Asia Pacific Journal of Health Law & Ethics
Vol.11 No. 2, March 2018, pp.16-32

Data-Driven Healthcare and Cybercrime: A Threat We Are Not Aware Of?

Igor Vuletić *

Abstract

This paper deals with the problem of cybercrime as a rising threat to the healthcare sector. Security incidents involving different forms of cyberattacks are on the rise and are becoming one of the top security threats nowadays. The healthcare system is not an exception: moreover, it seems that it is one of the most vulnerable sectors for cyberattacks. Hackers prefer targeting healthcare organizations (especially hospitals) because they are more willing to pay the ransom to gain their crucial data back. Cyberattacks on hospitals paralyze their entire operational process and cause damage to both institutions and patients. A typical example is the recent attack on several U.S. hospitals, when one of the targeted hospitals paid around $17,000 USD in ransom for the decryption of their digital information. The purpose of this paper is to draw attention to scientific debates on this important aspect of Big Data in the healthcare system. The author describes the phenomenology of cyberattacks in healthcare and points to certain legal issues—such as conflict of jurisdictions, inadequate defining of criminal offences and the general lack of consensus on the catalog of incriminations—that can adequately respond to the needs of contemporary cybercrimes.

Keywords: Cybercrime, Hacking, Malware, Ransom, Blackmail, Jurisdiction, Omission, Inchoate Crimes, Criminal Offence

I. Introduction

There is no doubt that Big Data has improved the healthcare system in many ways. Faced with the unsustainable costs of underutilized data management, healthcare has long looked for solutions that are more efficient. In that sense, digitalization of the system was

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

welcomed as the best possible solution for "personalized assessment of patient's health care."[1] Therefore, it is not surprising that healthcare systems (in the United States, but also worldwide) are rapidly adopting electronic healthcare records.

However, this golden medal also has its other, darker side. While the emergence of a digitalized era of healthcare records has improved the level of care for patients and enabled patients to make informed decisions about their medical treatment, the truth is that this new process has also made their personal data much more accessible. That is where the problem starts: healthcare databases contain a great deal of private information on patients, some of which even contain financial background information (e.g., Social Security number, data about payment of certain medical services, etc.). This makes the entire system an interesting target for cybercriminals. According to the World Privacy Forum, the street cost of stolen medical information goes for around $50, and the average payment for medical identity theft is even ten times higher than for regular identity theft (personal medical data allegedly costs around $20,000 on the black market).[2] On the other hand, as was recently pointed out by EUROPOL, the healthcare sector is more vulnerable to cyberattacks than any other sector.[3] Several years back, the FBI warned about cybersecurity systems in healthcare being lax in comparison to other sectors.[4]

This paper aims to draw the attention of legal researchers and criminologists to this important problem. The potential threat of cyberattacks on the healthcare system represents a great danger not only for patients, but also for the entire system. Yet, the phenomenon of Big Data in healthcare has not been scientifically discussed from the perspective of criminal law and criminology, at least not in a comprehensive way. My intention here is to fill this gap and provoke further scientific and practical debates.

In this paper, I will analyze some of the most well-known past cyberattacks on healthcare systems in the world. For example, just recently several hospitals across the United States

---

[1] Nitesh V. Chawla & Darcy A. Davis, *Bringing Big Data to Personalized Healthcare: A Patient-Centered Framework,* 28 J. Gen. Intern. Med. (2013), at 660.

[2] *See Security Trends in the Healthcare Industry: Data Theft and Ransomware Plague Healthcare Organizations,* IBM https://www.ibm.com/security/data-breach/mss-security-threat-research, at 4 (last visited March 7, 2017).

[3] *See* European Cybercrime Center, https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3 (last visited March 7, 2017).

[4] Federal Bureau of Investigation, https://info.publicintelligence.net/FBI-PHI-FTP.pdf (last accessed March 7, 2017).

faced a simultaneous cyber strike on their databases when a special type of computer virus that led to the complete collapse and inaccessibility of relevant data struck those hospitals. Hospitals had no option but to pay several thousands of dollars to regain access to their networks and to continue normal functioning. Similar cyberattacks (also known as ransomware) were also registered in Europe. Based on such analysis, I will try to identify and define the patterns of these attacks and to establish a comprehensive phenomenology of cybercrimes against the healthcare system. I believe that a clear definition of phenomenology is very important for a better understanding of this type of cybercrime. However, there are still large differences between systems of criminal law in the world, which aggravate efficient struggles against cybercrime, as a type of crime with a strong international component. Therefore, I will suggest the minimum offences that, in my opinion, each country worldwide should criminalize and implement into their national criminal code.

II. Phenomenology of Cyberattacks in Healthcare

The healthcare data system is attractive for cybercriminals. Although it may sound strange in the world of modern technology, the fact is that the low level of basic cybersecurity of medical equipment and data systems found in healthcare organizations makes them an easy target for cyberattacks. Unlike financial and retail organizations, which have long been the targets of cyberattacks and which have had the opportunity to develop more sophisticated methods of protection, healthcare organizations have only recently become targets and have not yet had the time to develop adequate systems of protection, which would mitigate the risks of the attacks. In addition, hackers prefer targeting hospitals because they are more willing to pay a ransom for the decryption of their crucial data. Hospitals perform very sensitive types of activity and the potential damage caused by such attacks strikes not only the organization and their staff, but also patients. That is one of the reasons why the attackers are experiencing more success against hospitals than against victims in other sectors. There is also one additional reason for the growth rate of cyberattacks in healthcare: unlike other personal data that are limited by expiration dates, healthcare data lasts forever and can be used for numerous malicious activities such as identity theft, insurance and healthcare fraud,

fraudulent tax returns, and so on.[5] In any case, cyberattacks in healthcare have become a reality around the globe and healthcare organizations are being forced to learn the lessons quickly, since the number of attacks in the healthcare industry is growing rapidly.[6]

Motives for cyberattacks in the healthcare sector vary: from stealing patients' private data in order to gain financial benefit to the pure intent to create chaos. Cybercrime in this sector is a lucrative business, without any doubt. To illustrate the potential, if we consider the fact that the value of a stolen credit card in the underground market in the United States is around $1, and if the stolen card is sold as part of a full identity profile with health insurance credentials, then it can reach the price of $500.[7] Only in 2013, 44% of all identity thefts in the United States were reported from the healthcare sector. In addition, healthcare industry data breach costs are almost three times higher than in any other industry.[8]

The healthcare industry has been the target of different types of cyberattacks. These attacks range from ransomware that compromises the integrity of systems and the privacy of patients to computer fraud and internet fraud. While other industrial sectors experience these attacks as well, the nature of the healthcare industry is what makes these attacks even more dangerous for today's society. For healthcare, cyberattacks usually have consequences that go beyond just pure financial damage. For the purposes of this paper, I will discuss the potential forms of cyberattacks divided into six typical groups (or six types) of attacks: 1) ransomware; 2) data breaches; 3) DDoS attacks; 4) insider threats; 5) computer fraud in the healthcare sector; and 6) human malware.

1. Ransomware

One of the most frequent forms of cyberattacks in the healthcare sector is ransomware. Ransomware is a type of malware that infects systems and files, making them inaccessible

[5] Caleb Barlow, *Attackers Shift Sights from Retail to Health Care in 2015,* Security Intelligence https://securityintelligence.com/attackers-shift-sights-from-retail-to-health-care-in-2015/ (last accessed March 7, 2017),

[6] Cyberattacks on the healthcare system in the U.S. increased 63% in 2016. See Kelly Sheridan, *Major Cyberattacks on Healthcare Grew 63% in* 2016, http://www.darkreading.com/attacks-breaches/major-cyberattacks-on-healthcare-grew-63--in-2016/d/d-id/1327779 (last accessed April 7, 2017).

[7] *Id.*

[8] Michelle Alvarez, *The Year of the Health Care Industry Security Breach,* Security Intelligencehttps://securityintelligence.com/the-year-of-the-health-care-industry-security-breach/ (last accessed March 7, 2017).

until a certain amount of ransom is paid. Ransom is usually required in monetary form but it can also be paid in virtual currency, e.g. bitcoin. Just recently, in May 2017, a global ransomware attack named "WannaCry" infected over 230,000 computers in around 150 countries worldwide and ransom was asked to be paid in bitcoins. In the literature, ransomware is defined as "a type of malware that uses malicious codes to intrude the system before users notice it, to encrypt important files, to require money using encrypted files as a hostage, and to give monetary damages to users."[9] One can say that ransomware is a kind of virtual blackmail. Ransomware attacks are constantly increasing and some estimations say that they will continue to rise in the future.[10]

When this happens in the healthcare industry, it slows down all critical processes or even makes them completely dysfunctional. The targets of ransomware attacks are usually hospitals. When faced with an attack, hospitals must switch to old, conservative methods of data storing, which then slows down the medical process and expends funds that could have been allocated elsewhere. In 2016, multiple hospitals across the U.S. were under the strike of ransomware. In these cases, hackers managed to crack an out-of-date server and upload malware to the system. Hackers performed this action without any participation or interaction with the victims, which is unusual. For example, Hollywood Presbyterian Hospital in California was hit by a virus called "Locky." Locky then locked out the users, obstructing them from accessing files and x-rays. This caused a series of delays in patient care and eventually resulted in the hospital paying a $17,000 (or 40 bitcoin) ransom to regain access to their data. A similar incident happened at Ottawa Hospital, where four victims activated malware by clicking on a phishing e-mail that encrypted their computer system.[11]

The actus reus of ransomware usually includes a certain amount of contribution by the victim. The perpetrator counts on the victim's naivety. The victim usually activates malware

[9] Sanggeun Song, Bongjoon Kim & Sangjun Lee, *The Effective Ransomware Prevention Technique Using Process Monitoring on Android Platform,* Mobile Information System (2016), 1.

[10] Limor Kessem and Caleb Barlow, *Ransomware Report: Top Security Threat Expected to Continue Rising in 2017,* Security Intelligencehttp://securityintelligence.com/ransomware-top-security-threat-expected-to-continue-rising-in-2017 (last accessed May 7, 2017).

[11] Chris Sienko, *Ransomware Case Studies: Hollywood Presbyterian and The 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 accessed April 7, 2017). 04/07/2017.

in one of the following ways: by reading e-mails containing a malicious attachment, by clicking on a malicious link, or by viewing an advertisement containing malware.[12] All three described techniques are commonly known as "phishing", in the sense of "obtaining computer credentials from users through manipulation or deceit."[13] Once stolen, computer credentials are misused in a variety of ways: from stealing identities and selling them on the online black market to using them for different types of cyber fraud. They can also be recycled and used for further, improved cyberattacks.[14] What makes the defensive strategies more difficult is the fact that cybercriminals continue to develop new tactics and techniques of attacks, which in turn makes it even more difficult to detect and prevent them on time.[15] That is why it is recommended that hospitals and healthcare providers invest in additional funding for education and training of the users to recognize and avoid phishing.[16] Organizations that do not take the necessary steps to prevent the attacks can suffer extremely serious consequences due to disabling of access to their files and computer systems in general. Therefore, each health organization should properly secure its networks, systems, and patients by continuously maintaining and updating their defense system.

2. Data breaches

A data breach is perhaps the most widespread type of cyberattack in general.[17] It can be defined as 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."[18] This type of cybercrime activity is so prevalent that experts usually warn that

[12] For a more detailed analysis of technical aspects of ransomware, see e.g. Alexander A. Grebenkov & Elena O. Yakovleva, *The State of Modern Malicious Software: Foundations of Study on Cyber-Armaments,* 11 Intern. Journ. of Applied Eng. Research (2016), 6832 – 6834.

[13] Adam Wright, Skye Aaron & David W. Bates, *The Big Phish: Cyberattacks Against U.S. Healthcare Systems,* 31 J. Gen. Intern. Med. (2016), 1115.

[14] *Id.* at 1116.

[15] At this moment, there are eight known main types of malicious software weapons that vary in the amount of harm they can inflict. *See* Grebenkov & Yakovleva, *supra* note 13 at 6834.

[16] Wright, Aaron & Bates, *supra* note 14 at 1117.

[17] Barlow, *supra* note 6.

[18] Gina Stevens, *Data Security Breach Notification Laws,* Cong. Res. Serv. Report for Congress (April 10, 2012)

organizations should assume not that they may be victims, but that they have already been victimized by a data breach.[19] According to the Ponemon Institute and Verizon Data Breach Investigations Report, the health industry is in second place for the most number of data breaches per year.[20] Breaches can occur in many different forms, such as credential-stealing malware, lost laptops, and so on. The aim of cybercriminals is either to sell the personal health information (PHI) or use it for their own personal gain. As some reports claim, "the average cost of a data breach incurred by a non-healthcare related agency, per stolen record, is $158 and for healthcare agencies the cost is an average of $355."[21] PHI is valuable because it can be used for many lucrative purposes, such as creating fake insurance claims, allowing for the purchase and resale of medical equipment, illegally gaining access to prescriptions, etc.

One very specific type of cyber-threat related to data breaches is the passive cyberattack focused on stealing PHI from implanted (or implantable) medical devices (IMDs), such as pacemakers or implanted cardioverter defibrillators, insulin pumps, biosensors, etc. IMDs are valuable to cybercriminals for two main reasons. First, they contain healthcare data. Second, they are usually connected to computer networks of healthcare organizations and they are able to provide hackers an entry into the network system of the health organization.[22]

3. DDoS attacks

DDoS stands for "Distributed denial of service" and a DDoS attack is a technique used by cybercriminals with the purpose of overwhelming a network so that it becomes inoperable. This kind of attack causes serious problems for healthcare providers. They need proper access to the network or else they are not able to provide proper patient care. The motives for the attacks can be quite diametrical: from opportunistic or even accidental

https://fas.org/sgp/crs/misc/R42475.pdf (last accessed April 7, 2017).

[19] Rafal Los, *"Assume Breach" Is Not a Defeatist Point of View,* http://darkmatters.norsecorp.com/2017/07/04/assume-breach-is-not-a-defeatist-point-of.view/ (last accessed April 7, 2017).

[20] *See Verizon's Data Breach Investigations Report,* https://www.bluefin.com/bluefin-news/verizons-data-breach-investigations-report-look-big-picture-part-2/ (last accessed April 7, 2017).

[21] *Security Trends in the Healthcare Industry, supra* note 3.

[22] John G. Browning & Shawn Tuma, *If Your Heart Skips a Beat, It May Have Been Hacked: Cybersecurity Concerns with Implanted Medical Devices,* 67 South Carol. Law Rev. (2016), 657.

reasons, to social, political, ideological or financial causes related to a situation that angers the cyber threat actors.[23]

One example of a DDoS attack is the case of Boston Children's Hospital. In 2014, a group of hackers targeted Boston Children's Hospital after the hospital recommended their patient, a 14-year-old girl, be admitted as a ward of the state and that custody be withdrawn from her parents. The doctors believed the child's ailment was actually a psychological disorder and that her parents were pushing for unnecessary treatments. The custody debate put Boston Children's Hospital in the middle of this controversial case, and the members of this cyber hacking group viewed this as a breach of the girl's basic rights. They took action by conducting DDoS attacks against the hospital's network, which resulted in the loss of internet access for almost a week. Patients and staff were unable to use their online accounts to check appointments, test results, and other case information. In the aftermath, the hospital spent more than $300,000 to compensate the damage from this attack.[24]

4. Insider threat

One of the major risks within health organizations is the risk of victimization by insiders. This type of risk is often neglected in security estimations. However, insiders pose a threat because of the legitimate access they have to organization systems. In addition, they may have certain knowledge of vulnerabilities of the system, or the opportunity to obtain that knowledge. In 2016, 68% of all network attacks in healthcare worldwide were carried out by insiders. Insider threat has two possible forms. The first is the threat posed by a malicious insider. In such a case, one can speak about an insider "attack" in a literal sense. In 2016, malicious insiders caused one third of insider incidents.[25] One such case happened recently in Texas, where an employee of a Texas hospital built a botnet, using the hospital network,

[23] Tim Casey, *Understanding Cyber Threat Motivations to Improve Defense,* White Paper, Intel Security and Privacy Office, https://www.mcafee.com/us/resources/deflect-targeted-attacks/wp-understanding-cyberthreat-motivations-to-improve-defense.pdf (last accessed May 7, 2017).

[24] Ryan Grim, *Why I Knocked Boston Children's Hospital off The Internet: A Statement from Martin Gottesfeld,* Huffington Post (September 18, 2016), http://www.huffingtonpost.com/entry/why-i-knocked-boston-childrens-hospital-off-the-internet-a-statement-from-martin-gottesfeld_us_57df4995e4b08cb140966cd3.

[25] Li Rouhan, *Info of 200,000 Babies Leaked, Causes Panic among Parents,* Global Times (April 8, 2016), http://globaltimes.cn/content/977702.shtml (last accessed March 7, 2017).

to attack rival hacking groups. He was detected after he posted a clip of himself on YouTube staging an infiltration of the hospital network. The video clearly shows the hospital's night security guard (later identified as Jesse William McGraw, a.k.a. "Ghost Exodus," the former leader of an anarchistic hacking group called the Electronic Tribulation Army) using a specific key to infiltrate the hospital. The investigation revealed that McGraw infected dozens of machines that contained sensitive patient records with malware. Additionally, he installed a backdoor in the HVAC unit, which, if it failed, would have caused damage to drugs and medicines and affected hospital patients during the hot Texas summer. McGraw pled guilty to computer tampering charges and was sentenced to 9 years and 2 months in prison. In addition, he was ordered to pay $31,881 in restitution and serve three years of supervised release following his prison term.[26]

The second type of insider threat is threat by inadvertent insiders, whose reckless acts enable intruders to gain access to personal health information. One of the most frequent forms of such recklessness is the case of lost unencrypted password-protected laptops. It is symptomatic that the rate of such reported loss in the healthcare sector is much higher than in other sectors.[27] Just recently, there was a report of illegally obtained personal information of children vaccinated at Chinese hospitals. This data was obtained partly thanks to the recklessness of the insiders.[28] One of the reasons for such a high rate of incidents caused by careless insiders is the lack of adequate security education. One report issued in 2016 identified employees in the healthcare system as one of the lowest performing in terms of awareness of basic cybersecurity, such as safe password practices and similar methods.[29] The best way to prevent this kind of insider threat is to train employees on how to recognize and report an insider threat and every other type of threat they spot.

---

[26] Kevin Poulsen, *Leader of Hacker Gang Sentenced to 9 Years for Hospital Malware,* Wired (March 18, 2011), https://www.wired.com/2011/03/ghostexodus-2/ (last accessed April 7, 2017).

[27] See Ponemon Institute *The Billion Dollar Lost Laptop Problem,* http://intelligenceinsoftware.com/featur/feature/it_software_strategy/lost_laptop/index.html#.WG_OBH2WLmM (last accessed March 7, 2017).

[28] Li Rouhan, *supra* note 23.

[29] See Wombat Security, *Beyond the Phish 2016,* https://info.wombatsecurity.com/beyondthephish, (last accessed May 7, 2017).

5. Computer fraud

Computer fraud is the oldest and one of the most frequent forms of cybercrime. Thanks to the global coverage of the internet, the amount of cyber fraud committed constantly grows and causes large material consequences to the victims. Consequently, this form of cybercrime has become a part of several international conventions and other regulatory instruments, as well as criminal codes in many countries in the last couple of years, especially within the European Union. The term "computer fraud" or "cyber fraud" is usually understood in two ways. "Direct" computer fraud implies the deceitful action of a person using a computer system as a medium. In such case, the person is the object of fraud. "Indirect" computer fraud, on the other hand, implies that a hacker is deceiving the computer system. Therefore, in that case, it is not the person, but the system itself which is the object of fraud.[30]

One of the most frequent forms of computer fraud is fraud by e-mail. Every internet user who has an e-mail address has at least once received an e-mail requesting them to deliver data about a bank account, social security number, and similar information. This criminal offence is usually connected with more than one state, which causes problems with jurisdiction *and ius puniendi* (see next chapter). In the literature, this type of fraud is also known by the name "Nigerian scam," "Scam 419"[31] or "Billion Dollar Scam" as it is referred to by the Federal Bureau of Investigation (FBI).[32] What is characteristic for this type of scam is that a hacker sends an e-mail with a false promise that the user will receive a certain (large) amount of money if he or she gives their bank account or social security number. After receiving the data, the hacker then misuses this data for illegal activities. It may seem naïve, but in fact, it is a very lucrative business, since one person in 10,000 sends the required data back.[33] In 2015, a medical center in the United States reported that they received a request from a pharmacy to confirm a large order of prescription drugs worth over $500,000. The investigation proved that the order was fraudulent. The goal of the cybercriminals in this

[30] Miha Šepec, *Slovenian Criminal Code and Modern Criminal Law Approach to Computer-Related Fraud,* 6 Int. Journal of Cyber Criminology (2012), 986.

[31] Elina I. Hartikainen, *The Nigerian Scam: Easy Money on the Internet, but from Whom?* University of Chicago (2006), 1.

[32] *See* FBI, https://www.ic3.gov/media/2017/170504.aspx (last accessed May 7, 2017).

[33] Šepec, *supra* note 28 at 992.

case was to attempt to take out a large line of credit with the pharmacy to purchase drugs. The potential damage would have been around $500,000 in prescription drugs. This case confirmed the importance of staff education, since the employee (calling to confirm when there is a change on an account) properly followed standard protocols and prevented the attackers from completing the attack.

6. Human malware

Although it may seem like science fiction, there is a real possibility that in the near future humans could be infected with malware. I have already mentioned the fact that hackers are able to access IMDs in order to gain valuable data or to enter the network systems of health organizations. However, some scientists claim that, by accessing IMDs, hackers are also able to cause actual physical harm to the human body.[34] It has already been scientifically proven that it is possible for a capable hacker to break into a human implant, input a virus that will cause the implant to stop running properly, and that way indirectly cause deterioration of the disease or even death. In such case it is very questionable whether such hacker could be tried for murder due to problems with the definition of crime, causality, etc. (see next section). New research has also found it possible to spread computer viruses via Wi-Fi routers.[35] Infected Wi-Fi routers can pose a serious long-term health or life risk to implant patients. This basically means that in the near future any compromised Wi-Fi network could be used to spread medical viruses to patients.

III. Legal Dimension of the Problem: Insight from the Perspective of Criminal Law

Due to its specific, immaterial nature, cybercrime in general opens many unsolved issues from a legal point of view.[36] These issues concern multiple branches of law. Moreover, they

[34] Browning & Tuma, *supra* note 23 at 638.

[35] See e.g. Johnny Milliken, Valerio Selis & Alan Marshall, *Detection and Analysis of the Chameleon WiFi Access Point Virus,* EURASIP Journal on Information Security (2013), 1 – 14.

[36] *See* Urlich Sieber, in *Europäisches Strafrecht* (Urlich Sieber, Franz-Hermann Brüner, Helmut Satzger & Bernd

are related to both material and procedural aspects, as well as evidence law. In this paper, I will focus only on the criminal law dimension of the problem. It is very questionable whether traditional legal frameworks in many countries across the globe are sufficient to fight back. Cybercrime challenges the traditional concepts of criminal law in many ways. In particular, the literature usually marks four main problems to which traditional criminal law is not able to respond to adequately: the quest for the unique definition of particular cybercrimes, the lack of adequate computer education of lawyers in this field, the conflict of jurisdictions, and the virtual nature of evidence material.[37] In my opinion, there is also a fifth problem, which is also the most pressing one: the need for redefinition of traditional institutes of substantive criminal law (e.g. omissions, inchoate crimes, complicity, the principle of legality, etc.) and their adjustment to cybercrimes.

Perhaps the most important practical aspect of this subject is the potential conflict of jurisdictions, which could be an aggravating factor each time some cases of international cyberattacks occur. An international element exists in any cyberattack that targets more than one country in the world. The virtual character of such attacks makes it possible for the consequences to appear in several countries. At the same time, it is difficult (if not impossible) to determine where the attacker (or attackers, if there are more of them, which is often the case) is located. In these cases, it is difficult to establish ius puniendi and decide on relevant substantive criminal law, especially if the law of the state in which the consequences occurred does not have adequate incriminations in their criminal code. For example, in many countries in the world, criminal codes still do not incriminate offences such as cyber fraud, cyber bullying, ransomware, etc., and the only option is to run criminal proceedings by traditional incriminations, which is often insufficient to run a trial against perpetrator. Therefore, it is necessary for countries to harmonize their criminal legislation with international standards. As it will be presented later in this paper, international standards nowadays contain several new incriminations adjusted to cybercrime standards.

The same applies to certain core institutes of criminal law, which cannot simply be transposed into a cybercrime context without further adjustments. The traditional system of sanctions of criminal law is designed for traditional forms of crime, and they often do

---

Heintschel-Heinegg eds., 2011), § 24, 1.

[37] Francesco Calderoni, *The European Framework on Cybercrime: Striving for an Effective Implementation,* 54 Crime Law Soc. Change (2010), 340 – 341.

not suit the needs of modern types of crime.[38] Cybercrime challenges national legislators to consider new types of criminal sanctions, such as different security measures of confiscation of electronic devices and blocking internet access. In Belgium, for example, a court has the authority to disable access towards certain data or to order the internet provider to cancel certain web pages. In France and Turkey, legislation predicts certain measures for banning the internet use for suspicious persons for a certain period.[39] Croatian criminal law also envisages a security measure of prohibition of internet access for perpetrators of crimes connected with computer systems.[40] However, legislators need to be aware of the universal right to respect freedom of access to online information. This right is guaranteed by several international documents and it has been made concrete in the jurisprudence of the European Court of Human Rights in Strasbourg.[41]

The main assumption in the efficient struggle against cybercrime is the harmonization of incriminations regarding this type of crime. There is a universal need for consensus on what should be criminalized and to what extent.[42] There are varying degrees of understanding of the scope and limits of cybercrimes. 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 the regional and supranational level. It seems that there is a certain reluctance towards criminal law, since it is broadly understood as *ultima ratio societas*.[43] The lack of harmonization in this area could be a problem if one bears in mind the *nullum crimen sine lege stricta* principle that bans courts from applying traditional incriminations on cybercrime cases based

[38] For efficiency of prison sanctions for cybercrime see Catherine D. Marcum, George E. Higgins & Richard Tewksbury, *Doing Time for CyberCrime: An Examination of the Correlates of Sentence Length in the United States,* 5 Int. Journ. of Cyber Criminology (2011), 825 – 835.

[39] A more detailed comparative overview in Thomas Weigend, *Information Society and Penal Law: General Report,* XIXth International Congress of Penal Law Preparatory Colloquium, Verona, 2012, Section I – Criminal Law. General Part, 51, 65, 66.

[40] See Leo Cvitanović and Ivan Glavić, *Regarding the Issue of the Security Measure of Prohibition to Access the Internet,* 19 Croat. Annual for Crim. Law and Practice 2 (2012), 891 – 916.

[41] Gabriel Gillett, *A World Without Internet: A New Framework for Analyzing a Supervised Release Condition That Restricts Computer and Internet Access,* 79 Fordham L. Rev. 217 (2011), 254.

[42] Sarah Summers, *EU Criminal Law and the Regulation of Information and Communication Technology,* 3 Bergen Journal of Criminal Law and Criminal Justice 1 (2015), 49.

[43] *Id.* at 49 – 55.

on analogy. Therefore, I will try to contribute to this discussion by proposing a minimum standard of incrimination for every national system of criminal law in the world to adopt. In my opinion, it would be necessary for each state to incriminate at least the following behaviors: unauthorized access towards computer systems or networks; interference in the proper functioning of computer systems; causing damage to digital data and unauthorized interception of such data; computer forgery and computer fraud. Below, I will briefly explain the essence of each of these criminal offences.

1. Unauthorized access towards computer systems or networks

This type of incrimination covers the typical cases of illegal access towards computer systems and networks, also known as hacking. Hacking is a kind of virtual trespass.[44] Such incrimination is of essential importance for the effective struggle against cybercrime since it covers the cases of most preparatory acts for more dangerous attacks (e.g. cyber fraud, DDoS attacks, etc.). Therefore, it is important for each state to establish the authority to run investigations and take other repressive measures already at this early stage, while no serious consequences have yet occurred. Of course, each state has to decide about the exact scope of criminal law protection. Systems vary between "rigid" ones that criminalize just pure illegal access without any actual damage caused, and more "flexible" ones which criminalize such behavior only if it has caused certain damage. One can use Art. 2 of Council of Europe's Convention on Cybercrime (2001) as a role model.[45]

2. Interference in the proper functioning of computer systems and causing damage to digital data

This criminal offence is a type of computer sabotage. The essence (or *actus reus*) of this offence is that the hacker interferes with the computer system or network and distracts the

[44] Susan W. Brenner, *U.S. Cybercrime Law: Defining Offenses,* 6 Information System Frontiers 2 (2004), 116.

[45] Council of Europe, *Convention on Cybercrime* (2001), at Art. 2 ("Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system").

users in their usual functioning and communication. This could be done by different types of activities focused on damaging or destroying the data relevant for a certain system (e.g. a healthcare system). Again, the scope of criminalization varies, depending on the scope of the caused damage, criminalization of the attempt, and so on. An adequate prototype for incrimination of such behavior can be found in Art. 4 and 5 of the Convention on Cybercrime.[46]

3. Unauthorized interception of digital data

The main task of this incrimination is to prevent unauthorized interception and interference in communication within the computer system. This is a type of computer espionage which can also be used as a tool or preparation for some other, more dangerous forms of cyberattacks. Each state must decide whether it will just criminalize the interception or if it will ask for additional assumptions. Also, it is up to each state to decide whether it will criminalize the forms of negligence and attempted crimes. Art. 3 of the Convention on Cybercrime could be a good role model for this type of incrimination.[47]

4. Computer forgery and computer fraud

By criminalizing computer forgery and fraud, the legislator covers behaviors that could not otherwise be punished due to the *nullum crimen sine lege stricta* principle, since traditional crimes of forgery and fraud are usually connected with the material nature of

[46] *Id.* at Art. 4 ("Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right. A Party may reserve the right to require that the conduct described in paragraph 1 result in serious harm"); *Id.* at Art. 5 ("Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data").

[47] *Id.* at Art. 3 ("Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data. A Party may require that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system").

"papers" and other material objects. Therefore, each state should introduce this type of criminal offence. Computer forgery covers unauthorized manipulation by computer data that is valuable for legal operations with the purpose to use such data as if it were real. Computer fraud, on the other hand, covers manipulation of data or interference in the computer system with the purpose of causing damage or gaining illegal benefits from such activity. As a good role model for these incriminations, one can look at Art. 7 and 8 of the Convention on Cybercrime,[48] but also the legislation of certain American states, such as Georgia, Nevada or Virginia[49]

IV. Conclusion

In this paper, my intent was to open a discussion on an emerging but not yet sufficiently recognized type of cybercrime, one targeted against healthcare organizations and the healthcare system in general. This type of cybercrime has been steadily on the rise due to several factors. Above all, it is very lucrative since personal health information has a much higher black market value than other types of data. Moreover, PHI has a permanent character—it is not time-limited by expiry dates and it can be used for different purposes. The other reason for the growing popularity of the healthcare sector 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. Health 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 this sector is the basic nature of its activity: since health

[48] *Id.*at Art. 7 ("Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible. A Party may require an intent to defraud, or similar dishonest intent, before criminal liability attaches"); *Id.* at Art. 8 ("Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the causing of a loss of property to another person by: any input, alteration, deletion or suppression of computer data; any interference with the functioning of a computer system, with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person").

[49] Susan W. Brenner, *supra* note 42 at 129.

organizations are performing sensitive processes that often include very critically ill patients, they are not able to just simply stop their activities. That is why they are more willing to pay a ransom than organizations in other sectors. Other sectors have been targets of cyberattacks for many years now, so they have had enough time and energy to develop higher standards of protection.

The phenomenology of cyberattacks is a living tissue: it is constantly developing. Based on the known attacks to date, in this paper I have described six possible modalities of cyberattacks in healthcare, supported by appropriate examples from recent practice. These attacks usually cause great financial damage to their victims and can have a broad scope of other consequences. Due to its immaterial (virtual) nature, they are 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 all possible types of cybercrime. Therefore, in this paper I have also focused on the legal dimension of the problem and suggested a minimum of the offences involved that every country should adopt as soon as possible. In that way, states can prevent themselves from becoming a safe zone for cybercriminals and hackers who misuse their capabilities. Since cybercrime and cyberterrorism are becoming two of the greatest threats of modern criminal law yet, at the same time, there are many questions that remain unanswered, I hope that this paper will provoke further legal debates on this very sensitive and practically important topic.

Received: January 4, 2018

Revised: February 14, 2018

Accepted: March 2, 2018