M. V. Zhuravel,
Bachelor of Laws Yaroslav Mudryi National Law University, Ukraine, LL.M in International Corporate Governance and Financial Regulation, University of Warwick, United Kingdom

UDC 341
DOI 10.37749/2308-9636-2020-2(206)-2

To my teacher Mr Philip Rees with gratitude for his continued support over the years and his faith in me

INCREASING YOUR CYBERSECURITY AWARENESS: UNDERSTANDING CYBERCRIME AND FINDING WAYS TO FIGHT IT

«No person, organisation, or computer can ever be 100% secure. Someone with the patience, money and skill can break into even the most protected systems».

(Scott Shackelford, Associate Professor of Business Law and Ethics, Indiana University, USA[1]).

Dependency on global cyberspace is rapidly increasing nowadays. Virtual reality generates opportunities for enterprises, governments and individuals; however it also poses significant threats to security on different levels including the national level, whereby key state infrastructures can become a target of cyber attacks. This was seen during the Covid-19 pandemic when the healthcare system in a number of countries experienced cyber threats, which in the example of the Czech Republic, led to severe disruption of the medical processes in a hospital. Thus, cybercrime can cause detrimental effects not only to individuals or business entities, but also to a large group of stakeholders. Infinite cyberspace, the anonymous character of cyber attackers, advances in technology and a lack of cybersecurity measures in place — these all give cybercrime a sophisticated and aggressive nature and as a result, make us more vulnerable to it. This article will consider different categories of cybercrime, namely, crimes against the person; crimes against property, and crimes against the government, drawing examples from real life cases. This will be followed by an exploration of the methods which should be employed in the fight against cybercrime. In addition, the EU legislative framework will be considered as an example of legal measures against cybercrime.

Key words: *Internet, cyberspace, cybercrime, cyber attack, cyber threat, cybersecurity, ransomware, cyber terrorism, European Union legal framework, NIS Directive, ENISA, ways.*

[1] Scott Shackelford, 'Take these 5 critical steps to protect yourself from cybercrime' *Fast Company* (17 August 2019) <https://www.fastcompany.com/90391332/take-these-5-critical-steps-to-protect-yourself-from-cybercrime> accessed 28 March 2020.

I. Introduction

Once Jacques Ellul, a 20th century French philosopher and sociologist, said: «Modern technology has become a total phenomenon for civilization, the defining force of a new social order in which efficiency is no longer an option but a necessity imposed on all human activity».[2] Ellul's words have gained greater relevance at the present time, since we live in the epoch of global digitalisation which drives the world's economic progress, shapes the legal framework and establishes new trends of social behaviour. Cyberspace has become a major part of our reality. Whether it is registering a social media account, transferring money via online banking, making orders on giant platforms like Amazon[3] or Taobao[4], paying the bills online or chatting to a friend on an app, not to mention large commercial transactions or other highly valuable processes and operations that are being conducted by electronic means, we have entered into cyberspace, and have to deal with cyber law matters. The scope and dynamics of our online activities, the amount of personal information that we store or unintentionally leave online, all create a greater threat to our privacy which can be abused by criminals. Anyone who uses the internet can become a victim of different types of cybercrime. The Identity Theft Resource Centre (ITRC), a US non-profit organisation, established to support victims of identity crime, reported a 17% increase in data breach cases in 2019 compared to 2018, naming hacking as the leading culprit followed by «unauthorised access».[5] Hacking, indeed, is one of the earliest forms of cybercrime originating back to the 1960s and involving identity theft, fraud and breach of privacy.[6] According to the ITRC, the estimated global cost of cybercrime will reach 6 trillion US dollars by 2021.[7] Given the times we live in and the increasing number of cyber attacks, it is, therefore, important to develop cybersecurity awareness and equip oneself with knowledge to become alert to potential cyber threats. Firstly, definitions of cyber and cybercrime will be presented and three categories of cybercrime will be outlined. The malware case of Yahoo and ransomware attack on Norsk Hydro ASA will be discussed. Under the category of «crimes against the government» we shall look at the cyber threats posed to the healthcare system in the current pandemic. Other examples of cybercrimes will be briefly mentioned. Thirdly, ways to combat cybercrime will be explored and a conclusion, together with the author's view on the topic, will be drawn towards the end of the article.

II. What is cybercrime? Some examples of cybercrime in real-life cases

The expert Martin Libicki's definition of «cyber» entails «command and control of computers».[8] Following this, cyber attacks are «all efforts to disrupt, deny, degrade, distort, or destroy the information that they rely upon, store, process and generate».[9] According to several law

[2] Jacques Ellul, quotation taken from Goodreads <https://www.goodreads.com/quotes/1297716-modern-technology-has-become-a-total-phenomenon-for-civilization-the> accessed 21 March 2020.

[3] <https:www.amazon.com>.

[4] Taobao is an online shopping platform in China established in 2003 by the Alibaba Group <https://baohero.com/taobao> accessed 7 April 2020.

[5] Identity Theft Resource Center, Data Breach Report for 2019 <https://www.idtheftcenter.org/identity-theft-resource-centers-annual-end-of-year-data-breach-report-reveals-17-percent-increase-in-breaches-over-2018/> accessed 20 March 2020.

[6] Erika Hernandez, 'The 16 Most Common Types of Cybercrime Acts' *VoIP Shield* (14 February 2018) <https://www.voipshield.com/the-16-most-common-types-of-cybercrime-acts/> accessed 20 March 2020.

[7] Identity Theft Resource Center, op.cit.

[8] Martin Libicki cited in Andrew Futter, 'Is Trident safe from cyber attack?' 5 February 2016) *European Leadership Network* <https://www.europeanleadershipnetwork.org/report/is-trident-safe-from-cyber-attack/> accessed 23 March 2020.

[9] Ibid.

dictionaries, cybercrime is a «crime that takes place through the use of computers, computer technology or the Internet».[10] In the early stages of cyber criminal activity, these crimes were normally committed by lone individuals. Nowadays, however, when cybercrimes are on the rise, they can involve large criminal groups and enterprises. Cybercrimes can be grouped into different categories. The most easily-distinguished are the following three categories: crimes against people, crimes against property and crimes against the government.[11] We will approach these categories by examining one crime from each in a number of real life cases.

Crimes against people include cyber-bullying, cyber-harassment and stalking, distribution of child pornography and human trafficking, credit card fraud, online defamation (libel or slander), identity theft, and spoofing.[12]

Identity theft is defined by the US government as the act of stealing personal data for fraudulent purposes, such as for financial or medical gain.[13] These actions can affect personal credit status and will require financial and time resources to restore one's reputation.[14] Perhaps the most infamous case of personal identity theft to date was the Yahoo case occurring from 2013 to 2016 when 3 billion user accounts were hacked and names of people together with their phone numbers, emails and passwords were stolen.[15] What went so fundamentally wrong that led to such a failure? Yahoo had been planning to move away from a discredited technology known as MD5, used to encrypt data.[16] However, hackers pre-empted this by launching an attack on Yahoo accounts and taking advantage of the weakness of MD5. It was claimed that, in fact, security specialists had been aware of the pitfalls of MD5 for over ten years and that MD5 was more vulnerable than other algorithms.[17] Yet it was five years before Yahoo decided to change the security encryption after Carnegie Mellon University's Software Engineering Institute officially warned security experts that MD5 «should be considered cryptographically broken and unsuitable for further use».[18] Although Yahoo contested the claim that the company did not spend sufficient funds on security, former security employees reported that they were not listened to when they requested the company to improve cryptography protections, on the grounds that these would be costly, complicated or were simply low in priority.[19] These major reasons were claimed to be behind the massive cyber data breach, which cost Yahoo loss of reputation as well as substantial financial losses. A class-action lawsuit was allowed by a US Court ruling in August 2017, which stated that Yahoo must face litigation from users who suffered breach of their personal information because all plaintiffs had an «alleged risk of future identity theft» and «loss of value of their personal identification information» as

[10] Thelaw.com: Law Dictionary & Black's Law Dictionary 2nd Ed. <https://dictionary.thelaw.com/cybercrime/> accessed 7 April 2020.

[11] Mary Clare Novak, 'Let's Talk About Cyber Law: Crime, Security, and Legislation' *Learning Hub* (20 November 2019) <https://learn.g2.com/cyber-law> accessed 20 March 2020.

[12] Ibid.

[13] The United States Government website, '*Identity Theft*', <https://www.usa.gov/identity-theft> accessed 20 March 2020.

[14] Ibid.

[15] Jonathan Stempel, Jim Finkle, 'Yahoo says all three billion accounts hacked in 2012 data theft' *Reuters* (3 October 2017) <https://www.reuters.com/article/us-yahoo-cyber/yahoo-says-all-three-billion-accounts-hacked-in-2013-data-theft-idUSKCN1C82O1> accessed 21 March 2020.

[16] Joseph Men, Jim Finkle et al., 'Yahoo security problems a story of too little, too late' *Reuters* (18 December 2016) <https://www.reuters.com/article/us-yahoo-cyber-insight/yahoo-security-problems-a-story-of-too-little-too-late-idUSKBN1470WT> accessed 1 April 2020.

[17] Ibid.

[18] Ibid.

[19] Ibid.

well as the expenses they occurred due to the necessity to protect themselves from identity theft.[20] The litigation process is still ongoing and the final hearing is scheduled for April 2020.[21] Under the proposed class action settlement, the defendants, Yahoo and Aabaco Small Business LLC, promised to pay $117,500,000 for a Settlement Fund which in turn will provide a minimum of two years of Credit Monitoring Services or cash payments to Yahoo users[22].

From this case it can be seen how important it is to have effective communication between managers and their departments. Taking into consideration the advice of IT specialists on updating company cybersecurity, especially for a digital company, is key. Investing a sufficient amount of funds into cybersecurity can save the company from disaster and, conversely, skimping on cybersecurity can lead to massive financial losses, expensive and lengthy litigation, damaged systems and loss of time in recovering a company's good name.

Crimes against property include unauthorised computer trespassing through cyberspace, transmission of a virus/malware including ransomware, distributed denial of service attacks, cyber-squatting, hacking, computer vandalism, and violations of intellectual property rights.[23]

Let us take ransomware as an example. According to Norton, a provider of security against viruses and the like, ransomware is a type of malware the aim of which is to «lock and encrypt a victim's computer or device data, then demand a ransom to restore access.»[24] Whilst the concept looks fairly simple, the consequences can be drastic. The data remains on the victim's computer/device; however, the attacker keeps it as hostage and sets a time limit for the victim to pay the ransom for the decryption tool in return. The data is encrypted with malware which does not allow the victim to obtain access to it.[25] An example of ransomware is well illustrated in the battle of Norsk Hydro ASA (Hydro) against LockerGoga ransomware.

In 2019 a number of manufacturing firms were targeted by ransomware known as LockerGoga.[26] This program works by encrypting files stored on desktops, laptops and servers and changes the user's passwords. It can delete files, encrypt a specific file or any type of files. Furthermore, it prevents the infected system from recovery after it is restarted.[27] Like other dangerous forms of ransomware, LockerGoga can shut down physical equipment, causing disruption to business operations. According to Business Insider, files of the firms which became victims of LockerGoga attacks were encrypted and the only file which was available was named «ReadMe» and included the following message:

[20] Hannah Kuchler, 'Yahoo says 2013 cyber breach affected all 3bn accounts' *Financial Times* (4 October 2017) <https://www.ft.com/content/9412c2b0-a87c-11e7-93c5-648314d2c72c> accessed 7 April 2020.

[21] Yahoo! Inc. Customer Data Security Breach Litigation Settlement <https://yahoodatabreachsettlement.com> accessed 27 March 2020.

[22] Ibid.

[23] Mary Clare Novak, op.cit.

[24] Alison Grace Johansen 'What is ransomware and how to help prevent ransomware attacks' NortonLifeLock <https://us.norton.com/internetsecurity-malware-ransomware-5-dos-and-donts.html> accessed 28 March 2020.

[25] Ibid.

[26] Aaron Holmes, 'The Biggest hacks of 2019 so far' *Business Insider* (11 September 2019) <https://www.businessinsider.com/biggest-hacks-and-data-breaches-of-2019-capital-one-whatsapp-iphone-2019-9> accessed 10 April 2020.

[27] Trend Micro Team, 'What You Need to Know About the LockerGoga Ransomware' (20 March 2019) <https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/what-you-need-to-know-about-the-lockergoga-ransomware> accessed 25 March 2020.

«Greetings! There was a significant flaw in the security system of your company. You should be thankful that the flaw was exploited by serious people and not some rookies. They would have damaged all of your data by mistake or for fun. [...] We exclusively have decryption software for your situation. [...] The payment has to be made in Bitcoins. The final price depends on how fast you contact us. As soon as we receive the payment you will get the decryption tool and instructions on how to improve your system security.»[28] This is an example of an aggressive form of malware as it aims to rob the company, damaging its network, and giving no opportunity for self-recovery. Meanwhile, it causes costly disruptions to business processes, which can heavily impact the short-term business outlook, leaving the company to deal with its drastic consequences.

One of the companies that fell victim to LockerGoga's attack was Norsk Hydro ASA (Hydro), a famous multinational manufacturer with 35,000 employees and a history going back 100 years.[29] The cyber attack disabled the company's network, IT infrastructure and their website, which was a disastrous situation for a conglomerate like Hydro. How did the company manage to overcome the challenge? The company reacted quickly and firmly. They took a very brave step and acted openly and honestly with the outside world by disclosing the details of the incident, not trying to cover up any truth. The company let the stock markets know that they had started operating on a manual basis. For internal communication, employees used Office365 on their tablets and mobile phones, and for external communication they relied on their Facebook page and on a temporary website named Azure.[30] In addition, Hydro shared information about the incident in daily webcasts, managing questions from the general public well. They cooperated with national cybercrime bodies, police and industry experts. The company refused to pay any ransom. Instead they put their efforts together to recover their back-up data. Furthermore, they uploaded videos of their recovery processes on the Internet, which showed how different teams and employees managed daily operations and stayed in an optimistic mood. In contrast to what one might think, the company's share price increased.[31] The battle for recovery cost Hydro an estimated £60 million — considerably more than the price that they would have paid to the criminals for the decryption tool.[32] Some critics may argue that Hydro should have simply bought the decryption tool, which would have saved money and a great deal of time used for recovery. However, Hydro's decision not to pay ransom and therefore, not cooperate with the criminals but instead to face the hardship and fight on deserves respect. Paying a ransom is not right for a number of reasons. Firstly, responding in this way to criminal attacks will send the wrong message to the world at large as such a decision can carry illegal and immoral implications. The company may look weak in the face of hardship and become an easy target for future attacks. Secondly, this may serve as an incentive for future cyber

[28] Trend Micro Team, 'What You Need to Know About the LockerGoga Ransomware' (20 March 2019) <https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/what-you-need-to-know-about-the-lockergoga-ransomware> accessed 25 March 2020.

[29] Kevin Beaumont, «How Lockergoga took down Hydro — ransomware used in targeted attacks aimed at big business' *Medium* (21 March 2019) <https://doublepulsar.com/how-lockergoga-took-down-hydro-ransomware-used-in-targeted-attacks-aimed-at-big-business-c666551f5880> accessed 17 March 2020.

[30] Ibid.

[31] Ibid.

[32] Luke Irwin, '£60 million in recovery costs for Norsk Hydro after refusing ransom demand' *IT Governance* (27 June 2019) <https://www.itgovernance.co.uk/blog/60-million-recovery-costs-for-norsk-hydro-after-ransom> accessed 10 April 2020.

activities and simply fund criminality. Thirdly, and not least of all, the victim cannot trust the criminal world, nor be sure that after paying the ransom their word will be kept and that a decryption code will be sent to the victim.[33]

Crimes against government may target key infrastructure and may pose a threat to national sovereignty or even be regarded as an act of war. These crimes can vary from hacking into a public body's computers, launching a malware attack on government electronic data systems, accessing confidential information, and committing cyber-warfare or cyber-terrorism.[34]

In the current pandemic caused by the Covid-19 outbreak, the healthcare systems of different countries are being hit by an increasing number of aggressive cyber attacks. Thus, already in March when many European countries were going through the pandemic, cyber criminals were taking advantage of the situation and launched malware attacks on the biggest testing centre against Covid-19, Brno University Hospital in the Czech Republic.[35] The malware caused a shutdown of the hospital's computer system, causing delays in surgery and relocation of patients to other hospitals.[36] Other examples of cyber attacks on the healthcare sector include hacking into the computer system of the UK's Hammersmith Medicines Research, which is a trial centre for a Covid-19 vaccine, resulting in exposure of sensitive information.[37] In the same month, the US Department of Health and Human Services became the target of malware which was aimed to cause a slow-down of the Department's systems.[38] Other countries which have experienced attempted cyber attacks on their hospitals are France and Spain.

There may be a variety of motives behind these cyber attacks and it can be justifiably argued that such types of attack can be easily classed as terrorism because they aim to destabilise the state healthcare system, causing massive disruptions to hospital operations, stealing files with sensitive data including methods of cure against the virus, vaccine development, and patients' progress towards recovery. Such attacks thus not only put the state healthcare infrastructure at risk, but they also endanger the lives of many patients who are in a critical condition and require urgent treatment to survive. These attacks, when successful, cause chaos in hospitals and can lead to drastic consequences for the public at large, especially at this current time of pandemic. Therefore, these malware attacks are extremely dangerous, massive in their scale and dramatic in their outcomes. The president of the European Commission, Ursula von der Leyen, said: «Cyber criminals follow us online and exploit our concerns about the coronavirus. Our fear becomes their business opportunity.»[39] Indeed, when medical staff are working around the clock, risking their own lives to save others, some others express the worst aspect of human nature by trying to

[33] Ibid.

[34] Mary Clare Novak, op.cit.

[35] Sophie Porter, 'Cyberattack on Czech hospital forces tech shutdown during coronavirus outbreak' *Healthcare IT News* (19 March 2020) <https://www.healthcareitnews.com/news/europe/cyberattack-czech-hospital-forces-tech-shutdown-during-coronavirus-outbreak> accessed 2 April 2020.

[36] Ibid.

[37] Elena Sanchez Nicolas, 'Cybercrime rises during coronavirus pandemic' *EUobserver* (25 March 2020) <https://euobserver.com/coronavirus/147869> accessed 7 April 2020.

[38] Hannah Murphy, Kiran Stacey, 'US health department targeted in cyber attack', *Financial Times* (16 March 2020) <https://www.ft.com/content/a4ac1ad1-0c86-4c7a-a6ac-d5296cbaecb8> accessed 28 March 2020.

[39] Elena Sanchez Nicolas, op.cit.

destabilise the national healthcare system, endangering lives and trying to make money out of people's pain and suffering.

A different example of cybercrime against the government, is hacking into government computers for the purpose of stealing money, an example of which is given by the Oklahoma case in 2019, when hackers attacked the State Pension Fund, committing a cyber theft of $4.2 million from the Oklahoma Enforcement Retirement System.[40] That is not the only instance when criminals broke into a municipal computer system to steal funds. Bloomberg reported that in 2019 alone, municipal authorities became victims to 73 ransomware attacks, which is 19 more cases than in 2018.[41] This can influence the credit rating of the state and consequently, it can negatively impact on the investment climate in the region.

III. Ways to fight cybercrime

As illustrated in the cases above, even giant corporations or state authorities with their own security departments can still become a prey to cybercriminals. Therefore, in the battle against cybercrime it is essential to develop a comprehensive approach which will encompass various methods to combat them.

The first and most powerful way to fight cybercrime at the national and international levels is to develop a strong legal framework which will combine hard and soft law, introducing common definitions of cybercrime, together with heavy punishment for cybercriminals and their accomplices. Cyberlaw is an evolving field of law which is a recent addition to the traditional legal system in many countries. According to the United Nations, 138 countries in the world have already enacted cybercrime laws.[42]

Since Ukraine has taken a more pro-European direction in recent times, strengthening its economic, legal and political ties with Europe, we shall consider the EU legal framework with regard to cybersecurity. The first and major piece of legislation in this area has been the Directive on Security of Network and Information Systems (NIS Directive)[43] which came into force in August 2016. The NIS Directive serves as a legal tool to strengthen cybersecurity across the EU. It places responsibility on EU member states to establish national NIS authorities and a network of Computer Security Incident Response Teams to foster effective cooperation amongst the member states and share information about cyber risks. The EU states should then continuously develop a cybersecurity culture across key economic sectors in their country, identifying businesses as «operators of essential services», including digital service providers and enable them to report risks.[44] Furthermore, the General Data Protection Regulation which came into effect in May 2018 guarantees protection of the personal data and privacy to all EU citizens.[45] The other milestone in regulating this area is

[40] Maria Elena Vizcaino, 'Oklahoma Pension Fund Cyber Attack Shows Rising Risk for Munis' *Bloomberg* (13 September 2019) <https://www.bloomberg.com/news/articles/2019-09-13/oklahoma-pension-fund-cyber-attack-shows-rising-risk-for-munis> accessed 29 March 2020.

[41] Ibid.

[42] United Nations Conference, Cyber Legislation Worldwide <https://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Cybercrime-Laws.aspx> accessed 28 March 2020.

[43] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union <http://data.europa.eu/eli/dir/2016/1148/oj> accessed on 29 March 2020.

[44] European Commission, The Directive on security of network and information system (NIS Directive) <https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive> accessed 3 April 2020.

[45] Regulation (EU) 2016/679 of the European Parliament and of the Council on 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation <http://data.europa.eu/elireg/2016/679/oj> accessed 10 April 2020.

the Cybersecurity Act 2019[46] which granted more powers to the European Network and Information Security Agency (ENISA) created in 2004 to assist EU member states with advice and solutions to various security issues. The variety of ENISA's work includes organising training and studies on cyber crisis management, implementing and further developing a national cybersecurity strategy, and taking part in drafting EU laws on information security.[47] The EU Cybersecurity Act gave ENISA a mandate for establishing a cybersecurity certification framework for information and communications technology (ICT) products, processes and services.[48] The certification framework involves a unique certification which is recognised by all EU member states and confirms that ICT products, processes and services are cyber secure.[49]

Last year marked another important event in the development of cybersecurity. The EU established a legal framework with a new sanctions regime which imposes restrictive measures to prevent and react to cyber attacks which pose a threat to the EU and its member states. This framework and the sanctions regime are stipulated in Council Decision 2019/797[50] and Council Regulation (EU) 2019/796.[51] According to the European Council, the EU will impose sanctions on physical and legal persons that are «responsible for cyber-attacks or attempted the cyber-attacks; who provide financial, technical or material support for such attacks or who are involved in other ways».[52] Some of the restrictions placed on persons who are found to be responsible for cyber attacks include a travel ban and an asset freeze against cyber criminals and persons who assist them.[53]

Mieke Eoyang, Allison Peters et al.[54] in their paper entitled «To Catch a Hacker: Toward a comprehensive strategy to identify, pursue, and punish malicious cyber actors» consider ways in which the cybersecurity of the USA can be strengthened. These apply not just to the USA but should be taken as advice to countries across the world. The experts emphasise the importance of improving law enforcement, identifying lack of resources and shortfalls in personnel training as obstacles to bringing criminals to justice. Investing funds in law enforcement staff training, incentivising them and retaining the best should become an important goal.[55] It is crucial, they point out, to continue funding research and development in order to produce effective solutions in cyber forensic technology.[56]

No less an important way to fight cybercrime is to adopt effective technical measures to deter cybercriminals. For instance, Trend Micro Inc. advises on

[46] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) PE/86/2018/REV/1 <http://data.europa.eu/eli/reg/2019/881/oj> accessed 5 April 2020.

[47] ENISA <https://europa.eu/european-union/about-eu/agencies/enisa_en> accessed 25 March 2020.

[48] <https://ec.europa.eu/digital-single-market/en/eu-cybersecurity-act> accessed 1 April 2020.

[49] Ibid.

[50] Council Decision (CFSP) 2019/797 of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States

[51] Council Regulation (EU) 2019/796 of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States

[52] European Council of the European Union, 'Cybersecurity in Europe: stronger rules and better protection' <https://www.consilium.europa.eu/en/policies/cybersecurity/> accessed 5 April 2020.

[53] Ibid.

[54] Mieke Eoyang, Allison Peters et al., 'To Catch a Hacker: Toward a comprehensive strategy to identify, pursue, and punish malicious cyber actors' *Third Way* (2018) <https://www.jstor.org/stable/resrep20153> accessed 12 April 2020.

[55] Ibid.

[56] Ibid.

steps which should be taken to fight against malware/ransomware.[57] Firstly, it emphasises the importance of regular backups of the files and the system. This allows organisations to clear infected systems and restore a former version within days. Industry experts have the «3-2-1 backup rule»: making three copies on media tools such as USB or hard disk and another copy «stored offsite».[58] Secondly, it is essential to keep all the systems and applications updated. It does not take much time to download updates but not doing so can put a user's computer at risk and make it more vulnerable in the face of cyber threats. One can enable automatic updates which will be installed on the system when they are available. In addition, it is important to have good anti-virus software that monitors the system and eliminates viruses and malware. Thirdly, one should have «secure system administration tools and implement network segmentation and data categorisation» to reduce the risk of disclosure of important data. Further advice includes enhancing protection of email gateways and strengthening security such as «application control» and «behaviour monitoring», which will enable the user to prevent undesirable alterations to his/her system.[59]

Managerial action to fight cybercrime include strategic planning, risk evaluation and risk management, effective cooperation with different departments in a company including IT/security department, and coordination and leadership. From the case of Yahoo and Hydro we can see how significant were the managerial decisions, not only for the short-term survival of the business but also for the long-term. Often managers, in order to save money, cut the investment in cybersecurity. Neglecting the advice or requests of IT experts within a company and skimping on investment in cybersecurity, however, can cost a company dearly in financial loss and damage to brand image. On the contrary, the clever managerial response by Hydro to the cyber attack led the company not only to survive but also to increase their share price in the face of disaster, which is a rare phenomenon. Vicky Ngo-Lam, a product marketing manager at Exabeam, a Smart SIEM company[60], advises business entities to prepare an incident response plan which should involve different stages:

Preparation: includes selecting staff and training them effectively or employing experts in the field.

Identification: detecting gaps in security and deciding how to fix them.

Containment: cleaning and restoring damaged areas.

Eradication: investigating causes of the incident and removing malware.

Recovery: restoring the systems, testing them and ensuring that they are working well.

Learning the lessons: team review and improving the incident response plan.[61]

Finally, foreign policy plays a major role in cybercrime deterrence. The policy may include diplomatic meetings and warnings as well as sanctions such as travel bans or economic sanctions imposed on cyber criminals. Diplomats are known for their mastery of word and effective communication. Their role in fighting the cybercrime is supportive and can be decisive. «The more intergovernmental cooperation and communication, the more

[57] Trend Micro team, 'What You Need to Know About the LockerGoga Ransomware' (20 March 2019) <https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/what-you-need-to-know-about-the-lockergoga-ransomware> accessed 30 March 2020.

[58] Ashley Pugh, '8 ways to fight cybercrime' *E-careers* (18 April 2019) <https://www.e-careers.com/connected/cyber-security-careers/8-ways-to-fight-cybercrime> accessed 28 March 2020.

[59] Ibid.

[60] Vicky Ngo-Lam, «Cyber Crime: Types, Examples, and What Your Business Can Do» Exabeam website (24 December 2019) <https://www.exabeam.com/information-security/cyber-crime/> accessed 5 April 2020.

[61] Ibid.

effective the response to any cyber-crime will be», states Sico van der Meer, a Research Fellow at the Clingendael Institute in the Netherlands.[62]

Conclusion

Since we rely on computers, the Internet and other digital technologies more and more in our daily lives, everyone is exposed to a range of potential cyber threats. The world is becoming more interconnected, which creates major opportunities for cyber criminals who are now increasingly frequent and aggressive in their nature. The words of Scott Shackelford: «No person, organisation, or computer can ever be 100% secure. Someone with the patience, money and skill can break into even the most protected systems»[63] have been proved numerous times in practice as newspapers headlines announce another notorious hacking or malware attack on governments or big corporations. Cases such as Yahoo or Hydro have demonstrated that cybersecurity can become a real challenge in spite of the company's size, name and reputation. A lack of cyber protection can exact a high price: substantial financial and data loss, disruption to daily operations, damage to a company's name, credit downgrading and a negative impact on share prices. Furthermore, it can risk people's lives as has been seen in the case of cyber attacks on the healthcare systems across countries during the Covid-19 pandemic. Therefore, cybersecurity in the 21st century has become a priority for governments, top company management and each of us as private citizens and the matter requires a holistic approach for its solution. There are a number of ways to deter and fight the cybercrime, namely legal, technical, managerial and diplomatic action. In my opinion, they are all significant as they offer protection from various angles. Having strong laws and regulations in place which will introduce heavy punishment to criminals and their accomplices coupled with an effective law enforcement mechanism will play an instrumental role in fighting and deterring cybercrime. Developing hard law as well as strengthening soft law is essential. Following recent trends in cybercrime, it is crucial to evaluate the potential risks and plan strategically to keep the legal framework as updated as possible, encompassing all societal needs of today and enabling society to deal with the legal problems that it is facing. Without a strong legal platform we will not be able to fight cybercrime efficiently and effectively. Furthermore, strengthening foreign policy in the form of continuous cooperation between countries in investigating cybercrimes, identifying cyber criminals and prosecuting them will have a positive impact on shaping a common cyber secure future. Continuous diplomatic efforts to align policies and procedures will further contribute to it. Surely, cybersecurity requires a great deal of IT technical knowledge and skills. However, every individual can take more precautions against becoming a victim of a cybercrime. Already by taking small steps in cybersecurity, such as following advice from IT specialists on updating computer program, changing passwords on accounts, ignoring strange-looking emails from unknown senders or simply leaving as little sensitive information as possible online can potentially save nerves, time and finance in the future. Keeping oneself alert to potential cyber fraud is key. As for business entities and organisations, it has become essential nowadays to employ, train and retain IT staff who will constantly monitor and assess the state of cybersecurity of the company's systems. Company managers should be more willing

[62] Sico van der Meer, 'Foreign Policy Responses to International Cyber-attacks' Clingendael University (September 2015) <https://www.jstor.org/stable/resrep05303> accessed 7 April 2020.

[63] Scott Shackelford, op.cit.

to cooperate with IT experts, be open to their suggestions and be encouraged to invest more in cybersecurity. Fighting cybercrime is a global issue and therefore, requires a mutual effort and cooperation between different states, the business world, IT experts and public at large.

Bibliography

EU Legislation

Council Decision (CFSP) 2019/797 of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States ST/7299/2019/INIT <http://data.europa.eu/eli/dec/2019/797/oj> accessed 10 April 2020.

Council Regulation (EU) 2019/796 of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States ST/7302/2019/INIT <http://data.europa.eu/eli/reg/2019/796/oj> accessed 10 April 2020.

Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (NIS Directive) <http://data.europa.eu/eli/dir/2016/1148/oj > accessed 10 April 2020.

Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (Text with EEA relevance) PE/86/2018/REV/1 <http://data.europa.eu/eli/reg/2019/881/oj> accessed 7 April 2020.

Regulation (EU) 2016/679 of the European Parliament and of the Council on 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) <http://data.europa.eu/elireg/2016/679/oj> accessed 10 April 2020.

Online Journals

Eoyang M., Peters A, et al., 'To Catch a Hacker: Toward a comprehensive strategy to identify, pursue, and punish malicious cyber actors' (2018) *Third Way* <https://www.jstor.org/stable/resrep20153> accessed 12 April 2020.

Futter A, 'Is Trident safe from cyber attack?'(Report 5 February 2016) *European Leadership Network* <https://www.europeanleadershipnetwork.org/report/is-trident-safe-from-cyber-attack/> accessed 23 March 2020.

Goodman W, 'Tougher in Theory than in Practice?' (2010) Vol. 4, No. 3 *Strategic Studies Quarterly* pp.102-135 <https:www.jstor.org/stable/10.2307/26269789> accessed 30 March 2020.

Kirsh E. M, et al., 'Recommendations for evolution of cyber law' (September 1996) 2 (2) *Journal of Computer Mediated Communications,* published online 23 June 2006 <https://onlinelibrary.wiley.com/doi/full/10.1111/j.1083-6101.1996.tb00056.x> accessed 28 March 2020.

McKenzie M. T, 'Is Cyber Deterrence Possible?' (2017) *Air University Press* <https://www.jstor.org/stable/resrep13817.9> accessed 21 March 2020.

Pawlak P., Biersteker T, 'Laws of Gravitation. Due diligence obligations in cyberspace' (2019) European Union Institute for Security Studies (EUISS) <https://www.jstor.org/stable/resrep21136.10> accessed 3 April 2020.

Van der Meer S, 'Foreign Policy Responses to International Cyber-attacks' (September 2015) Clingendael University <https://www.jstor.org/stable/resrep05303> accessed 08 April 2020.

Government and Organisational websites

ENISA <https://europa.eu/european-union/about-eu/agencies/enisa_en> accessed 25 March 2020.

European Commission: The Directive on security of network and information systems (NIS Directive) <https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive> accessed 5 April 2020.

European Commission: The EU Cybersecurity Act <https://ec.europa.eu/digital-single-market/en/eu-cybersecurity-act> accessed 10 April 2020.

Council of the European Union, 'Cybersecurity in Europe: stronger rules and better protection' <https://www.consilium.europa.eu/en/policies/cybersecurity/> accessed 5 April 2020.

Identity Theft Resource Center, Data Breach Report for 2019 <https://www.idtheftcenter.org/identity-theft-resource-centers-annual-end-of-year-data-breach-report-reveals-17-percent-increase-in-breaches-over-2018/> accessed 20 March 2020.

The United States Government website, 'Identity Theft' <https://www.usa.gov/identity-theft> accessed 20 March 2020.

United Nations Conference, Cyber Legislation Worldwide <https://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Cybercrime-Laws.aspx> accessed 5 April 2020.

Company websites and professional blogs

Cisomag, 'Cybercrime Will Cost the World US 6$ Trillion by the End of the Year: Study' *Cisomag* (23 March 2020) <https://www.cisomag.com/cybercrime-will-cost-the-world-us6-trillion-by-the-end-of-the-year-study/> accessed 27 March 2020

Beaumont K, 'How LockerGoga took down Hydro — ransomware used in targeted attacks aimed at big business' *Medium* (21 March 2019) <https://doublepulsar.com/how-lockergoga-took-down-hydro-ransomware-used-in-targeted-attacks-aimed-at-big-business-c666551f5880> accessed 18 March 2020.

Hernandez E, 'The 16 Most Common Types of Cybercrime Acts' *VoIP Shield* (14 February 2018) <https://www.voipshield.com/the-16-most-common-types-of-cybercrime-acts/> accessed 20 March 2020.

Irwin L, '£60 million in recovery costs for Norsk Hydro after refusing ransom demand' *IT Governance* (27 June 2019) <https://www.itgovernance.co.uk/blog/60-million-recovery-costs-for-norsk-hydro-after-ransom> accessed 10 April 2020.

Johansen A. G, 'What is ransomware and how to help prevent ransomware attacks' *NortonLifeLock* <https://us.norton.com/internetsecurity-malware-ransomware-5-dos-and-donts.html> accessed 28 March 2020.

Lam V, 'Cyber Crime: Types, Examples, and What Your Business Can Do' *Exabeam* company website (24 December 2019) <https://www.exabeam.com/information-security/cyber-crime/> accessed 18 March 2020.

Novak, M.C, 'Let's Talk About Cyber Law: Crime, Security, and Legislation' *Learning Hub Tech* (20 November 2019) <https://learn.g2.com/cyber-law> accessed 29 March 2020.

Pugh A, '8 Ways to fight cybercrime' *E-careers* (18 April 2019) <https://www.e-careers.com/connected/cyber-security-careers/8-ways-to-fight-cybercrime> accessed 25 March 2020.

Shackelford S, 'Take these 5 critical steps to protect yourself from cybercrime' *Fast Company* (17 August 2019) <https://www.fastcompany.com/90391332/take-these-5-critical-steps-to-protect-yourself-from-cybercrime> accessed 7 April 2020.

Trend Micro team, 'What You Need to Know About the LockerGoga Ransomware' Trend Micro Inc. (20 March 2019) <https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/what-you-need-to-know-about-the-lockergoga-ransomware> accessed 20 March 2020.

Yahoo! Inc. Customer Data Security Breach Litigation Settlement <https://yahoodatabreachsettlement.com> accessed on 27 March 2020.

Online news articles

Holmes A, 'The biggest hacks of 2019 so far' *Business Insider* (11 September 2019) <https://www.businessinsider.com/biggest-hacks-and-data-breaches-of-2019-capital-one-whatsa pp-iphone-2019-9> accessed 14 April 2020.

Kunchler H, 'Yahoo says 2013 cyber breach affected all 3bn accounts' *Financial Times* <https://www.ft.com/content/9412c2b0-a87c-11e7-93c5-648314d2c72c> accessed 3 April 2020.

Men J, Finkle J, et al. 'Yahoo security problems a story of too little, too late' *Reuters* (18 December 2016) <https://www.reuters.com/article/us-yahoo-cyber-insight/yahoo-security-problems-a-story-of-too-little-too-late-idUSKBN1470WT> accessed 1 April 2020.

Murphy H, Stacey K, 'US health department targeted in cyber attack' *Financial Times* (16 March 2020) <https://www.ft.com/content/a4ac1ad1-0c86-4c7a-a6ac-d5296cbaecb8> accessed 29 March 2020.

Porter S, 'Cyberattack on Czech hospital forces tech shutdown during coronavirus outbreak' *Healthcare IT News* (19 March 2020) <https://www.healthcareitnews.com/news/europe/cyberattack-czech-hospital-forces-tech-shutdown-during-coronavirus-outbreak> accessed 25 March 2020.

Sanchez Nicolas E, 'Cybercrime rises during coronavirus pandemic' *EUobserver* (25 March 2020) <https://euobserver.com/coronavirus/147869> accessed 28 March 2020.

Stempel J, Finkle J, 'Yahoo says all three billion accounts hacked in 2013 data theft' *Reuters* (3 October 2017) <https://www.reuters.com/article/us-yahoo-cyber/yahoo-says-all-three-billion-accounts-hacked-in-2013-data-theft-idUSKCN1C82O1> accessed 20 March 2020.

Vizcaino M. E, 'Oklahoma Pension Fund Cyber Attack Shows Rising Risk for Munis' *Bloomberg* (13 September 2019) <https://www.bloomberg.com/news/articles/2019-09-13/oklahoma-pension-fund-cyber-attack-shows-rising-risk-for-munis> accessed 21 March 2020.

Other

Baohero formerly Taobao Agent <https://baohero.com/taobao> accessed 1 April 2020.

Goodreads on Jacques Ellul <https://www.goodreads.com/quotes/1297716-modern-technology-has-become-a-total-phenomenon-for-civilization-the> accessed 23 March 2020.

Thelaw.com: Law Dictionary & Black's Law Dictionary 2nd Ed. <https://dictionary.thelaw.com/cybercrime/> accessed 7 April 2020

Список використаної літератури

Законодавство ЄС

Рішення Ради (ЕС) 2019/797 від 17 травня 2019 року щодо обмежувальних заходів проти кібератак, що загрожують Союзу чи його державам-членам ST/7299/2019/INIT <http://data.europa.eu/eli/dec/2019/797/oj> дата звернення: 10 квітня 2020 року.

Регламент Ради (ЄС) 2019/796 від 17 травня 2019 року щодо обмежувальних заходів проти кібератак, що загрожують Союзу чи його державам-членам ST/7302/2019/INIT <http://data.europa.eu/eli/reg/2019/796/oj> дата звернення: 10 квітня 2020 року.

Директива (ЄС) 2016/1148 Європейського Парламенту і Ради від 6 липня 2016 року про заходи для високого спільного рівня безпеки мережевих та інформаційних систем на території Союзу <http://data.europa.eu/eli/dir/2016/1148/oj> дата звернення: 10 квітня 2020 року.

Регламент (ЄС) 2019/881 Європейського Парламенту і Ради від 17 квітня 2019 року про ENISA (Агентство Європейського Союзу з питань мережевої та інформаційної безпеки) та про сертифікацію кібербезпеки інформаційних та комунікаційних технологій та скасування Регламенту (ЄС) № 526/2013 (Закон про кібербезпеку) PE/86/2018/REV/1 <http://data.europa.eu/eli/reg/2019/881/oj> дата звернення: 7 квітня 2020 року.

Регламент (ЄС) 2016/679 Європейського парламенту і Ради від 27 квітня 2016 року про захист фізичних осіб щодо обробки персональних даних та про вільний рух таких даних та про скасування Директиви 95/46 / ЄС (Загальне Положення про захист даних <http://data.europa.eu/elireg/2016/679/oj> дата звернення: 10 квітня 2020 року.

Онлайн-публікації

Іоян М., Пітерс А. та ін., «Ловити хакера: на шляху до всебічної стратегії виявлення, переслідування та покарання зловмисних кібер-акторів» (2018 рік) Тьод вей <https://www.jstor.org/stable/resrep20153> дата звернення: 12 квітня 2020 року.

Фатер А, «Чи захищений Трідент від кібератаки?» (Звіт 5 лютого 2016 р.) Юропієн Лідершіп Нетворк <https://www.europeanleadershipnetwork.org/report/is-trident-safe-from-cyber-attack/> дата звернення: 23 березня 2020 року.

Гудман В, «Сильніший в теорії, ніж на практиці?» (2010 р.), Вип. 4, № 3 Стратеджік Стадіс Квотерлі стор.102-135 <https:www.jstor.org/stable/10.2307/26269789> дата звернення: 30 березня 2020 року.

Кірш Е. М. та ін., «Рекомендації щодо розвитку кібер-права» (вересень 1996 р.) 2 (2) Джорнал оф Комп'ютер Медіейтид Комунікейшнс, опублікований в Інтернеті 23 червня 2006 р. <https://onlinelibrary.wiley.com/doi/full/10.1111/j.1083-6101.1996.tb00056.x> дата звернення: 28 березня 2020 року.

МакКензі М. Т, «Чи можливе стримування кібер-атак?» (2017 р.) Університет Повітряних Сил <https://www.jstor.org/stable/resrep13817.9> дата звернення: 21 березня 2020 року.

Павлак П., Бієрстекер Т, «Закони гравітації. Зобов'язання щодо належної ретельності в кіберпросторі» (2019 р.) Європейський Союзний Інститут Досліджень Безпеки (EUISS) <https://www.jstor.org/stable/resrep21136.10> дата звернення: 3 квітня 2020 року.

Ван Дер Мер С, «Реагування зовнішньої політики на міжнародні кібератаки» (вересень 2015 р.) Університет Клінгедель <https://www.jstor.org/stable/resrep05303> дата звернення: 08 квітня 2020 року.

Урядові та організаційні веб-сайти

Агенство Європейського Союзу з питань мережевої та інформаційної безпеки <https://europa.eu/european-union/about-eu/agencies/enisa_en> дата звернення: 25 березня 2020 року.

Європейська Комісія, Директива про безпеку мережевих та інформаційних систем <https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive> дата звернення: 5 квітня 2020 року.Європейська комісія: Закон про кібербезпеку ЄС <https://ec.europa.eu/digital-single-market/en/eu-cybersecurity-act> дата звернення: 10 квітня 2020 року.

Рада Європейського Союзу «Кібербезпека в Європі: більш жорсткі правила та кращий захист» <https://www.consilium.europa.eu/en/policies/cybersecurity/> дата звернення: 5 квітня 2020 року.

Айдентіті Тефт Ресурс Сентер, Звіт про порушення даних за 2019 рік <https://www.idtheftcenter.org/identity-theft-resource-centers-annual-end-of-year-data-breach-report-reveals-17-percent-increase-in-breaches-over-2018/> дата звернення: 20 березня 2020 року.

Веб-сайт уряду Сполучених Штатів Америки: визначення поняття «Крадіжка особистих даних» <https://www.usa.gov/identity-theft> дата звернення: 20 березня 2020 року.

Конференція Організації Об'єднаних Націй: Кібер-законодавство у всьому світі <https://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Cybercrime-Laws.aspx> дата звернення: 5 квітня 2020 року.

Веб-сайти компанії та професійні блоги

Цисомег, «Кіберзлочинність обійдеться в світі 6 трильйонів доларів США до кінця року: дослідження» Цисомег (23 березня 2020 р.) <https://www.cisomag.com/cybercrime-will-cost-the-world-us6-trillion-by-the-end-of-the-year-study/> дата звернення: 27 березня 2020 року.

Бомонт К, «Як ЛокерГога атакував Гайдро — вірус, який використовується в цілеспрямованих атаках, спрямованих на великий бізнес» Мідіум (21 березня 2019 р.) <https://doublepulsar.com/how-lockergoga-took-down-hydro-ransomware-used-in-targeted-attacks-aimed-at-big-business-c666551f5880> дата звернення: 18 березня 2020 року.

Ернандес Е, «16 найпоширеніших типів діянь кіберзлочинності» Воіп Шілд (14 лютого 2018 р.) <https://www.voipshield.com/the-16-most-common-types-of-cybercrime-acts/> дата звернення: 20 березня 2020 року.

Ірвін Л, «60 мільйонів фунтів витрат на відновлення Норськ Гайдро після відмови від вимоги викупу» Айті Гавененс (27 червня 2019 р.) <https://www.itgovernance.co.uk/blog/60-million-recovery-costs-for-norsk-hydro-after-ransom> дата звернення: 10 квітня 2020 року.

Йохансен А. Г, «Що таке вірусне програмне забезпечення з ціллю вимоги викупу та як запобігти атакам таких вірусних програм» НортонЛайфЛок <https://us.norton.com/internetsecurity-malware-ransomware-5-dos-and-donts.html> дата звернення: 28 березня 2020 року.

Лам В, «Кіберзлочинність: типи, приклади та засоби запобігання для бізнесу» Веб-сайт компанії Ексабім (24 грудня 2019 р.) <https://www.exabeam.com/information-security/cyber-crime/> дата звернення: 18 березня 2020 року.

Новак, М. К, «Поговоримо про кібер-право: злочинність, безпека та законодавство» Льонін Хаб Тех (20 листопада 2019 р.) <https://learn.g2.com/cyber-law> дата звернення: 29 березня 2020 року.

П'ю А, «8 способів боротьби з кіберзлочинністю» І-кариарс (18 квітня 2019 р.) <https://www.e-careers.com/connected/cyber-security-careers/8-ways-to-fight-cybercrime> дата звернення: 25 березня 2020 року.

Шеклфорд С, «Зробіть ці 5 необхідних кроків, щоб захистити себе від кіберзлочинності» Фаст Кампані (17 серпня 2019 р.) <https://www.fastcompany.com/90391332/take-these-5-critical-steps-to-protect-yourself-from-cybercrime> дата звернення: 7 квітня 2020 року.

Команда Тренд Майкро, «Що потрібно знати про вірусне програмне забезпечення з цілею вимоги викупу ЛокерГога» (20 березня 2019 р.) <https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/what-you-need-to-know-about-the-lockergoga-ransomware> дата звернення: 20 березня 2020 року.

Яху Інк. (Yahoo! Inc.) <https://yahoodatabreachsettlement.com> дата звернення: 27 березня 2020 року.

Онлайн-новини

Холмс А, «Найбільші хакер-зломи в 2019 році» Бізнес Інсайдер (11 вересня 2019 р.) <https://www.businessinsider.com/biggest-hacks-and-data-breaches-of-2019-capital-one-whatsapp-iphone-2019-9> дата звернення: 14 квітня 2020 року.

Кунчлер Х, «Згідно Аху, всі 3 млрд акаунтів було зломано» Файненшл Таймс <https://www.ft.com/content/9412c2b0-a87c-11e7-93c5-648314d2c72c> дата звернення: 3 квітня 2020.

Мен Джей, Фінкл Джей та ін. «Проблеми безпеки Яху — історія про занадто мало та запізно» Ройтерс (18 грудня 2016 р.) <https://www.reuters.com/article/us-yahoo-cyber-insight/yahoo-security-problems-a-story-of-too-little-too-late-idUSKBN1470WT> дата звернення: 1 квітня 2020 року.

Мьорфі Х, Стейсі К, «Департамент охорони здоров'я США був мішенню кібер-атаки» Файненшл Таймс (16 березня 2020 р.) <https://www.ft.com/content/a4ac1ad1-0c86-4c7a-a6ac-d5296cbaecb8> дата звернення: 29 березня 2020 року.

Портер С, «Кібератака на чеські лікарні спричинила технічне вимкнення під час спалаху коронавірусу» Хелс Кеа Айті Ньюс (19 березня 2020 р.) <https://www.healthcareitnews.com/news/europe/cyberattack-czech-hospital-forces-tech-shutdown-during-coronavirus-outbreak> дата звернення: 25 березня 2020 року.

Санчес Ніколяс Е, «Зростання рівню кіберзлочинність під час пандемії коронавірусу» ЄС Обзервер (25 березня 2020 р.) <https://euobserver.com/coronavirus/147869> дата звернення: 28 березня 2020.

Штемпель Джей, Фінкл Джей, «Яху стверджує, що всі три млрд облікових записів було зломано в крадіжці даних в 2013 році» Ройтерс (3 жовтня 2017 р.)

<https://www.reuters.com/article/us-yahoo-cyber/yahoo-says-all-three-billion-accounts-hacked-in-2013-data-theft-idUSKCN1C82O1> дата звернення: 20 березня 2020 року.

Візайн М. Е, «Кібер-атака пенсійного фонду Штату Оклахома показує ризик для Муніса» Блумберг (13 вересня 2019 р.) <https://www.bloomberg.com/news/articles/2019-09-13/oklahoma-pension-fund-cyber-attack-shows-rising-risk-for-munis> дата звернення: 21 березня 2020 року.

Інші

Баохіроу, раніше агент ТаоБао <https://baohero.com/taobao> дата звернення: 1 квітня 2020 року.

Гудрідс: цитати Жак Ілюль <https://www.goodreads.com/quotes/1297716-modern-technology-has-become-a-total-phenomenon-for-civilization-the> дата звернення: 23 березня 2020 року.

Thelaw.com: Юридичний словник та юридичний словник Блек 2-е видання. <https://dictionary.thelaw.com/cybercrime/> дата звернення: 7 квітня 2020 року.

Журавель М. В. Підвищення рівня обізнаності щодо кібербезпеки: розуміння кіберзлочинності та пошук способів боротьби з нею.

Оскільки ми живемо в епоху глобальної цифровізації, яка рухає економічний прогрес у світі, формує правові рамки та встановлює нові тенденції соціальної поведінки, кіберпростір став основною частиною нашої реальності. Чи то реєстрація облікового запису в соціальних мережах, чи то переказ грошей через Інтернет-банкінг, замовлення на гігантських платформах, таких як Amazon чи Taobao, оплата рахунків в Інтернеті, не кажучи вже про великі комерційні транзакції та інші цінні операції, які проводяться електронними засобами, ми вступили в кіберпростір і маємо справу з питаннями кібер-права. Віртуальна реальність породжує можливості для підприємств, урядів та приватних осіб, однак це також створює значні загрози безпеці на різних рівнях, включаючи національний рівень, через що ключова державна інфраструктура може стати об'єктом кібератак.

Це було помічено під час пандемії COVID-19, коли система охорони здоров'я низки країн зазнала кіберзагрози, що на прикладі Чехії призвело до серйозних порушень медичних процесів у лікарні. Таким чином, кіберзлочинність може спричинити згубний вплив не тільки для фізичних осіб або суб'єктів господарювання, але й для великої групи зацікавлених сторін. Розмах і динаміка нашої онлайн-діяльності, кількість особистої інформації, яку ми зберігаємо або ненавмисно залишаємо в Інтернеті, — це все створює більшу загрозу для нашої конфіденційності. Кожен, хто користується Інтернетом, може стати жертвою різних видів кіберзлочинності. У цій статті будуть розглянуті різні ка-

тегорії кіберзлочинності, а саме злочини проти особи, злочини проти власності та злочини проти уряду, спираючись на приклади реальних справ. Далі буде вивчено шляхи, які слід використовувати в боротьбі з кіберзлочинністю. Крім того, законодавча база ЄС буде розглянута як приклад правових заходів проти кіберзлочинності.

Ключові слова: *Інтернет, кіберпростір, кіберзлочинність, кібератака, кіберзагроза, кібербезпека, викуп, кібертероризм, законодавча база Європейського Союзу, Директива NIS, ENISA, способи.*

Журавель М. В. Повышение осведомленности о кибербезопасности: понимание киберпреступности и поиск способов борьбы с ней.

Поскольку мы живем в эпоху глобальной цифровизации, которая движет экономический прогресс в мире, формирует правовые рамки и устанавливает новые тенденции социального поведения, киберпространство стало основной частью нашей реальности. Будь то регистрация аккаунта в социальных сетях или перевод денег через Интернет-банкинг, заказы на гигантских платформах, таких как Amazon или Taobao, оплата счетов в Интернете, не говоря уже о коммерческих транзакциях и других ценных операциях, проводимых электронными средствами, мы вступили в киберпространство и имеем дело с вопросами кибер-права. Виртуальная реальность порождает возможности для предприятий, правительств и частных лиц, однако это также создает значительные угрозы безопасности на различных уровнях, включая национальный уровень, из-за чего ключевая государственная инфраструктура может стать объектом кибератак.

Это было замечено во время пандемии COVID-19, когда система здравоохранения ряда стран претерпела киберугрозы, что на примере Чехии привело к серьезным нарушениям медицинских процессов в больнице. Таким образом, киберпреступность может иметь пагубное влияние не только для физических лиц или субъектов хозяйствования, но и для большой группы заинтересованных сторон. Размах и динамика нашей онлайн-деятельности, количество личной информации, которую мы сохраняем или нечаянно оставляем в Интернете, — это все создает большую угрозу для нашей конфиденциальности. Каждый, кто пользуется Интернетом, может стать жертвой различных видов киберпреступности. В этой статье будут рассмотрены различные категории киберпреступности, а именно преступления против личности, преступления против собственности и преступления против правительства, опираясь на примеры реальных дел. Далее будет изучено пути, которые следует использовать в борьбе с киберпреступностью. Кроме того, законодательная база ЕС будет рассмотрена как пример правовых мер против киберпреступности.

Ключевые слова: *Интернет, киберпространство, киберпреступность, кибератака, киберугрозы, кибербезопасность, выкуп, кибертерроризм, правовая база Европейского Союза, директива NIS, ENISA, пути.*