19. Cyberattacks may have significant financial consequences in addition to patient well-being and psychological effects. The effect is also exacerbated by more intellectual property loss, market interruption, and business impacts. However, not everything is immediately monetary. Damages to someone's or some institution's reputation may be irreversible and unrepairable. Cyberattacks on hospitals and other vital facilities have a social impact in general. They erode public trust in the sector and its institutions. They also lead to public distrust of authority and the government. As a result, cyber threats will have both social and political consequences. Disinformation campaigns instill distrust, create doubt, and other negative effects. They might also influence geopolitical situations.

Applicability of International Law and Regulations

Cyber threats are complicated, and the threat actors' identities are obscured. Furthermore, since cyberspace is borderless by default, cyber activities are international by nature. States, on the other hand, create their own legislative and political regimes. These considerations create a conundrum as cyberattacks occur covertly in an international manner while the world is fragmented into nation-states, each with its own set of laws and regulations.

The Budapest Convention

The Convention is the first international protocol on offenses committed over the Internet and other electronic networks, and it addresses issues such as copyright infringements, computer-related piracy, child pornography, and network protection breaches. It also includes several powers and processes, such as computer network search and interception. Its primary goal is to promote a shared criminal strategy aimed at protecting society from cybercrime, especially through the adoption of effective legislation and the promotion of international cooperation.[31] This convention is the only legally enforceable international agreement on the subject. It acts as a model for every nation seeking to draft robust cybercrime legislation, as well as a forum for inter-state cooperation.

The Budapest Convention makes it illegal to violate the confidentiality, integrity, and availability of electronic data and programs, as well as computer-related offenses, content-related offenses, and copyright and associated rights violations. It has developed protocols to improve the efficiency of investigations.[32] It also establishes a legal framework for international collaboration among States Parties to the Convention, including spontaneous intelligence exchanges, extradition, and international mutual assistance, as well as permanent contact points.

Many countries are using the Convention on Cybercrime as a framework to improve their regulations. Main stakeholder collaboration, like public-private collaboration, has been

---

[31] The Budapest Convention. Treaty No.185. *Convention on Cybercrime*. Budapest, Hungary. 23.11.2001. https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185 (30.05.2021)
[32] Id. Ref. 31.

bolstered. The Project on Cybercrime has developed guidelines to improve law enforcement and Internet service provider cooperation in the prosecution of cybercrime.

The UN Group of Governmental Experts on Information Security (GGE)

As the incidents became more severe, such as attacks on healthcare networks and essential facilities, countries all over the world convened meetings across UN platforms. In response to these trends, the UN Group of Governmental Experts on Information Security (GGE) was established in 2004 with the aim of restoring secure global information and telecommunications networks. As a result, the United Nation Group of Governmental Experts, or shortly GGE group was created as a unit to outline the fundamentals of cybersecurity and the measures that need to be taken to improve interstate relations and increase international cybersecurity by encouraging the use of international law to protect and control nations' practices in cyberspace. GGE meetings have resulted in reports whenever the talks have ended with consensus between the experts from various nations.

The 2013 and 2015 reports state that international law is applicable and regards it as an essential part of maintaining peace and stability in the use of ICTs. It further notes that the United Nations Charter exists in its entirety, including the fundamental rights of states and the provision for peaceful resolution of conflicts.[33] It emphasizes the importance of the principles of state sovereignty, sovereign equality, settlement of disputes by peaceful means, and non-intervention in the internal affairs of other states, and compliance with obligations to respect and protect human rights and fundamental freedoms with regards to the use of Information Communication Technologies. In addition, the report mentions existing international legal norms such as humanity, necessity, proportionality, and distinction.[34] It also states that states must satisfy their contractual obligations when it comes to internationally wrongful acts that are liable to them under international law.[35] While it was decided that further research into the application of international law to the use of ICTs was necessary, the recommendations in the GGE report on the subject seek to gain a better understanding of the use of ICTs, which is critical for promoting an open, secure, stable, affordable, and peaceful ICT environment.

Voluntary Norms, Confidence Building Measures and Capacity Building

In the 2015 GGE report, responsible state behavior in the use of ICTs is introduced as a set of informal, non-binding standards.[36] These norms contain both positive and negative responsibilities aimed at curbing malevolent activities. The voluntary norms include a broad variety of topics, including state collaboration, attribution of malicious ICT use, internationally wrongful activities, human right violations, non-interference with states' vital resources and supply chains, and notification of ICT vulnerabilities to emergency response teams in case of cyberattacks.

---

[33] THE UN GENERAL ASSEMBLY: *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*. 22.07.2015. 12. (UN Report, 2015) https://www.un.org/ga/ search/view_doc.asp?symbol=A/70/174 (30.05.2021)

[34] UN Report, 2015. 3.

[35] UN Report, 2015. 2.

[36] UN Report, 2015. 7.

The GEE identifies a number of core confidence-building measures for fostering an open, secure, sustainable, affordable, and peaceful ICT environment for all.[37] These instruments facilitate continuous and improved dialogue, knowledge exchange, and other accountability measures between the states, with an emphasis on policy confidence-building. In practical terms, such interventions could include defining points of contact and facilitating knowledge exchange through voluntary classification of ICT incidents and sharing of critical infrastructure categories. These initiatives, when combined with teamwork at various levels, have the potential to help nations develop trust among themselves.

The GGE reports stress the importance of international collaboration and assistance in enhancing state capacity for cooperation and joint action, which is critical for international security. Through capacity-building and cooperative efforts, all states can learn from each other about the threats that they face and find effective responses to them. The establishment and implementation of cooperative mechanisms such as CERTS, technical training, information and technology exchange, appropriate frameworks for consistency, and, ultimately, cooperation in the investigation, are all important collaborative initiatives.[38] These measures could be the basis by which states can assist each other to bridge the digital gaps.

Laws and Regulations Within the EU

The European Union Agency for Cybersecurity (ENISA)

The European Union Agency for Cybersecurity (ENISA) is the Union's agency tasked with ensuring a significant level of cybersecurity all around the continent. Established in 2004 and reinforced by the EU Cybersecurity Act, ENISA contributes to EU cyber policy, promotes the trustworthiness of ICT services, systems, and processes through cybersecurity certification schemes. It promotes working collaboratively with Member States and EU bodies to assist Europe in preparing for future cyber risks.

It is a regulatory body that was established by the European Parliament's Regulation (EC) No 460/2004 on March 10, 2004, with the intent of enhancing Network and Information Security (NIS) for all internetwork operations in the EU. ENISA is now governed by Regulation No 526/2013,[39] which took effect in 2013 and repealed the previous one. ENISA collaborates with all EU member states to offer a wide variety of support. The intention is to provide the member states with guidelines about how to deal with security breaches. As a whole, it strives to assist member states in policy development and implementation. Further to that, ENISA provides direct assistance to collaborate the technical teams within the European Union.[40] ENISA has published several reports that address many of the key cybersecurity concerns. ENISA also collaborates with established international standard

---

[37] UN Report, 2015. 6.

[38] UN Report, 2015. 10.

[39] EU Regulation No 526/2013. Concerning the European Union Agency for Network and Information Security (ENISA) and repealing Regulation (EC) No 460/2004. https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:JOL_2013_165_R_0041_01&qid=1397226946093&from=EN (30.05.2021)

[40] ENISA: *A Trusted and Cyber Secure Europe. European Union Agency for Cybersecurity*. June 2020. https://www.enisa.europa.eu/publications/corporate-documents/enisa-strategy-a-trusted-and-cyber-secure-europe (30.05.2021)

bodies outside the EU such as the International Organization for Standardization (ISO) and the International Telecommunication Union (ITU).[41]

NIS Directive

The European Parliament adopted the Directive on Network and Information Systems Protection, or NIS Directive,[42] on July 6, 2016. The directive took effect in August 2016, and all EU Member states had 21 months to integrate the directive's provisions into their own state legislation. The NIS Directive aims to create an overall higher level of cybersecurity in the EU. The NIS Directive seeks to raise the standard of cybersecurity within the EU as a whole. The directive has a substantial influence on internet service providers and essential service operators. Providers of essential services are those organizations whose services would be severely harmed if they are attacked which can potentially result in critical social or economic consequences. The essential service providers are accountable for reporting any major security incidents they encounter to Computer Security Incident Response Teams (CSIRT). The NIS Directive holds them liable for any security breaches, even though they might outsource the management of their information systems to third parties.[43] Furthermore, the NIS directive requires the EU member states to establish a policy that includes CSIRTs, as well as National Competent Authorities (NCAs) and Single Points of Contact (SPOCs) whose task is to deal with cybersecurity breaches in a manner that reduces their damage.[44] So, all significant incidents must be reported to them. Furthermore, all EU member states are urged to exchange cybersecurity information and data.

The EU Cybersecurity Act

The EU Cyber Security Act or the CSA sets up a mechanism for cybersecurity certification for digital goods, services, and processes in the EU. The CSA complements the NIS Directive and ENISA plays a vital role in developing and sustaining the European cybersecurity qualification process.[45] The CSA is held in the Council of 17 April 2019 and came into force on 27 June 2019.[46] The act tries to enhance the essential service network stability of essential services and critical sectors. Furthermore, the ENISA was set as the

---

[41] Steve PURSER: *Standards for Cyber Security*. In: Melissa E. Hathaway (ed.): Best Practices in Computer Network Defense: Incident Detection and Response. Nato Science for Peace and Security Series – D. Information and Communication Security. 35. IOS Press. 2014.

[42] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union. http://data.europa.eu/eli/dir/2016/1148/oj (30.05.2021)

[43] Lara WHITE – Marcus EVANS: *NIS Directive Published: EU Member States Have Just Under Two Years to Implement*. Data Protection Report. 21.07.2016. https://www.dataprotectionreport.com/2016/07/nis-directive-published-eu-member-states-have-just-under-two-years-to-implement/ (30.05.2021)

[44] DELOITTE: *Agreement reached on EU Network and Information Security (NIS) Directive*. Luxembourg. January 2016. https://www2.deloitte.com/lu/en/pages/risk/articles/agreement-new-eu-network-information-security-directive.html (30.05.2021)

[45] EUROPEAN COMMISSION: *Shaping Europe's digital future-The EU Cybersecurity Act*. 29.03.2021. https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-act (30.05.2021)

[46] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) PE/86/2018/REV/1 http://data.europa.eu/eli/reg/2019/881/oj (30.05.2021)

central coordinating body for cybersecurity competence and advisory. As a result of CSA, ENISA's capabilities and services have been expanded. The agency's mission is to include cybersecurity assistance and facilitate the adoption of EU cybersecurity policies throughout member states.

General Data Protection Regulation (The GDPR)

The General Data Protection Regulation or the GDPR of the European Union lays down rules aimed at protecting the personal data of its citizens concerning the processing of personal data and rules relating to the transfer of such data outside the Union and the European Economic Area.[47] The GDPR has been in effect since 2018 and extends to all organizations that exist in the EU or deal with the personal data of EU residents. When an EU citizen's data is stored, the individual is now entitled to the GDPR, regardless of where the data is processed. The GDPR emphasizes the importance of consent as the companies who keep data on EU people are obliged to provide the users the same easy way to restrain from sharing or processing their data. The GDPR also prohibits the transmission of a citizen's personal data outside of the EU or to a third party without the permission of the citizen. The EU Data Protection Board (EDP), the overarching board, is in charge of GDPR regulations.

Conclusion

The raging pandemic all around the globe prompted governments to prohibit social activities and impose stringent shutdown procedures that made e-schooling, home offices, and e-meetings almost a must. Consequently, crisis management, tracking of COVID-19 affected individuals, virus statistics and data, and client records in the hospital database all add to the urgency of using the internet and technologies to combat the plague. Such dependencies have significantly elevated cyberattacks and cybercrime which are directed towards healthcare facilities and critical infrastructure while threatening patient safety and well-being.

The vulnerabilities in the healthcare sector occur due to the weak digital infrastructure, limited human resources to tackle security issues, financial and resource limitations, and deficiencies in its cybersecurity management. Moreover, like in other vulnerabilities, the biggest weakness in security is the human factor. As that being said, the staff working in these critical sectors often lacks enough updates and training about security weaknesses, vulnerabilities, and cyber threat trends. Governments' initiatives to strengthen cyber security tools for the healthcare sector and critical infrastructure can help to defend against such incidents. This act would require both good planning and some financial resources. Furthermore, providing training for hospital staff and facility workers can further reduce the likelihood of cyber incidents taking place first hand.

In terms of laws and regulations, there have been developments both within the EU and in the UN to tackle attacks to such important facilities which might have serious, life threatening consequences. It is clear that the technology is expanding at a faster speed than the international community can follow up. Nevertheless, regional cooperation is likely to

[47] Directive 95/46/EC on General Data Protection Regulation. Article 1., Regulation (EU) 2016/679 of the European Parliament and of the Council (27 April 2016). https://eur-lex.europa.eu/eli/reg/2016/679/oj (30.05.2021)

become more effective towards cyber security and data protection as we can observe from the developments that took place within the EU. Yet, more international commitment is required on the surfacing issues. The stimulus to create a more peaceful cyberspace only grows as both the use of ICTs and cyber attacks increases.

On the other hand, new common grounds and understanding can be achieved through new tools and dynamics, such as cyber diplomacy, confidence-building mechanisms, and encouragement of responsible state behavior in cyberspace. Greater cooperation within the EU can help achieve better regulation and capacity building to tackle disruptive events in Cyberspace. The EU already has various basic regulatory and protective measures. More inclusive ones can be built upon those principles to prepare the Union towards a more secure digital future.