IV.5

CYBER WARFARE

Chapter 14

Cyberattacks/Incidents and Responding to Them

Barbara Kaczmarczyk

Abstract

The 21st century has brought forth the digital age. In the past, various types of activities and services could only be performed in the real world, and could be understood without computers. Currently, digital development has rendered possible the performance of numerous, if not almost all, everyday activities online. Services such as online shopping, booking trips, and opening bank accounts are also currently more financially profitable than traditional methods, as well as less time-consuming. Importantly, it is also possible to conduct elections and educational or product promotional campaigns via the Internet in today's digital world, and to conduct fast, free searches for various different pieces of information and large datasets. Digitalisation has undoubtedly contributed to the development of many areas of human life, groups, and institutions. The development of civilization and the digital world also led to the rise of various mechanisms, such as incidents or cyberattacks, that can disrupt these processes. Some of the reasons underlying incidents or cyberattacks, which are highly varied, include achieving quick financial success and destabilising the functioning of specific groups or organisations. Therefore, it is very important to recognise how incidents or cyberattacks work and how to prepare for them, prevent them, and if they occur, how to respond to them. It is also important to restore the status to that before the occurrence of the incidents or the cyberattack.
Research methodology: The article was developed based on Polish and international literature on the subject of security and cybersecurity, as well as Internet sources. During the research process, interviews with cybersecurity experts were conducted.

Keywords: cyber incident, cyberattack, cybersecurity, cyber space, cyber defence

Barbara Kaczmarczyk (2024) 'Cyberattacks/Incidents and Responding to Them'. In: Katarzyna Zombory – János Ede Szilágyi (eds.) *Shielding Europe with the Common Security and Defence Policy. The EU Legal Framework for the Development of an Innovative European Defence Industry in Times of a Changing Global Security Environment,* pp. 619–661. Miskolc–Budapest, Central European Academic Publishing.

https://doi.org/10.54237/profnet.2024.zkjeszcodef_14

1. Introduction

The 1940s saw the beginning of work on computers at the University of Pennsylvania, where Eckert and Muachly started building the first computer. They created the Electronic Numerical Integrator and Computer,[1] also known as ENIAC, a machine with an area of over 160 m^2 and a weight of 27 tons, which was considered the first computer in the world. Scientific developments continued, and in the 1970s and 1980s, the first negative computer-related event occurred, caused by the destabilisation of the functioning of the computer network. These phenomena are related to the topics of cyberspace (cyberspace) and digital environment, which also happen to be the places where cybersecurity works.

When considering incidents and cyberattacks, one should start by identifying what they are and in what space they operate.

An incident should be understood as an event that has or may have an adverse impact on cybersecurity.[2] It occurs in cyberspace, which is why we can talk about a security incident, which means that it is an event that may violate the confidentiality, integrity or availability of information and resources of an organization. In the context of security, an incident refers to a sudden and unexpected event that may have negative consequences for people, property, data or infrastructure. Security incidents can concern various aspects of an organization, including personal data, hardware or software.[3] In relation to the term cyberattacks, one definition of cyberattack[4] describes it as an intentional act intended to alter, disrupt, deceive, degrade, or destroy computer systems, networks, and programs serving resident work or enabling the use of these systems or networks. Cyberattacks are hence threats related to the use of computer networks and various criminal activities, such as obtaining material and intangible benefits. This definition can be supplemented by the purpose of such actions, which is often to disrupt security. These attacks are conducted using various methods, such as phishing, malware, ransomware, and distributed denial of service (DDoS) attacks.[5] They are carried out in an unauthorised manner with the purpose of stealing data, or even disrupt or damaging someone's reputation.

Vulnerabilities in systems and software errors facilitate attacks. They are dangerous primarily for national security, but can also be a threat for all other important sectors of society.[6] Cyberattacks[7] occur in cyberspace, defined as the space in which all activities based on information technology, electronic communication, and data processing occur. It is a place where information is exchanged using

1 Celebrating Penn Engineering History: ENIAC, *no date*.
2 Art. 2 ust. 5 Act of 5 July 2018 on the national cybersecurity system; Dz.U. 2018, poz.1560.
3 Based on *Incydent bezpieczeństwa informacji – kiedy następuje?* [Information security incident – when does it occur and what to do?], 2024.
4 Czekaj, 2020. Based on Wasiuta and Klepik, 2019, pp. 175–179.
5 More: European Court of Auditors, 2019.
6 Based on Wasiuta and Klepk, 2019.
7 Based on *Cyberatak* [Cyber attack], 2020.

networks, systems, and the Internet. Accompanying the land, sea, air, and space environments, cyberspace has also been recognised and classified as a new environment category where warfare can be carried out.[8] Cyberspace[9] and the threats emerging in it, which are developing at a rapid pace, have led people to start to think, discuss, and consequently create cybersecurity measures.[10] Related undertakings have, nonetheless, become difficult because everything that occurs in a given environment can be both safe and dangerous. For this reason, risk management strategies, crisis management systems, critical infrastructure management systems, and technical security measures have been developed and implemented. The essence of these measures is to ensure the integrity, confidentiality, and availability of data in the cyberspace, as well as its protection against various types of cyber incidents. Accordingly, information security effectiveness has become increasingly important, to the point that it is now, in the era of digitalisation, crucial to information protection. In this context, information environment analysis (also known as IEA) is very important, comprising data identification, analysis, verification, and interpretation in a changing environment. This showcases that determining the sources of information and their credibility are important undertakings when navigating the cyberspace.

This is especially important if we consider that many decisions can be made based on the acquired information, and that these decisions always accompany consequences. For example, in areas in which information use can translate to either life or death situations, such as in security management, crisis management, and warfare, the cruciality of reliable information is indisputable. This is because information reliability in these settings, which tend to be under constant time pressure, translate into right decisions, saving lives, securing health, and upholding property. In contrast, a lack of information credibility might have irreversible negative effects, such as country destabilisation.[11]

Following this rationale, discussions surrounding the information environment should also touch upon cybersecurity. The importance and power of information should be thoroughly emphasised in the modern world, where information is ubiquitous and of great importance in all areas of life. There is also the recent advent of the Internet, which enabled information to spread easily, instantly, and unlimitedly. In general, information should be treated as an abstract object that can be saved in an encoded format (on information media), transmitted, processed using computer programs, and used to control devices. It is also important to distinguish, in information environments, between an information system and an information technology (IT) system. Information systems feature multilevel structures designed to process input and output information, whereas IT systems refer to the separate,

8 Marczyk, 2018, pp. 59–60; based on European Union Agency for Cybersecurity, 2021.
9 Based on Wasiuta and Klepk, 2019.
10 Cendrowski, 2020.
11 Based on *Analiza ryzyka w obszarze cyberbezpieczeństwa – jakie jest jej znaczenie?* [Risk analysis in the area of cybersecurity – what is its importance?], no date.

computerised parts of information systems, including computers, data storage devices, software, human resources, and knowledge bases.

These descriptions also bring to the fore the concept of IT system security, referring to all activities focused on securing data stored on devices and disabling their accessibility to unauthorised people. Moreover, the concept of information security is defined as 'the desired level of protection of necessary information resources, technologies for their creation and use, as well as the rights of business entities', meaning that such security focuses on assuring that the information system will uphold its stable functioning under all conditions, both at the international and national levels. Each system processes specific types of data, and the main threats to information systems include human errors, crises (i.e. accordingly, additional information systems should be located remotely to reduce the risk of failure), equipment damage and failures (i.e. which can be dealt with by creating backup copies), and planned threats (i.e. avoiding such threats requires the installation of antivirus programs).

Network security depends on several factors, which are generally illustrated in the Cyberspace Security Model across its three pillars, which are[12] (a) confidentiality, which refers to data confidentiality and privacy; (b) inviolability/integrity, which refers to data integrity and system integrity; (c) availability.

2. Evolution of cyberattacks and incidents – case studies

Over the years, there have been many cyberattacks and incidents targeting different systems. The first appeared in 1971 and was a test, but cyberattacks began to take different forms and become increasingly aggressive over time, focusing on specific intentions. They evolved annually until they eventually became war weapons. This section explores the development of cyberattacks from their very beginning, key cases, as well as procedures to be followed in the event of this type of attack. Regarding procedures, it is important to emphasise that they should be aimed at preparing for cyberattacks through planned actions, preventing them, and restoring the status before attack occurrence. These procedures must also be developed considering the individual needs of specific entities, along with the guidelines and recommendations of security entities.

There is a wide catalogue of cyberattacks that occurred in the beginnings of this phenomenon, the most popular and important of which include the following: (a) the "Creeper" virus, (b) the Elk Cloner virus for Apple II, (c) PC virus, (d) Morris virus, (e) the attack on Microsoft, (f) DDoS attacks during the Y2K Crisis, (g) the

12 *Triada CIA – Podstawowe Spojrzenie Na Bezpieczeństwo Informacji* [The CIA Triad – A Basic View of Information Security], 2021.

cyberattacks on Estonia, (h) the Stuxnet attack, (i) the ransomware attack on Target, (j) the WannaCry attack, (k) the SolarWinds attack.

The "Creeper" virus appeared in 1971[13] in the United States of America, and was the first virus to appear on the Internet. Its creator was Bobs Thomas, an employee of a technology company. Its appearance initiated discussions on malware and cybersecurity, and it is because of this virus that terms such as virus, malware, and cybersecurity are now used worldwide. The virus infected computers with the TENEX operating system and that used the ARPANET network. This network was built by the United States Department of Defense as a research experiment, and marked the beginning of the modern Internet. The "Creeper" should be treated as a "program" virus and its activity was not aimed at harming, but only at spreading in the ARPANET network. Its appearance in the operating system was marked by the display of the message 'I'm the creeper, catch me if you can!' The infections with the "Creeper" then lead to the creation of the "Reaper" program, created to remove this virus from infected systems. This incident became the basis for work on computer security standards; importantly, at that time, there were not many options available for protecting a system against this type of virus, and awareness of this phenomenon was only starting to arise.

Regarding the management of this virus in case it infects a system, the following steps should be followed: (a) isolate the system from others to prevent its spread, (b) analyse the behaviour of the virus to develop effective removal tools and strategies, and (c) manually remove it from the infected systems. Importantly, the creation of this virus gave rise to the "Reaper" program, which in turn led to discussions about viruses, malware, and cybersecurity. This entails that the "Creeper" virus gave stakeholders impetus to start developing and discussing Internet security rules, the first antivirus tools, and operating system security and updating.

The Elk Cloner virus appeared in 1982[14] in the United States of America and was one of the first computer viruses to appear on Apple II computers. Its creator, Rich Skrenta, was a teenage student at the University of Illinois. The goal with the Elk Cloner virus was not to create danger but to raise awareness about viruses and their ability to spread on computers. This virus did not cause any loss or damage, and but rather displayed a humorous message warning about its capabilities when launched.

Regarding the management of this virus in case it infects a system, the following steps should be followed: (a) isolate the system isolation (i.e. floppy disks should not be used on other computers); (b) scan floppy disks; (c) create and use backups; (d) increase user awareness (i.e. educate the public about IT security and applying rules for using floppy disks of unknown origin); (e) update software.

13 Encyclopedia by Kaspersky, no date; Thomson and Nichols, 2009.

14 Sarkar, 2023; Thomson and Nichols, 2009; *Elk Cloner. La cápsula del tiempo* [Elk Cloner. The Time Capsule], 2009.

The first PC virus appeared back in 1986,[15] Which was also a breakthrough year for viruses. The "PC" (Brain) virus was one of the most harmful ones, and its attacks were focused on the MS-DOS system, which was still used on PCs and mostly in business environments. It was created by the Pakistani programmers Basita and Amjad Farooga. The actions of this virus were much more advanced than those of the two aforementioned viruses, as it infected sectors of hard drives and led the computer to boot with the infected code instead of the original boot. That is, the virus took over control over the booting process, launching the Brain program simultaneously to the original boot every time a computer was booted. Despite the complexity of the operation of the virus, it is did not incorporate any type of intent, such as stealing data or information, but rather was experimental. The virus creators actually included their data, such as telephone number, address, and information about the infection, in the computer code. Despite the lack of malicious intent, this still configured the first malware threat in the world, and it is important to note that computers at the time of the malware's creation were relatively small in scale.

Regarding the management of this virus in case it infects a system, the following steps should be followed: (a) isolate the infected system (i.e. cut the computer off from the network); (b) check the computer's data (i.e. the user should check for data corruption on the hard drive); (c) analyse the code and its operation; (d) remove the virus manually; (e) contact the creators (i.e. thanks to the personal data included in the message of the virus); (f) alert the community.

The Morris virus appeared in 1988,[16] created by Robert Tappan Morris, who studied at Cornell University. This virus was assessed as having significant capabilities to attack targets on the Internet, and its purpose was to spread across computer networks to study the rules governing the spread and structure of the Internet. Thus, this program was still not aimed at data theft or information destruction. The attacks of the Morris virus spread worldwide across numerous computer stations owing to poorly secured passwords, email program vulnerabilities, and finger program errors. The consequences of these attacks were the paralysis of many systems and the infection of computers, which experienced difficulties in booting. Owing to such activities, society has become more aware of the importance of IT security strategies, and many system protection tools and strategies have been developed.

Regarding the management of this virus in case it infects a system, the following steps should be followed: (a) isolate the system (i.e. disconnect the computer from the network); (b) change passwords (i.e. especially accounts with weak passwords); (c) update and secure the software (i.e. to prevent vulnerabilities in programs, including Internet emails); (d) perform virus analysis and removal (i.e. including manual removal of infected files and system cleaning); (e) report the incident (i.e. to appropriate institutions or Internet service providers).

15 Thomson and Nichols, 2009.

16 *The Morris Worm: 30 Years Since First Major Attack on the Internet*, 2018.

The attack on Microsoft[17] took place in 1995 by Kevin Mitnick, a hacker who broke into Microsoft's computer systems, configuring the first serious hacker attack in the context of computer security. The hacker was subsequently found and arrested in the same year. In fact, during the 1980s and 1990s, Mitnick also hacked into the computers of various other companies. After his arrest, the talented criminal decided to change the direction of his actions and started engaging in legal work and computer security, eventually becoming an expert in the field.

The DDoS attacks during the Y2K Crisis took place in 2000,[18] with the literature on the subject focusing mainly on problems related to the transition of computers from a two-digit year to a four-digit year during the Y2K Crisis. This was a problem related to time counting, and during this specific period, we still did not have advanced tools to monitor and take action to detect these incidents, nor awareness in this area.

The cyberattacks on Estonia occurred in 2007,[19] and were the first of their kind. It was the result of political disagreements between Russia and Estonia on from the relocation of a Soviet monument located in Tallinn, Estonia. The DoS attacks were then organised and carried out by the Russian organisation "Nasi" and independent Russian hackers. An important context is that Estonia had switched to making payments only via an electronic system and withdrawn traditional money from circulation in the country right before the cyberattacks, meaning that the cyberattacks could easily destabilise the functioning of the state. The perpetrators attacked sectors of the state government such as the following: (a) financial sector, causing people to be unable to perform financial operations and access bank accounts; (b) governmental sector, causing the blocking of the websites of the parliament, Ministries of defence and justice, political parties, uniformed services, and education; (c) defence sector, blocking access to the websites of the Ministry of Defence and forcing the Estonian defence system to close some foreign connections; (d) tourist sector, as Estonian people traveling abroad could not access their bank accounts, and foreign offices had their booking systems for trips to Estonia blocked; (e) media sector, as it was not possible to post information on websites nor to modify websites; (f) the infrastructure sector.

The consequences of these attacks were cutting off Estonia from the rest of the world, blocking the flow of financial resources, manipulating the contents posted on government websites, and paralysing services. Estonians could not lead their daily lives normally, leading to chaos and tension in the national society. Therefore, this attack showed, for the first time, and as Estonian President Toomas Hendrik pointed out live in his statement, that 'Nowadays, infrastructure can be destroyed online, it does not require missiles'. Despite the whole dire situation, Estonia did not report

17 *Microsoft Faces Blistering Attack On-Line Leaders Say Software Giant Wants To Extend Its Dominance*, 1995.

18 *Y2K bug*, no date.

19 *A look at Estonia's cyber attack in 2007*, 2009.

on major financial losses owing to the events. The response to this series of issues was the development, in Estonia, of robust defence capabilities to respond to this type of threat and attack. In fact, the literature on this subject indicates that Estonia has become a pioneer in cybersecurity, and has significantly increased its financial outlays on resources and well-qualified experts on cybersecurity. Internationally, the incident drew the world's attention to this new, very real threat, leading to an increased awareness of the need to immediately strengthen defence systems, both at the technical and political levels, in the cyberspace.

Regarding the management procedures necessary in case of such cyberattacks, the following steps should be followed: (a) activate the cyberspace defence system (i.e. identify the origin, type, and purpose of the attackers) and improve security (i.e. after analysis, weak points should be checked actions taken to seal them); (b) government entities should provide an immediate response (i.e. resource security should be established, and the targets of the attacks and potential consequences should be determined); (c) establish crisis communication (i.e. a safe communication channel should be established for securing cooperation and communication between the government, society, the media, and spokespeople for security entities); (d) promote international cooperation (i.e. international partners and allies should be informed about the attack and cooperation with the Security Agencies of other countries should be confirmed); (e) increase defence capabilities (i.e. the institution's/state's defence strategy should be developed, and financial expenditure on the development of cybersecurity and common action strategies should be increased).

The Stuxnet attack occurred in 2010,[20] with the Stuxnet malware having been created as part of Operation Olympic Games, which aimed to attack Iran's nuclear program. It was part of the operation that attacked the Supervisory Control and Data Acquisition (SCADA) systems, entered false data into these systems, and took control of the industrial equipment of Iran. One of the first iterations of this malware was used to spy on and reprogram the industrial installations associated with Iran's nuclear program. It used zero-day exploits, that is, unknown errors in the software. According to both the literature on the subject and the experts interviewed, this was the first cyberattack on a critical global infrastructure, and led 2,000 of the 8,700 centrifuges used by Iran to be replaced. No country or organisation has ever admitted to having been part of this operation, but suspicion has been directed towards the intelligence agencies in the United States of America and Israel. Iran's lost credibility in the world stage in the context of its nuclear program, owing to this attack. Therefore, the Stuxnet allowed for an advanced attack that disrupted the operation of industrial control systems, led countries and organisations worldwide to intensify their work on IT security, and sparked international discussions on ethics and the consequences of cyberattacks on critical infrastructure.

Regarding the management procedures necessary in case of such cyberattacks, the following steps should be followed: (a) analyse the malware; (b) restore the system

20 Falliere, O Murchu and Chien, 2010.

using a backup; (c) update the system; (d) monitor network flows; (e) strengthen security; (f) cooperate with cybersecurity experts; (g) promote employee education.

The ransomware attack on Target occurred in 2013[21] in the United States of America. Despite the name commonly afforded to the event, this was an incident and not a ransomware attack. Specifically, hackers managed to illegally access the computer systems of Target, a large retail company in the United States of America, leading to the compromise of the financial and personal data of over 40 million customers. The incident was focused extracting information about the company's payment systems and using the customer data for making other unauthorised payment transactions.

Regarding the management procedures necessary in case of such attacks, the following steps should be followed: (a) isolate the system; (b) report the incident; (c) assess the scope of the incident; (d) identify the incident; (e) stop the attack; (f) restore the system using a backup; (g) analyse payments made during the event; (h) analyse the causes of the incident; (i) implement preventive measures; (j) inform the affected parties; (k) promote employee education.

The WannaCry attack occurred in 2017,[22] and was estimated to be the largest attack of this type in history, affecting nearly 300,000 computers in over 150 countries. This malicious ransomware encrypts files on infected computers and then demands a ransom in the form of Bitcoin cryptocurrency for victims to receive the password to decrypt the files. This attack was characterised by the use of an exploit, called "EternalBlue", focused on vulnerabilities in the Windows operating system, which not only spread quickly but also infected various computers on the same network. This attack was performed at the global scale, affected many countries, and was targeted at government entities that focused on guaranteeing national security. It is described that this exploit had been previously created by the intelligence agency at the United States of America. The consequences of the attack included the closure of very important institutions for various countries worldwide, such as those described herein: the British health service, national railways and banks in Russia and over 1,000 computers in the Ministry of Interior of Russia, Indian airlines, universities in Italy, and various companies (e.g. MegaFon, EMERCOM, Nissan Telefonica, Deutsche Bahn), hospitals, and units in public institutions. Thus, the attack destabilised and disrupted state functioning, and resulted in enormous economic and social costs, as both entrepreneurs and state institutions were forced to pay a ransom in exchange for their own data.

The attack gave further fuel for the expansion of discussions surrounding cybersecurity, and led to the onset of digital security analyses involving not only threats but also management and liability issues. The theft by hackers of a tool originally created by an intelligence agency made us realise that this type of tool may eventually fall into the hands of organised criminal groups, rendering it important for

21 Gopal, 2022.
22 *What is WannaCry ransomware?*, no date.

security stakeholders to also have access to able to destroy such products. This attack also urged institutions to emphasise the development and introduction of procedures to counteract such negative phenomena, such as by promoting the regular updating of operating systems, the implementation of effective solutions (e.g. firewalls, antivirus programs), and greater financial and material expenditure on cybersecurity.

Regarding the management procedures necessary in case of such cyberattacks, the following steps should be followed: (a) isolate the system; (b) stop network traffic; (c) inform security entities; (d) inform the staff; (e) launch a procedure in the event of a ransomware attack; (f) report the incident to security units; (g) determine the source of the attack; (h) identify suspicious activity on the network; (i) check for system updates; (j) activate additional security measures, such as firewall and antivirus programs; (k) inform and warn the public; (l) backup security; (m) restore systems to pre-attack levels; (n) monitor cryptocurrency payments; (o) analyse the attack; (p) prepare and present a report; (r) promote staff education; (s) educate the public; (t) implement the developed solutions; (u) cooperate with security entities.

The SolarWinds attack took place in 2020,[23] and was deemed one of the most advanced cyberattacks to date. It targeted the SolarWinds company, which focuses on software for monitoring networks and IT systems, aiming to break into their IT systems. Access to the systems of the clients of the company was possible by introducing a malicious software update code. The attack was aimed at obtaining confidential data from government institutions, technology companies, and other industrial sectors, indicating that the operation had espionage purposes. This incident gave way to the awareness of the leaky conditions of supply chain systems and their vulnerabilities to attacks, causing companies using this type of supply chain management system to run detailed analyses of their internal security strategies. So far, the focus of these attacks has been on internal issues and not on the product delivery process.

Regarding the management procedures necessary in case of such cyberattacks, the following steps should be followed: (a) disconnect the systems; (b) notify security entities; (c) alert staff; (d) secure resources; (e) analyse losses; (f) analyse the attack source; (g) change passwords and keys; (h) check backups; (i) implement system updates; (j) monitor the situation; (k) counteract further attacks; (l) update software and use anti-virus programs and firewalls; (m) promote staff education; (n) promote public education; (o) cooperate with security entities; (p) prepare a report after analysing the situation; (r) verify procedures; (s) update procedures; (t) implement procedures; (u) conduct risk analysis.

23 Oladimeji and Kerner, 2023.

3. Cyberattack types

Based on many years of experience related to computer development and cyberattacks, stakeholders have created several categories of cyberattacks, which continue to evolve and expand to this very day and as reality changes. According to Grzelak and Liedl, the most common threats in the cyberspace are the following:[24] (a) attacks using malicious software (e.g. malware, viruses, and worms); (b) identity theft; (c) theft (extortion) and data modification or destruction; (d) blockage of service access (e.g. mail bombs, DoS, and DDoS[19]); (e) spam (i.e. unwanted or unnecessary electronic messages); (f) social engineering attacks (e.g. obtaining confidential information by impersonating a trustworthy person or institution, also known as phishing).

Threat identification is at the foundation of prevention efforts against cyberattacks, enabling institutions to prepare for these eventualities through the effective implementation of protective measures and safety procedures. Therefore, a Catalogue of Information Security Threats is provided in this section, listing threats to information security (e.g. cyberattacks, threats caused by human activity, security vulnerabilities, software errors) and describing the risks that they pose regarding loss of data confidentiality, integrity, and availability.

The catalogue comprise cyberattacks related to the following, although it is important to emphasise that new types of cyberattacks are constantly being evaluated and are likely to enter future catalogues: (a) malware, (b) phishing, (c) ransomware, (d) DDoS attacks, (e) attacks on industrial control systems (ICS) and SCADA systems, (f) attacks on web applications, (g) attacks on wireless networks, (h) attacks on Internet of Things (IoT) systems, (i) email attacks, (j) password and authentication attacks, (l) attacks on critical infrastructure, (m) attacks on mobile applications, (n) attacks on blockchain and cryptocurrencies, (o) system hacking, (p) data disclosure, (r) internal threats, and (s) network security incidents.

Malware (e.g. viruses, Trojans, spywares, and computer worms): (a) the virus is a malicious code that attacks healthy files, infects programs, and can be compared to a biological virus that needs a host for replication; (b) computer worms are very similar to computer viruses (except that they do not need a "host for replication" and instead can self-replicate), generally operate on the Internet, and can be transferred via portable memory; (c) Trojans, also known as Trojan horses, work under the guise of a useful application and have a wide scope applications, being useful for deleting specific system files, intercepting information entered via the keyboard, or using the computer to send spam.[25]

Phishing involves attempts at obtaining confidential personal information by using the guise of a trusted person or a credible institution. A characteristic of this activity is the need for the quick provision of information, which leads phishing procedures to induce specific, quick actions by the victim for the computer to be

24 Grzelak and Liedel, 2012, p. 131.
25 Nowak-Brzezińska, 2017, p. 19.

infected with a Trojan or spyware. Phishing can take the form of a message sent via email or an instant messenger, persuading the user to click on a link containing a fake organisational website. This applies mainly to banks. This type of cyberattack aims at collecting personal data and persuading people to download Trojan software. Perpetrators make every effort to ensure that the situation generated is as credible as possible.[26]

The ransomware is a type of malware aimed at infecting and/or blocking a computer system by stealing and encrypting selected files. It is a type of fraud aimed at extorting funds from victims in exchange for the lost data. Ransomwares hence not only encrypt the data but also steal it, and tend to be used especially on attempts at acquiring classified, sensitive datasets that would lead to embarrassment, especially for public sector representatives, in case disclosed. After a ransomware attack is successful, data recovery is only possible using a decryption key, for which the perpetrators demand a ransom.[27]

DoS and DDoS attacks[28] involve blocking access to the service by taking up all free resources (e.g. flooding a service with excessive amounts of data or queries), leading to system overload and suspension.

Attacks on ICS and SCADA systems focus on critical infrastructure violation and are made viable through the exploitation of security vulnerabilities that enable system manipulation. This practice disrupts production, destroys equipment, and causes failures, leading to serious consequences such as power outages and physical damage to infrastructure. Protection against this type of attacks is possible by using advanced security solutions, including network monitoring, system segmentation, and regular security updates.[29]

Attacks on web applications are attempts at gaining unauthorised access to, modifying, or destroying applications available online. Methods such as SQL injection, cross-site scripting (also known as XSS), and cross-site request forgery (also known as CSRF) are used to break app security and gain access to data. Related activities are often aimed at stealing information, changing the application's functions, or infecting it with malware. Effective protection against these attacks requires constant application security monitoring, penetration testing, and security measure implementation (e.g. application firewalls and two-factor authentication mechanisms).[30]

Attacks on wireless networks target radio communication infrastructure, and the most frequently used methods are man-in-the-middle attacks, de-authentication, and breaking encryption keys. The goal of such attacks is often to take control of the network, access data, or eavesdrop on communications, and they take advantage of gaps in security protocols such as WPA2. The use of strong encryption methods,

26 Nowak-Brzezińska, 2017, pp. 21–22.
27 *Poradnik ransomware* [Guide ransomware], no date.
28 Based on European Court of Auditors, 2019; *Cybersecurity: how the EU tackles cyber threats*, no date.
29 Liderman, 2020, p. 6.
30 *Ataki na aplikacje webowe. Jakie są najczęstsze i jak się bronić?* [Attacks on web applications. What are the most common ones and how to defend yourself?], 2022.

constant network traffic monitoring, and constant device and system updates can protect against such attacks to some extent.[31]

Attacks on IoT systems focus on devices and networks integrated with IoT, and attackers exploit vulnerabilities in devices such as cameras, sensors, and home devices in attempts to gain unauthorised access or control over, or even to steal, data. These types of attacks often relate to espionage, disrupting device functions and violating users' privacy. Methods of protection against such attacks include strong authentication mechanisms, data encryption, software updates, and network activity monitoring.[32]

Email attacks are used by cybercriminals and customarily involve the use false links inside email contents or attachments with the purposes of data theft, system infection, privacy breach, among others. Protection against this type of attack is possible through increasing user awareness, knowledge about cyberattack mechanisms, and making use of antivirus programs.[33]

Password and authentication attacks involve breaking access security mechanisms. The methods used are often brute force, dictionaries, and data leaks to test the same authentication data in other services. Phishing and keyloggers form additional threats used for conducting fraud and sending malware for the purpose of intercepting confidential information. Defence against this type of attack is possible by using strong passwords, two-step verification procedures, monitoring login activity, changing passwords, knowledge of how this type of cyberattack works, and having the ability to react in the event of an attack.[34]

Attacks on critical infrastructure focus on compromising the systems and resources necessary for the functioning of society and state security, including key industrial sectors such as energy, transport, communication. Methods include cyberattacks on industrial control systems, sabotage, and terrorist acts, and examples of consequences include energy supply disruptions, transport disruptions, and communication system failures. The security of critical infrastructure requires complex defence strategies, robust cybersecurity measures, and international cooperation.[35]

Attacks on mobile applications encompass methods such as reverse engineering, code injection, and man-in-the-middle attacks, and tend to lead to personal data theft, unauthorised access to private information, and malware infections. These attacks are possible due to security vulnerabilities in the applications or operating systems. Actions to counteract these attacks include programming practices, data

31 Waraksa, Żurek and Niski, 2011, p. 88.

32 *Internet Rzeczy, ochrona prywatności a bezpieczeństwo danych* [Internet of Things, privacy protection and data security], 2021.

33 *Phishing: co to jest?* [What is phishing?], no date.

34 *Czym jest uwierzytelnianie dwuskładnikowe, uwierzytelnianie dwuetapowe?* [What is two-factor authentication, two-step authentication?], 2023.

35 Barć, 2021, p. 7.

encryption, updates, and activity monitoring to minimise the risk of attacks on mobile applications.[36]

Attacks on blockchain and cryptocurrencies attempt to violate the integrity and security of these technologies, with attackers using various methods (e.g. double spending, 51% attack, and Sybil attack) to introduce disinformation, disorganisation, take control of the network, manipulate transactions, promote financial fraud, and fund theft. Additional threats include smart contract vulnerabilities, phishing among cryptocurrency users, and attacks on stock exchanges. Security against such attacks is achieved through the use of solid security protocols, code audits, user education, and blockchain network activity monitoring.[37]

System hacking refers to the illegal process of accessing computer systems to manipulate or breach them, steal confidential information, change system settings, introduce malware, crack passwords, solve authentication mechanisms, and using exploits. It often involves methods like security vulnerability exploitation, buffer overflow attacks, and gaining illegal access to data. The effects of system hacking can be serious, with consequences ranging from loss of privacy to organisational operation disruption. Effective protection involves developing appropriate security measures, system updates, and network activity monitoring.[38]

Data disclosure encompasses the accidental or illegal disclosure of confidential or private information (e.g. personal and customer data or confidential documents) to the public, with major reasons being security system errors, data leaks, or intentional attacks. The consequences of data disclosure include identity theft, privacy breaches, and financial losses. Counteracting this type of incident is possible by using strong security measures, monitoring data, and complying with appropriate regulations regarding personal data protection.[39]

Internal threats are generated intentionally (e.g. data theft, sabotage, and corporate crime) or unintentionally (e.g. error or lack of employee knowledge) by company employees with access to specific resources or security measures. These actions can result in leaks and loss of data or other damages. Countermeasures include regular employee training, raising awareness of risks, and using modern technological security measures.[40]

A network security incident is an unwanted or illegal incident that affects data integrity, availability, or confidentiality on a computer network, the consequences of which may include attacks, data leaks, loss of access to the system, system failures, financial losses, loss of company reputation, and privacy invasion. Effective

36 Niewiadomska-Szynkiewicz and Litka, 2023, pp. 96–99.

37 *Blockchain – aspekty techhnologiczne oraz przykłady zastowań* [Blockchain – technological aspects and examples of applications], no date.

38 Pala, 2015, pp. 115–116.

39 *Naruszenie ochrony danych przez podmiot przetwarzający. Czym jest i jak postępować, kiedy do niego dojdzie* [Data protection breach by the processor. What is it and what to do when it happens], 2021.

40 European Union Agency for Cybersecurity, 2020a.

countermeasures include applying a network security policy, monitoring network traffic, and increasing employee awareness.[41]

A catalogue of information security threats should be created, made open for all stakeholders, and be constantly updated, with especial attention to areas that can destabilise state functioning in case of disruption, namely: (a) data and privacy attacks, (b) attacks on government institutions and enterprises, (c) on delivery companies, (d) on social media, and (e) on data processing systems.

Data and privacy attacks are aimed primarily at access, theft, and manipulation of business and/or private databases, with customary methods being phishing, malware, and security vulnerability exploitation. The consequences of these attacks are financial losses and the violation of rights at the personal and/or business level.[42]

Attacks on government institutions and enterprises often attempt to violate their structures or penetrate them, and tend to involve organised criminal activities focused on destabilising entities that constitute the state security system and/or the economic sector. The methods used for this type of activity include cyber intrusions, phishing, and ransomware. Acquiring governmental data often associates with ransom requests, obtention of confidential information to be passed on for hostile entities or countries, and system operation disruption. Attacks of this type are particularly dangerous and therefore require complex security strategies, constant monitoring, employee education, and intersectoral cooperation for a coordinated response to possible threats.[43]

Attacks on delivery companies aim at disrupting transportation and delivery operations. Attackers who want to disrupt the supply chain may use various strategies, such as cyber intrusions, ransomware, or fake advertisements. Targets may include logistical data, shipment data, and ransom demands for the release of blocked shipments. The consequences of this type of attacks are supply interruptions, the consequential financial losses, and data losses. Protection against this type of attack requires the use of IT security measures, the monitoring of logistics traffic, and educating employees on cybersecurity.

Attacks on social media are often performed through hacking, phishing, and DDoS attacks, and tend to aim at disrupting activities or taking control of social media platforms. Successful attacks may then lead to the publishing of false information, and the creation of false scenarios that then discredit people and/or organisations. The main goals tend to be information manipulation, disinformation,

41 Pacut, 2023.

42 Zhu et al., 2018.

43 Based on (2024) List fifteen the largest threats. [Online]. Available at: https://www.enisa.europa.eu/publications/report-files/ETL-translations/pl/etl2020-enisa-list-of-top-15-threats-ebook-en-pl.pdf and (2024) ENISA Threat Landscape 2021. [Online]. Available at: https://www.enisa.europa.eu/publications/etl-2021/enisa-threat-landscape-2021-2022-final_pl.pdf (Accessed: 10 January 2024) and (2024) Vademecum of information security. [Online]. Available at: https://vademecumbezpieczenstwainformacyjnego.uken.krakow.pl/ (Accessed: 06 January 2024), p. 22.

industrial espionage, and achieving financial gains through data theft or blackmailing. These attacks affect user security, information credibility (e.g. especially of public figures), and the trust and credibility of companies. Protection against them requires effective cybersecurity measures and the monitoring of online activity and user education.

Attacks on data processing systems are aimed at disrupting the operation of infrastructure that processes information or obtaining the related data. The techniques used security vulnerability exploitation, SQL injection, and malware attacks. Common consequences involve data confidentiality losses, operational system disruptions, and financial losses. Prevention measures include the implementation of effective safeguards, monitoring activity, regular updates, and educating employees about cybersecurity.

4. Major cyberattacks threatening security

Cyberattacks are very dangerous because they do not recognise any territorial boundaries. Examples include the decisions over the attacks being potentially made in places like Moscow, Beijing, or Pyongyang, whereas the operations or cyber activities themselves may use IT networks located anywhere in the world. Cyberattacks can be broadly divided into four categories, as follows:[44] (a) interception, involving attacks against confidentiality; (b) interruption, involving attacks against availability or usability; (c) modification, involving attacks against availability and usability; (d) fabrication, involving attacks against authenticity. Importantly, cyberattack risks exist when there are threats, which in turn are created through cybersecurity vulnerabilities and gaps.

Cybersecurity is a field under development and is characterised by being dynamic. Furthermore, in order to control the emerging phenomenon of cyberattack, many institutions have developed various reports on cyberattacks. To secure data reliability, this study used data presented by the European Union Agency for Cybersecurity (ENISA) from 2022.[45]

44 Based on European Union Agency for Cybersecurity, 2020b; European Union Agency for Cybersecurity, 2021; Cendrowski, 2020, p. 22.

45 *European Union Agency for Cybersecurity (ENISA)*, no date.

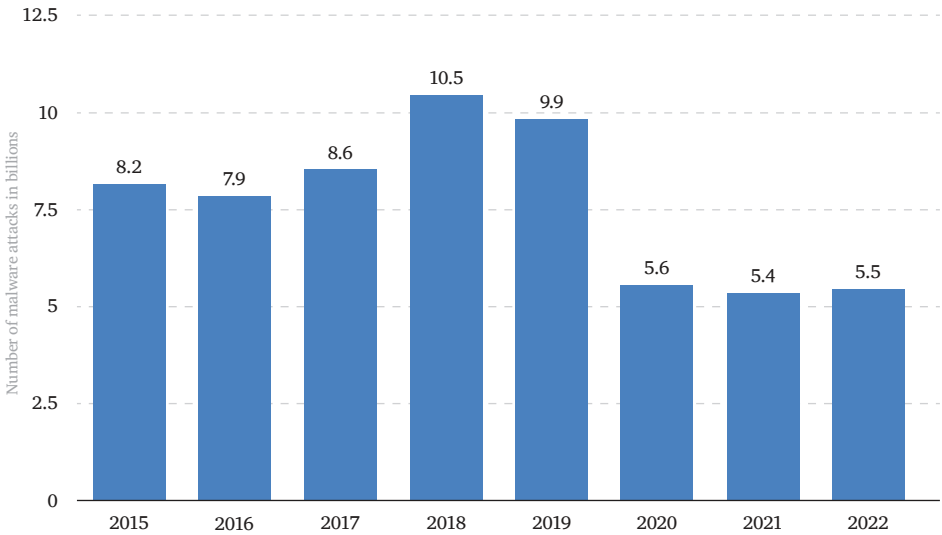
Figure 1.[46]

There are many threats on the Internet, with both experts and the ENISA reporting[47] the following as major ones. First, ransomwares, which are the most disturbing because hackers are increasingly using more sophisticated and aggressive techniques to acquire ransom for restoring access to accounts and data. The average ransom value has more than doubled in just one year (2019, EUR 71,000; 2020, EUR 150,000), and 2021 saw a 57-fold increase in ransom requests compared to 2015, reaching a value of EUR 18 billion. Second, malwares, which target systems and include spywares, Trojan horses, viruses, and worms. Statistics and commentaries are presented below the chart.

46 *ENISA Threat Landscape 2022*. [Online]. Available at: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022, p. 10 (Accessed: 10 February 2024).
47 European Union Agency for Cybersecurity, 2021.

Figure 2.[48]

Annual number of malware attacks worldwide from 2015 to 2022 (in billions)



Source
SonicWall
© Statista 2023

In 2022, the number of malware attacks worldwide reached 5.5 billion (an increase of 2% compared to the previous year), while 2018 saw the highest number of malware attacks in recent years, when 10.5 billion such attacks were reported worldwide.[49] In the same year, malwares were blocked more than 205 million times, and a popular type of malware targeted mainly the Asia-Pacific region. In general, websites are the most common vector for malware attacks, and recent industry data has shown that malware attacks were often received via exe files.[50] A decline in this threat was observed only during the COVID-19 pandemic.

Moreover, the emergence of the so-called cryptojacking activities, which aim at using the victim's computer equipment without his/her knowledge to steal cryptocurrency, resulted in a significant increase in the number of cyberattacks. For example, considering only the first half of 2022, there was a four-time increase in attack numbers compared with the numbers in the previous four years.[51]

48 *Annual Number of Malware Attacks Worldwide from 2015 to 2022.* [Online]. Available at: https://www.statista.com/statistics/873097/malware-attacks-per-year-worldwide/ (Accessed: 10 January 2024).
49 Petrosyan, 2024.
50 Ibid.; European Court of Auditors, 2019.
51 Petrosyan, 2024.

There are also threats related to social engineering, which includes persuading people to open documents and visit websites that unknowingly make their own systems and services available for access to others. These initiatives involve both intentional and unintentional human behaviours, and the most frequently used techniques are phishing (through emails) and smishing (through SMS). In Africa, Europe, and the Middle East, approximately 60%[52] of network security breaches made possible through social engineering were reported. The hackers mainly impersonated financial and technology sector specialists to attack cryptocurrency exchanges and their owners.

Other threats include data breaches, with 82% of the recorded data security breaches being associated with human activity, mainly with human errors. These threats can be divided into (a) data security breaches (intentional actions) and (b) leaks (unintentional actions). The main reasons for data breaches were the desire to obtain funds at 90% and espionage at (10%).

Accessibility threats should also be mentioned, including (a) DDoS attacks, which are very complex, encompass a wide range of activities, are targeted at mobile networks, have been often used in the Russian–Ukrainian war, and also take place on the network. These types of attacks were also used against websites containing information about COVID-19 vaccinations. Another threat relates to (b) efforts at destroying Internet accessibility, with one example being the Russian–Ukrainian war, where 15% of the Internet infrastructure in Ukraine has been destroyed[53] since its onset. Censorship has also been imposed on social media and news portals.

Disinformation, referring to the use of the mass media to transmit false information in order to cause fear, uncertainty, and chaos in society and among nations, is another a significant threat. This method has been used by Russia in relation to information regarding the course of their invasion in Ukraine. The use of wide-scale disinformation methods is also becoming more common with the advent of artificial intelligence, deepfake technology (i.e. creating false recordings, images, and sounds indistinguishable from the original ones), bots (i.e. capable of pretending to be people), and threats to the supply chain (i.e. to obtain customer data and to attack the supplier and the recipient; these attacks are becoming increasingly easier owing to the different number of suppliers).

4.1. Sectors of life at risk

Cyberattacks affect public sectors and people's lives at varying intensities. Based on research conducted by the ENISA regarding reported cyberattacks from July 2021 to June 2022, there are seven areas where these attacks occurred most frequently, which are the following:[54] (a) public administration/government (24%), (b) digital

52 *Cyberbezpieczeństwo: główne i nowe zagrożenia* [Cybersecurity: main and new threats], 2022.
53 *Cyberbezpieczeństwo: główne i nowe zagrożenia* [Cybersecurity: main and new threats], 2022.
54 Petrosyan, 2024.

service providers (13%), (c) society (12%), (d) services (12%), (e) finance/banking sector (9%), (f) healthcare (7%), (g) and other areas (23%).

4.2. Most frequently attacked industries

In 2022, the education sector was heavily attacked by malwares, with an average of 2,314 attacks per week and more than five million malware attacks. This sector was followed by government and military organisations and then healthcare units.[55]

4.3. Costs

These cyberattacks are estimated to have led to huge financial losses, albeit the losses and damages are not restricted to finance and instead extend to the personal and social levels. Based on the data presented in the European Union (EU) Report, the following costs were incurred.[56] First, it was for the economy, as small and medium-sized enterprises in the EU do not feel safe in the EU digital market, and this is despite its design to ensure confidence and security on the Internet. This lack of sense of safety results from the fact that, by the end of 2021, 28% of the recorded cyberattacks in the EU had targeted small and medium-sized enterprises, and this number is constantly growing. Second, for democracy, as disinformation causes trust losses in society and leads to divisions. Third, for peace and security, as data manipulation (e.g. through the use of bots and disinformation activities) affects the democratic resilience of countries and introduces chaos and tensions. According to ENISA data, during the Russian–Ukrainian war, cyberattacks were carried out in parallel with conventional fighting methods in an attempt to disrupt the capabilities of government agencies and entities and lead to trust losses among the public, especially in political leadership. Fourth, for essential services and critical sectors such as health, finance, transport, energy, water, and gas, which are dependent on digital technology and devices connected to different networks. Owing to such dependence, interference in their functioning offers risks to life and health. Hospitals also saw disruptions in their care systems, cancelled/interrupted surgeries, and there were threats to the supply of services. There were also threats associated with the use of smart homes and devices.

55 Petrosyan, 2024.
56 *SMEs and Cybercrime*, 2022.

5. Causes and effects of cyberattacks: A summary

As shown above, the catalogue of cyberattacks contains numerous entries. The table below presents the following types of cyberattacks: malware; phishing; ransomware; DDoS attacks; attacks on industrial control systems; attacks on web applications; attacks on wireless networks; attacks on IoT systems; email attacks; password and authentication attacks; attacks on critical infrastructure; attacks on mobile applications; attacks on blockchain and cryptocurrencies; system hackings; data disclosure; internal threats; network security incidents; data and privacy attacks; attacks on government institutions and enterprises; attacks on delivery companies; attacks on social media; attacks on data processing systems.

Importantly, each cyberattack has specific capabilities and is used for a specific purpose, the reasons for using various types of cyberattacks may sometimes be the same, and the choice of a specific cyberattack depends on the knowledge, skills, and technical capabilities of the perpetrators of cyberattacks. Each form of cyberattack has specific negative consequences that may affect the functioning of the public, families, social groups, the government and, consequently, the state. They can be used to disrupt or destroy many areas important for the state or citizens. The table below shows cyberattack types, the reasons for their use, and the consequences in all possible areas. Presenting the data in this form allows for comparisons regarding the degree of danger of individual forms of cyberattack.

In summary, the main reasons for using cyberattacks are the desires of perpetrators to achieve financial benefits, destabilise the functioning of the government, enterprises, and competition, and obtain sensitive information from various sectors (e.g. financial, economic, governmental sectors). As a consequence of cyberattacks, chaos, disinformation, and tensions arise among society. All this contributes to the destruction of states from within, making them easy targets for aggressors to attack.

Table 1.

Cyberattack type	Reasons	Consequences
Malware	– trying to earn money – trying to harm a person/ company/country – controlling computers/mobile devices for illegal purposes – taking control of devices to attack other entities	– destruction, acquisition, or deletion of data – spying or controlling computer systems – taking control of devices – computer attacks on other organisations through a victim organisation

Cyberattack type	Reasons	Consequences
Phishing Phishing attack	– extorting confidential personal information – financial fraud	– loss of identity – loss of sensitive data – insults and embarrassments – loss of financial resources – obtaining confidential data – taking over databases – loss of image – cyberstalking – loss of trust (e.g. customers) – destabilisation – loss of market positions
Ransomware	– extorting payment for removing the infection – extorting confidential information	– loss of financial resources – loss of control over devices – taking over databases – obtaining confidential data
DDoS attack	– occupation of system resources (e.g. server, memory, and power) – preventing the functioning of a given service on the Internet – preventing the use of a given Internet domain – attempting to eliminate competition on the market	– loss of customers – loss of image – loss of trust (e.g. customers) – interruptions in the operation of trading systems (financial losses)
Attacks on industrial control systems	– trying to earn money – preventing the operation of a given enterprise – attempting to steal digital data	– breach of trust in the enterprise/organisation – leakage of unfavourable data to the public – sales of digital data – disturbance in the functioning of production processes – disturbance of functioning of the population regarding needs related to activities of daily living
Attacks on web applications	– stealing data (e.g. customers and application users) valuable to hackers	– financial losses – weakening the brand image – loss of user trust – data leakage of sensitive application users – loss of confidential data

Cyberattack type	Reasons	Consequences
Attack on wireless networks	– stealing confidential data for illegal purposes – stealing bank account details – stealing passwords and taking over user accounts on websites	– loss of privacy and data security – loss of financial resources and control over finance on banking websites – leakage of sensitive user data – loss of passwords, accounts, and control over the device and websites
Attacks on IoT systems	– taking control of IoT devices and causing damage to them, or using them in attacks on more targets – spying and blackmailing device users – extorting through access to confidential information	– loss of control over the IoT device – data breach or loss by device users – sensitive data leakages – insulting and embarrassing – cyberstalking – loss of privacy and security
Email attacks	– stealing email accounts to extort funds and/or confidential information – stealing email data	– breach or loss of confidential or sensitive data – financial losses – cyberstalking – disruption of internet operations – loss of passwords, accounts, and control over the device
Password and authentication attacks	– extorting confidential personal information – phishing sensitive data	– loss of passwords, accounts and control over the device and websites – loss of sensitive data – loss of confidential data – insulting and embarrassing – loss of good name

Cyberattack type	Reasons	Consequences
Attacks on critical infrastructure	– disrupting the country's/institution's activities – causing market confusion – stimulating social unrest – loss of trust in government/institutions – spreading disinformation to destabilise the state – weakening of the economy	– disruption of the operation of critical infrastructure systems (e.g. emergency services, healthcare, energy supply, communication and information and communication technology networks, financial, water and food supply, transport, production, and administration) – destabilisation of critical infrastructure key to state security and citizens – destabilising the functioning of state economy – weakening social security – social unrest – insulting, discrediting, and loss of trust
Attacks on mobile applications	– stealing data (e.g. customers and application users) valuable to hackers – stealing bank details – stealing passwords and taking over application accounts	– financial losses – loss of accounts in applications – loss of control over data in the application by the user – cyberstalking – weakening the brand image – loss of user trust – data leakage of sensitive application users – loss of confidential data
Attack on blockchain and cryptocurrencies	– stealing funds – disrupting the financial market – strengthening one cryptocurrency at the expense of the other	– loss of financial resources – leakage of sensitive data – loss of access to financial resources – elimination of competition

Cyberattack type	Reasons	Consequences
System hackings	– gaining access to the system and its resources – obtaining confidential and sensitive data – disrupting the system	– loss of access to the system and its resources – loss of confidential data – loss of sensitive data – breach of confidential data and system availability – insulting and embarrassing – loss of financial resources – taking over databases – destabilisation – loss of market position
Data disclosure	– stealing confidential and sensitive data and databases – stealing funds – stealing bank details	– loss of confidential data – loss of sensitive data – loss of databases – loss of financial resources – insulting and embarrassing – loss of customers – loss of image
Internal threats	– stealing bank details – stealing confidential data – stealing databases	– loss of confidential data – loss of sensitive data – loss of databases – loss of financial resources – destabilisation
Network security incident	– obtaining confidential data – disrupting system integrity	– loss of data confidentiality – loss of financial resources – irregularities in the operation of security systems
Data and privacy attacks	– identity theft – obtaining confidential and sensitive data	– loss of sensitive data – loss of identity – loss of image – taking over databases – insulting and embarrassing – loss of financial resources – cyberstalking

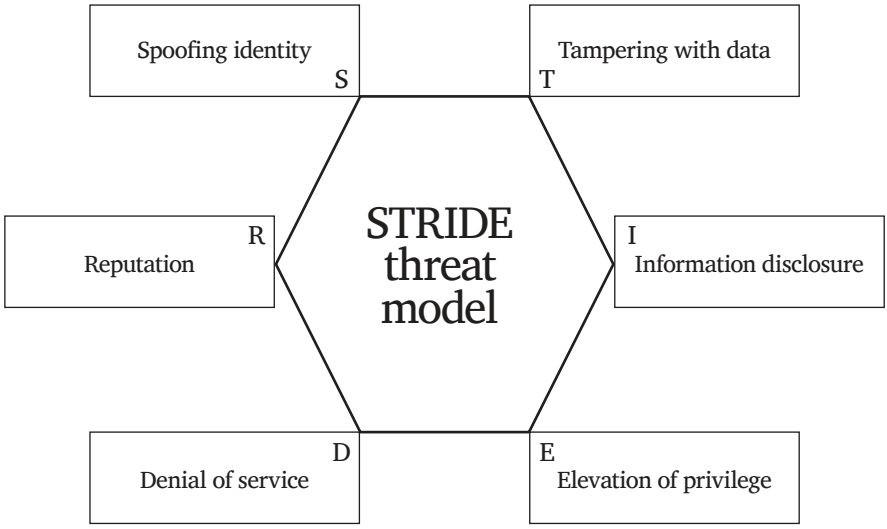
Cyberattack type	Reasons	Consequences
Attacks on government institutions and enterprises	– disrupting the country's/institution's activities – disrupting the activities of financial institutions – causing market confusion – causing social unrest – loss of trust in the government/institution – spreading disinformation to cause destabilisation – weakening of the position and trust in the institution/government – weakening of the economy	– loss of databases – loss of confidential data – destabilisation of the institution/country – duplicating fake news campaigns (e.g. for disinformation and/or social unrest purposes) – insulting and compromising – loss of trust (e.g. customers and/or citizens) – customer acquisition – financial losses – loss of market position – loss of image
Attacks on delivery companies	– weakening of the economy – extorting confidential personal data – fraud of payment card details – taking over bank data – obtaining financial resources	– loss of bank details – financial losses – loss of personal data – loss of confidential data
Attacks on social media, websites	– stealing sensitive data – stealing bank details – stealing passwords and taking over application accounts	– loss of passwords and accounts – financial losses – loss of sensitive data – loss of confidential data – insulting and embarrassing – loss of image – cyberstalking – loss of control over data in the application by the user
Attacks on data processing systems	– takeover of databases – interception of confidential and sensitive data – taking over bank details	– loss of sensitive and confidential data – insulting and embarrassing – loss of financial resources – taking over databases – loss of image – destabilisation – loss of market position

6. Cyberspace as a combat place

As mentioned above, cyberspace has been recognised as the fifth battlefield dimension where war can take place. This dimension is special because its users are anonymous and may often feel unpunished. Importantly, special technologies have been created to increase anonymity on the Internet (e.g. the Onion Router, also known as TOR) or proxies, and there are organisations that support human rights and protect user privacy on the Internet through free software and open networks. It is commonly said that anonymity on the Internet is ensured. The pursuit of anonymisation on the Internet and the constantly developing devices that improve navigation in the cyberspace show that this space exposes confidentiality to possible violations more than traditional ones. The desire for anonymity is associated with a sense of threat that may arise from using the Internet and transmitting data. There are many ways to remain anonymous online, but the possible attacks and their types are perhaps too numerous to list, as new technology continues to surprise as they improve hackers' possibilities and the latter enhance their skills.

The most popular attacks that can de-anonymise our network connection include those described herein: (a) browser attacks, such as those that force a TOR browser to unblock and provide information about the computer and the correct IP address; (b) node flooding, which involves the control of the network connection by the attacker, not by the client; (c) correlation attack, encompassing an flooding of large amounts of data coming in and out of the client's network. There are other possible attacks that are shown in the STRIDE model below.

Figure 3. STRIDE threat model[57]



57 Słota-Bohosiewicz, 2018, p. 300.

The STRIDE model is an acronym for: S, spoofing identity; T, tampering with data; R, repudiation; I, information disclosure; D, (ang.) denial of service; E, (ang.) elevation of privilege.[58]

The cyberspace is also a place where a new type of war is unfolding, often referred to as the information war. This type of warfare is defined as actions undertaken by one side to achieve information advantages, which in turn support the national military strategy by influencing the enemy's information and their information systems while protecting own information and information systems. These activities allow those involved to exert control over the content, flow, and availability of important information. There are two types of information warfare in the cyberspace, the first of which is (a) netwar, referring to a psychological warfare in the cyberspace, which provides propaganda aimed at shaping the morale of soldiers and society, and particularly at weakening the opponent's mental stability. It involves the integration of psychology, social communication, and modern information technologies. The second is (b) cyberwar, referring to activities carried out in the cyberspace to penetrate the enemy's infrastructure and then gain control over it or destroy it at the appropriate moment, while protecting own infrastructure. Nation states often hide their cyberspace activities under the guise of hacktivists, hackers, private armies, terrorist groups, and others. This is why they more often use the name cyberattack.

Importantly, there are threats of various sizes and levels of danger in the cyberspace, with some of the most dangerous ones being the following. First, cybercrime, referring to illegal, IT-based activities of non-state entities aimed at gaining profits. Second, cyber conflicts, describing conflicts related to cyberspace activities, which can generally be divided into activism (i.e. non-destructive activity in the cyberspace used to support different campaigns) and hacktivism (i.e. a combination of activism and criminal activities through the use of hacking methods against specific targets on the Internet to disrupt their functioning without causing serious losses). The latter is aimed not so much at destroying the opponent's resources but rather at drawing attention to a given problem. Third, cyberterrorism, describing politically-motivated attacks or threats of attacks on computers, networks, or information systems in order to destroy infrastructure and intimidate or force governments and the public to carry out far-reaching political and social actions in the broader sense of the word. It also involves the use of the cyberspace for communication, propaganda, and disinformation by terrorist organisations. Fourth, cyber espionage, referring to the use of the cyberspace for intelligence purposes, such as for obtaining information by bypassing or weakening systems, accessing the control mechanisms of hardware and software, and hacking into protected systems. Fifth, cyber surveillance, which is the control of society through information and communication technology (ICT) tools, and is most often used in authoritarian and totalitarian states. This is a phenomenon very similar to cyberterrorism, and may involve limiting citizens' access to the cyberspace.

58 Słota-Bohosiewicz, 2018, p. 299.

7. EU's actions in counteracting cyber incidents

7.1. EU institutions

The dynamic developments of and in the cyberspace have been forcing us to make great efforts at upholding security in this space at appropriate levels. Owing to the delineations above, the European Commission is taking actions aimed at establishing a close cooperation between EU countries and those that emphasise the role of the EU in ensuring network security. It is also making efforts to have this area recognised under EU policies. Over the years, as the cyberspace developed, several directorates have been established to deal with the issue of cybersecurity. These are the following: first, the Directorate-General for Communications Networks, Content and Technology (DG CNECT), the directorate responsible for shaping EU policy in the areas of electronic communications, digital content, technological innovation and, in general, the development of ICT. The main areas covered by the directorate are communication networks, digital content, digital technologies, and innovation and research.[59] Second, DG HOME (Cybercrime), responsible for the Digital Single Market and Security Union.[60] Third, the Directorate-General for Informatics (DG DIGIT), responsible for the IT management of EU institutions and supporting the development and implementation of IT technologies aimed at supporting the objectives of public administration and digital transformation. Its main activity areas are IT management, cybersecurity, digital transformation, support for technological innovations, and IT services.[61]

The implementation of these various tasks and responsibilities requires the support of various agencies in the EU, which include those described hereinafter: (a) ENISA, (b) European Cybercrime Center (also known as EC3), (c) European Union Computer Emergency Response Team (also known as CERT-EU), (d) European External Action Service (also known as EEAS). They also played important roles in the context of EU Member States and private sector organisations.

The ENISA, established in 2004 and headquartered in Heraklion, Crete, Greece, is responsible for upholding the highest level of security in the cyberspace in Europe. It serves as an advisory body in the field of network and information security, with its main goals being supporting EU Member States in the following: developing and implementing network and ICT security strategies; threat analysis; best practices promotion; education in the field of cybersecurity; international cooperation aimed at exchanging information and experiences; support in crisis situations related to information security.[62] The ENISA plays a key role in coordinating cybersecurity activ-

59 *Communications Networks, Content and Technology*, no date.
60 *Migration and home affairs*, no date.
61 *Digital Services*, no date.
62 *European Union Agency for Cybersecurity (ENISA)*, no date.

ities at the EU level, contributing to improvements to the cyber defence, along with the stability, of networks and information in territories of the EU and its Member States.[63]

The European Cybercrime Center, established in 2013 and based in the Hague, the Netherlands, is a unit of the European Law Enforcement Agency (also known as Europol) established to combat and prevent cybercrime. Its main tasks coordinating EU Member State activities, developing cooperation among law enforcement agencies and the private and public sectors, cooperating with relevant bodies in operational and investigative work, analysing and distributing information on the evolution of cyber threats, and conducting educational campaigns aimed at raising awareness of cyberattacks. As a key body of the EU strategy to combat cyber threats, it undertakes previously planned operational actions aimed at preventing cyberattacks,[64] as well as operational, analytical, and educational tasks.

The European Union Computer Emergency Response Team, established in 2011, is part of the ENISA and aims at preventing and responding to cyberattacks, as well as developing cybersecurity resources at the EU level. Its main tasks are responding analysing and responding to cybersecurity incidents, coordinating response activities among EU institutions and bodies, and providing technical and advisory support to EU Member States.[65]

The European External Action Service, established in 2010 under the Treaty of Lisbon, it is an institution responsible for managing and supporting the EU's foreign and security policies. Its main tasks are coordinating EU external activities, managing EU civil and military missions and operations as part of crisis management operations, peacekeeping, humanitarian aid, managing EU diplomacy and representation, providing support for political plans, analysing the international situation, cooperating with international partners.[66] This body has a unique entity status, combining elements of the European Commission and the Council of the European Union.

EU Member States are obliged to ensure their own cybersecurity and their activities in relation to EU policy should be carried out through the Council, within which there are numerous bodies coordinating activities and sharing information, such as the Horizontal Working Group on Cyberspace.

Private sector organisations encompass industry entities, Internet managers, and academia, serving as partners in relevant activities and influencing the creation and implementation of policies through contractual public–private partnerships.

63 Based on Lessmann et al., 2017.

64 *European Cybercrime Centre -EC3*, no date.

65 *CERT-EU*, no date.

66 European Union External Action – The Diplomatic Service of the European Union. [Online]. Available at: https://www.eeas.europa.eu/_en (Accessed: 10 January 2024).

7.2. Schedule of cybersecurity actions

The EU has been taking various actions to promote its resilience in the cyberspace and defence against cyber incidents, some of which are described in this subsection.[67] The first related activities took place on 9 June 2016, when the Council of the European Union started to work on improving the criminal justice system within the context of the cyberspace, specifically in relation to bilateral legal assistance, more effective cooperation with service providers, and factors determining jurisdiction. In addition, the Council addressed the need to improve the European Judicial Network on Cybercrime, endeavouring to strengthen the network of judicial authorities and increase the number of cybersecurity experts. The next important activity was the agreement on 24 October 2017, named the Cybersecurity Action Plan and the European Union Cybersecurity Reform Decision, which decided the nature of Internet security for the public and private sectors. Two months later, on 20 December 2017, close cooperation was established between EU entities in the fight against cyberattacks, and there was a decision to establish a Computer Emergency Response Team for all EU institutions, bodies, and agencies. This Team was aimed at coordinating the actions of EU institutions in response to cyberattacks on EU entities.

In 2018, various actions were taken to promote cybersecurity. In 16 April 2018, the Council adopted conclusions on the damages caused by cyberattacks, pointing to the essence of the cyberspace – which is supposed to be a global, free, and stable space wherein human rights and freedoms are respected – and also raised the issue of growing the cyberspace capabilities of non-EU countries and non-state entities. In 13 September 2018, the Council entered into negotiations with the European Parliament regarding the need to reach an agreement on the Cybersecurity Act, which was intended to increase the EU's cyber resilience by creating an EU-wide certification framework for ICT products, services, and processes. They also agreed on the modernisation of the ENISA, which was functioning at that time. In October 2018, the Council called for strengthening cybersecurity in the EU, and discussed the issue of intensifying preventive and response activities to emerging threats online, as well as hybrid, chemical, biological, radiological and nuclear threats. This was especially related to the cyberattacks carried out against the Organization for the Prohibition of Chemical Weapons in The Hague, the Netherlands. Finally, in December 2018, the Embassy of the European Union approved the Cybersecurity Act, which enabled the creation of EU-wide certification and strengthened the ENISA. As a result, devices connected to the Internet have been covered by EU-wide cybersecurity certifications.

In March 2019, the Council started negotiations with the Parliament on ways to consolidate knowledge on cybersecurity, and the European Cybersecurity Research and Competence Center was established, constituting a top-level knowledge base. A month later, the Council adopted the Cybersecurity Act, which established the

67 European Court of Auditors, 2019.

certification system in the EU and the European Union Agency for Cybersecurity. In May 2019, the Council was granted the power to impose sanctions to prevent and respond to cyberattacks, as such attacks were considered to constitute an external threat to EU Member States. Specifically, it was allowed to impose sanctions on entities and individuals who have done the following: (a) have carried out or attempted to commit a cyberattack; (b) supported these individuals financially, technically, and/or materially; (c) are directly involved in the attack at every stage of its preparation. To achieve common foreign and security policy objectives, these regulations were made applicable to non-EU entities or countries, as well as to international organisations targeting cyberattacks. On 3 December 2019, an important event discussed the importance of the 5G network for the European economy and the risks associated with it.

On 5 June 2020, the need to negotiate a European regulation on the Cybersecurity Competence Center and the Network of National Coordination Centers I for the development of the 5G network was established. A month later, on 9 June 2020, the Council took steps to implement the EU digital strategy, highlighting that the scale and complexity of cybersecurity threats was increasing, along with the need to improve the EU's response to cyberattacks. The first sanctions for carrying out cyberattacks were imposed on six people and three entities on 30 July 2020, involving the above-mentioned travel ban and asset freeze sanctions. On 2 December 2020, the Council highlighted various new risks arising from connecting many office and home devices to the Internet, and emphasised that these are new threats to sensitive private and public data. On 9 December 2020, the European Center for Cybersecurity in Industry, Technology and Research in Bucharest was provided with the task of coordinating research and innovation in the field of cybersecurity in the EU, and combining cybersecurity investments with research, technology, and industrial development. Three days later, on 11 December 2020, talks began about establishing an EU Cybersecurity Competence Center. Thereafter, on 15 December 2020, the Council pointed to the need to strengthen resilience and counteract hybrid threats, including disinformation. It prepared a statement in the context of the COVID-19 pandemic as well as various other crises, and emphasised the need to develop a comprehensive approach that will define the principles of coordination and cooperation for counteracting threats and disinformation on the Internet.

In 2021, some issues related to the EU's cybersecurity strategy were raised, with much attention paid to citizens and businesses in the context of their protection against cyber threats. Issues of promoting the security of IT systems and global protection, as well as a safe cyberspace, were also discussed, and it was stressed that cybersecurity is crucial for Europe, which must be resilient, green, and digital. On 22 March 2021, the importance of the EU in achieving leadership in the digital realm and defining its strategic capabilities was discussed. A month later, on 20 April 2021, the European Center for Industrial, Technological and Research Competences in the field of cybersecurity was established, being tasked

to cooperate with a network of designated national centres to increase Internet security. An interim agreement was also reached, on 29 April 2021, to enable ISPs to continue to detect, remove, and report online child sexual exploitation. This year, there were also the following processes: (a) extension of sanctions for cyberattacks against EU countries (from 17 May 2021 to 18 May 2022); (b) the Council maintained its position on the need to develop initiatives regarding crisis management in cyberspace (19 October 2021); (c) the Council agreed to develop a new cybersecurity directive (13 December 2021).

In 2022, the EU Ministers emphasised the need to intensify European cooperation in the area of cybersecurity, especially after the various cyber threats that emerged owing to the situation in Ukraine, and, consequently, by the increase in the number of cyber incidents in the EU. As a result, between 8 and 9 March 2022, 27 ministers adopted a political declaration aimed at strengthening the EU's cybersecurity capabilities. In addition, the Council and the European Parliament made efforts to create the Digital Operational Resilience Regulation (DORA), which provides a technical framework to enable all companies to achieve the goal of strengthened cybersecurity. On 11 May 2022, special procedures were included in the regulation with the aim of preventing ICT disruptions, and temporary terms of agreement were set on the proposed NIS2 Directive, which was to replace the Directive on the security of network and information systems (NIS). The main goal was to achieve the highest level of cybersecurity in all EU countries (13 May 2022). The Council's actions were also important during this period, and encompassed the following: (a) the Council extended the rules regarding sanctions (16 May 2022) and approved (23 May 2022) the principles and policies of the EU, as well as the EU plan, to strengthen security and defence policies (Strategic Compass) by the end of 2030; (b) adopted Sorava's conclusions on a coordinated EU response to hybrid campaigns (21 June 2022); (c) accepted conclusions on ICT supply chain security (17 October 2022); (d) defined a common cybersecurity policy and the EU actors responsible for security (11 November 2022); (e) adopted the NIS2 directive (28 November 2022).

In 2023, the Council adopted the following: (a) conclusions on cyber defence, emphasising that each EU country has the obligation to further strengthen its own resilience to cyberattacks while enhancing its cybersecurity and cyber defence (23 May 2023); (b) an interim agreement with security entities on a common cybersecurity framework for EU entities (26 June 2023); (c) a common position on the Cyber Resilience Act (19 July 2023); (d) updated the policy framework, which now includes efforts at increasing the resilience to cyberattacks, the intensity of cooperation between EU Member States, and the ability to defend against cyberattacks (19 November 2023). The evolution of the security challenges was also analysed, and the competences of various EU entities were defined in the year of 2023. There were also discussions involving the need to build strong EU cybersecurity and the need to define sanctions for the use of cyberattacks.

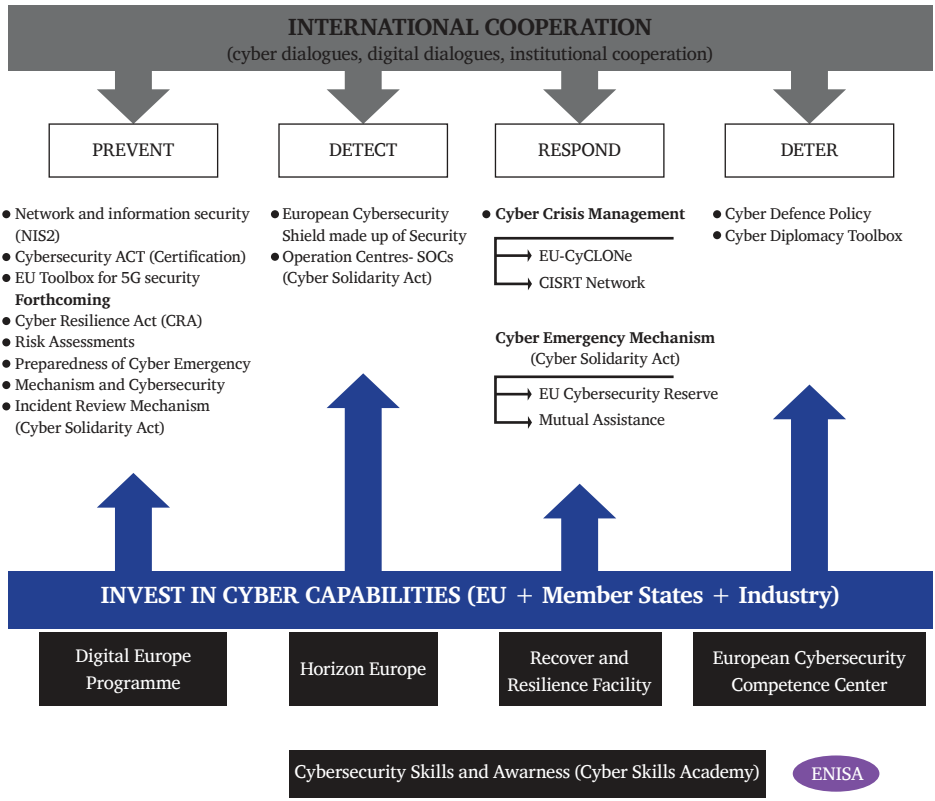
7.3. International cooperation

The EU has taken many actions to ensure security in the cyberspace, one of which is the EU Cybersecurity Strategy, which assumes actions aimed at increasing the EU's ability to fight against cyberattacks and effectively and quickly recover from related attacks. The cyberspace enables many activities that can be both beneficial and downright dangerous for nations, and the cyberattacks that are becoming the most common are those aimed at stealing data and spying on users or government data; that is, attacks targeting both the private and public sectors.[68] This underpins the importance of securing the safe use of the network by all sectors.

The EU Cybersecurity Strategy aims to strengthen the EU's common cybersecurity and its response to cyberattacks. It is also important that human rights and the rule of law are protected, and to safeguard these principles, the strategy has been divided into the following areas:[69] (a) resilience, technological sovereignty, and leadership; (b) operational capability to prevent, deter, and respond; (c) cooperation for the development of a global and open cyberspace. Cybersecurity has been included in the "Digital Europe" program, which aims to strengthen the coordination of cybersecurity among EU Member States, and finance the maintenance of their resilience to cyberattacks. Research is constantly being carried out to improve the existing EU strategies and policies, and the main goal is to improve the cooperation and investment in cyber defence in order to provide better protection against the increasing number of cyberattacks.[70] Achieving these goals will surely require EU Member States to cooperate in preventing, detecting, and responding to cyber threats as well as improving cyber security. These goals are presented in detail in the diagram below.

68 European Court of Auditors, 2019, pp. 13–16.
69 Based on International Civil Aviation Organization, 2022.
70 *Cyberbezpieczeństwo* [Cybersecurity], no date.

Scheme 1. International cooperation



The diagram provides an overview of the EU's work on various fronts to promote its cyber resilience, safeguarding its online society, communication, data, and economy.

8. Responding to cyber incidents and cyberattacks: Good practices

8.1. Sectors and groups at risk

Nowadays, in the era of digitalisation and ubiquitous threats in the cyberspace, everyone, from citizens, their families, and large groups, should be ready to respond to online incidents. Statistics show that individuals, large corporations, and

government entities are all attacked, showcasing that cyber threats pose a real risk to enterprises, public institutions, non-profit organisations, and other entities. More specifically, some groups that are particularly vulnerable to these threats include those outlined herein: (a) business sector (e.g. business organisations, small and medium-sized enterprises); (b) financial sector (e.g. banks, financial institutions, financial services companies); (c) government sector (e.g. possible loss of sensitive data regarding personnel and citizens, which may lead to disruption of state functioning stability); (d) health sector (possibility of losing patient data, which may have serious consequences for patient safety); (e) energy sector (possibility of disruption of energy supplies); (f) manufacturing sector; (g) infrastructure sector; (h) education sector (possible loss of student and teacher data and possible disruptions in the educational system); (i) non-profit sector (possibility of losing data of sponsors and sponsored persons, along with the disruption of social, humanitarian, and charitable assistance activities); (j) cloud and IT service provider sector (disruption in the supply of services may disrupt the functioning of the organisation and disrupt the lives of citizens); (k) civil society (individual users and corporate employees); (l) security teams; (m) crisis management teams; (n) incident response teams; (o) management of boards of directors.

Good practices for dealing with a cyber incident should include several stages, as follows: defining who is at risk; taking actions to prevent cyber incidents; preparing for cyber incidents, responding to the incidents (incident management); restoring the state to normal after the cyber incident has been removed.

8.2. Prevention[71]

The first stage is incident prevention, which is a strategic stage of an effective cyber security plan. The related procedures at this stage include those outlined herein: (a) raising awareness and education about cyber threats (e.g. through regular training and information campaigns); (b) implementing safety rules (e.g. applies to management, executive staff, teachers, children); (c) using security measures (e.g. strong passwords, frequently changing passwords, creating access restrictions, prohibiting the use of unregistered devices, and media); (d) software updates (especially applicable to operating systems and applications); (e) using technical security measures (e.g. firewalls, anti-virus systems, and protection against ransomware); (f) controlling access (e.g. through creating permissions and access restrictions); (g) security monitoring (e.g. using systems that detect inappropriate behaviour); (h) developing a policy for the use of IT systems; (i) monitoring employee activities; (j) establishing network security; (k) creating protections against phishing; (l) managing system and application configurations; (m) exchanging information with entities about threats; (n) conducting external security audits.

71 Based on International Civil Aviation Organization, 2022.

8.3. Preparation[72]

The preparation stage for cyberattacks includes activities such as those presented in the list that follows: (a) developing an incident management plan comprising[73] the definition of procedures and stages of response to various events, role divisions, competences, and responsibilities between responsible entities; (b) establishing an incident team (i.e. the Computer Security Incident Response Team, also known as CSIRT); (c) participating in training and exercises in the context of cyber threats; (d) implementing monitoring and detection systems; (e) implementing access management systems; (f) applying technical security measures; (g) developing recovery plans; (h) regularly conducting external security audits; (i) applying legal plans; (j) promoting external cooperation with law enforcement agencies, cybersecurity organisations, and other industry organisations to exchange information and best practices about cybersecurity organisations and others.

8.4. Response/incident management[74]

The response stage for cyberattacks includes activities such as the following: (a) recognising incidents, which is carried out by system monitoring (i.e. early detection of incidents), analysing event logs, reporting suspicious activity by staff, reporting of suspicious activities by automatic threat detection systems; (b) classifying and assessing the incident, which is carried out by identifying the nature and scale of the event, as well as analysing and assessing potential impacts on the organisation (e.g. financial damage, data loss, impact on reputation, and operational functioning); (c) isolating resources affected and taking immediate actions to thwart the spread of an attack; (d) notifying appropriate teams (e.g. IT Security Team, the Computer Security Incident Response Team, Crisis Management Team, relevant internal teams); (f) managing the Computer Security Incident Response Team; (g) collecting data to be analysed and documented afterwards; (h) conducting incident analysis; (i) notifying appropriate external parties (e.g. law enforcement agencies, international structures, partner institutions, among others); (j) restoring services and systems and verifying that the corrective steps taken are effective and safe; (k) analysing post-event conclusions and introducing changes to the strategy and security measures, as well as improvement activities; (l) implementing training and education through developing and disseminating educational materials, and using experience to increase the ability to counteract incidents; (m) reporting and documentation covering the scope of activities, conclusions, and recommendations.

72 Based on International Civil Aviation Organization, 2022.
73 Based on International Civil Aviation Organization, 2022.
74 *Podręcznik postępowania z incydentami naruszenia bezpieczeństwa komputerowego* [Procedure manual with incidents of violation computer security], 2021.

8.5. Reconstruction[75]

The reconstruction stage comes after the end of an incident and is of particular importance for dealing with cyberattacks. This is because the efforts of many entities must be coordinated to ensure a successful restoration of the status to that before the occurrence of the cyberattack. It comprises activities such as the following: (a) conducting loss analysis; (b) analysing the causes of the incident; (c) strengthening security; (d) promoting staff education; (e) increasing awareness of the public and staff; (f) applying internal and external information policy; (g) making efforts to secure system recovery; (h) resting the services; (i) verifying the effectiveness of actions taken so far; (j) updating system patches; (k) reviewing and updating plans; (l) verifying procedures; (m) improving procedures; (n) tightening cooperation with external entities; (o) promoting information exchanges.

9. Summary

The analysis of the literature on the subject, reports, internet sources, and of research conducted with experts allows the conclusion that the cyberspace has become important in almost all sectors of life. It is a dimension of life that allows us to take actions that can bring both benefits and losses and stores a very large amount of information, including sensitive information, which can be stolen and used and may cause financial and health losses. Cyberattacks can thus contribute to causing crises, panic in society, chaos, tension, unrest, and even war, and these attacks seems to also be getting more complex and aggressive as time goes on. It is very important for the whole society, as well as private and government organisations, to be aware of cyberattacks and to be able to respond to them. Effective cyberattack detection and response is now becoming a challenge for countries worldwide, especially as cross-border attacks become particularly important and require coordination of the EU crisis response mechanism. In light of these complex scenarios, it is key that the EU makes grand efforts to protect its critical infrastructure, but achieving these goals, if we consider the current challenges in the network, may require the involvement of all EU Member States.

75 Based on International Civil Aviation Organization, 2022.

References

Barć, M. (2021) 'Rodzaje Ochrony Infrastruktury Krytycznej' [Types of infrastructure protection], *Rocznik Bezpieczeństwa Morskiego*, special issue, pp. 1–15; https://doi.org/10.5604/01.3001.0015.0196.

Cendrowski, W. (2020) 'Cyberbezpieczeństwo' [Cybersecurity], *UKEN: Vademecum Bezpieczeństwa Informacyjnego*, 9 March 2020. [Online]. Available at: https://vademecumbezpieczenstwainformacyjnego.uken.krakow.pl/2020/03/09/cyberbezpieczenstwo/ (Accessed: 6 January 2024).

Czekaj, Ł. (2020) 'Cyberatak' [Cyber attack], *UKEN: Vademecum Bezpieczeństwa Informacyjnego*, 9 March 2020. [Online]. Available at: https://vademecumbezpieczenstwainformacyjnego.uken.krakow.pl/2020/03/09/cyberatak/https://vademecumbezpieczenstwainformacyjnego.uken.krakow.pl/2020/03/09/cyberatak/ (Accessed: 10 January 2024).

Encyclopedia by Kaspersky (no date). [Online]. Available at: https://encyclopedia.kaspersky.com/knowledge/years-1970s/ (Accessed: 8 November 2023).

European Court of Auditors (2019) 'Challenges to effective EU cybersecurity policy', *Briefing Paper*, March 2019. [Online]. Available at: https://www.eca.europa.eu/Lists/ECADocuments/BRP_CYBERSECURITY/BRP_CYBERSECURITY_EN.pdf (Accessed: 10 January 2024).

European Union Agency for Cybersecurity (2020a) *Zagrożenia Wewnętrzne: Krajobraz zagrożeń wg Agencji Unii Europejskiej ds. Cyberbezpieczeństwa* [Internal Threats: Threat Landscape according to the European Union Agency for Cybersecurity]. [Online]. Available at: https://www.enisa.europa.eu/publications/report-files/ETL-translations/pl/etl2020-insider-threat-ebook-en-pl.pdf (Accessed: 20 November 2023).

European Union Agency for Cybersecurity (2020b) *Wykaz piętnastu największych zagrożeń* [The list of fifteen of the largest threats]. [Online]. Available at: https://www.enisa.europa.eu/publications/report-files/ETL-translations/pl/etl2020-enisa-list-of-top-15-threats-ebook-en-pl.pdf (Accessed: 5 January 2024).

European Union Agency for Cybersecurity (2021) *Krajobraz Zagrożeń 2021 wg Agencji Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA)* [Threats Landscape 2021 According To European Union Agency For Cyber Security (ENISA)], October 2021. [Online]. Available at: https://www.enisa.europa.eu/publications/etl-2021/enisa-threat-landscape-2021-2022-final_pl.pdf (Accessed: 6 January 2024).

Falliere, N., O Murchu, L., Chien, E. (2010) *W32.Stuxnet Dossier*, November 2010. [Online]. Available at: https://web.archive.org/web/20191104195500/https://www.wired.com/images_blogs/threatlevel/2010/11/w32_stuxnet_dossier.pdf (Accessed: 2 January 2024).

Gopal, R.V. (2022) 'Complete Case Study – Target Data Breach', *Medium*, 4 December 2022. [Online]. Available at: https://medium.com/@rithikvgopal/complete-case-study-target-data-breach-2-ba4bb365a82e (Accessed: 2 January 2024).

Grzelak, M., Liedel, K. (2012) 'Bezpieczeństwo w Cyberprzestrzeni. Zagrożenia i Wyzwania dla Polski – zarys problemu' [Security in cyberspace. Threats and challenges for Poland – outline of the problem], *Bezpieczeństwo Narodowe*, 22(2), pp. 125–139.

International Civil Aviation Organization (2022) *Cybersecurity Action Plan*, January 2022. [Online]. Available at: https://www.icao.int/aviationcybersecurity/Documents/CYBERSECURITY%20ACTION%20PLAN%20-%20Second%20edition.EN.pdf (Accessed: 10 December 2023).

Lessmann, F. et al. (2017) 'Study on the Evaluation of the European Union Agency for Network and Information Security, European Comission', *European Commission: Directorate-General for Communications Networks, Content and Technology*. [Online]. Available at: https://op.europa.eu/en/publication-detail/-/publication/ed504f6e-9c1c-11e7-b92d-01aa75ed71a1/language-en (Accessed: 10 January 2024).

Liderman, K. (2020) 'Ochrona informacji sterującej w sieciach i systemach przemysłowych – propozycja podstaw edukacyjnych' [Protection of control information in industrial networks and systems – a proposal for educational foundations], *Przegląd Teleinformatyczny*, 8(26), pp. 3–30; https://doi.org/10.5604/01.3001.0015.0604.

Marczyk, M. (2018) 'Cyberprzestrzeń jako nowy wymiar aktywności człowieka – analiza pojęciowa' [Cyberspace as a new dimension of human activity – conceptual analysis of the area], *Przegląd Teleinformatyczny*, 6(24), pp. 59–72; https://doi.org/10.5604/01.3001.0012.7212.

Niewiadomska-Szynkiewicz, E., Litka, R. (2023) 'Ataki na urządzenia mobilne I metody ich wykrywania' [Attacks on mobile devices and methods of detecting them], *Cybersecurity and Law*, 1(9), pp. 95–107; https://doi.org/10.35467/cal/169303.

Nowak-Brzezińska, A. (2017) *Zagrożenia i bezpieczeństwo komputerów i danych* [Threats and security of computers and data]. Warsaw: Projekt UPGOW, European Social Fund.

Oladimeji, S., Kerner, S.M. (2023) 'SolarWinds hack explained: Everything you need to know', *TechTarget*, 3 November 2023. [Online]. Available at: https://www.techtarget.com/whatis/feature/SolarWinds-hack-explained-Everything-you-need-to-know (Accessed: 20 December 2023).

Pacut, M. (2023) 'Co to jest naruszenie bezpieczeństwa danych (data breach)?' [What is a data breach?], *Net Complex Blog*, 28 April 2023. [Online]. Available at: https://www.netcomplex.pl/blog/co-to-jest-naruszenie-bezpieczenstwa-danych-data-breach (Accessed: 20 November 2023).

Pala, M. (2015) 'Wybrane aspekty bezpieczeństwa w cyberprzestreni' [Selected aspects of security in cyberspace], *De Securitate et Defensione. O bezpieczeństwie i Obronności*, 1(1), pp. 113–130.

Petrosyan, A. (2024) 'Annual number of malware attacks worldwide from 2015 to 2022 (in billions)', *Statista*, 22 April 2024. [Online]. Available at: https://www.statista.com/statistics/873097/malware-attacks-per-year-worldwide/ (Accessed: 10 April 2024).

Sarkar, D. (2023) 'Elk Cloner – The First Computer Virus', *Linkedin*, 26 July 2023. [Online]. Available at: https://www.linkedin.com/pulse/elk-cloner-first-computer-virus-debadrita-sarkar (Accessed: 11 January 2024)

Słota-Bohosiewicz, A. (2018) 'Przeciwdziałanie cyberszpiegostwu w organizacji' [Counteracting cyber espionage in an organization], *Obronność – Zeszyty Naukowe Wydziału Zarządzania i Dowodzenia Akademii Sztuki Wojennej*, 4(28), pp. 294–312.

Thomson, I., Nichols, S. (2009) 'Top ten worst viruses', *PC & Tech Authority*, 4 May 2009. [Online]. Available at: http://web.archive.org/web/20180614194509/https://www.pcauthority.com.au/news/top-ten-worst-viruses-143993 (Accessed: 8 November 2023).

Waraksa, M., Żurek, J., Niski, R. (2011) 'Interfejsy radiowe w bezprzewodowych sieciach sensorowych' [Security of data transmission in wireless sensor networks], *Zeszyty Naukowe Akademii Morskiej w Gdyni*, 2011/70, pp. 79–87.

Wasiuta, O., Klepk, R. (eds.) (2019) *Information security handbook*. Kraków: AT Wydawnictwo- LIBRON, Uniwersytet Pedagogiczny.

Zhu, L., Zheng, B., Shen, M., Yu, S., Gao, F., Li, H., Shi, K., Gai, K. (2018) 'Research on the Security of Blockchain Data: A Survey', *Journal of Computer Science and Technology*, 35(4), pp. 843–862; https://doi.org/10.48550/arXiv.1812.02009I.

I 10 virus informatici peggiori della storia [The 10 Worst Computer Viruses in History] (no date) *Hardware Upgrade*. [Online]. Available at: https://www.hwupgrade.it/forum/showthread.php?t=1978965 (Accessed: 10 February 2024).

Ataki na aplikacje webowe. Jakie są najczęstsze i jak się bronić? [Attacks on web applications. What are the most common ones and how to defend yourself?] (2022) *Da Vinci Studio*, 26 October 2022. [Online]. Available at: https://www.davinci-studio.com/pl/blog/ataki-na-aplikacje-webowe-jakie-sa-najczestsze-i-jak-sie-bronic/ (Accessed: 22 January 2024).

Analiza ryzyka w obszarze cyberbezpieczeństwa – jakie jest jej znaczenie? [Risk analysis in the area of cybersecurity – what is its importance?] (no date) *Szkoła Biznesu Politechniki Warszawskiej*. [Online]. Available at: https://biznes.edu.pl/analiza-ryzyka-w-obszarze-cyberbezpieczenstwa-jakie-jest-jej-znaczenie/ (Accessed: 13 January 2024).

ABlockchain – aspekty technnologiczne oraz przykłady zastowań [Blockchain – technological aspects and examples of applications] (no date) *Lazarski University*. [Online]. Available at: https://www.lazarski.pl/pl/34024-blockchain-aspekty-technologiczne-oraz-przyklady-zastosowan (Accessed: 20 November 2023).

Celebrating Penn Engineering History: ENIAC (no date) *University of Pennsylvania*. [Online]. Available at: https://www.seas.upenn.edu/about/history-heritage/eniac/ (Accessed: 3 November 2023).

CERT-EU (no date) *Cyber security intelligence*. [Online]. Available at: https://www.cybersecurityintelligence.com/cert-eu-1925.html (Accessed: 10 January 2024).

Communications Networks, Content and Technology (no date) *European Commission*. [Online]. Available at: https://commission.europa.eu/about-european-commission/departments-and-executive-agencies/communications-networks-content-and-technology_en (Accessed: 10 January 2024).

Cyberbezpieczeństwo [Cybersecurity] (no date) *European Commission*. [Online]. Available at: https://digital-strategy.ec.europa.eu/pl/policies/cybersecurity (Accessed: 10 January 2024).

Cyberbezpieczeństwo: główne i nowe zagrożenia [Cybersecurity: main and new threats] (2022) *European Parliament*, 27 January 2022. [Online]. Available at: https://www.europarl.europa.eu/news/pl/headlines/society/20220120STO21428/cyberbezpieczenstwo-glowne-i-nowe-zagrozenia#ssh_slides (Accessed: 30 November 2023).

Cybersecurity: how the EU tackles cyber threats (no date) *European Council*. [Online]. Available at: https://www.consilium.europa.eu/en/policies/cybersecurity/ (Accessed: 10 November 2023).

Czym jest uwierzytelnianie dwuskładnikowe, uwierzytelnianie dwuetapowe? [What is two-factor authentication, two-step authentication?] (2023) *Progreso*, 18 September 2023. [Online]. Available at: https://progreso.pl/pl/blog/czym-jest-uwierzytelnianie-dwuskladnikowe-uwierzytelnianie-dwuetapowe (Accessed: 20 November 2023).

Digital Services (no data) *European Commission*. [Online]. Available at: https://commission.europa.eu/about-european-commission/departments-and-executive-agencies/digital-services_pl (Accessed: 10 January 2024).

Elk Cloner. La cápsula del tiempo [Elk Cloner. The Time Capsule] (2009) *WeLiveSecurity*, 11 August 2009. [Online]. Available at: https://www.welivesecurity.com/laes/2009/08/11/elk-cloner-capsula-tiempo/ (Accessed: 11 January 2024).

European Cybercrime Centre -EC3 (no date) *Europol*. [Online]. Available at: https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3 (Accessed: 10 January 2024).

European Union Agency for Cybersecurity (ENISA) (no date) [Online]. Available at: https://european-union.europa.eu/institutions-law-budget/institutions-and-bodies/search-all-eu-institutions-and-bodies/european-union-agency-cybersecurity-enisa_pl (Accessed: 10 January 2024).

Incydent bezpieczeństwa informacji – kiedy następuje? **[**Information security incident – when does it occur and what to do?] (2024) *Ce cert*, 7 June 2024. [Online]. Available at: https://cecert.pl/incydent-bezpieczenstwa-informacji-kiedy-nastepuje-i-jak-wtedy-postepowac/ (Accessed: 10 February 2024).

Internet Rzeczy, ochrona prywatności a bezpieczeństwo danych [Internet of Things, privacy protection and data security] (2021) *Deloitt*e, 8 February 2021. [Online]. Available at: https://lgl-iplaw.pl/2021/02/internet-rzeczy-iot-internet-of-things-wygoda-czy-prawo-do-prywatnosci-wirtualnej-i-cyberbezpieczenstwo/ (Accessed: 20 November 2023).

A look at Estonia's cyberattack in 2007 (2009) *NBC News*, 8 July 2009. [Online]. Available at: https://www.nbcnews.com/id/wbna31801246 (Accessed: 2 January 2024).

Microsoft Faces Blistering Attack On-Line Leaders Say Software Giant Wants To Extend Its Dominance (1995) *The Spokesman–Review*, 20 July 1995. [Online]. Available at: https://www.spokesman.com/stories/1995/jul/20/microsoft-faces-blistering-attack-on-line-leaders/ (Accessed: 2 January 2024).

Migration and home affairs (no date) *European Commission*. [Online]. Available at: https://commission.europa.eu/about-european-commission/departments-and-executive-agencies/migration-and-home-affairs_en (Accessed: 10 January 2024).

The Morris Worm: 30 Years Since First Major Attack on the Internet (2018) *FBI*, 2 November 2018. [Online]. Available at: https://www.fbi.gov/news/stories/morris-worm-30-years-since-first-major-attack-on-internet-110218 (Accessed: 2 January 2024).

Naruszenie ochrony danych przez podmiot przetwarzający. Czym jest i jak postępować, kiedy do niego dojdzie [Data protection breach by the processor. What is it and what to do when it happens] (2021) *Polska Agencja Rozwoju Przedsiębiorczości*, 8 July 2021. [Online]. Available at: https://www.parp.gov.pl/component/content/article/72064:naruszenie-ochrony-danych-przez-podmiot-przetwarzajacy-czym-jest-i-jak-postepowac-kiedy-do-niego-dojdzie (Accessed: 20 November 2023).

Phishing: co to jest? [What is phishing?] (no date) *Trend Micro*. [Online]. Available at: https://www.trendmicro.com/pl_pl/what-is/phishing.html (Accessed: 20 November 2023).

Podręcznik postępowania z incydentami naruszenia bezpieczeństwa komputerowego [Procedure manual with incidents of violation computer security] (2021) *Pełnomocnik Rządu do Spraw Cyberbezpieczeństwa*, Warszawa, 2021. [Online]. Available at: https://www.gov.pl/web/baza-wiedzy/podrecznik-postepowania-z-incydentami-naruszenia-bezpieczenstwa-komputerowego (Accessed at: 10 December 2021).

Poradnik ransomware [Guide Ransomware] (no date) *CERT Polska*. [Online]. Available at: https://cert.pl/uploads/docs/CERT_Polska_Poradnik_ransomware.pdf (Accessed: 22 January 2024).

SMEs and Cybercrime (2022) *European Commission*, May 2022. [Online]. Available at: https://europa.eu/eurobarometer/surveys/detail/2280 (Accessed: 10 February 2024).

Triada CIA – Podstawowe Spojrzenie Na Bezpieczeństwo Informacji [The CIA Triad – A Basic View of Information Security] (2021) *Security bez tabu*, 15 July 2021. [Online]. Available at: https://securitybeztabu.pl/triada-cia-podstawy-bezpieczenstwa/ (Accessed: 22 January 2024).

What is WannaCry ransomware? (no date) *Kaspersky*. [Online]. Available at: https://www.kaspersky.com/resource-center/threats/ransomware-wannacry (Accessed: 20 December 2023).

Y2K bug (no date) *National Geographic*. [Online]. Available at: https://education.nationalgeographic.org/resource/Y2K-bug/ (Accessed: 2 January 2024).