Annals of Health Law

Volume 27
Issue 2 *Summer 2018*

Article 9

2018

Healthcare, Privacy, Big Data and Cybercrime: which one is the weakest link?

Marin Mrcela

Igor Vuletic

Recommended Citation
Marin Mrcela & Igor Vuletic *Healthcare, Privacy, Big Data and Cybercrime: which one is the weakest link?*, 27 Annals Health L. 257 (2018).
Available at: https://lawecommons.luc.edu/annals/vol27/iss2/9

Healthcare, Privacy, Big Data and Cybercrime: which one is the weakest link?

Marin Mrčela[*]

Igor Vuletić[+]

INTRODUCTION

Today, cybercrime poses one of the largest risks in every sector that utilizes computer data-based operating systems.[1] While computerization certainly improved the quality of service, it simultaneously made confidential information accessible for illegal operations from anywhere in the world.[2] One might say that the computer era revolutionized the ordinary nature of crimes, allowing them to transcend from the physical world, to the virtual or immaterial.[3] The healthcare sector broadly accepted the many advantages offered by the digitalization process, with adoption accelerating during the last decade.[4] In the new digitalized environment, it is unquestionable that big

[*] Marin Mrčela, Ph.D., Justice of the Republic of Croatia Supreme Court; President of GRECO (The Group of States Against Corruption, Council of Europe); Assistant Professor at Faculty of Law Osijek, Josip Juraj Strossmayer University of Osijek, Croatia; marin.mrcela@vsrh.hr.

[+] Igor Vuletić, Ph.D; Associate Professor at the Chair of Criminal Law, Faculty of Law Osijek, Josip Juraj Strossmayer University of Osijek, Croatia; ivuletic@pravos.hr.

[1] *See* HEALTH CARE INDUSTRY CYBERSECURITY TASK FORCE, REPORT ON IMPROVING CYBERSECURITY IN THE HEALTH CARE INDUSTRY 1–2 (2017), https://www.phe.gov/Preparedness/planning/CyberTF/Documents/report2017.pdf [hereinafter, HEALTH CARE INDUSTRY CYBERSECURITY TASK FORCE].

[2] David F. Linowes, *Your Personal Information Has Gone Public*, 2D COMPUTERIZATION AND CONTROVERSY 637 (Kling, 1996), https://www.sciencedirect.com/science?_ob=PdfExcerptURL&_imagekey=3-s2.0-B9780124150409501330-main.pdf&_piikey=B9780124150409501330&_cdi=283111&_orig=PublicationURL&_zone=rslt_list_item&_fmt=abst&_eid=3-s2.0-B9780124150409501330&_isbn=9780124150409&_user=572708&md5=c4ac82414f74df0c0a5c1b04d7ddd41d&ie=/excerpt.pdf%20target=.

[3] Susan W. Brenner, *Cybercrime Jurisdiction*, 46 CRIME LAW SOC. CHANGE 189, 189 (2006).

[4] *See* Nitesh V. Chawla & Darcy A. Davis, *Bringing Big Data to Personalized Healthcare: A Patient-Centered Framework*, 28 J. GEN. INTERN. MED. 660, 661 (2013); *Big Data Cloud Database & Computing*, QUBOLE, https://www.qubole.com/resources/big-data-cloud-database-and-computing/ ("Cloud computing is the commodification of computing time and data storage by means of standardized technologies.") (last visited May 22, 2018).

data and the "cloud" enables hospitals to provide the best possible care for patients.[5]

However, while other sectors have used the cloud for many years, the healthcare sector is still relatively new in this sensitive business.[6] For example, financial and commercial entities have been the targets of cyber-attacks for many years and in response, developed the skills necessary to defend and protect their consumers.[7] Accordingly, the financial and commercial sectors experienced both the benefits and risks of digitalization, while receiving the opportunity to develop protective measures to cyber-attacks.[8] Conversely, it can be said that healthcare organizations still lack sufficient standards of protection, despite their status as lucrative targets for cybercriminals.[9] By way of illustration, the average payment for medical identity theft is ten times higher than for identity theft in other sectors.[10]

As the number of attacks on health care entities continues to rise, the lack of adequate protection makes healthcare organizations more vulnerable than other potential targets for cyber criminals.[11] Cyber criminals, or "hackers," prefer to target hospitals because they are more willing to pay ransom for the decryption of their crucial data after a cyberattack.[12] Because hospitals perform sensitive activities, such attacks potentially damage not only the organization and its staff, but its patients as well.[13] Correspondingly, cyber attackers carry out more successful cyber-attacks against victims associated with hospital data breaches in comparison to victims in other sectors.[14] The rate of cyberattacks in health care also increased because unlike other personal data limited by expiration dates, healthcare data exists in perpetuity, and resultantly may be used for numerous malicious activities such as

[5] Chawla & Davis, *supra* note 4, at 661.

[6] *Id.*

[7] Monica Brink, *Financial services and the great cloud conundrum,* INFORMATION-AGE (Jan. 26, 2017) http://www.information-age.com/financial-services-great-cloud-conundrum-123464162/.

[8] *Id.*; Shamun Mahmud, *Commercial & Public Sector Faces Same Cybersecurity, Cloud, and Mobile Concerns*, DLT SOLUTIONS (Jan. 17, 2013), http://www.dlt.com/blog/2013/01/17/commercial-public-sector-face-cybersecurity-cloud-mobile-concerns/.

[9] HEALTH CARE INDUSTRY CYBERSECURITY TASK FORCE, *supra* note 1, at 1.

[10] Laurie Zabel, *The Real Cost of A Data Breach*, HEALTH IT OUTCOMES (June 6, 2017), https://www.healthitoutcomes.com/doc/the-real-cost-of-a-data-breach-0001 (describing that personal medical data allegedly costs around $20,000 on the black market).

[11] Kelly Sheridan, *Major Cyberattacks on Healthcare Grew 63% In 2016*, DARK READING (Dec. 22, 2016, 2:15 PM) http://www.darkreading.com/attacks-breaches/major-cyberattacks-on-healthcare-grew-63—in-2016/d/d-id/1327779.

[12] Igor Vuletić, *Data-Driven Healthcare and Cybercrime: A Threat We Are Not Aware of?*, EWHA INST. FOR BIOMED. L. & ETHICS (2017), http://www.eible.org/igor-vuletic/.

[13] *Id.*

[14] *Id.*

identity theft, insurance fraud, health care fraud, and fraudulent tax returns.[15] In 2013, the healthcare sector reported 44% of all identity theft in the U.S.[16] In addition, the healthcare industry data breach costs are almost three times higher than in any other industry.[17]

This Article aims to draw the attention of scholars and practitioners to an important vulnerability in the healthcare sector, not only to identity theft, but also to other forms of cyber-attacks and related legal issues and challenges. To begin, this article will describe some of the most notorious cyberattacks on healthcare systems in both the European Union ("EU") and United States ("US"). Based on this analysis, Part I will suggest phenomenology of cybercrimes against the healthcare system. Next, this Article will argue that a clear definition of phenomenology is crucial for a better understanding of this type of cybercrime. Part II of this Article will be devoted to the legal, normative aspect of the problem. To combat cybercrimes, lawyers must necessarily follow modern trends and educate themselves in the field of computer technology. Further, relevant legal provisions need to follow modern trends and provide an adequate legal framework to fight this form of crime. In addition, this Article will discuss two important legal issues regarding cybercrimes: the need for harmonization of legislation in the area of cybercrimes, and the problem of jurisdiction in the context of the health care system and patients' privacy as protected subjects. The first problem is of a substantive nature, while the second is procedural. Both issues have a cornerstone value, since they appear to be fundamental assumptions of the effective struggle against cybercrime, a phenomenon with international element.

The main characteristic of cybercrimes is their immaterial or virtual nature, enabling perpetrators to carry out attacks from another part of the world.[18] This makes it difficult to connect a certain attack to specific place or even a specific legal order.[19] Therefore, many legal scholars point to the fact that it is important to establish unique definitions of cybercrimes in order to prevent cybercriminals from eventually avoiding criminal liability by consequence of the legal gaps and different, incongruent legal systems across

[15] Adam Wright, et al., *The Big Phish: Cyberattacks Against U.S. Healthcare Systems*, 31 J. GEN. INTERN. MED. 1115, 1115–17 (2016); Caleb Barlow, *Attackers Shift Sights from Retail to Health Care in 2015,* SECURITY INTELLIGENCE (Dec. 24, 2015), https://securityintelligence.com/attackers-shift-sights-from-retail-to-health-care-in-2015/,

[16] Laura Shin, *Medical Identity Theft: How the Health Care Industry is Failing Us*, FORTUNE (Aug. 31, 2014), http://fortune.com/2014/08/31/medical-identity-theft-how-the-health-care-industry-is-failing-us/.

[17] Michelle Alvarez, *The Year of the Health Care Industry Security Breach*, SECURITY INTELLIGENCE (Dec. 1, 2015) https://securityintelligence.com/the-year-of-the-health-care-industry-security-breach/.

[18] Brenner, *supra* note 3, at 189, 198.

[19] *Id.*

the world.[20] In this context, this Article will discuss the scope of behaviors that should be criminalized at an international level.[21] Particularly, this Article will emphasize relevant international documents, EU legislations (including examples of good practice from certain member states of EU), and U.S. Federal law.[22] The dominant research method used in this Part of the Article will be the comparative method.

I. PHENOMENOLOGY OF CYBERATTACKS IN THE HEALTH CARE SECTOR

The first step to understanding the nature of cyber-attacks in the healthcare industry is to familiarize oneself with the technologies present in the modern healthcare market.[23] For purposes of this Article, we will adopt *Tschider's* classification of digital health technologies, including implanted devices, non-implanted devices, wearables, mobile apps, web applications and general administrative information technology ("IT").[24] It is important to differentiate between implanted and non-implanted devices. Although both types of devices can be connected to a network, non-implanted devices do not "pervasively interact with the body."[25] Wearables are devices that are often used in exercise, such as a Fitbit – which measures and combines different data important for exercise and health (e.g. heart rate, sleep data, calories etc.).[26] Wearables do not have any actual physical influence on the human body.[27] Web applications and general administrative IT also provide support to health-related activities (e.g. storage of medical data, maintaining software etc.).[28] *Tschider* explains that implanted or affixed devices pose the biggest risk, since those can either "directly deliver medication or other stimulus to the human body or gather biological health information directly."[29]

In this Part, we will establish phenomenology of cyber-attacks in the healthcare sector. For the purposes of this Article, the term "phenomenology" should be understood in its criminological sense, as an

[20] *See* e.g. Francesco Calderoni, *The European Framework on Cybercrime: Striving for an Effective Implementation*, 54 CRIME LAW SOC. CHANGE 339, 340–41 (2010); Brenner, *supra* note 3, at 190.

[21] Calderoni, *supra* note 20, at 350.

[22] *Id.* at 339–57.

[23] Charlotte A. Tschider, *Enhancing Cybersecurity for the Digital Health Marketplace*, 28 ANNALS HEALTH L. 1, 7–8 (2017).

[24] *Id.* at 5–7, 36.

[25] *Id.* at 5.

[26] *Id.* at 6.

[27] *Id.* at 5–6.

[28] *Id.* at 6.

[29] *Id.*

empirical analysis of forms of certain criminal behavior.[30] Phenomenology, along with etiology,[31] forms an integrative part of modern criminology.[32] Recently, the healthcare industry has been a target of different types of cyber-attacks.[33] These attacks range from ransomware, which compromises the integrity of systems and privacy of patients, to computer and Internet frauds.[34] While other industries experience these attacks as well, the nature of the healthcare industry makes these attacks even more dangerous for today's society.[35] This is partially due to cyber-attacks in other sectors having a predominantly financial effect, while cyber-attacks in the health care industry will usually have consequences that go beyond purely financial damage.[36] For the purposes of this paper, the potential forms of cyber-attacks shall be divided in six overarching groups: 1) ransomware; 2) data breaches; 3) DDoS attacks; 4) insider threats; 5) computer fraud in healthcare sector; and 6) human malware.

A. Ransomware

One of the most common cyber-attacks in the healthcare industry is ransomware.[37] Ransomware is a type of malware that infects systems and files, making them inaccessible until a certain amount of ransom, stipulated by the hacker, is paid by the entity.[38] The ransom usually demands paper money, but it can also be in virtual currency, such as bitcoin.[39] In May 2017, a global ransomware attack named "*WannaCry*" infected over 230,000 computers in approximately 150 countries and ransom was demanded in bitcoins.[40] In literature, ransomware is defined as "a type of malware that uses malicious codes to intrude the system before users notice it, to encrypt

[30] *Id.* at 4–7.

[31] Etiology in sense of empirical research of causes of criminal behavior.

[32] Davor Derenčinović and Anna-Maria Getoš, *Uvod u kriminologiju s osnovama kaznenog prava* (Zagreb: Faculty of Law, 2008), at 19, 31.

[33] Barlow, *supra* note 15; HEALTH CARE INDUSTRY CYBERSECURITY TASK FORCE, *supra* note 1, at 5.

[34] *Cyber Attacks: In the Healthcare Sector*, CTR FOR INTERNET SECURITY, https://www.cisecurity.org/cyber-attacks-in-the-healthcare-sector/ (last visited May 22, 2018).

[35] Barlow, *supra* note 15.

[36] HEALTH CARE INDUSTRY CYBERSECURITY TASK FORCE, *supra* note 1, at 6; *Cyber Attacks: In the Healthcare Sector*, *supra* note 34.

[37] *Ransomeware: In the Healthcare Sector*, CTR FOR INTERNET SECURITY, https://www.cisecurity.org/ransomware-in-the-healthcare-sector/ (last visited May 22, 2018).

[38] *Id.*

[39] Olivia Solon & Alex Hern, *'Petya' Ransomware Attack: What Is It and How Can It Be Stopped?*, THE GUARDIAN (June 28, 2017), https://www.theguardian.com/technology/2017/jun/27/petya-ransomware-cyber-attack-who-what-why-how.

[40] *Id.*

important files, to require money using encrypted files as a hostage, and to give monetary damages to users."[41] Essentially, ransomware may be characterized as a kind of virtual blackmail. The use of ransomware is constantly increasing, and current estimations indicate that its use will continue to increase in the future.[42]

When ransomware happens in the healthcare industry, it slows down all critical processes and may go as far as to make them completely dysfunctional.[43] In the healthcare industry, hackers particularly target hospitals with ransomware.[44] When facing ransomware cyber-attacks, hospitals must switch to old, conservative methods of data storing, which correspondingly slows down the medical process and expends funds that could have been allocated to projects, research, and patient care.[45] Ransomware attacks are more prevalent than most realize. In 2016, at least 14 hospitals across the United States experienced ransomware attacks.[46] In these cases, hackers managed to crack out-of-date servers, which enabled them to upload malware in the system.[47] Unusually, hackers performed this action without any participation or interaction with victims, making it dissimilar from other "physical," or traditional crimes.[48] A specific healthcare industry-related incidence was in 2016, when a virus called "Locky" hit Hollywood Presbyterian Hospital in California.[49] Locky, given its namesake unsurprisingly locked out the hospital staff, which effectively obstructed their access to patients' files, radiological imaging, and other

[41] Sanggeun Song, et al., *The Effective Ransomware Prevention Technique Using Process Monitoring on Android Platform*, MOBILE INFORMATION SYSTEM 1, 1 (2016), https://www.hindawi.com/journals/misy/2016/2946735/.

[42] Limor Kessem & Caleb Barlow, *Ransomeware Report: Top Security Threat Expected to Continue Rising in 2017*, SECURITY INTELLIGENCE (Dec. 14, 2016), https://securityintelligence.com/ransomware-top-security-threat-expected-to-continue-rising-in-2017/.

[43] *Ransomeware: In the Healthcare Sector*, *supra* note 37.

[44] *Id.*

[45] *Id.*

[46] Jessica Davis, *Ransomware: See the 14 Hospitals Attacked so Far in 2016*, HEALTHCARE IT NEWS (Oct. 5, 2016), http://www.healthcareitnews.com/slideshow/ransomware-see-hospitals-hit-2016?page=1; *see also* Chris Sienko, *Ransonware Case Studies: Hollywood Presbyterian Ottawa Hospital*, INFOSEC INSTITUTE, http://resources.infosecinstitute.com/category/healthcare-information-security/healthcare-attack-statistics-and-case-studies/ransomware-case-studies-hollywood-presbyterian-and-the-ottawa-hospital/#gref (last visited May 22, 2018).

[47] *Id.*

[48] *Id.*

[49] *Id.*; Richard Winton, *Hollywood Hospital Pays $17,000 in Bitcoin to Hackers; FBI Investigating*, L.A. TIMES (Feb. 18, 2016 10:44 AM), http://www.latimes.com/business/technology/la-me-ln-hollywood-hospital-bitcoin-20160217-story.html.

medical tests.[50] This caused serious delays in patient care, and eventually resulted in the hospital paying $17,000, or the equivalent of 40 bitcoin, ransom to re-gain access to their data.[51] A similar virus affected Ottawa Hospital in Ontario, Canada, where four victims activated malware by clicking on a phishing e-mail that encrypted their computer system.[52] This example illustrates the significance of proper computer training of healthcare staff to minimize the risk of such attacks.

There are two elements to a criminal offense, *actus reus* and *mens rea*.[53] The *actus reus* is the element external to the defendant's mind, consisting of an act committed by the defendant along with certain circumstances that constitute criminal offense.[54] The *mens rea* (also known as the mental element of crime) reflects the state of mind of the defendant in relation to specific *actus reus*.[55] The *actus reus* of ransomware usually includes a certain amount of contribution from the victim as the perpetrator counts on the victim's naivety.[56] The victim usually activates malware by either reading emails containing a malicious attachment, clicking on a malicious link, or by viewing an advertisement containing malware.[57] All three techniques are commonly known as "phishing," which is the process of "obtaining computer credentials from users through manipulation or deceit."[58] Once stolen, computer credentials can be misused in a variety of ways, from stealing identities and selling them online in the black markets, to using them for different types of cyber frauds.[59] Further, stolen computer credentials can be recycled and used for additional, improved cyber-attacks.[60] What makes defense strategies more difficult in the cybercrime context is that cybercriminals continue to develop new tactics and techniques to carry out attacks, which makes it even more difficult to timely detect and prevent new

[50] Sienko, *supra* note 46; Winton, *supra* note 49.

[51] Sienko, *supra* note 46.

[52] *Id.*; *Ottawa Hospital Hit With Ransomware, Information on Four Computers Locked Down*, NAT'L POST (Mar. 13, 2016 2:10 PM EDT), http://nationalpost.com/news/canada/ottawa-hospital-hit-with-ransomware-information-on-four-computers-locked-down.

[53] R. A. Duff, *Intention, Agency and Criminal Liability: Philosophy of Action and the Criminal Law* (Blackwell, 1990), at 7–8.

[54] *Id.*

[55] *Id.*

[56] Song et al., *supra* note 41, at 2.

[57] Wright et al., *supra* note 15, at 1115; For more detailed analysis of technical aspects of ransomware, see Alexander A. Grebenkov & Elena O. Yakovleva, *The State of Modern Malicious Software: Foundations of Study on Cyber-Armaments*, 11 INT'L J. OF APPLIED ENG'R RES. 6832, 6832–34 (2016).

[58] Wright et al., *supra* note 15, at 1115.

[59] *Id.* at 1116.

[60] *Id.*

attacks in the future.[61] That is why it is recommended for hospitals and healthcare providers to invest in additional funding for the education and training of their personnel to recognize and avoid phishing.[62] Unfortunately, the organizations that do not take necessary common-sense measures to preemptively prevent cyber-attacks can suffer extremely serious consequences due to access to their files and computer system in general becoming disabled.[63] Therefore, due to the extensive damages that may follow a cyber-attack, it is pertinent that each healthcare organization should properly secure networks, systems, and patients, by continuously maintaining and updating their defense system.

B. Data breach

According to some authors, a data breach is probably the most widespread type of cyber-attack.[64] A data breach is a "loss or theft, or other unauthorized access to sensitive personally identifiable information that could result in the potential compromise of the confidentiality or integrity of data."[65] This type of cybercrime activity is so prevalent that experts warn organizations to assume not that they *may* be victims of a data breach, but that they have *already been* victimized.[66] According to the Ponemon Institute and Verizon Data Breach Investigations Report, the healthcare industry was ranked second place based on the number of data breaches per year, with only the finance industry exceeding it in the number of attacks.[67] Breaches can occur in many different forms, such as credential-stealing malware, lost laptops, improper configuration, and overly complex access permissions, among others.[68] The goal of cybercriminals is either to sell the protected health

[61] Currently, there are eight main types of malicious software weapons, which vary in the amount of harm they can inflict. *See* Grebenkov & Yakovleva, *supra* note 57, at 6834.

[62] Wright et al., *supra* note 15, at 1115, 1117.

[63] *Id.*

[64] Barlow, *supra* note 15.

[65] Gina Stevens, CONG. RES. SERV., DATA SECURITY BREACH NOTIFICATION LAWS, REPORT FOR CONGRESS 1 (Apr. 10, 2012), https://fas.org/sgp/crs/misc/R42475.pdf.

[66] Garrett Baldwin, *Assume breach: The cyber threat to traders*, FUTURES MAGAZINE (Sept. 17, 2015), http://www.futuresmag.com/2015/09/17/assume-breach-cyber-threat-traders; Ray Pompon, *Living in an Assume Breach World*, HELP NET SECURITY (Aug. 24, 2017), https://www.helpnetsecurity.com/2017/08/24/assume-breach-world/; J.M. Porup, *Why My Motto as a Security Journalist Is "Assume Breach"*, SOURCE (June 15, 2017), https://source.opennews.org/articles/why-my-motto-security-journalist-assume-breach/.

[67] *Verizon's Data Breach Investigations Report – A look at the Big Picture (Part 2)*, BLUEFIN https://www.bluefin.com/bluefin-news/verizons-data-breach-investigations-report-look-big-picture-part-2/ (last visited May 22, 2018).

[68] Kont et al., *Insider Threat Detection Study*, NATO COOPERATIVE CYBER DEFENCE CENTRE OF EXCELLENCE 18, https://ccdcoe.org/sites/default/files/multimedia/pdf/Insider_Threat_Study_CCDCOE.pdf (last visited May 22, 2018).

information ("PHI") or to use it for their own personal gain.[69] Certain reports even go so far as to claim that "[t]he average cost of a data breach incurred by a non-healthcare related agency, per stolen record, is $158. For healthcare agencies the cost is an average of $355."[70] PHI is valuable because it can be used for many lucrative purposes, including creating fake insurance claims, allowing for the purchase and resale of medical equipment, or illegally gaining access to prescriptions, among others.[71]

Another, more specific type of cyber threat related to data breach is a so-called passive cyber-attack, which focuses on stealing PHI from implanted (or implantable) medical devices ("IMDs"), such as pacemakers or implanted cardioverter defibrillators, insulin pumps, and biosensors.[72] IMDs are particularly valuable to cybercriminals for two main reasons. First, IMDs contain sensitive healthcare data.[73] Second, they are usually connected to the computer networks of the healthcare organizations, so they are able to provide hackers with an entry into the network system of a health organization.[74] Therefore, it is important to provide adequate protection to IMDs against cyber-attacks.

C. DDoS Attacks

"Distributed Denial of Service," attacks, commonly known as DDoS attacks,[75] are a technique used by cybercriminals to overwhelm a network so that it becomes inoperable.[76] Given the interconnectedness of health systems in the United States, DDoS attacks cause significant problems for healthcare providers.[77] Because it is almost impossible to detect a DDoS attack, DDoS is a relatively simple way for cybercriminals to infiltrate a specific network

[69] *Id.* at 15–17 (providing a discussion of malicious insiders' motivations).

[70] *Data Breaches: In the Healthcare Sector*, CTR FOR INTERNET SECURITY, https://www.cisecurity.org/data-breaches-in-the-healthcare-sector/ (last visited May 22, 2018).

[71] *Id.* at 1 (indicating that PHI can also be used to file fraudulent tax returns, open credit accounts, obtain official government-issued documents such as passports or driver's licenses, create new identities. It is especially important to realize that unlike social security numbers, PHI never expires.).

[72] John G. Browning & Shawn Tuma, *If Your Heart Skips a Beat, It May Have Been Hacked: Cybersecurity Concerns with Implanted Medical Devices,* 67 S. C. L. REV. 637, 654 (2016).

[73] *Id.* at 657.

[74] *Id.*

[75] *DDoS Attacks: In the Healthcare Sector*, CTR FOR INTERNET SECURITY, https://www.cisecurity.org/ddos-attacks-in-the-healthcare-sector/ (last visited May 22, 2018).

[76] *Id.*

[77] *Id.*

and to map it.[78] Network mapping is usually defined as a process used to "discover and visualize physical and virtual network connectivity via a group of interrelated tasks that facilitate the creation of a network map, including flow charts, network diagrams, topology detection and device inventories. It is geared toward the creation of visual aids and materials that can be used for a broad array of purposes, especially network maintenance."[79] In addition, DDoS is often used as a predecessor for other types of cyber-attacks, such as ransomware.[80] To provide proper patient care, providers need full access to the certain healthcare organization's network.[81] The motives for the attacks can be quite diametrical, and may include opportunism, or social, political, ideological or financial causes related to a situation that angers the cyber-attack actors.[82]

One example of a recent DDoS attack within the healthcare industry is the 2014 DDoS attack on Boston Children's Hospital ("BCH").[83] In 2014, a group of hackers targeted BCH after the hospital recommended to state law enforcement that custody be withdrawn from a 15-year-old patient's parents after diagnosing her with "medical child abuse"; Massachusetts law enforcement accordingly responded by admitting the patient as a ward of the state.[84] Prior to making their recommendation, BCH physicians determined that the child's ailment was actually a psychological disorder and that her parents were pushing for unnecessary treatments.[85] The custody debate put BCH in the midst of this controversial case, and the members of the cyber hacking group Anonymous viewed BCH's actions as a breach of the patient's

[78] CORERO & GTT DDOS TRENDS REPORT, CORERO GTT 1, 6 (2017), https://www.gtt.net/wp-content/uploads/2017/11/Corero-GTT-DDoS-Trend-Report.pdf.

[79] *Network Mapping,* TECHOPEDIA, *https*://www.techopedia.com/definition/29783/network-mapping (last visited May 22, 2018).

[80] *DDoS Attacks: In the Healthcare Sector*, *supra* note 75.

[81] *Id.*

[82] Tim Casey, *Understanding Cyberthreat Motivations to Improve Defense,* WHITE PAPER, INTEL SECURITY AND PRIVACY OFFICE (Feb. 2015), https://lists.oasis-open.org/archives/cti/201607/msg00044/Intel_Corp_Threat_Agent_Motivations_Feb2015.pdf.

[83] *Anyone is a Target: DoS Attack Case Analysis on Boston Children's Hospital*, RADWARE (2014), file:///Users/laurenbatterham/Downloads/Radware_Boston_Childrens_Hospital_Case_Study%20(1).pdf.

[84] Mike Miliard, *FBI Arrests Massachusetts Man for Anonymous 2014 Cyberattack on Boston Children's Hospital*, HEALTH IT NEWS (Feb. 19, 2016 10:41 AM), http://www.healthcareitnews.com/news/fbi-arrests-massachusetts-man-anonymous-2014-cyberattack-boston-childrens-hospital; *See also* David Kushner, *The Hacker Who Cared Too Much*, ROLLINGSTONE (June 29, 2017), https://www.rollingstone.com/culture/features/how-a-crusade-to-save-children-landed-a-hacker-in-prison-w489735 (providing a narrative to the circumstances surrounding the DDoS attack).

[85] *Id.*

basic rights.[86] Correspondingly, Anonymous took action by conducting DDoS attacks against the hospital's network, which resulted in a loss of Internet access for almost a week.[87] Patients and staff were unable to use online accounts to check appointments, test results, and other case information.[88] In the aftermath, the hospital spent more than $300,000 to compensate the damage from this attack.[89] Based on this example, it can be inferred that the damage caused by such attacks is severe. It is therefore important for the healthcare sector to continue developing and improving protection software, as well as continuing to invest in staff member training.

D. Insider Threats

One of the major risks within health care organizations is the risk of victimization by insiders.[90] This risk often results from its unforeseen occurrence in the organization, which results in negligent treatment of its security estimations.[91] Generally, an insider or insider threat may be defined as "the potential for an individual who has or had authorized access to an organization's assets to use their access, either maliciously or unintentionally, to act in a way that could negatively affect the organization."[92]

Insiders pose a particular threat because of the legitimate access they have to an organization's system, with knowledge of its vulnerabilities or the opportunity to obtain that knowledge.[93] For instance, in 2016, sixty-eight percent of all network cyber-attacks on healthcare organizations throughout the world were carried out by insiders.[94] According to the National Cybersecurity and Communications Integration Center's Report, individuals that exhibit certain characteristics (such as introversion, greed or financial

[86] Miliard, *supra* note 84. The FBI managed to arrest members of this hacking group.

[87] *Id.*

[88] *DDoS Attacks: In the Healthcare Sector, supra* note 75.

[89] *Id.*

[90] *Combating the Insider Threat,* NAT'L CYBERSECURITY AND COMMUNICATIONS INTEGRATION CENTER (May 2, 2014), https://www.us-cert.gov/sites/default/files/publications/Combating%20the%20Insider%20Threat_0.pdf. For the purpose of this article, the term *insider* is used in a sense of a current or former employee, contractor, or other business partner who has or had authorized access to organization's network system.

[91] *Healthcare Data Breaches 'Mostly Caused by Insiders'*, DATEX (Feb. 25, 2017), https://www.datex.ca/blog/healthcare-data-breaches-mostly-caused-by-insiders.

[92] Daniel Costa, *CERT Definition of 'Insider Threat' – Updated*, CARNEGIE MELLON UNIV., SOFTWARE ENGINEERING INST.: INSIDER THREAT BLOG (Mar. 7, 2017), https://insights.sei.cmu.edu/insider-threat/2017/03/cert-definition-of-insider-threat—-updated.html.

[93] *Healthcare Data Breaches 'Mostly Caused by Insiders', supra* note 91.

[94] *Id.*

need, ethical flexibility, narcissism, intolerance to criticism, lack of empathy etc.) are more likely to carry out insider attacks.[95] It is therefore important for the healthcare sector to establish more efficient ways of screening employees through frequent psychological tests.

Insider threats come in two possible forms. The first is the malicious insider, where there is an insider *attack*.[96] A malicious insider is an insider who is "a current or former employee, contractor, or other business partner who has or had authorized access to an organization's network, system, or data and intentionally misused that access to negatively affect the confidentiality, integrity, or availability of the organization's information or information systems."[97] In 2016, malicious insiders caused at least one third of the insider incidents.[98] One such case recently occurred in Texas at the Carrell Clinic Hospital, where a hospital employee built a botnet (botnet is a string of connected computers coordinated together to perform a task)[99] and subsequently used the hospital network to attack rival hacking groups.[100] The employee was discovered after he posted a YouTube clip of himself staging an infiltration of the hospital network.[101] The video clearly shows the hospital's night security guard, later identified as Jesse William McGraw, aka "Ghost Exodus," the former leader of an anarchistic hacking group called the Electronic Tribulation Army, using a specific key (a cyber key as a smart key used as a gatekeeper for the hospital's network *system*) to infiltrate the

[95] *Combating the Insider Threat, supra* note 90, at 1.

[96] *Id.* at 1.

[97] *Id.*

[98] *Insider Threats as the Main Security Threat in 2017,* TRIP WIRE (Apr. 11, 2017), https://www.tripwire.com/state-of-security/security-data-protection/insider-threats-main-security-threat-2017/.

[99] *Malware 101: What is a Botnet?*, SYMANTEC CORPORATION (2017), https://us.norton.com/internetsecurity-malware-what-is-a-botnet.html; *Botnet,* DDOSPEDIA (2018), https://security.radware.com/ddos-knowledge-center/ddospedia/botnet/. Botnet might be legal, but in many cases it is a collection of compromised computers often referred to as "zombies" infected with malware that allows an attacker to control them. Botnet owners or "herders" are able to control the machines in their botnet by means of a covert channel such as IRC (Internet Relay Chat), issuing commands to perform malicious activities such as distributed denial-of-service (DDoS) attacks, sending of spam mail, and information theft.

[100] Press Release, Federal Bureau of Investigation, Arlington Security Guard Arrested on Federal Charges for Hacking into Hospital's Computer System (June 30, 2009), https://archives.fbi.gov/archives/dallas/press-releases/2009/dl063009.htm (on file with Federal Bureau of Investigation, Dallas Division); *see also* Kevin Poulsen, *Leader of Hacker Gang Sentenced To 9 Years for Hospital Malware,* WIRED (Mar. 18, 2011), https://www.wired.com/2011/03/ghostexodus-2/.

[101] *Id.*; Robert Wilonsky, *Hacker Known as "GhostExodus" Sentenced to More Than Nine Years in Federal Prison,* DALLAS OBSERVER (Mar. 18, 2011), http://www.dallasobserver.com/news/hacker-known-as-ghostexodus-sentenced-to-more-than-nine-years-in-federal-prison-7145501.

hospital.[102] The investigation revealed that McGraw infected dozens of machines that contained sensitive patient records with malware, and installed a backdoor in the heating, ventilation, and air conditioning unit, which, if failed, would cause damage to drugs and medicines and affect hospital patients during the hot Texas summer.[103] McGraw pled guilty to computer tampering charges and was sentenced to 9 years and 2 months in prison.[104] In addition, he was ordered to pay $31,881 in restitution and serve three years of supervised release following his prison term.[105]

The second type of insider threat is from inadvertent insiders, whose reckless acts enable intruders to gain access to PHI.[106] One of the most frequent forms of inadvertent insider attacks is when an insider loses an unencrypted password-protected laptop.[107] It is unsurprising that the rate of such reported loss in the healthcare sector is much higher than in other sectors.[108] Namely, the healthcare sector invests less funds in IT education of employees than other sectors targeted by cyber criminals.[109] Recently, there was a report of personal information of children vaccinated at Chinese hospitals being illegally obtained, partly thanks to the recklessness of insiders in misplacing their laptops.[110] This attack compromised the personal information of over 200,000 children in East China's Shandong Province of Jinan, including cellphone numbers and home addresses.[111] These data could

[102] Poulsen, *supra* note 100; *See also Former Security Guard, Who Hacked Into Hospital's Computer System, Is Sentenced To 110 Months In Federal Prison*, U.S. Department of Justice (Mar. 18, 2011), https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2012/03/15/mcgrawSent.pdf. For a detailed account of the YouTube video, see Press Release, *supra* note 100.

[103] Poulsen, *supra* note 100.

[104] Former Security Guard, Who Hacked Into Hospital's Computer System, is Sentenced to 10 Months in Federal Prison, Dep't of Justice (Mar. 18, 2011), https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2012/03/15/mcgrawSent.pdf.

[105] *Id.*

[106] *The Billion Dollar Lost Laptop Problem,* Intelligence in Software, http://www.intelligenceinsoftware.com/it_software_strategy/lost_laptop/index.php (last visited May 22, 2018) (For the purpose of this paper, an unintentional insider threat is a current or former employee, contractor, or business partner who has or had authorized access to an organization's network, system, or data and who, through action or inaction without malicious intent, causes harm or substantially increases the probability of future serious harm to the confidentiality, integrity, or availability of the organization's information or information systems.); *see also* Costa, *supra* note 92.

[107] *The Billion Dollar Lost Laptop Problem*, *supra* note 106.

[108] *Id.*

[109] *Id.*

[110] L. Ruohan, *Info of 200,000 Babies Leaked, Causes Panic Among Parents,* Global Times (Apr. 8, 2016), globaltimes.cn/content/977702.shtml.

[111] *Id.*

be used by organized criminal groups for baby-kidnapping for human trafficking purposes.[112] This example illustrates that China has the same problem as the U.S. – a lack of adequate supervision on the protection of personal information in healthcare sector.

One reason for such a high rate of incidents caused by careless insiders is the lack of adequate security education.[113] One 2016 report identified employees in healthcare systems as one of the lowest performing groups on basic cybersecurity evaluations, such as safe password practices.[114] The best way to prevent an insider's threat is to train employees on how to recognize and report the insider threat. Therefore, it is worth considering prescribing mandatory insider threat awareness training to employees before being granted access to classified information. Such training would involve both methods and training on how to avoid, report, and prevent such attacks. In addition, employers should establish and maintain a record of all cleared employees who have completed the training.

E. Computer Fraud

Computer fraud is the oldest and one of the most frequent forms of cybercrime.[115] Due to the global nature of the Internet, the number of computer frauds is in constant growth and causes large material consequences to the victims.[116] Therefore, this form of cybercrime is often featured in international conventions on cybercrime and regulatory instruments; in addition, it has also become a part of criminal codes in many countries in the last couple of years, especially within the EU.[117] The terms "computer fraud" or "cyber fraud" are usually understood in two ways: direct and indirect.[118] By *direct* computer fraud, one implies deceitfulness of the person using a computer system as a medium.[119] Here, the person is the

[112] *Id.*

[113] *Cyber Security Awareness Report from Wombat Security Reveals Knowledge Gaps that Pose Major Enterprise End-User Security Risks,* CISION PR NEWSWIRE (Sept. 1, 2016), https://www.prnewswire.com/news-releases/cyber-security-awareness-report-from-wombat-security-reveals-knowledge-gaps-that-pose-major-enterprise-end-user-security-risks-300321366.html.

[114] *Id.*

[115] *A Brief History of Cybercrime*, WAVEFRONT, (2013), http://www.wavefrontcg.com/A_Brief_History_of_Cybercrime.html.

[116] *Growth in Cyber Fraud Attacks Outpacing Growth of Transactions: Report,* SECURITY WEEK (2017), https://www.securityweek.com/growth-cyber-fraud-attacks-outpacing-growth-transactions-report.

[117] *Id.*

[118] Miha Šepec, *Slovenian Criminal Code and Modern Criminal Law Approach to Computer-Related Fraud,* 6 INT. J. OF CYBER CRIMINOLOGY 984, 986 (2012).

[119] *Id.*

object of fraud.[120] *Indirect* computer fraud, on the other hand, implies that the hacker is deceiving the computer system.[121] In that case, it is the system itself, rather than the human being that is the object of fraud.[122]

One of the most frequent forms of computer fraud is carried out via e-mail.[123] Estimates indicate that an Internet user who holds an e-mail address has received at least one e-mail asking for data about their bank account, social security number, or other personal data.[124] This criminal offense is usually connected with more than one state, which causes problems with jurisdiction and *ius puniendi*.[125] In literature, this type of fraud is also known by the name of "*Nigerian scam*" or "*Scam 419,*" and is referred to by the Federal Bureau of Investigation ("FBI") as the "*Billion Dollar Scam*."[126] In this type of scam, a hacker sends an e-mail with a false promise that the user will receive a certain amount of money if he or she gives the hacker his or her bank account or social security number.[127] The data is then used illegally.[128] While it sounds naive, it is a very lucrative business for hackers since one person in 10,000 sends the required data back.[129]

F. Human malware

While it now seems like science fiction, there is a real possibility that humans could be infected with malware in the near future.[130] Presently, hackers are able to access IMDs in order to gain valuable data or to enter the network systems of health organizations.[131] However, some scientists claim that, by accessing IMDs, hackers are also able to cause physical harm to the human body.[132] It is scientifically proven that it is possible for a capable hacker to break into a human implant and input a virus that will cause the implant to stop running properly.[133] Indirectly, this could cause deterioration of the disease or even death.[134] In such a case, it is questionable whether the

[120] *Id.*
[121] *Id.*
[122] *Id.*
[123] *Id.* at 988.
[124] *Id.*
[125] *See infra*, Part II.
[126] Elina I. Hartikainen, THE NIGERIAN SCAM: EASY MONEY ON THE INTERNET, BUT FOR WHOM? 1 (Univ. of Chicago 2006); FEDERAL BUREAU OF INVESTIGATION, *The 5 Billion Dollar Scam* (May 4, 2017), https://www.ic3.gov/media/2017/170504.aspx.
[127] Hartikainen, *supra* note 126.
[128] *Id.*
[129] Šepec, *supra* note 118, at 988.
[130] Browning & Tuma, *supra* note 72, at 657.
[131] *Id.* at 657.
[132] *Id.* at 638.
[133] *Id.* at 644.
[134] *Id.* at 647.

hacker could be tried for murder due to the definition of the crime and causality among other factors.[135] Additionally, new research found it possible to spread computer viruses via wireless Internet routers,[136] resulting in infected wireless Internet routers that can pose serious, long-term health or life risks to implant patients, due to the possibility that any compromised wireless Internet network could be used to spread medical viruses to patients.[137]

II. Legal Issues

In general, due to its specific and virtual nature, cybercrime opens many unsolved legal issues.[138] These issues concern multiple branches of law, relating to substantive (e.g. sentencing and punishment, *actus reus* and *mens rea* etc.) and procedural aspects of law (e.g. conflict of jurisdictions), and evidence law.[139] It is likely that cybercrime will become more prevalent because it offers multiple advantages in comparison to traditional forms of crime.[140] Scholars point out that cyberspace provides the guarantee of anonymity, enables criminals to target thousands of victims at the same time, and lets automated systems carry out the actual illegal activities.[141] It is questionable whether traditional legal frameworks across the globe are sufficient to fight back.[142] There are four main problems as to why traditional criminal law is not able to respond adequately: 1) the quest for unique definition of particular cybercrimes, 2) the lack of adequate computer education of lawyers in this field, 3) the conflict of jurisdictions, and 4) the problems related to the virtual nature of evidence material.[143] The most important of the aforementioned reasons is the potential conflict of jurisdictions, which could be an aggravating factor each time international cyber-attacks occur.[144] This section will only focus on this issue, and is divided into two subsections. The first section will discuss the issues connected with jurisdiction. The second will address the differences between national substantive criminal laws and the need for harmonization.

[135] *Id.* at 670

[136] *See* e.g. Johnny Milliken, et al., *Detection and analysis of the Chameleon WiFi access point virus,* 2 EURASIP J. ON INFO. SEC. 1, 2 (2013).

[137] *Id.* at 7.

[138] *See* Urlich Sieber, et al., EUROPÄISCHES STRAFRECHT § 24, 1 (Baden-Baden: Nomos 2011).

[139] *Id.*

[140] *Id.*

[141] Brenner, *supra* note 3, at 194.

[142] Francesco Calderoni, *The European Framework on Cybercrime: Striving for an Effective Implementation*, 54 CRIME LAW SOC. CHANGE 339, 339 (2010).

[143] *Id.* at 340–41.

[144] *Id.* at 342.

A. Establishing Jurisdiction for Cybercrimes

Jurisdiction is a main assumption to start proceedings against the defendant who committed certain criminal act. Generally, jurisdiction is defined as a "government's general power to exercise authority over persons and things."[145] Criminal law predominantly establishes jurisdiction based on territorial nexus with the criminal offense, the perpetrator and the victim.[146] However, jurisdictional issues tend to be more complicated in situations with international elements.[147]

International elements exist in any cyber-attack that targets more than one country.[148] Such attacks are also known as "transnational" cybercrimes.[149] Transnational cybercrime exists if either perpetrators act from territories of different countries or their targets are situated in more than one country, or both.[150] The virtual character of transnational cybercrimes makes it possible for the crimes' consequences to affect several countries.[151] At the same time, it is difficult (if not impossible) to determine the location of the attacker, or more frequently, attackers.[152] By way of illustration, imagine a ransomware virus cyber-attack, committed by the organized group of hackers located in Nigeria, Ukraine and Serbia, against several hospitals in the United Kingdom, the United States, Australia, Canada and United Arab Emirates ("U.A.E."). This type of cyber-attack operation can have different consequences on jurisdiction.[153] First, jurisdiction could be completely lacking if none of the involved countries is able to assert jurisdiction.[154] Second, jurisdiction could exist, but at the same time, it could be impossible to assert due to the specific factual problems (e.g., problems with extradition of the perpetrator).[155] Third, the so-called *positive* conflict of jurisdictions could arise if more than one country claims their right to jurisdiction, or *negative* if none of them want to engage.[156] In combination, these factors and complications could eventually lead to the undesirable outcome of allowing the perpetrator to avoid criminal liability.[157] This legal gap enables organized cybercriminals to develop strategies and to intentionally operate from those

[145] *Jurisdiction,* Black's Law Dictionary (10th ed. 2014).

[146] Brenner, *supra* note 3, at 192.

[147] *Id.* at 194.

[148] *Id.*

[149] *Id.*

[150] *Id.* at 194–95.

[151] *Id.* at 194.

[152] *Id.*

[153] *Id.* at 190.

[154] *Id.*

[155] *Id.*

[156] *Id.* at 197.

[157] *Id.*

parts of the world that do not have adequate legal framework regarding criminal jurisdiction.[158]

How do we prevent such a scenario? International treaties dealing with the problem of jurisdiction add almost nothing essential to the solution. The Council of Europe's Convention on Cybercrime addresses the problem by proclaiming that if there is a positive conflict of jurisdictions, that "the Parties involved shall . . . consult. . . to determin[e] the most appropriate jurisdiction."[159] The United Nations Convention against Transnational Organized Crime contains an almost identical provision.[160] Different national systems approach this problem in various ways. States vary from expansive approaches, that allow jurisdictions to include the right of the state to prosecute even if the digital signal is only passing through their territory, to a narrower approach that always requires nexus with either the perpetrator, the victim, the actual place of the crime or occurrence of consequences.[161] The main difference between these two approaches is that the expansive approach enables more countries to establish jurisdiction.[162]

One solution would be to re-define the principle of "universal" jurisdiction so that it covers cases of contemporary cybercrimes with international elements, at least in cases with far-reaching consequences (see Table 1). The principle of universal jurisdiction was designed to give sovereignty to each state in the world, regardless of the existence of a nexus with its territory or citizenship of the perpetrator or the victim.[163] The purpose of such principle is to establish international solidarity between states and to prevent certain areas in the world from becoming shelters for international criminals.[164] The principle of universal jurisdiction in modern law has two interpretations: narrow and wide.[165] In a narrow sense, colloquially known as the "World's law" principle or in German as "Weltsrechtsprinzip", it refers to the right of each state to prosecute crimes against basic values of international community (e.g., war crimes, genocide, crimes against humanity etc.).[166] In a wide sense, universal jurisdiction applies to all criminal offenses of a certain

[158] *See generally id.*

[159] Convention on Cybercrime, art. 22, Nov. 23, 2001, E.T.S. 185., Article 22.

[160] United Nations Convention Against Transnational Organized Crime and the Protocols Thereto, Article 15, Nov. 15, 2000.

[161] Brenner, *supra* note 3, at 195.

[162] *Id.*

[163] Jake Ruelens, *Universal Jurisdiction: An Analysis from a Comparative and International Law Perspective. A Future of Universal Jurisdiction Over Serious Crimes Under International Law*, UNIVERSITY OF GHENT 1, 7 (2015) (unpublished masters thesis, University of Ghent) (on file with the University of Ghent Masters of Law Program).

[164] *Id.* at 30.

[165] *Id.* at 9.

[166] *Id.* at 7.

gravity.[167] In both cases, if the universal jurisdiction rule is applicable, the state can prosecute independently of the fact that the commission of the crime does not have any nexus with that concrete state.[168] However, the condition *sine qua non* is that the perpetrator is reachable; in other words: there is no possibility of *in absentia* trials.[169]

Table 1 shows the results of this research on eleven randomly selected countries, concerning the scope of universal jurisdiction and its applicability on potential cybercrime attacks against the healthcare organizations anywhere in the world. The research illustrates that only a minority of countries are able to prosecute cybercrimes based on universal jurisdiction, which *a contrario* means that all of them are suitable to become "shelters" for organized hacking groups.

Table 1: Applicability of Universal Jurisdiction Principles on Cybercrimes (An Overview of 11 Countries)[170]

State	**The scope of Universal Jurisdiction**	**Applicability to Cybercrimes**
Albania	International crimes and other crimes under special treaties	No
Armenia	Crimes provided in special treaties	No
Bulgaria	International crimes and other crimes under special treaties	No
Canada	International crimes	No
Croatia	International crimes and other crimes punishable by 5 years or more	Yes, but only for the most severe forms.
Czech Republic	All crimes that are regulated as criminal offenses in crimes where they were committed, if the perpetrator is present in CR	Yes.

[167] *Id.*

[168] *Id.* at 8.

[169] *Id.* at 10–11.

[170] For purposes of this article, the authors have conducted research of relevant universal jurisdictional provisions in criminal codes of enlisted countries. The results of the research is pooled toghether to create the table in order to achieve clarity.

Denmark	All crimes penalized under D. Law with prison sentence over one year	Yes, but only for the most severe forms.
Finland	All crimes penalized under F. Law with prison sentence over six months	Yes.
Macedonia	International crimes and other crimes punishable by 5 years or more	Yes, but only for the most severe forms.
Georgia	Crimes provided in special treaties	No
Ukraine	Crimes provided in special treaties	No

Finally, the international community should consider amending the jurisdiction of the International Criminal Court ("ICC") for cases of organized cybercrimes when their commission causes severe damage with global consequences. ICC is the first independent and permanent international tribunal, established with a purpose of prosecuting international crime that are difficult (or impossible) to prosecute before domestic courts and that could have global consequences.[171] The international community has interests that such crimes are prosecuted and their perpetrators are punished by the law.[172] Organized attacks on healthcare organizations, committed simultaneously against several hospitals in different countries (as it was the case in *WannaCry*) would surely constitute such a crime. That way, the international community would have an efficient way of overstepping the boundaries set by the lack of adequate universal jurisdiction rules in national systems of criminal law.

B. Harmonization of National Substantive Criminal Laws

Even if a state can assert jurisdiction, it is not in a position to actually try the perpetrator due to the lack of an adequate legal framework at the substantive level.[173] Namely, one of the basic principles of criminal and constitutional law is legality (also known as *nullum crimen sine lege, nulla*

[171] *Id.* at 21.

[172] *Id.*

[173] Iulia Crisan, *The Principles of Legality "Nullum Crimen, Nulla Poena Sine Lege" and their Role,* 5 EFFECTIUS 1, 3 (2010), http://effectius.com/yahoo_site_admin/assets/docs/The_principles_of_legality_nullum_crimen_nulla_poena_sine_lege_and_their_role__Iulia_Crisan_Issue5.16811416.pdf.

poena sine lege).[174] In countries that adopt civil law tradition (i.e., "continental" law systems), the principle of legality is the cornerstone of a defendant's rights when facing criminal charges.[175] As one of the most precious legacies of enlightenment philosophy, the *nullum crimen* principle requires the state not to prosecute if its legislative framework lacks clarity regarding the elements or penalty of a certain crime.[176] If certain behavior was not foreseen as a criminal offense *before* it was committed, a person could not be held liable for it.[177] If the court spots this kind of legislative "gap," it will not be authorized to fill it with analogy, otherwise it would breach this basic principle of criminal law, *nullum crimen sine lege stricta*.[178] For example, one cannot talk about the hypothetical crime of theft or robbery in a case where A and B forced C to "hand over" a virtual sword in an online computer game, in which the sword had a value of $800.[179] Those crimes are traditionally connected with the existence of a materialized object, which is not the case if one deals with a virtual sword.[180] Accordingly, to prosecute such virtual behaviors as a crime, certain states would have to have a specialized type of virtual theft or robbery.[181] The opposite solution would lead to the unarguable conclusion that the defendant's rights were breached, and it would offer him or her the basis for a claim against the state. The applicant could to address the European Court of Human Rights in Strasbourg and claim the breach of Article 7 of the Convention, that prohibits the retroactive criminalization of acts and omissions and proscribes that no person may be punished for an act that was not a criminal offense at the time of its commission.[182] Further, similar cases can be found in comparative practice.[183] The Belgian Constitutional Court established the breach of the principle of equality when a Belgian legislator incriminated cyber-stalking as a special offense, but at the same time predicted a higher sentence than for general crime of stalking.[184]

In some countries, criminal codes still do not incriminate offenses such as

[174] *Id.* at 2.

[175] *Id.*

[176] *Id.*

[177] *Id.*

[178] *Id.*

[179] *See* T. Weigend, *Section I – Criminal Law General Part– Information Society and Penal Law General report,* 84 REVENUE INTERNATIONAL DE DROIT PENAL 49, 56–57 (2013).

[180] *Id.*

[181] *Id.* at 64.

[182] Convention on Cybercrime, *supra* note 160, at Article 7.

[183] *See generally,* J. C. Schuhr, *Analogie und Verhaltensnorm im Computerstrafrecht, Am Beispiel der Datenveränderung (§ 303a StGB und Art. 4 Convention on Cybercrime)*, ZEITSCHRIFT FüR INTERNATIONALE STRAFRECHTSDOGMATIK 8–9 (2012).

[184] *Id.*

cyber fraud, cyber bulling, and ransomware.[185] Thus, it is necessary for the states to harmonize their criminal legislation with international standards. For example, Slovenian Criminal Code provisions regarding computer fraud are still not harmonized with the Convention on Cybercrime.[186] This, in turn, forces Slovenian Courts to fill in the gap with the forbidden analogy, as discussed *supra*.[187] In one such case, a perpetrator was convicted for (regular) theft for unauthorized access to a bank computer system when he used an ATM to enter the system and cause financial damage.[188] The High Court in Ljubljana rejected the idea of fraud since the latter, according to Slovenian law, can only be committed against a real person, and not against a computer system.[189] Resultantly, the High Court convicted the perpetrator for theft, and based the conviction on a broad interpretation of the term "breaking and entering."[190] In its opinion, the High Court stated that an ATM is nothing else but an official space of the bank, and that entering the ATM system is the same as entering the bank.[191] The Supreme Court of Slovenia affirmed that opinion in several other cases.[192] Similar jurisprudence also occurred in Slovenia's neighboring country of Croatia prior to amendments of the Croatian Criminal Code that introduced computer fraud as a self-standing criminal offense.[193] Although the above-mentioned cases do not refer to healthcare organizations as targets, they have illustrative value for this subject since they show the trouble that courts face when dealing with insufficient legislative frameworks.

Therefore, it is justified to conclude that the main assumption for the efficient struggle against cybercrime is a harmonization of incriminations regarding this conduct. There is a universal need for consensus on what should be criminalized and to what extent.[194] In addition, there are varying

[185] *See generally*, K. Lyons, et al., *Online Abuse: How Different Countries Deal with it,* THE GUARDIAN (Apr. 12, 2016, 2:04 PM), https://www.theguardian.com/technology/2016/apr/12/online-abuse-how-harrassment-revenge-pornography-different-countries-deal-with-it; Miguel Angel Mendoza, *Challenges and Implications of Cybersecurity Legislation*, WELIVESECURITY (Mar. 13, 2017, 2:00 PM), https://www.welivesecurity.com/2017/03/13/challenges-implications-cybersecurity-legislation/.

[186] Also known as the Budapest Convention. Šepec, *supra* note 118, at 987.

[187] *Id.* at 993.

[188] *Id.*

[189] *Id.* at 994.

[190] *Id.*

[191] *Id.*

[192] *Id.*

[193] *Id.*

[194] Sarah Summers, *EU Criminal Law and the Regulation of Information and Communication Technology*, 3 BERGEN J. OF CRIM. L. & CRIM. JUST. 48, 49 (2015).

degrees of understanding of the scope and the limits of cybercrimes.[195] Some types of activities are broadly recognized, but there are still several areas in which there is a lack of consensus. This issue exists at both the regional and supranational level.[196] It seems that there is certain reluctance towards criminal law, since it is broadly understood as *ultima ratio societas*.[197] The Council of Europe's Convention on Cybercrime in 2001 prescribes minimum incriminations that each member state should adopt to effectively face the problem of cybercrime.[198] Those crimes cover behaviors such as illegal access to a computer's data or network, interference in computer system, illegal interception of computer system or data, computer forgery and fraud.[199]

CLOSING REMARKS

There is no doubt that big data improved the healthcare industry in many ways. Faced with the unsustainable costs of underutilized data management, the industry has long looked for more efficient solutions. Therefore, it is unsurprising that healthcare systems in the U.S. and worldwide are rapidly adopting electronic healthcare records. However, there is another, darker and more dangerous side: this new process makes patients personal data facilely accessible. Healthcare databases contain massive amounts of private patient information,[200] some of which even contains financial background information (e.g., patients' social security numbers, data about payment of certain medical services, etc.). Taken together, all of these factors make the entire healthcare industry an attractive target for cybercriminals.

The intention of this Article was to provoke a discussion on an emerging, but not yet sufficiently recognized type of cybercrime that is targeted against healthcare organizations and the healthcare industry in general. This type of cybercrime has been steadily on the rise due to several factors including the increased vulnerability of healthcare sector and the very specific legal issues (jurisdictional problems and differences in legal regulation between different legal systems in the world) that aggravate efficient criminal proceedings. Above all, cybercrime is a very lucrative endeavor, since PHI has a higher black-market value than other types of data. Moreover, PHI has a permanent

[195] *Id.* at 50.

[196] *Id.* at 49.

[197] *Id.* at 54.

[198] Convention on Cybercrime, *supra* note 160, Art. 2–8.

[199] *Id.*

[200] Some legislations decide to provide additional protection to patients' privacy by enforcing specific laws. One example of good practice is Health Insurance Portability and Accountability Act of 1996 (or HIPAA), a United States legislation that provides data privacy and security provisions for safeguarding medical information.

character, is not time-limited by expiration dates, and it can be used for different purposes. The other reason for the growing popularity of the healthcare industry as a target among hackers and cyber gangs is the fact that health organizations (especially hospitals) are not yet up to date with modern standards of protection. Other industries have been targets of cyber-attacks for many years and have had enough time and energy to develop higher standards of protection. However, healthcare organizations have not yet had sufficient time and organizational skills to improve their security systems. The third reason for the growing trend of attacks in the healthcare industry is the basic nature of its activity: since healthcare organizations perform sensitive processes that often involve critically ill patients, they are unable to simply stop their activities. Thus, healthcare organizations are more willing to pay a ransom than other sectors. All these factors make the healthcare sector a more vulnerable target than the other sectors, which is why this problem should be one of the top priorities in further improvements and analysis in this sector.

The phenomenology of cyber-attacks is a living tissue, and it is constantly developing. Based on known attacks, this article described six possible modalities of cyber-attacks in health care, supported by examples from recent practice. These cyber-attacks cause great financial damage to their victims, can have a broad scope of other consequences, and due to their immaterial, virtual nature, are often difficult to trace and to prove. Criminal prosecutors who deal with this type of crime often face insurmountable obstacles in conflicts of jurisdiction, lack of adequate computer knowledge and infrastructure, and the absence of criminal legislation that would even criminalize different types of cybercrime. Therefore, this Article also focused on the legal dimension of the problem and suggested a minimum of the offenses, which every country should adopt as soon as possible. If this is accomplished, states can prevent themselves from becoming a safe zone for cybercriminals and hackers who misuse their capabilities.

While cybercrime and cyberterrorism are becoming one of the greatest threats in modern criminal law, there are still many questions that remain unanswered. We hope that this Article will inspire further legal debates on this very sensitive and practically important topic.