Cyberspace, Cybercrime, Cyberterrorism

Filip Radoniewicz

Abstract The purpose of this chapter is to synthetically characterize the phenomenon of cybercrime, cyberterrorism and cyberwar. It presents attempts to define computer crimes and their classification, history of criminalization of this phenomenon together with related difficulties. The author consistently distinguishes cybercrime from cyberterrorism and cyberwar.

1 Cyberspace

The term "cyberspace", the combination of the two words "cybernetics" and "space", meaning cybernetic space, was coined in the 1980s. It is thought that the originator of this term was William Gibson, a Canadian writer, who used it in his novel *Neuromancer* of 1984, to define computer-generated virtual realities, which the protagonists inhabit. The notion found its place in mass culture, and it is currently used to define virtual space, understood as space for communication via computer networks.[1] This term is sometimes (incorrectly) used as a synonym for the Internet.[2]

As regards Polish Law, cyberspace is defined, i.a., in Article 2(1a) of the State of Emergency Act of the 21st of June 2002,[3] Article 3(1)(4) of the Natural Disasters Act of the 18th of April 2002,[4] and Article 2(1b) of the Act of the 29th of August 2002 on Martial Law and the Competences of the Commander-in-Chief of the Army

[1] For more details, see Kosiński (2013), pp. 462–463.

[2] Cf. Liderman (2012), pp. 62–63; Wall (2013), pp. 10–11.

[3] Act of 21 June 2002 of the State of Emergency Act, consolidated text, Polish Journal of Laws of 2016, item 886, as amended.

[4] Act of 18 April 2002 on Natural Disasters, consolidated text, Polish Journal of Laws of 2017, item 1897, as amended.

F. Radoniewicz (✉)
Akademickie Centrum Polityki Cyberbezpieczeństwa/Academic Center for Cybersecurity Policy, Akademia Sztuki Wojennej w Warszawie/War Studies University in Warsaw, Warsaw, Poland
e-mail: filip.radoniewicz@radoniewicz.eu

© The Author(s) 2022

K. Chałubińska-Jentkiewicz et al. (eds.), *Cybersecurity in Poland*,
https://doi.org/10.1007/978-3-030-78551-2_4

and the Rules of the Commander-in-Chief's Subordination to the Constitutional Authorities of the Republic of Poland,[5] according to which the term is understood as *"a space for the processing and exchange of information, created by information and communication systems, defined in Articles 3(3)* of the Act of the 17th of February 2005 on the Computerisation of the Operations of Entities Performing Public Tasks*, including the links between them and their relations with users."* Within the meaning of the said Act on Computerisation, a communication and information system is a set of interfacing IT hardware and software, providing the facility to process, store, send, and receive data via ICT networks, with the use of an end device suitable for a given network type. According to this relatively comprehensive definition developed by the legislator, cyberspace includes not only communication and information systems, comprising hardware and software facilitating the performance of system functions (processing, storage and sending computer data), but also computer data and interactions between devices and their users.[6]

2 Cybersecurity

The concept of cybersecurity is currently defined under Polish law in the National CyberSecurity System Act of the 5th of July 2018.[7] Given the significant role this legal Act plays in the field of "cybersecurity law", it may be assumed that the definition can be applied across the entire legal system. Pursuant to Article 2(4) of the NCSA, cybersecurity is

> the ability of information systems to resist actions, which compromise the availability, authenticity, integrity, and confidentiality of processed data, or the related services provided by those information systems.

Under Article 2(4) of the NCSA, the legislator referred to the notions of confidentiality, integrity, availability, and authenticity, i.e., the so-called information-security components (of computer data and communication and information systems). Traditionally, the list has been limited to three "main" components. In addition to confidentiality (covered by protection at the earliest point in time), the list comprised availability and integrity. Availability means the facility to use the

[5] Act of 29 August 2002 on Martial Law and the Competences of the Commander-in-Chief of the Army and the Rules of the Commander-in-Chief's Subordination to the Constitutional Authorities of the Republic of Poland (consolidated text, Polish Journal of Laws of 2016, item 851, as amended).

[6] For more details see Aleksandrowicz and Liedel (2014), pp. 23–27; Banasiński (2018), pp. 23–27; Kosiński (2013), pp. 462–463; Liderman (2017), pp. 62–63; Trąbiński (2018), pp. 70–74; D. Wall (2013), pp. 10–11.

[7] Act of 5 July 2018 on the National Cybersecurity System (consolidation text Polish Journal of Laws of 2020, item 1369, as amended, herein after "NCSA").

information by authorized persons whenever necessary. According to the guidelines included in the Recommendation of the OECD Council[8] concerning Guidelines for the Security of Information Systems C(92)188 of the 26th of October 1992, availability means that data is accessible and usable on a timely basis in the required manner. Under Article 4(d) of Regulation 460/2004, availability means that data is accessible and services are fully operational. According to the definition laid down in Recommendation C (92)188, integrity is understood as the characteristic of data and information being accurate and complete, and the preservation of accuracy and completeness. It refers to the integrity of both data and computer systems. As for information processed in an IT network, integrity means that the sent and received data are identical. This feature is defined in a similar way in Article 4(f) of Regulation (EC) No 460/2004 of the European Parliament and of the Council of the 10th of March 2004 establishing the European Network and Information Security Agency[9] (repealed, but the replacement regulations did not include the definition), as "the confirmation that data, which has been sent, received, or stored are complete and unchanged." It is worth mentioning that this is a theoretical scenario, which is impossible in practice. The vast majority of the currently existing ICT networks, including the Internet, are based on packet-switching technology (for more details, see further remarks in the discussion on the definition of information systems). This means that the data sent via such networks are divided into packets (millions of packets in the case of large data portions), which are then sent (often along various routes) and "compiled" together at the end point. It often happens that the some of the packets "get lost on the way" (it is easy to check, there are small differences between the sizes of the sent and the received file). Confidentiality means access to data only by authorized persons, excluding third parties. It involves the protection of data against the reading and copying of data by unauthorized individuals. The guidelines set out in recommendation C (92)188 define confidentiality as the characteristic of data and information being disclosed only to authorized persons, entities and processes at authorized times and in the authorized manner. In turn, under Article 4(g) of Regulation 460/2004, confidentiality is understood as the protection of communications or stored data against interception and reading by unauthorized persons.[10]

In addition to the ("core") attributes discussed above, one can currently speak of other properties of information. In line with the ISO 27001 standard (PL-EN IDO/IEC 27001, an international standard specifying the requirements for information-security management systems), information security is interpreted as the maintenance of the confidentiality, integrity, and availability of information. However, other components, such as authenticity, accountability, and reliability, may also be taken into consideration. Authenticity guarantees that the identity of a

[8]Recommendation of the Council concerning Guidelines for the Security of Information Systems of 26 November 1992, C(92)188/FINAL.

[9]OJ EU 2004 L 77/1.

[10]Radoniewicz (2016), pp. 143–144.

given entity or resource is as declared. Accountability means the assurance that the actions of such an entity can be assigned in a straightforward way only to this specific entity. Reliability is a property designating cohesive and intentional conduct and results.

These terms are defined in a similar way in the Regulation of the Council of Ministers of the 12th of April 2012 on the National Interoperability Framework, the minimum requirements for public records, the exchange of information in electronic form, and the minimum requirements for communication and information systems.[11]

- Authenticity: a property consisting of the fact that the origin or contents of data defining an object are as declared (§ 2(2))
- Availability: a property consisting of the fact that a given ICT-system resource can be used on demand, in a specified time, by an entity authorized to work in the communication and information system (§ 2 (4));
- Integrity: a property consisting of the fact that a given communication and information system resource has not been modified in an unauthorized manner (§ 2 (5));
- Confidentiality: a property consisting of the fact that information must not be provided or disclosed to unauthorized natural persons (§ 2 (14)).
- Accountability: a system property, which involves the attribution of a specified action to a natural person or process, and placing it within a specific time frame (§ 2 (18)).

The concept of "cybersecurity", as defined under Article 4(2) of the NCSA, was meant to constitute the equivalent of the expression "the security of network and information systems", as defined in NIS Directive[12] as the capacity of network and information systems to resist, at a given level of confidence, all actions, which compromise the availability, authenticity, integrity, or confidentiality of stored or transmitted or processed data, or the related services provided by, or accessible via, those network and information systems. It is clear that the two definitions differ in terms of defining elements. First, the term "information system" was used as the equivalent of "network and information system". Second, the legislator removed the phrase "at a given level of confidence", referring to "the ability to resist", with a view to 'relativising' the expression. It should be stressed that the phrase was present in the first draft of the Act, i.e. in the version referring to social consultations (prior to the work on the Bill in the Sejm, the lower house of the Polish Parliament, but was not included in the final version of the Bill,[13] due to the controversies, which had

[11]Regulation of the Council of Ministers of 12 April 2012 on the National Interoperability Framework, the minimum requirements for public records, the exchange of information in electronic form, and the minimum requirements for communication and information systems, Polish Journal of Laws of 2017, item 2247, as amended.

[12]OJ EU 12016 L 194/1.

[13]See: https://legislacja.rcl.gov.pl/projekt/12304650, accessed on 01/12/2020.

occurred during the consultations. First of all, the consultations indicated the need to define the phrase.[14] As shown above, the author of the Bill chose a simpler solution. Another difference is the narrowing down in the schedule of actions listed in the definition laid down in the Act by omitting the word "all" before "actions", which stressed the broadest possible scope of such activities, at the same time replacing the conjunction "or" with "and" in the catalogue of such actions. Therefore, one is dealing with conjunctions here, not alternatives, which seems to imply that the actions referred to in the said provisions must be simultaneously directed against the confidentiality, integrity, availability, and authenticity of the processed data, or the related services provided by those network and information systems. The next difference also resulted in the narrowing down of the scope of the definition, as the services "accessible via" information systems were omitted, and only "provided" services were retained. The definition in the NIS Directive mentions stored or transmitted or processed data, whereas the Polish legislator limited the list to the concept of "processing", which is a generic term in relation to storage and transmission.

To conclude the discussion on the differences between the definitions, it should be stressed that the definition in the NIS Directive was used in the National Framework of the Cybersecurity Policy of the Republic of Poland for 2017–2022 (Resolution of the Council of Ministers No. 52/2017 dated the 27th of April 2017 on the National Framework of Cybersecurity Policy of the Republic of Poland), as well as in the draft Cybersecurity Strategy.

3 The Notion of Cybercrime

To date, no legislator has decided to introduce the legal definition of a computer crime into the legal system. There have been attempts to define this term as part of penal-law studies. A comprehensive definition proposed by Ulrich Sieber during an OECD Expert Committee meeting in Paris in 1983, later included in the OECD report, according to which "computer crime is any illegal, unethical, or unauthorised behaviour involving the automatic data processing and/or transmission of data"[15] can be considered one of the first. A general definition of computer crime was developed several years later for Interpol. According to this definition, computer crime means "criminal activities in the scope of computer technologies", which can be divided into the following groups.

(1) The breach of resource-access rights
(2) Fraud with the use of computers

[14]See, for example, Remarks expressed by the Business Centre Club, the Polish Chamber of Commerce for Electronics and Telecommunications, and the Polish Chamber of Digital Broadcasting—See https://legislacja.rcl.gov.pl/projekt/12304650, Accessed on 1 December 2020.

[15]Sieber (1998), pp. 20–21; cf. Czechowski and Sienkiewicz (1993), p. 52.

(3) The modification of computer resources
(4) The reproduction of software
(5) Hardware and software sabotage
(6) Offences committed with the use of BBS
(7) The storage of illegal resources
(8) Crime on the Internet.[16]

Along with technological advancements, the terms describing the phenomenon of computer crime are also evolving. The earliest ones are, of course, "computer crime", "computer-related crime", "crime by computer", and "digital crime", the last one having a broader scope than "computer crime." The development of the Internet in recent years has led to the creation of a strong, and practically inseparable, relationship between information and telecommunication technologies. For this reason, numerous suggestions for terms and definitions have been coined to describe the phenomenon of computer crime. These include "Internet crimes", "e-crimes", "net crimes", virtual crimes", and finally "cybercrimes", "IT crimes", and "data-processing crimes."[17]

Without doubt, the term, which has gained greatest popularity is "cybercrime", used both in the literature on the subject and in some international documents (in particular, in the Convention on Cybercrime).

During the Tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders,[18] held in Vienna in April 2000, it was found that cybercrime referred to any crime, which can be committed by means of a computer system or network, in a computer system or network, or against a computer system or network. At the same time, the following classification of cybercrime was proposed.

(1) In a narrow sense (computer crime), meaning any illegal behaviour directed by means of electronic operations, which targets the security of computer systems and the data processed by them, i.e.

   – unauthorized access
   – damage to computers, computer data, or computer programmes
   – computer sabotage
   – unauthorized interception, and
   – computer espionage

(2) Cybercrime in a broader sense ("computer-related crime"): any illegal behaviour committed by means of, or in relation to, a computer system or network, including such crimes as illegal possession, and offering or distributing information by means of a computer system or network.[19]

[16] Fischer (2000), pp. 27–28.

[17] Adamski (2000), pp. 32–33. Cf. Fischer (2000), pp. 23–31; Wójcik (1999), pp. 52–57; Clough (2013), p. 9.

[18] *The Tenth United Nation Congress on the Prevention of Crime and Treatment of Offenders*.

[19] Cf. Smarzewski (2014), p. 267; Shinder and Tittel (2004), pp. 35–36.

4 The Classification of Cybercrimes

First, it is necessary to point to the simplest possible dichotomous classification of computer crime, divided into "old" and "new" offences. This refers to the "novelty" of an offence as such (not as a computer crime). The first group includes conventional (common) offences, which had gained a new or modified form due to technological developments (e.g. fraud, harassment, dissemination of child pornography). "New" offences are those, which came with the development of computers and advancements in information technology, and its further convergence with telecommunications. Obtaining unauthorized access to, or unauthorized modification of, computer data can serve as a classic example here.[20]

Both in the literature on the subject and in the legislations of various countries, it is possible to find a similar "tripartite" division of cybercrime[21] into computer crimes, computer-facilitated crimes, and computer-supported crimes.[22]

The above classification was also adopted in the Convention on Cybercrime.[23] Offences amounting to illegal acts categorized in the first group was grouped together under the single title "Offences against the confidentiality, integrity, and availability of computer data and systems." Offences in the second group are to be found in the subsequent three Sections of the Convention, and they are referred to as "computer-related offences", "content-related offences", and "offences related to infringements of copyright and related rights."

The last group in the tripartite division does not fall within the ambit of substantive penal law, but rather procedural law, in particular the law of evidence. Therefore, they are usually not considered in discussions on computer crime.

The issue of defining and classifying computer crimes has been taken up in the Polish literature on the subject. Andrzej Adamski pointed out that under the penal

[20]Cf. Grabosky (2006), pp. 12–14.

[21]Clough (2013), p. 10. Cf. Dudka (1998), p. 105. For information on the classification of computer crimes, see also Chałubińska-Jentkiewicz (2019), pp. 251–261; Kosiński (2013), pp. 463–465; Siwicki (2012), pp. 241–252; Smarzewski (2014), pp. 264–267.

[22]At the Forensic Science Society Convention held in April 2001 in Huntingdon, a classification of computer crime was made based on the criteria of the techniques applied by offenders, and the nature of their acts. It is a detailed version of the tripartite division described above. The classification features six categories of computer crime (cybercrime): computer-assisted crime (in which the committing of such a crime is facilitated by using computers), computer-enabled crime (in which computers enable the committing of such a crime), computer-only crime (which cannot be committed without using computer technology), Internet-assisted crime (which can be committed both in a conventional (common) way and via the Internet), Internet-enabled crime (in which it is easier to commit a given crime with the use of the Internet), and Internet-only crime (crime possible only via the Internet), meaning those offences in which the data sets on servers or data packets sent between network nodes are used by the perpetrators in the course of their actions (Hołyst 2009, pp. 19–20).

[23]The Council of Europe Convention on Cybercrime of 23 November 2001, https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185 accessed on 1 December 2020.

law, it is possible to differentiate between two meanings of the term "computer crime", from the substantive and procedural-law perspective,[24] and from the substantive-law perspective, in the latter of which two types of attacks can be identified.

(1) Attacks in which computer systems, applications, data, and information, are the subjects of crime, for example, hacking. The Polish legislator treats them (similarly to other penal-law legislations) as separate types of offence in which information is a generic object of protection. In the Polish Penal Code, such acts were addressed in Chapter XXXIII Offences Against Information Protection (offences in which computers, networks or computer data constitute the target of the perpetrator's actions), which corresponds to the first group of crimes, in which computers are the subject of illegal activities (the computer as a target).
(2) Attacks in which the targets include various legally protected rights, whereas a computer, computer network, data-processing systems and electronic devices serve as tools. They are used for committing both common offences, e.g. fraud, forgery, and unconventional crimes, such as money laundering (corresponding to the second group of offences included in the aforementioned tripartite division—"the computer as an instrument").

From the procedural perspective, computer crimes are offences in which computer systems can store evidence of criminal activities. Therefore, the group of computer crimes from the procedural perspective includes, in particular, any prohibited acts in which access to information processed in a computer system is required for prosecution purposes. This includes situations in which a computer system was an instrument used in an attack, and instances in which such a system was the target of the attack.[25]

In the Polish literature on the subject, some attention has been given to the issue of singling out Internet crime as a subcategory of computer crimes.

As B. Świątkiewicz noted, Internet crime cannot be treated as the equivalent of computer crime, since the Internet is a tool used for committing a wide range of offences, which are not necessarily reflected in the statutory criteria of a crime as laid down in the Penal Code.[26] First and foremost, it is certain that the term covers a narrower scope. Michał Sowa suggests that "Internet crime" can be defined as offences

> "for which the opportunities provided by the Internet" (web services) or services provided by people via the Internet allow the perpetrator to perform an intentional criminal act, or its individual stages, or at least facilitate the performance of such a criminal act.[27]

[24] Adamski (2000), p. 30.
[25] Adamski (2000), pp. 34–35.
[26] Świątkiewicz (2005), p. 111.
[27] Sowa (2001), p. 28.

Based on the above definition, it is possible to distinguish between Internet crime, in the strict sense of the term (types of prohibited acts, in which the main activities are conducted with the use of the Internet) and Internet crime in the broad sense (in which the committing of a given prohibited act is facilitated by the use of the Internet, including those offences in which the Internet is only a means to an end, or a tool to achieve the expected results outside the network).[28]

5 Challenges Related to the Emergence of Computer Crime

There are numerous characteristics of new technologies, which facilitate criminal activities, and, which at the same time hinder the prevention and prosecution of crime.

First of all, it is the sheer reach of the phenomenon. The Internet has provided communication opportunities on an unprecedented scale. It is estimated that approx. one and a half billion people have Internet access, which accounts for 24% of the world's population. It is an enormous number of potential perpetrators and victims.

The second feature is availability. The use of computers and the Internet has never been easier or cheaper. On the one hand, the prices of computer hardware and computer-network communications have fallen considerably, and, on the other hand, the use of technological advancements has become easier than in the past. The times when computers were enormous and expensive devices, requiring additional advanced knowledge to be operated are long gone. The Internet can currently be used on mobile phones. Computer programmes have a friendly graphical user interface, and the vast majority of users cannot imagine operating a computer in the so-called text mode (using command lines in MS Windows systems, or consoles in Unix/Linux systems).

Third is the ability to remain anonymous (often not as reliable as it might seem), which both Internet users and potential perpetrators of crimes committed via the Internet can enjoy. It creates an illusion of full confidentiality (or even secrecy) of all the activities performed by network users, and the related chance of avoiding potential penal liability.

Fourth is the possibility to collect a substantial quantity of information across a small space, from which the data can be easily retrieved, and in which it can be reproduced and disseminated without limitations.

The fifth feature is its global reach, which means that the offences committed by perpetrators in one country can have a negative effect in another country. This can create extremely complex situations. For instance, this is the case when a perpetrator based in country A carries out a DDoS attack (Distributed Denial of Service) against a server located in country B, using computers located in countries C and D, while residents of countries E and F can suffer the consequences of such activities.

[28] Sowa (2001), pp. 29–30.

The last, yet equally important, factor, indicated in the literature on the subject, which hinders counteracting computer crime, includes circumstances related to investigating crimes and conducting penal proceedings. The ephemeral nature of computer data is a source of problems related to collecting and securing evidence. There are also problems arising from the international reach of the network, and the private nature of many of them, which obstructs the access to, e.g., traffic data, which is stored on servers only for a specified period of time. The obvious consequence of the technical nature of computer crime is the fact that individuals dealing with the prosecution of perpetrators must have knowledge of state-of-the-art technology and the appropriate hardware.[29]

When discussing the issue of cybercrime definitions and classifications, it is worth mentioning those acts, which cannot be placed in the category of computer crime.

6 Cyberterrorism and Cyberwar

Susan W. Brenner makes a precise distinction between computer crime and the phenomena of cyberterrorism,[30] and cyberwarfare, treating them as notions separate from cybercrime. She assigns a very broad sense to the former term, making the assumption that it includes terrorist attacks which are planned, carried out, and coordinated, via computers and computer networks, while the latter is defined as actions taken by states using information technology with a view to achieving military or other strategic goals.[31]

The second most frequently cited definition of cyber-terrorism, provided by D. Denning, has a much narrower meaning. According to this author, cyber-terrorism is a combination of terrorism and cyberspace. In general, it is understood as unlawful attacks and threats of attacks against computers, networks, and information collected in networks to intimidate or coerce governments, or the residents, of a given state, to fulfil political or social objectives. Moreover, in order to be classified as cyberterrorism, a given attack should result in violence against people and property, or cause such a degree of harm that it could evoke fear. Attacks resulting in death or injuries, explosions, plane crashes, water pollution, or severe economic loss, might serve as examples here. Major attacks against critical infrastructures can be treated as cyber-terrorist attacks, depending on their outcomes. The category does not include attacks, which lead to the disruption of non-critical services, or mainly result in financial problems.[32]

[29]Clough (2013), pp. 5–8; Radoniewicz (2016), pp. 128–129.

[30]Unlike D.L. Shinder and E. Tittel, who classified cyberterrorism as cybercrimes involving the use of violence. See remarks above.

[31]Brenner (2010), p. 16.

[32]Verton (2004), p. 20.

7 Terrorism in EU Law

The first EU legal instrument aimed at counteracting terrorism was Council Framework Decision of the 13th of June 2002 2002/475/JHA on combating terrorism[33] (further referred to as "Framework Decision 2002/475"). The document was replaced by Directive (EU) 2017/541 of the European Parliament and of the Council of the 15th of March 2017 on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA, which is based on the Framework Decision, and substantially replicates its solutions (this refers to, e.g., the definition of a terrorist offence), at the same time clarifying some solutions and adding new ones.

Most of all, Directive 2017/541 established the minimum rules concerning the definition of criminal offences and sanctions in the field of terrorist offences,[34] offences related to a terrorist group, and offences related to terrorist activities, as well as measures for the protection of, support for, and assistance to, victims of terrorism. The definition of a terrorist offence laid down in Article 3 of Directive 2017/541 (similar to the one included in Framework Decision 2002/475) is composed of two elements, i.e. objective (*actus reus*) and subjective (*mens rea*) elements. For a prohibited act to be considered a terrorist offence, first of all, it must meet an objective criterion, i.e., it must be one of the acts listed in an exhaustive schedule included in Article 3(1)(a) to (i),[35] or the threat to commit any of the acts (Article 3(1)(j)). Second, a terrorist offence must meet at least one of the subjective premises listed in the second part of the definition, i.e. it must be committed with one of the aims listed in paragraph 2, including

[33]Council Framework Decision 2002/475/JHA of 13 June 2002 on combating terrorism, OJ EC 2002 L 164/3.

[34]Framework Decision 2002/475 and Directive 2017/541 refer to "terrorist offences", while the provisions of the Polish Penal Code of 6 June 1997 (consolidated text, Polish Journal of Laws of 2020, item 1444, as amended, hereinafter "PC") refer to "offences of a terrorist nature".

[35]The following acts were listed in Article 3(1): (a) attacks on a person's life which can cause death; (b) attacks on the physical integrity of a person; (c) kidnapping or hostage-taking; (d) causing extensive destruction to a government or public facility, a transport system, an infrastructure facility (including an information system), a fixed platform located on the continental shelf, a public place or private property, likely to endanger human life, or result in major economic loss; (e) seizing aircraft, ships, or other means of public or goods transport; (f) the manufacture, possession, acquisition, transporting, supply or use of explosives or weapons, including chemical, biological, and radiological or nuclear weapons, as well as research into, and development of, chemical, biological, radiological, or nuclear weapons; (g) releasing dangerous substances, or causing fires, floods or explosions, the effect of which is to endanger human life; (h) interfering with or disrupting the supply of water, power, or any other fundamental natural resource, the effect of which is to endanger human life; (i) illegal system interference, as referred to in Article 4 of Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA, in cases in which Article 9 (3) or points (b) or (c) of Article 9(4) of that Directive apply, and illegal data interference, as referred to in Article 5 of that Directive in cases in which point (c) of Article 9(4) of that Directive applies (see further remarks).

(1) seriously intimidating a population
(2) unduly compelling a government or an international organisation to perform or abstain from performing any act
(3) seriously destabilising or destroying the fundamental political, constitutional, economic, or social structures of a country or an international organisation.[36]

Under Article 4 of Directive 2017/541, Member States are obliged to make sure that directing a terrorist group,[37] and participating in the activities of a terrorist group, are acts punishable as criminal offences. It was pointed out that the latter should also be understood as including supplying information or material resources, or by funding its activities in any way, in the knowledge of the fact that such participation will contribute to the criminal activities of the terrorist group.

Pursuant to the subsequent Articles of Directive 2017/541, Member States are obliged to criminalise "offences related to terrorist activities", involving certain activities, which are not terrorists acts per se, but might constitute the preparation to commit terrorist acts.[38]

Under Article 15(1) of Directive 2017/541, the offences referred to in the Directive should be punishable by effective, proportionate, and dissuasive, criminal penalties, which may entail surrender or extradition.

The terrorist offences referred to in Article 3 of Directive 2017/541, and in Article 14 of the said document (aiding and abetting, inciting and attempting offences laid down in the Directive),[39] should be punishable by custodial sentences heavier than

[36]The aforementioned Framework Decision 2002/475 was enacted into the Polish legal framework by way of the Act of the 16th of April 2004 on amending the Penal Code and certain other Acts (Journal of Laws of 2004, No. 93, item 889). For more details, see Chapter 23 of this monograph. See also Radoniewicz (2015), pp. 192–196.

[37]According to the definition laid down in Article 2(3) of Directive 2017/541, the terms should be understood as "a structured group of more than two persons, established for a period of time and acting in concert to commit terrorist offences." According to the definition included in the second part of the cited provision, "structured group" means a group which is not randomly formed for the immediate commission of an offence, and that does not need to have formally defined roles for its members, continuity of membership or a developed structure."

[38]They include the following offences: public provocation to commit a terrorist offence (Article 5); recruitment for terrorism (Article 6); providing training for terrorism (Article 7); receiving training for terrorism (Article 8); travelling for the purpose of terrorism (Article 9); organising or otherwise facilitating travelling for the purpose of terrorism (Article 10); terrorist financing (Article 11), and other offences related to terrorist activities, listed in Article 12: (a) aggravated theft with a view to committing one of the offences listed in Article 3; (b) extortion with a view to committing one of the offences listed in Article 3; (c) drawing up or using false administrative documents with a view to committing one of the offences listed in points (a) to (i) of Article 3(1), point (b) of Article 4, and Article 9.

[39]Aiding and abetting the offences referred to in Articles 3 to 8, 11 and 12 (and Article 14(1)), inciting the offences referred to in Articles 3 to 12 (and Article 14(2)), and attempting to commit the offences referred to in Articles 3, 6, 7, Article 9(1), point (a) of Article 9(2), and Articles 11 and 12, with the exception of possession as provided for in point (f) of Article 3(1), and the offences referred to in point (j) of Article 3(1) (and Article 14(3)), should be punishable by law.

those imposable under national law for such offences, which have no element of "terrorist intent" (Article 15(2).

The offences listed in Article 4 of Directive 2017/541 (offences relating to a terrorist group) should be punishable by custodial sentences, with a maximum sentence of not less than 15 years for the offence referred to in point (a) of Article 4 (directing a terrorist group), and a maximum sentence of not less than 8 years for the offences listed in point (b) of Article 4 (participating in the activities of a terrorist group) (Article 15(3)).

When a criminal offence referred to in Article 6 (recruitment for terrorism) or 7 (providing training for terrorism) is directed towards a child, this may, in accordance with national law, be taken into account when sentencing (Article 15(4) of Directive 2017/541).

8 Cyberterrorism: Terrorism in Cyberspace

The first binding European Union legal Act relating to attacks against security in cyberspace was Council Framework Decision 2005/222/JHA of the 24th of February 2005, on attacks against information systems[40] (Framework Decision 2005/222). Work on the draft began in 2001, as a result of the European Commission's announcement of the so-called Communication on Cybercrime,[41] containing certain proposals for substantive and procedural-law provisions, directed at combating computer crime, at both the national and Community levels. The outcome of those activities was, i.a., a proposal for the aforementioned framework decision.[42]

In citing Framework Decision 2005/222, it was indicated that its objective was to improve cooperation between the judicial authorities and law-enforcement services of Member States, through approximating the rules on criminal law in Member States in the field of attacks against information systems. The legislative activities at the EU level were substantiated by the need to counteract attacks against information systems, due to the possible relationship between this type of offence and organised crime, and terrorist attacks against information systems, which formed part of the critical infrastructure of the Member States.

First and foremost, under Framework Decision 2005/222, the most important terms were defined ("information system", "computer data", "legal person" and "without right"), and Member States were obliged to make sure that illegal access

[40]Council Framework Decision 2005/222/JHA of 24 February 2005, on attacks against information systems, OJ EU 2005 L 69/67.

[41]Communication from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions COM(2000)890 on Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime of 26 January 2001.

[42]Proposal for a Council Framework Decision on attacks against information systems, COM (2002) 0173.

to information systems, illegal system interference, and illegal data interference, were punishable as offences. The document also refers to the issues of the liability of legal persons, jurisdiction, and the use the network of operational points of contact available twenty four hours a day, seven days a week, for the purpose of exchanging information on attacks against information systems.

The limited number of offences referred to in Framework Decision 2005/222, the need to incorporate new threats, and the wish to adapt the existing legal regulations to new European Union initiatives in the field of cybersecurity, and to supplement them in order to regulate the matter comprehensively, led to a decision to commence work on a new legal instrument addressing the issue of cybercrime. The result was the enactment of Directive 2013/40/EU of the European Parliament and of the Council of the 12th of August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA[43] (Directive 2013/40).

In citing the Directive, it was stressed that attacks against information systems, and, in particular, attacks linked to organised crime, and the potential for terrorist or politically motivated attacks against information systems, were a growing menace, and that they could pose a real threat to information systems forming part of critical infrastructures of Member States and the European Union.

The contents of Directive 2013/40 are largely based on the provisions of Framework Decision 2005/222/JHA, at the same time providing for certain new solutions (new types of prohibited acts: the illegal interception of computer data, and offences related to the use of "hacking tools", and the specification of additional aggravating circumstances to consider when sentencing offenders).

For the purpose of Directive 2013/40 (and previously for the purpose of Framework Decision 2005/222), an "information system" is defined as a device or group of inter-connected or related devices, one or more of which, pursuant to a programme, automatically processes computer data, as well as computer data stored, processed, retrieved or transmitted by that device or group of devices for the purposes of its or their operation, use, protection and maintenance (Article 2(a)).

The above definition can be characterised by a broad objective scope. Given the above, an information system should be understood as both a single data-processing device (e.g. a computer or a smart phone) and a computer network, including small networks (e.g. LAN[44]), covering several computers, and large-scale structures consisting of interconnected networks (e.g. MAN[45]).[46]

[43]Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA, OJ EU 2013 L 218/8.

[44]LAN—Local Area Network.

[45]MAN (Metropolitan Area Network)—covering numerous interconnected local area networks, networks of this type are developed by public institutions, universities (university networks) or private entities (enterprises).

[46]Due to the volume limits of this study, the issue will not be discussed in detail. For more details, see Radoniewicz (2016), pp. 244–249; Radoniewicz (2019a), pp. 42–47.

Under Article 2(b) of Directive 2013/40, the term "computer data" was defined as a representation of facts, information, or concepts in a form suitable for processing in an information system, including a program suitable for causing an information system to perform a function.

Under Article 2(d) of Directive 2013/40, "without right" means conduct referred to in this Directive, including access, interference, or interception, which is not authorized by the owner, or by another rights holder, of the system, or of part of it, or not permitted under national law.

Article 3 of the said Directive includes an obligation imposed on Member States to ensure that, when gained intentionally, access without right to the whole or to any part of an information system, is punishable as a criminal offence committed by infringing a security measure. Access to information systems is understood as the possibility of using their resources (i.e. using the data stored in the systems, and the use of hardware, which, in fact, results in access to data and software used for controlling such access).

Another offence defined in Directive 2013/40 is illegal system interference, which consists of seriously hindering or interrupting the functioning of an information system by inputting computer data, by transmitting, damaging, deleting, impairing, altering, or suppressing such data, or by rendering such data inaccessible, intentionally and without right (Article 4 of Directive 2013/40). This mostly includes activities involving logic operations directed against information systems, with a view to hindering or disrupting system functions by affecting the processing of the computer data of the software used for the purpose.

Under Article 5 of Directive 2013/40, Member States are obliged to criminalise logical attacks directed against computer data. The provision identifies illegal data interference as deleting, damaging, impairing, altering, or suppressing computer data in an information system, or rendering such data inaccessible. Such interference includes both deleting data and installing software on the compromised computer, facilitating further illegal activities (e.g. data theft), or carrying out a DDoS attack (Distributed Denial of Service) by using malware to connect a compromised computer to a botnet.

The first "new" prohibited act (in relation to Framework Decision 2005/222) was illegal interception, defined in Article 6 of Directive 2013/40 as intercepting, by technical means, non-public transmissions of computer data to, from, or within, an information system, including electromagnetic emissions from an information system carrying such computer data, intentionally and without right.

Another type of offence, which was not provided for in Framework Decision 2005/222, is referred to in Article 7 of Directive 2013/40. Under the said provision, Member States are required to criminalise the intentional production, sale, procurement, importing, possession, and distribution, or otherwise making available, of tools (colloquially referred to as "hacking tools") used, without right, to commit any of the offences referred to in Articles 3 to 6 of Directive 2013/40, in which such acts are performed with the intention to commit the said offences.

"Tools" means

(1) a computer programme, designed or adapted primarily for the purpose of committing any of the offences referred to in Articles 3 to 6
(2) a computer password, access code, or similar data, by which the whole or any part of an information system is capable of being accessed.

In line with Article 9(1) of Directive 2013/40, the offences referred to in the said Directive (including incitement, aiding and abetting, and attempting to commit offences under Articles 4 and 5—see Article 8(1) and (2)), should be punishable by effective, proportionate, and dissuasive, criminal penalties. At the same time, it is stipulated that the offences referred to in Articles 3 to 7 of Directive 2013/40 (which means that it does not apply to incitement, aiding and abetting, and attempting to commit offences) should be punishable by a maximum term of imprisonment of at least 2 years, at least for cases which do not involve a minor (Article 9(2)).

Furthermore, Article 9 of Directive 2013/40 provides for a number of aggravating circumstances. However, they only apply to offences listed in Articles 4 and 5 (i.-e. illegal system interference and illegal data interference). The first aggravating circumstance includes a situation in which a significant number of information systems have been affected through the use of a tool, referred to in Article 7 of Directive 2013/40, designed or adapted primarily for that purpose. In such an event, the perpetrator should be sentenced to a maximum term of imprisonment of at least 3 years (Article 9(3) of Directive 2013/40).

Under Article 9(4) of Directive 2013/40, aggravating circumstances, resulting in the possibility of the perpetrator's being sentenced for a maximum sentence of imprisonment of at least 5 years, include the commitment of offences within the framework of a criminal organisation, as defined in Framework Decision 2008/841/JHA of the 24th of October 2008 on the combating organised crime,[47] causing serious damage, and the committing of an offence against a critical-infrastructure information system.[48]

[47]Framework Decision 2008/841/JHA of 24 October 2008 on the fight against organised crime, OJ EU 2008 L 300/42. Pursuant to Article 1(1) of the said Decision, "criminal organisation" means a structured association, established over a period of time, of more than two persons acting in concert with a view to committing offences which are punishable by deprivation of liberty or a detention order of a maximum of at least four years, or a more serious penalty, to obtain, directly or indirectly, financial or other material benefit. "Structured Association" means an association which was not randomly formed for the immediate committing of an offence, nor does it need to have formally defined roles for its members, continuity of membership, or a developed structure (Article 1(2) of Framework Decision 2008/841). A solution similar to the one stipulated in Framework Decision 2005/222 was adopted in Directive 2013/40, under which the penalty provided in Framework Decision 2008/841 was not taken into consideration when establishing whether a given structured association can be considered a criminal organisation.

[48]Under Article 2(a) of Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures, and the assessment of the need to improve their protection, OJ EU 2008 L 345/75, the term critical infrastructure means an asset, system, or part thereof, located in Member States, which is essential for the maintenance of vital societal functions, and the health, safety, security, economic, or social well-being of people, and the disruption or

The last aggravating circumstance affecting penal liability (Article 9(5)) is a situation in which the offences referred to in Articles 4 and 5 are committed by misusing the personal data of another person (identity theft).[49]

The Directive was criticised for the failure to provide severe sanctions, especially in relation to acts, which can be classified as terrorist attacks against IT systems. This reservation can currently be considered outdated. Discussing the issue of making more stringent the penal liability of a perpetrator accused of an offence of a terrorist nature, one should take into account the legal regulations laid down in Directive 2017/541. Pursuant to point (i) of Article 3(1), in conjunction with Article 3(2) of the said Directive (see remarks above), illegal system interference as referred to in Article 4 of the Directive in cases in which Article 9(3) or points (b) or (c) of Article 9(4) of that Directive applies, and illegal data interference as referred to in Article 5 of that Directive, in cases in which point (c) of Article 9(4) of that Directive applies, constitute a terrorist offence. This means that terrorist offences should include acts involving illegal system interference committed with one of the aims listed in Article 3(2) of Directive 2017/541, with the use of one of the tools referred to in Article 7 of Directive 2013/40, designed or adapted primarily for that purpose, in which a significant number of information systems have been intentionally affected, or in which substantial damage has been inflicted. In addition, an unlawful act under Article 5 should be considered a terrorist offence if it has been directed against a critical-infrastructure information system.[50]

References

Adamski A (2000) Prawo karne komputerowe, Warsaw
Aleksandrowicz TR, Liedel K (2014) Społeczeństwo informacyjne – sieć, cyberprzestrzeń. Nowe zagrożenia. In: Aleksandrowicz TR, Liedel K, Piasecka P (eds) Sieciocentryczne bezpieczeństwo. Wojna, pokój i terroryzm w epoce informacji, Warsaw
Banasiński C (2018) Podstawowe pojęcia i podstawy prawne bezpieczeństwa w cyberprzestrzeni. In: Banasiński C (ed) Cyberbezpieczeństwo. Zarys wykładu, Warsaw
Brenner SW (2010) Criminal threats from cyberspace crime, media, and popular culture. Preager
Chałubińska-Jentkiewicz K (2019) Cyberodpowiedzialność. Toruń
Clough J (2013) Principles of cybercrime. Cambridge University Press, New York
Czechowski R Sienkiewicz P (1993) Przestępcze oblicza komputerów, Warsaw
Dudka K (1998) Kontrola korespondencji i podsłuch w polskim procesie karnym, Lublin
Fischer B (2000) Przestępstwa komputerowe i ochrona informacji, Kraków
Grabosky P (2006) Electronic crime. Pearson Prentice Hall, Upper Saddle River
Hołyst B (2009) Internet jako miejsce popełnienia przestępstwa, Prokuratura i Prawo, 4

destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions.

[49]See more Radoniewicz (2018), pp. 111–121.

[50]Cf. Radoniewicz (2016), pp. 267–268. For more details about combating cyberterrorism in UE, see Radoniewicz (2019b), pp. 193–205.

Kosiński J (2013) Cyberprzestępczość. In: Jasiński W, Mądrzejowski W, Wiciak K (eds) Przestępczość zorganizowana. Fenomen. Współczesne zagrożenia. Zwalczanie. Ujęcie praktyczne, Szczytno
Liderman K (2012) Bezpieczeństwo informacyjne, Warsaw
Liderman K (2017) Bezpieczeństwo informacyjne, Warsaw
Radoniewicz F (2015) Techniki implementacji do polskiego porządku prawnego postanowień decyzji ramowych Rady Unii Europejskiej dotyczących prawa karnego materialnego, Przegląd Prawa Konstytucyjnego 3
Radoniewicz F (2016) Odpowiedzialność karna za hacking i inne przestępstwa przeciwko danym komputerowym i systemom informatycznym, Warsaw
Radoniewicz F (2018) Identity theft in the polish criminal code. In: red. Brzostek A, Nowikowska M, Taczkowska-Olszewska J (eds) Reform of protection of personal data system - purpose, tools. Poznań
Radoniewicz F (2019a) In: Kitler W, Taczkowska-Olszewska J, Radoniewicz F (eds) Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz, Warsaw
Radoniewicz F (2019b) Zwalczanie cybeterroryzmu w prawie UE – aspekty karnomaterialne. Cybersecurity and Law 2
Shinder DL Tittel E (2004) Cyberprzestępczość. Jak walczyć z łamaniem prawa w sieci [Original title: "Scene of the Cybercrime. Computer Forensics Handbook"], Polish Version: Gliwice
Sieber U (1998) Legal aspects of computer-related crime in the information society – Comcrime-study, Würzburg
Siwicki M (2012) Definicje i podział cyberprzestępstw. Prokuratura i Prawo 7–8
Smarzewski M (2014) Cyberprzestępczość a zmiany w polskim prawie. In: Sepioło-Jankowska I (ed) Reforma prawa karnego. Księga po Zjeździe Młodych Karnistów, Warsaw
Sowa M (2001) Ogólna charakterystyka przestępczości internetowej, Palestra 5–6
Świątkiewicz B (2005) Przestępstwa internetowe w praktyce policyjnej, Studia Prawnicze 4
Trąbiński P (2018) Podział kompetencji w zapewnianiu cyberbezpieczeństwa. In: Szpor G, Gryszczyńska A (eds) Internet. Strategie bezpieczeństwa. Warsaw
Verton D (2004) Black Ice. Niewidzialna groźba cyberterroryzmu [Original title: Black Ice: The Invisible Threat of Cyber-Terrorism], Polish edition: Gliwice
Wall D (2013) Cybercrime. The Transformation of Crime in the Information Age, Malden
Wójcik JW (1999) Przestępstwa komputerowe. Część I. Fenomen cywilizacji, Warsaw

Filip Radoniewicz PhD; legal advisor; adjunct in the Department of Cybersecurity Law and New Technologies at the Institute of Law, War Studies University, Warsaw; expert at the Academic Centre for Cybersecurity Policy, (War Studies University) and in the Ministry of Justice; he worked as an assistant judge (in the Fourth Criminal and Sixth Penitentiary Department of the Regional Court in Lublin); graduate of post-graduate studies: "European Union Law" at the Jagiellonian University, "Human Rights and Freedoms", co-organized by the Institute of Legal Sciences of the Polish Academy of Sciences and the Helsinki Foundation for Human Rights, and "Computer Network Administration" at the Lublin University of Technology; author or co-author of approximately fifty publications, mainly in the field of broadly understood criminal law, new technology law and human rights. Selected publications: F. Radoniewicz (2016) Odpowiedzialność karna za hacking i inne przestępstwa przeciwko danym komputerowym i systemom informatycznym/Criminal liability for hacking and other offences against computer data and information systems/, Wolters Kluwer, Warszawa; Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz /Act on the National Cybersecurity System. Commentary/ (2019) ed. W. Kitler, J. Taczkowska-Olszewska, F. Radoniewicz, CH. Beck, Warszawa.

Open Access This chapter is licensed under the terms of the Creative Commons Attribution 4.0 International License (http://creativecommons.org/licenses/by/4.0/), which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license and indicate if changes were made.

The images or other third party material in this chapter are included in the chapter's Creative Commons license, unless indicated otherwise in a credit line to the material. If material is not included in the chapter's Creative Commons license and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder.