PAPERS

Jacek Gerwatowski[1]
ORCID: 0000-0002-9127-7528

Cyberterrorism as an Effect of the Evolution of New Information Technologies in the First and Second Decades of the 21st Century

The development of information technologies, cyberspace and other tools operating thanks to them has undoubtedly brought us many facilitations (for example in the fields of science and communication) – we cannot even imagine our everyday lives without them. The speed and efficiency of information transfer are increasing all the time and the costs of access to the network and equipment operating costs are acceptable. Many users of both computers and mobile devices are unable to work without Internet access due the tasks they perform. The scale of development in this area can be illustrated by the mobile devices market. Based on this example, if we look just several years back, we will realise that at that time it was monopolised by phones with a monochrome display[2], and only a few models had access to the Internet. GPRS (General Packet Radio Service) technology was used to transmit data, which operated at the speed of 30–80 kb/s.

Similarly, the GSM (*Global System for Mobile Communications*) network was based on a radio signal transmitted by antennas mounted on the ground. Despite very limited possibilities (temporal signal fading, instability), a relatively efficient use of less complex services (such as access to electronic banking) has become possible since the entry of the EGPRS (Enhanced Data rates for GSM Evolution) technology into use. The boom in the market of smartphones that can take full advantage of the Internet access took place after 2007[3].

[1] Jacek Łukasz Gerwatowski – 4th year doctoral student in security sciences at the Faculty of Social Sciences of the University of Natural Sciences and Humanities in Siedlce. His scientific interests include information security.
Correspondence address: <jg453@stud.uph.edu.pl>.

[2] Meaning one-colour. The word comes from mono – single, and chroma – colour.

[3] *See*: Długołęcki S, Ewolucja telefonii komórkowej i mobilnego internetu. *Electronic source*: https://www.pcworld.pl/news/Ewolucja-telefonii-komorkowej-

The dynamics of technological progress and the development of the IT sphere are illustrated by the data presented by Simon Kemp on the website https://datareportal.com/[4]. According to the data from 2019, the number of Internet users in Poland was 30.07 million people. The number of active users of social media was at the level of 18 million people, and 16 million people used social media on mobile devices. Compared to 2018, the number of Internet users increased by 1.1%, *i.e.* by 325,000 people. The number of active users of social media increased by 1 million people, *i.e.* by 5.9%. The number of users of social media on mobile devices increased by as much as 2 million people, or 14% compared to 2018[5]. In 2019, the average daily time spent using the Internet from any device was around 6 hours. As for the average daily use of social media, it was 1 hour and 45 minutes, and the average daily time spent watching TV, including broadcast, streaming and video-on-demand, was approximately 3 hours. The average daily time spent listening to streaming music was around 1 hour. The frequency of using the Internet in Poland in 2019 was as follows: 82% of users used the Internet every day, 13% of users used the Internet at least once a week, 5% of users declared using the Internet at least once a month. Less than 1% used the Internet less than once a month[6]. Globally, in 2019 the number of Internet users amounted to 4.388 billion people, *i.e.* 57% of the population[7].

The number of active users of social media was at the level of 3.484 billion people, which accounted for 45% of the population. 3.256 billion people were users of social media on mobile devices, that is, 42% of the population. The global number of Internet users increased by 367 million people, *i.e.* 9.1%, compared to 2018. The number of active social media users in the period from January 2018 to January 2019 increased by 288 million, or 9%, and the number of social media users on mobile devices increased by 10%, or 297 million people[8].

However, we cannot forget that the Internet is only a tool. And just like any other tool, it can also be used for evil purposes. For example, such as criminal activity, terrorism as well as agitation and recruitment

i-mobilnego-iternetu,375151.html, *accessed*: 21 January 2020; Redakcja DailyWeb, *4G, LTE, 3G, 2G — czym różnią się od siebie poszczególne technologie? Electronic source*: https://dailyweb.pl/4g-lte-3g-2g-czym-roznia-sie-od-siebie-poszczegolne-technologie/, *accessed*: 21 January 2020.

[4] Datareportal, All the numbers you need. *Electronic source*: https://datareportal.com/reports/digital-2019-poland, *accessed*: 3 February 2021.

[5] *See*: Digital 2019: Poland. *Electronic source*: https://datareportal.com/reports/digital-2019-poland, *accessed*: 20 January 2020.

[6] *Ibid*.

[7] *See*: Simon Kemp, Digital 2019: Global Digital Overview, 31 January 2019. *Electronic source*: datareportal.com/reports/digital-2019-global-digital-overview, *accessed*: 20 January 2020, According to the information posted on the website, the human population in 2019 was 7.676 billion people.

[8] *Ibid*.

of various groups[9]. Other effects of misuse of the opportunities offered by the Internet include: paralysis of private enterprises and state institutions, disclosure of secret and private information, such as personal data, destruction or deletion of data which have a key importance for the functioning of the state and the private sector, communication paralysis.

It should be clearly stated that, at the moment, information is a valuable product. It can be stolen, sold, destroyed, and used to receive material or ideological benefits[10].

Definition of terrorism and cyberterrorism in literature and research

Before we answer the main question of that article – what exactly cyberterrorism is it is necessary to explain the concept of terrorism[11]. Terrorism has not been defined in any unequivocal way. This problem is characterised by many different factors. The international community has also failed to work out a common definition[12]. This term can be defined as "organised and planned activities that are undertaken both by individuals acting alone, and by groups of people. Terrorist actions are taken in violation of the existing law. Their intention is to force the state authorities and the society to behave and benefit in certain ways, often violating the welfare of outsiders; these activities are carried out ruthlessly by various means (physical violence, use of weapons and explosives, mental stress), in conditions of the publicity given to them and fear created deliberately in society. Terrorist activities have multiple motives. These are ideological motives"[13].

The common element of both concepts is the use of violence (or the threat of its use) by different types of extremist, political, religious or armed groups to achieve their own goals. This violence is most often directed against the civilian population.

Brunon Hołyst characterises terrorism as "the use of terror by extremist groups which, by means of political killings, hostage kidnapping, aircraft,

[9] Bielski K, Cyberterroryzm — nowe zagrożenie bezpieczeństwa państwa w XXI wieku. *Acta Politica*, 2015, No. 34, p. 93.

[10] Janowska A, Cyberterroryzm — rzeczywistość czy fikcja?, [in:] Haber L.H (Ed.), Społeczeństwo informacyjne — wizja czy rzeczywistość? Tom 1, Krakow, 2003, p. 446.

[11] *See*: Liedel K, Współczesne zamachy terrorystyczne: forma, metoda, cel. *Electronic source*: http://rcb.gov.pl/wspolczesne-zamachy-terrorystyczne-forma-metoda-cel/, *accessed*: 15 January 2020; Fiszer J, Terroryzm jako zagrożenie dla bezpieczeństwa euroatlantyckiego i nowego ładu międzynarodowego, [in:] Fiszer J, Olszewski P (Eds), System euroatlantycki w wielobiegunowym ładzie międzynarodowym. Warsaw, 2013, pp. 267–292.

[12] Bielski K, Cyberterroryzm..., *op.cit.*, p. 95.

[13] *See*: Encyklopedia PWN online, keyword: terroryzm. *Electronic source*: https://encyklopedia.pwn.pl/haslo/terroryzm;3986796.html>, *accessed*: 14 January 2020.

sea and other hijacking, tries to draw public attention to its slogans and demands or force governments to make certain concessions"[14].

On the other hand, according to Victor Grotowicz, "terrorism is a form of political extremism that uses methods of massive acts of violence to eliminate the state based on a democratic constitutional order. The intention of terrorists is to completely destabilise the state system, to create mass revolutionary movements and, consequently, to overthrow the old system and replace it with a new one"[15].

The US Federal Bureau of Investigation characterises terrorism as "an unlawful use of force or violence against persons or property to intimidate or coerce a government, civilian population, or a part of the aforementioned. The purpose of terrorist activities is to promote social or political goals"[16].

Bartosz Bolechów, in his book "Terrorism. Actors, extras, audiences", presents an extensive definition of terrorism. The cited author defines it as follows: "Terrorism is a fear-inducing method of repetitive acts of violence, politically motivated, used against non-fighting targets by individuals, groups or state actors operating in semi-secrecy, where, unlike other forms of political violence, the direct target of the attack is not the primary target. Immediate targets are chosen randomly (opportunistically) or selectively (symbolic or representative targets) and serve as message generators. Terrorism is therefore a form of psychological manipulation and violent communication between terrorists and their audiences through the victims. The auditoriums are to become the object of terror (when it comes to intimidation), demands (when it comes to extortion) or attention (when it comes to propaganda)"[17].

The multitude of ways of defining terrorism is distinctly illustrated by the fact that Alex Schmid, on the basis of the analysis of over 100 definitions, distinguished the main features of this concept (see Table 1).

Table 1

Main features of terrorism according to A. Schmid

No.	Feature	Frequency of occurrence (%)
1.	Violence, strength	83.5
2.	Political character	65
3.	Fear, emphasis on terror	51

[14] *See*: Hołyst B, Terroryzm. Tom 1. Warsaw, 2011, p. 52.

[15] Grotowicz V, Terroryzm w Europie zachodniej. Warsaw–Wrocław, 2000, p. 13.

[16] Wojciechowski S, Terroryzm. Analiza pojęcia. *Przegląd Bezpieczeństwa Wewnętrznego*, 2009, No. 1, p. 57.

[17] Bolechów B, Terroryzm. Aktorzy, statyści, widownie. Warsaw, 2010, p. 9. Wider Schmid A.P, Jongman A.J, Political Terrorism. A New Guide to Actors, Authors, Concepts, Data Bases, Theories & Literature, New Brunswick–London, 2005, p. 28.

4.	Threat	47
5.	Effects (psychological) and reactions (predictable)	41.5
6.	Distinguishing between the concepts of victim and the purpose of action	37.5
7.	Purposeful, planned, systematic, organised action	32
8.	Combat methods, strategy, tactics	30.5
9.	Abnormality, conflict with accepted rules, lack of humanitarian restrictions	30
10.	Extortion, enslavement, causing submission	28
11.	Search for publicity, advertising	21.5
12.	Randomness, impersonality, indiscrimination	21
13.	Civilians, people not involved in combat – neutral and standing aside as victims	17.5
14.	Intimidation	17
15.	Stressing the innocence of victims	15.5
16.	Group, movement, organisation as a perpetrator	14
17.	Using symbolism, demonstrating your strength to others	13.5
18.	Incalculability, unpredictability, unexpected acts of violence	9
19.	Covert nature of an organisation using terrorist methods	9
20.	Uniqueness, seriality or advertising nature of violence	7
21.	Criminal nature of attacks	6
22.	Requests for third parties	4

Source: Wojciechowski S, Terrorism. Analysis of the concept, "*Review of Internal Security*" 2009, No. 1, p. 58 [after:] A.P Schmid A.P, A.J Jongman A.J, Political terrorism. A new guide to actors, authors, concepts, data bases, theories and literature, New Brunswick 1998; Weinberg L, Pedahzur A, Hirsch-Hoefler S, The Challenges of conceptualizing terrorism, "*Terrorism and Political Violence*" 2004, Vol. 16, No. 4

There are many types of terrorism. Given its diverse territorial scope, it becomes obvious that there is a distinction between international and domestic terrorism. On the basis of the criterion of the entity engaged in terrorist activity, a distinction can be made between state terrorism and anti-state terrorism. State terrorism can be characterised as "the intimidating action of state power against citizens"[18]. In this case, the state

[18] Hołyst B, Kryminologia. Warsaw, 1986, p. 116, Wałek T, Pojęcie, geneza i klasyfikacja zjawisk terrorystycznych. *Securitologia*, 2018, No. 2, p. 120, Resztak I, Zjawisko terroryzmu. *Prokuratura i Prawo*, 2012, No. 7/8, pp. 156–157.

engages in different forms of terrorist activities and provides financial support and shelter to terrorist groups. Anti-state terrorism is carried out by individuals, movements or groups whose intention is to destabilise the structures of the state and disturb the social order[19]. Another criterion is motivation. In this case, we can distinguish between political terrorism and non-political terrorism. In the case of political terrorism, the perpetrators of the intimidation are driven by political reasons, including ideological or religious issues[20].

In the field of political terrorism, Paul Wilkinson distinguishes: revolutionary terrorism, sub-revolutionary terrorism and repressive terrorism[21].

Repressive terrorism is generally used by the state and its police apparatus. It aims to tame and subordinate specific groups and individuals. Sub-revolutionary terrorism should be understood as the activity of ideologically motivated small groups or individuals who can use violence for different purposes. Undoubtedly, we can distinguish, for example: punishment, revenge, and intimidation. However, these actors are unable to make fundamental changes. The purpose of revolutionary terrorism is to cause a revolution aimed at introducing fundamental changes into the structure of the state. Within the framework of non-political terrorism, we can distinguish between criminal terrorism and pathological terrorism[22].

On the basis of domestic considerations, political terrorism is classified in different ways. We can find, for example, a division according to the criterion of "zones of social life threatened by terrorist action"[23]. The mentioned criterion was presented by Albert Pawłowski. On its basis, the author distinguishes individual terrorism and economic terrorism. Individual terrorism has been defined as "acts of violence directed against the lives of people who are specifically selected or labelled only as a group". Economic terrorism "affects the existing economic relations, in particular, the right to exercise ownership by factory owners and landowners"[24]. In addition to the abovementioned, we can also distinguish criminal terrorism and pathological terrorism. Criminal terrorism covers common crimes committed by perpetrators who use terrorist methods to make profits. Pathological terrorism should be understood as terrorist acts committed by persons with mental disorders. Their motives cannot be clearly established, but undoubtedly they are the result of frustration or hatred towards specific people, social groups or institutions[25].

---

[19] Resztak I, Zjawisko…., *op.cit.*, pp. 156–157.

[20] *See*: Hołyst B, Terroryzm…, *op.cit.*, pp. 87–88.

[21] *See*: Wilkinson P, Stewart A.M (Eds), Contemporary Research on Terrorism. Aberdeen, 1987.

[22] Resztak I, Pojęcie, historia i typologia zjawiska terroryzmu. *Науковий вісник*, 2011, No. 4, p. 532.

[23] Pawłowski A, Typologia terroryzmu politycznego, [in:] Muszyński J (Ed.), Terroryzm polityczny. Warsaw, 1991, p. 94; Resztak I, Zjawisko…, *op.cit.* p. 157.

[24] Pawłowski A, Typologia…, *op. cit.*, p. 94; Resztak I, Zjawisko…, *op.cit.*, p. 157.

[25] For more information, *see*: Szalaty M, Współczesne organizacje terrorystyczne, [in:] Kwiatkowska-Darul V (Ed.), Terroryzm. Materiały z sesji nau-

Repressive terrorism is used by a dominant social group when privileges of that group become threatened. We can also distinguish insurgent terrorism of an ethnic-nationalist-separatist character[26] and socio-revolutionary terrorism, striving to change the political system[27]. The distinction presented above was made by taking as a criterion the content that a terrorist group wants to communicate through the use of violence[28].

Taking into account the tactics used by perpetrators, we distinguish between regressive terrorism, defensive terrorism[29] and offensive terrorism[30].

Due to the programme assumptions of terrorist organisations, we can distinguish direct causative terrorism (concerns goals calculated for their own effectiveness)[31], indirect causative terrorism (aims to force a change of course in politics without taking power)[32] and propaganda terrorism (which is supposed to ignite a mass rebellion)[33].

The list of terrorist organisations of the U.S. Department of State includes, for example, such organisations as: ISIS, Hamas, Hezbollah, ETA, Palestinian Liberation Front, Al-AKSA Martyrs Brigade, Boko Haram, Kurdistan Workers' Party, Communist Party of the Philippines, Asa'ib Ahl al-Haq, and Islamic Revolutionary Guard Corps[34].

An effect of the terrorist attacks of September 11, 2001 is that, in December of that year, the European Union developed a list of persons, groups, and entities that were subject to sanctions in connection with their participation in terrorist acts. These sanctions were introduced by Council Common Position 2001/931/CFSP[35]. This allowed for the implementation of UN Security Council Resolution 1373 of 28 November

kowej, Toruń, 11 kwietnia 2002 r. Toruń, 2002, pp. 77–78; Indecki K, Prawo karne wobec terroryzmu i aktu terrorystycznego. Łódź, 1998, pp. 32–37.

[26] For more information, *see*: Izak K, Zagrożenie terroryzmem i ekstremizmem w Europie na podstawie wybranych przykładów. Teraźniejszość, prognoza ewolucji i kierunki rozwoju. *Przegląd Bezpieczeństwa Wewnętrznego*, 2011, No. 5, p. 124.

[27] For more information, *see:* Izak K, Townshend C, Terroryzm. *Przegląd Bezpieczeństwa Wewnętrznego*, 2018, No. 18, p. 208.

[28] Wiak K, Prawnokarne środki przeciwdziałania terroryzmowi. Lublin, 2009, p. 33.

[29] For more information, *see:* Zajda M, Teoretyczne aspekty terroryzmu. *Security, Economy & Law*, 2015, No. 8, p. 71.

[30] For more information, *see:* Moskiewski M, ks. Socha J, Terroryzm jako problem etyczny. *Studia Gdańskie*, 2005–2006, vol. XVIII–XIX, p. 41; Borkowski R, Terroryzm, [in:] tenże (Ed.), Konflikty współczesnego świata. Krakow, 2001, p. 118.

[31] For more information, *see:* Zajda M, Teoretyczne..., *op.cit.*, p. 71.

[32] *Ibid*.

[33] Resztak I, Zjawisko..., *op. cit.*, p. 158.

[34] Full list is available at <https://www.state.gov/foreign-terrorist-organizations/>, 21 January 2020.

[35] Council Common Position 2001/931 / CFSP of 27 December 2001 on the application of specific measures to combat terrorism (EU Official Journal L 344 of 2001).

2001. The list is reviewed at least every six months. It includes people and groups that operate in the territory of the European Union and beyond its borders[36].

The abovementioned Council Community Position 2001/931/CFSP was amended by Council Decision (CFSP) 2017/2073 of 13 November 2017 amending Common Position 2001/931/CFSP on the application of specific measures to combat terrorism[37] and under other documents, for example Council Decision (CFSP) 2021/142 of 5 February 2021 on updating the list of persons, groups and entities covered by Art. 2, 3 and 4 of Common Position 2001/931/CFSP on the application of specific measures to combat terrorism and repealing Decision (CFSP) 2020/1132[38].

The basic tools and techniques used in terrorist activities are[39]:
— kidnappings,
— threats,
— bomb attacks,
— weapons of mass destruction,
— homicides,
— hostage-taking,
— cyberterrorism,
— bioterrorism[40].

The bombings, killings, kidnappings, and hostage-taking are referred to as classical terrorism. Subsequent methods such as weapons of mass destruction, cyberterrorism and bioterrorism appeared and developed in the 20th century[41].

Essence of cyberterrorism

Cyberterrorism is one of the forms of terrorism. It has been known since the 1980s. In most cases, the targets of cyber-terrorist

[36] For more information, *see:* the European Council, The EU Terrorist List. *Electronic source*: https://www.consilium.europa.eu/en/policies/fight-against-terrorism/terrorist-list/, *accessed*: 21 January 2020; Council Common Position 2009/468 / CFSP of 15 June 2009 updating Common Position 2001/931 / CFSP on the application of specific measures to combat terrorism and repealing Common Position 2009/67 / CFSP (Official Journal EU L 151 of 2009), p. 45).

[37] (Official Journal of the European Union L 295 of 2017, p. 59).

[38] (Official Journal of the European Union L 43 of 2021, p. 14).

[39] Zajda M, Teoretyczne..., *op.cit.*, p. 69.

[40] Bioterrorism is a form of terrorism that involves the use of biological agents, most often bacteria or viruses. The use of biological weapons from the point of view of terrorists is "attractive" due to the low production costs, large range of destruction and ease of transmission. More: Binczycka-Anholcer M, Imiołek A, Bioterroryzm jako jedna z form współczesnego terroryzmu. *Hygeia Public Health*, 2011, No. 46, pp. 326–333; Kuzdraliński A, Bioterroryzm. *Electronic source*: http://www.e-biotechnologia.pl/Artykuly/bioterroryzm, *accessed*: 20 January 2020.

[41] Zajda M, Teoretyczne..., *op. cit.*, p. 69.

attacks are the banking infrastructure, government websites, and critical infrastructure. The terrorists' interest in using cyber attacks increased after the attacks on the World Trade Center in New York. Cyberspace in Poland consists of: ICT systems, networks and services having particular importance for the internal security of the state, operated by state and local government institutions, the banking system, as well as systems ensuring the functioning of transport, energy, water and gas infrastructure, transportation in the country, information and health protection systems, the destruction or damage of which could pose a threat to: human life or health, national heritage and the environment to a significant extent, or serious material losses.

Cyberterrorism is a form of terrorism that generally involves using computers and information systems as the main criminal tool, or making them the main target of these activities[42]. Use of such methods can lead to the blockage of computer systems and data loss. The attack tools are different types of malware, for example: server locks, viruses, rabbit programs, worms[43], trojan horses, programs that exploit errors in operating systems and utility software, and applications designed to destabilise the operation system. One of the factors contributing to the rapid development of this type of crime is probably easy access to the web. We can also assume that the specific nature of the global network is not without significance, which allows the perpetrator to be partially anonymous. It should also be noticed that crimes committed in cyberspace provide the perpetrator a higher level of security than any other type of criminal activity – both in terms of the administration of justice and the actions of other criminals[44].

The authorship of the term "cyberterrorism" is attributed to Barry Collin, who worked in the Institute for Security and Intelligence in California and used it in the 1980s to formulate a link between cyberspace and terrorism.

The purpose of cyberterrorism is not just limited to data loss. Propaganda and information campaigns, recruitment, radicalisation of the exchange and collection of information[45] are also elements. The Internet gives terrorists the opportunity to reach a larger audience.

It is difficult to clearly define what cyberterrorism is. The problem with working out a precise definition may be caused by the dynamic nature of this phenomenon. We should also pay attention to the multiplicity of its characters, which are subject to permanent changes under the influence

[42] *See*: Gerwatowski J, Bezpieczeństwo informacyjne w jednostkach samorządu terytorialnego. *Kwartalnik Studia Prawnoustrojowe*, 2019, No. 44, p. 92; Von Zur-Mühlen R, Computerkriminalität. Gefahren und Abwehr. Neuwied–Berlin, 1973.

[43] *See*: Dajana, Czym są robaki komputerowe i jak je usunąć? *Electronic source*: https://www.omegasoft.pl/Robak-komputerowy, *accessed*: 21 January 2020.

[44] Wasilewski J, Cyberprzestępczość. Wybrane aspekty prawnokarne i kryminalistyczne, praca doktorska, Uniwersytet w Białymstoku, Wydział Prawa, Katedra Prawa Karnego. Białystok, 2017, p. 74.

[45] Jankowski P, Cyberterroryzm jako współczesne zagrożenie dla administracji publicznej. *Młody Jurysta*, 2018, No. 4, p. 16.

of the development of civilization due to technological progress[46]. Sometimes even journalists or experts misuse the term cyberterrorism to refer to a phenomenon that does not always result from the activities of terrorist groups[47]. That kind of situation undoubtedly poses a certain risk as it may lead to the devaluation of the concept of cyberterrorism.

According to the definition proposed by Mark Pollitt, an agent with the Federal Bureau of Investigation (FBI), "Cyberterrorism is a deliberate, politically motivated attack on information[48], computer systems, computer programs and data that result in the use of violence against non-fighting targets by transnational groups or undercover agents"[49].

The US National Infrastructure Protection Center defines cyberterrorism as "a criminal act committed with the use of a computer and telecommunication capabilities, which uses force, destruction and/or the interruption of services in order to create fear, by creating confusion or uncertainty in a given population, for the purpose of influencing governments and populations in such a way as to use their reactions to achieve specific ideological, political or social goals"[50].

Dorothy Denning defines cyberterrorism in the following way: "a threat or unlawful attack against an information system or collected data. The effect is to intimidate or force state authorities or their representatives to make concessions or expected behaviors to support specific goals (for example political). In order for such activities to be classified as information terrorism, an attack should cause significant losses or such effects that cause a general feeling of fear"[51].

To quote James Levis, cyberterrorism consists in "using computer networks as a tool to paralyse or seriously limit the possibility of effective use of national structures (such as energy, transport, government institutions, etc.) or to intimidate or force a government or population to act"[52].

---

[46] Olak A, Krauz A, Zjawisko terroryzmu we współczesnym świecie. *Kultura bezpieczeństwa*, 2014, No. 15, p. 189.

[47] Jankowski P, Cyberterroryzm..., *op.cit.*, p. 16.

[48] Information can take many forms. It can be in electronic, verbal or paper form. Information must be effectively protected against undesirable interference, this also applies to a number of processes in which it is generated, modified and transmitted., For more information, see: Stefanowicz B, Informacja, wiedza, mądrość, Vol. 66, Warsaw, 2013, pp. 8–17 (author's note).

[49] Hołyst B, Cyberterroryzm. *Zabezpieczenia*, 2010, No. 3, p. 37.

[50] Quote from Szubrycht T, Cyberterroryzm jako nowa forma zagrożenia terrorystycznego. *Zeszyty Naukowe Akademii Marynarki Wojennej*, 2005, No. 1, p. 175.

[51] *Ibid.*, p. 175; Karatysz M, Zjawisko cyberprzestępczości a polityka cyberbezpieczeństwa w regulacjach prawnych Rady Europy, Unii Europejskiej i Polski. *Refleksje*, 2013, No. 7, p. 141; El Ghamari M, Ochrona cyberprzestrzeni — wyzwanie naszych czasów? *Bezpieczeństwo i Technika Pożarnicza*, 2018, No. 49, p. 26; Denning D, Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy, [in:] Arquilla J, Ronfeldt D (Eds), Networks and Netwars: The Future of Terror, Crime, and Militancy. Santa Monica, 2001, p. 241.

[52] Sadowski J, Cybernetyczny wymiar współczesnych zagrożeń. *Studia nad*

The International Criminal Police Organization, Interpol, uses the following division of computer crime[53]:
1. Violation of access rights to resources, in particular:
— hacking,
— data capture,
— stealing time;
2. Resource modification with a logic bomb, Trojan horse, virus, or computer worm;
3. Fraud using a computer, in particular:
— ATM fraud,
— falsification of input or output devices (*e.g.* magnetic or microprocessor cards),
— fraud by providing false identification data,
— fraud in sales systems,
— fraud in telecommunications systems;
4. Reproduction of programs, including:
— games in all their forms,
— any other computer programs,
— integrated circuit topography;
5. Tampering with both hardware and software;
6. Crimes committed with the use of BBSs (Bulletin Board Systems);
7. Storage of illegal collections;
8. Crime on the Internet.

An additional difficulty in developing an unequivocal definition of cyberterrorism may be the fact that cyberterrorism is a problem on many different levels, for example such as:[54]
— informatics,
— information safety,
— IT safety[55],
— national and international legal regulations,
— personal data.

Cyberterrorism is not only the field of hackers, terrorist organisations, and crackers[56]. It is also used for their purposes by: spies, activists, national liberation and insurgent movements, terrorist organisations, as well as those with ordinary frustrations[57].

Bezpieczeństwem, 2017, No. 2, p. 60; Lewis J.A, Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats. Washington, 2002, p. 1.

[53] Gruza E, Goc M, Moszczyński J, Kryminalistyka — czyli rzecz o metodach śledczych. Warsaw, 2008, p. 562.

[54] *Cf.*: Lichocki E, Cyberterroryzm państwowy i niepaństwowy — początki, skutki i formy. Gdynia, 2011, p. 1.

[55] The ICT system includes devices, tools, methods of conduct and procedures used by specialist employees when ensuring safe production, storage, processing or transfer of information.

[56] Cracker – a person who breaks computer security (cracking) in order to steal or destroy data.

[57] *Cf.*: Lichocki E, Cyberterroryzm..., *op.cit.,* p. 2.

Examples of cyber-terrorist attacks

Cyberattacks are an everyday challenge for citizens and countries with their critical infrastructure[58], banks and giant corporations, institutions, and officials. As it is generally known, the IT systems of government and local government administration offices in Poland are sometimes the target of cyber attacks. But unfortunately it also still happens that as a result of mistakes, offices themselves become a source of threats to information security. The following situations can be presented as examples:

— The personal data of the initiators of the 2013 referendum leaked from the City Hall in Piotrków Trybunalski[59].
— At the end of 2019, the Municipal Office in Kościerzyna was attacked by a hacker. The attack encrypted the office's data. The criminals demanded a ransom in cryptocurrency to decrypt the files[60].
— In the Municipal Office in Toruń, the attackers managed to change the content (defacement) of the website; the same situation took place in the case of the website belonging to the Wielkopolska Provincial Office in Poznań[61].

[58] Act on crisis management of April 26, 2007 (Dz.U., 2007, No. 89, item 590 as amended) in Article 3 defines critical infrastructure as systems and their functionally related objects, including building structures, devices, installations, key services for the security of the state and its citizens and for ensuring the efficient functioning of public administration, as well as institutions and entrepreneurs. It includes, among others systems: energy supply, energy resources and fuels, communication systems, ICT network systems, financial systems, water and food supply systems, transport systems.

[59] *See:* Dane osobowe wyciekły z urzędu miasta w Piotrkowie. Prokuratura wszczęła śledztwo po donosie GIODO. *Electronic source*: https://piotrkowtrybunalski.naszemiasto.pl/dane-osobowe-wyciekly-z-urzedu-miasta-w-piotrkowie/ar/c1-3299451, *accessed*: 30 January 2020.

[60] Łosińska-Okoniewska E, W gminie Kościerzyna udało się odzyskać dane po ataku hakera. *Dziennik Bałtycki*, 18 December 2019; *Electronic source*: https://dziennikbaltycki.pl/w-gminie-koscierzyna-udalo-sie-odzyskac-dane-po-ataku-hakera/ar/c1-14664883, *accessed*: 29 January 2020; Surażyńska J, Urząd Gminy Kościerzyna opublikował oświadczenie na temat ataku hakera. *Electronic source*: https://koscierzyna.naszemiasto.pl/urzad-gminy-koscierzyna-opublikowal-oswiadczenie-na-temat/ar/c1-7468085, *accessed*: 30 January 2020; redakcja koscierzyna24.info, Atak hakerski w Gminie Kościerzyna. Sprawę przejmuje prokuratura. *Electronic source*: https://www.koscierzyna24.info/wiadomosci/3657,atak-hakerski-w-gminie-koscierzyna-sprawe-przejmuje-prokuratura, *accessed*: 30 January 2020.

[61] AO, Hakerzy przejęli oficjalną stronę internetową Urzędu Miasta w Toruniu. *Electronic source*: https://nowosci.com.pl/hakerzy-przejeli-oficjalna-strone-internetowa-urzedu-miasta-w-toruniu/ar/10835662, *accessed*: 31 January 2020; Cichocka A, Ofensywa urzędu po ataku hakerskim. Będą kolejne zabezpieczenia strony. *Nowości. Dziennik Toruński*, 3 September 2015; *Electronic source*: https://

— The police in Kielce detained a person who reported to the Provincial Office in Kielce and informed that he had managed to break into one of the office's servers[62].
— The website of the town hall of Łódź, along with some services (for example signing up for an appointment at the Driving License and Vehicle Registration Department), was blocked for several days by hackers. The town hall of Łódź paid 43,000 PLN to the company that "cleaned" the system after the attack and to "restore" the website[63].
— By redirecting to fake bank transfer accounts in five municipal offices (Błażowa, Belsk Duży, Gidle, Rząśnia, Jaworzno), attackers managed to steal over 2 million PLN[64].
— At the end of 2019 the Kościerzyna Commune Office was attacked by a hacker. The data of the office was encrypted. For decrypting the files, the criminals demanded a ransom in cryptocurrency[65].

According to the data of CSIRT GOV (Computer Security Incident Response Team), in 2015 the largest number of attempts at botnet malware infections concerned generally such sectors as services – 30.72%, key enterprises – 21.62%, and administration – 7.22%[66].

As for the costs of cyber attacks: in the case of the Rząśnia commune – 500,000 PLN, the Gidle commune – 300,000 PLN, the Podlaskie Province Roads Authority – about 3.7 million PLN[67].

---

nowosci.com.pl/ofensywa-urzedu-po-ataku-hakerskim-beda-kolejne-zabezpieczenia-strony/ar/10835408, *accessed*: 31 January 2020.

[62] Redakcja Niebezpiecznik.pl, Zatrzymała go policja, bo zgłosił dziurę urzędnikowi. *Electronic source*: https://niebezpiecznik.pl/post/zatrzymala-go-policja-bo-zglosil-blad-na-stronie-urzedu-wojewodzkiego/, *accessed*: 30 January 2020; minos, Atak na serwer Urzędu Wojewódzkiego. *Electronic source*: https://echodnia.eu/swietokrzyskie/atak-na-serwer-urzedu-wojewodzkiego/ar/8645979, *accessed*: 30 January 2020.

[63] Lisiak-Felicka D, Szmit M, Cyberbezpieczeństwo administracji publicznej w Polsce. Wybrane zagadnienia. Krakow, 2016, p. 12; Baranowska J, Atak hakerski kosztował UMŁ 43 tys. zł. *Electronic source*: https://lodz.naszemiasto.pl/atak-hakerski-kosztowal-uml-43-tys-zl/ar/c1-1950650, *accessed*: 30 January 2020.

[64] Nowak M, Zatrzymano przestępców, którzy ukradli 2 mln zł. Wśród nich najbardziej poszukiwany polski haker. *Electronic source*: https://www.spidersweb.pl/2015/10/policja-polsilver-torepublic.html, *accessed*: 31 January 2020.

[65] Haertle A, Hasło do systemu wyborczego na stronie urzędu — Ty też mogłeś testować. *Electronic source*: https://zaufanatrzeciastrona.pl/post/haslo-do-systemu-wyborczego-na-stronie-urzedu-ty-tez-mogles-testowac/, *accessed*: 30 January 2020.

[66] MSWiA, Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2015 roku. Warsaw, 2016, p. 19.

[67] Kajut P, Samorządy toczą nierówną walkę z przestępcami. *Electronic source*: https://www.prawo.pl/samorzad/samorzady-tocza-nierowna-walke-z-cyberprzestepcami,100471.html, 31 January 2020; IKMJ Cyberbezpieczeństwo w Polsce — statystyki. *Electronic source*: https://ikmj.com/cyberbezpieczenstwo-w-polsce-statystyki/, *accessed*: 31 January 2020; Maroszek W,

Another example of a cyber-terrorist attack that can be cited here is, for example, the WannaCry virus[68]. It is a ransomware responsible for the paralysis of information systems of institutions around the world including the British health service, Russian Ministry of the Interior, the central bank, and the press news agency. Costs generated by WannaCry are predicted at nearly $US4 billion[69].

According to estimates, companies around the world may have lost up to $10 billion as a result of a ransomware called NotPetya (also known as Petya). The operating principle of this ransomware was very similar to WannaCry. NotPetya blocked infected devices and demanded $300 in bitcoin to decrypt them. Institutions in Ukraine and Russia suffered the most in the attack – for example: Council of Ministers of Ukraine, Ukrainian National Bank, Russian Central Bank, and even the radiation monitoring of the decommissioned Chernobyl nuclear power plant[70].

Undoubtedly, we should also mention here the Spectre/Meltdown security vulnerabilities[71]. These are hardware vulnerabilities which have been found in nearly all Intel processors and have existed since 1995. Such vulnerabilities are caused by the design of the processors themselves, because they make it possible to read information stored in the cache, for example login data, and so-called website cookies.

In 2016, even 2.5 million smart devices such as webcams, Wi-Fi routers, and refrigerators were infected in an attack of malware called Mirai. The attack proceeded in the following way: first, the software detected and then infected inadequately secured IoT devices[72]. The infected devices were then turned into botnets used to carry out cyber attacks. According

Niewiedza groźniejsza od hakerów. *Electronic source*: https://regiony.rp.pl/trendy/23136-niewiedza-grozniejsza-od-hakerow, *accessed*: 1 February 2020.

[68] *See*: Fordoński R, Kasprzak W, WannaCry ransomware cyberattack as violation of international law. *Studia Prawnoustrojowe*, 2019, No. 44, pp. 47–73.

[69] Struzik A, Miliardy dolarów strat oraz skradzionych kont — największe cyberataki i wycieki danych ostatnich lat. *Electronic source*: https://sarota.pl/biuro-prasowe/miliardy-dolarow-strat-oraz-skradzionych-kont-najwieksze-cyberataki-i-wycieki-danych-ostatnich-lat/, *accessed*: 27 February 2021.

[70] Redakcja Orange.pl, Największe ataki hakerskie w historii. *Electronic source*: https://www.orange.pl/poradnik/twoj-internet/najwieksze-ataki-hakerskie-w-historii/, *accessed*: 28 January 2020.

[71] Malicki P, Meltdown i Spectre i ich wpływ na użytkowników komputerów osobistych. *Electronic source*: https://www.cyberdefence24.pl/kryptologia-wiadomosci/meltdown-i-spectre-i-ich-wplyw-na-uzytkownikow-komputerow-osobistych, *accessed*: 13 March 2020.

[72] "Internet of Things" is the term used to describe one of the newer IT concepts. It consists in connecting material objects with each other and with Internet resources by means of an extensive computer network. By definition, the Internet of Things includes any object that can be connected to the worldwide web. These can be all modules included in smart homes – electronics and household appliances, lighting, heating installation, all counters and clocks. In addition, cars, sensors and their readers, *e.g.* used in industry, transport or trade, can also be part of the Internet of Things.

to data presented by CERT Poland, up to 14,000 devices were intercepted per day in Poland. Such a wide scale of infection is probably the result of the Mirai source code being made public on the Internet[73].

In September of 2016, the Yahoo company revealed that two years earlier, the data of up to 500 million users had been stolen. In December of the same year, information about another leak was presented. That time, a billion records had been leaked. The cyber criminals stole such data as: encrypted passwords, usernames, birthdays, secondary e-mail addresses, and phone numbers. They also took control of Yahoo's internal service management tool. That gave them the opportunity to impersonate selected accounts, including: representatives of foreign intelligence services, employees of investment companies and banks, American officials, Russian politicians, and journalists. Yahoo admitted that the leak concerned the data of all users of the service, which could total even 3 billion accounts[74].

Examples of attacks on the banking sector include attacks against the Canadian Bank of Montreal and the Imperial Bank of Commerce, and the Russian PIR Bank[75].

Cybercrime statistics

According to the information included in the report of the activities of CERT Polska for 2018[76], the most frequently reported types of incidents were related to phishing[77], spam, and the distribution of malware. Of all of the incidents, 431 were of offensive and illegal content such as spam,

[73] Największe cyberataki i wycieki ostatnich lat. *Electronic source*: https://mobileclick.pl/najwieksze-cyberataki-i-wycieki-danych-ostatnich-lat/, *accessed*: 28 January 2020; Mocek K, Największe cyberataki i wycieki danych ostatnich lat. *Electronic source*: https://www.pcformat.pl/News-Najwieksze-cyberataki-i-wycieki-danych-osttnich-lat,n,20127, *accessed*: 28 January 2020.

[74] *Ibid.*; Nowak P, Miliardy dolarów strat oraz skradzionych kont — największe cyberataki i wycieki danych ostatnich lat. *Electronic source*: https://wavepc.pl/miliardy-dolarow-strat-oraz-skradzionych-kont-najwieksze-cyberataki-i-wycieki-danych-ostatnich-lat/, *accessed*: 30 January 2020.

[75] Palczewski S, Największe cyberataki na sektor finansowy 2018 roku. *Electronic source*: https://www.cyberdefence24.pl/najwieksze-cyberataki-na-sektor-finansowy-2018r, *accessed*: 29 January 2020.

[76] *See*: NASK, CERT Polska, Krajobraz bezpieczeństwa polskiego Internetu. Raport roczny z działalności CERT Polska, 2018. Warsaw, 2019, pp. 11–13.

[77] Phishing can be defined as a technique in which fraudsters pretending to be a trustworthy institution, such as a bank, to obtain confidential data. An example is the situation related to Alior Bank – in December 2017, criminals sent Internet users an e-mail requesting verification of their account. Some customers received information about it being blocked. After clicking on the link in the message, the Internet user was taken to a fake bank website which looked identical to the bank's real website. If they provided login details here, their account was taken over by the fraudsters.

discrediting and insulting, as well as child pornography and violence. 862 cases involved malware. Of the 101 information-gathering incidents, the largest groups were those related to scanning. Only one eavesdropping incident was registered in this group. Another group of incidents were intrusion attempts – their total number was 153, including 30 cases involving the use of known system vulnerabilities, and 37 with attempted unauthorised logging.

On the other hand, when it comes to attacks on information security, their total number was 46 cases. 21 of them were related to unauthorised access to information. The most numerous group, accounting for as much as 50.23% of all recorded incidents, was computer fraud, their total number being about 1,878, with 1,655 of them related to phishing.

In the case of attacks on the economic sector: 643 cases were attacks on the banking sector. 13 cases were attacks on the healthcare sector, there were 20 attacks on the energy sector, 51 cases were related to the transport sector, and two cases were related to the water sector.

Counteracting cyberterrorism in Poland and around the world

In Poland, the fight against cybercrime is the task of: the Internal Security Agency (hereinafter: ABW), the Ministry of National Defence, the Ministry of Administration and Digitization, the Ministry of the Interior, the Military Counterintelligence Service, as well as private sector entities. Generally, the tasks in this area belong to activities of the Internal Security Agency and Police. The main duty of the ABW is: identifying, preventing and combatting various types of threats to the internal security of the state[78], for example: drug trafficking on an international scale, espionage, terrorism, illegal production of weapons, ammunition and explosives, weapons of mass destruction as well as narcotic drugs and psychotropic substances, their possession and trade[79]. The Counter-Terrorism Group functions as part of the organisational structure of the ABW. The duties of this group include, for example[80]:

— analysis of the legal regulations related to terrorism issues and preparing proposals for legislative changes to improve the methods and forms of combatting terrorism,

[78] For more information, *see:* NASK/CERT Polska, System bezpieczeństwa cyberprzestrzeni RP. Ekspertyza dotycząca rekomendowanego modelu organizacji systemu bezpieczeństwa cyberprzestrzeni w Polsce, wykonana na zlecenie Ministerstwa Administracji i Cyfryzacji. Warszawa, 2015, p. 5.

[79] *See*: Oleksiewicz I, Rola służb specjalnych w polityce zwalczania cyberterroryzmu RP. *Humanities and Social Sciences*, 2017, Vol. XXII, p. 227; ustawa z 24 maja 2002 o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (Dz.U., 2002, No. 74, item 676), Article 5. For more information about the tasks of ABW, see: Biuro Bezpieczeństwa Narodowego, Biała Księga Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej. Warsaw, 2013.

[80] Oleksiewicz I, Rola…, *op.cit.*, p. 228.

— collecting information about the phenomenon of terrorism, monitoring it around the world and monitoring the resulting threats to Poland,
— participation in organising cooperation with the authorities of other countries in the field of counteracting terrorism,
— creating the concepts of counteracting terrorism and giving opinions on projects and programs in this area,
— preparing information and materials related to terrorism for the use of the minister – head of the Centre for Combatting Organised Crime and International Terrorism,
— preparing analyses and forecasts of the threat of terrorism,
— organising training and conferences that are devoted to the issues of counteracting terrorism and preparing educational materials in this field.

The CAT (Anti-Terrorist Center) was also established within the ABW. The CAT is a unit of a coordinational and analytical character. It is established to counteract and combat terrorism. The main duties of the Anti-Terrorist Center include, for example[81]:
— supporting decision-making processes in the event of a real threat of a terrorist attack,
— coordinating operational and reconnaissance activities in the field of combatting terrorism,
— after terrorist attacks, supporting the activities of the services and institutions participating in the anti-terrorist defence of the Republic of Poland,
— performing analytical and IT activities in the field of preparing situational and synthetic reports and preparing information for the state management,
— cooperating in this field with the structures of the European Union and North Atlantic Treaty Organization.

The training activities carried out by the Governmental Computer Incident Response Team for state institutions operating in Poland in the field of effective protection against network attacks also cannot be forgotten about. The indicated unit is part of the Teleinformatic Security Department belonging to the ABW structures. This unit performs the following tasks[82]:
— coordinating reactions to events related to attacks on the Internet,
— issuing and announcing alarms,
— dealing with the received reports, including collecting evidence by a specially appointed team of court experts.

One of the outcomes of the work of this unit was the development of the ARAKIS-GOV system. This is an early warning system for threats on the

[81] *See*: Makarski A, Centrum Antyterrorystyczne Agencji Bezpieczeństwa Wewnętrznego. Geneza, zasady działania oraz doświadczenia po pierwszym roku funkcjonowania. *Przegląd Bezpieczeństwa Wewnętrznego*, 2010, No. 2, pp. 104–106; Oleksiewicz I, Rola…, *op. cit.*, p. 228.

[82] Oleksiewicz I, Cyberterroryzm jako realne zagrożenie dla Polski. *Rocznik Bezpieczeństwa Międzynarodowego*, 2018, Vol. 12, No. 1, p. 62.

Internet. ARAKIS-GOV is the result of cooperation between the ABW Teleinformation Security Department and the CERT Poland team operating within the Scientific and Academic Computer Network[83].

An important role in combatting cybercrime at the national level is no doubts held by the government programme for the protection of cyberspace of the Republic of Poland for the years 2017–2022. Its purpose is the implementation of the Directive (EU) 2016/1148 of the European Parliament and the Council from 6 July 2016 about measures for a high common level of security of network and information systems across the Union[84]. Its strategy, in particular, focuses on[85]:

— information and communication security objectives,
— main entities involved in the implementation of an ICT security strategy,
— ICT security purposes,
— providing guidance for educational, information, and training programmes related to cybersecurity,
— performing activities related to research and development plans in the field of ICT security,
— preventing and responding to incidents and restoring the normal state disturbed by an incident, including the principles of cooperation between public and private sectors,
— defining the approach to risk evaluation,
— maintaining the approach to international cooperation in the field of cybersecurity.

The basis of international cooperation in the field of combatting and counteracting cybercrime is the Budapest Convention[86]. Cooperation includes, for example: sharing information, issuing early warnings, exchanging best practices, and joint incident response exercises.

Combatting cybercrime in the member states of the European Union is supported, for example, by: funding programmes, identifying gaps and increasing capacity to investigate and fight cybercrime[87]. The European Commission supports linking bodies between law enforcement, universities, and the private sector. It also cooperates with Europol's European Cyber-

[83] *See*: Pudzianowski J, System wczesnego ostrzegania o zagrożeniach w sieci Internet. *Electronic source*: https://rcb.gov.pl/system-wczesnego-ostrzegania-o-zagrozeniach-w-sieci-internet/, *accessed*: 12 February 2020; Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego, System ARAKIS-GOV. *Electronic source*: https://csirt.gov.pl/cer/system-arakis-gov/310,System-ARAKIS-GOV.html, *accessed*: 12 February 2020.

[84] OJ UE L 194, 2016, p. 1 (hereinafter: Directive No. 2016/1148).

[85] For more information, see: Ministerstwo Cyfryzacji, Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017–2022. Warsaw, 2017 pp. 7–26, Oleksiewicz, Rola…, *op.cit.*, p. 227.

[86] Council of Europe Convention on Cybercrime, adopted in Budapest on 23 November 2001 (Dz.U., 2015, item 728).

[87] In 2013 – under the Prevention of and Fight against Crime (ISEC) program. After 2013 – under the Internal Security Fund (instrument under the multiannual financial framework).

crime Centre (EC3) and Eurojust to align political solutions to best practice from an operational point of view[88]. These activities should also be supported by closer cooperation between governments, universities, and the private sector in the European Union, as well as research and development works[89].

Another very importnant regulation in a field of cybersecurity is Regulation of the European Parliament and the EU Council 2019/881 of 17 April 2019 on ENISA (European Union Agency for Cybersecurity; hereinafter: ENISA) and cybersecurity certification in the field of information and communication technologies and repealing Regulation (EU) No 526/2013 (cybersecurity act)[90].

ENISA, through providing advice and assistance, offers its scientific and technical independence, and the transparency of its operating procedures, is a centre of expertise in the field of cybersecurity. The catalogue of ENISA's tasks is extensive. For example, the tasks of ENISA include[91]:

— promoting a high level of knowledge in the field of cybersecurity, including cyber hygiene and digital skills for citizens, organisations and businesses,
— promoting cooperation, including information exchange and coordination at the EU level, between the Member States, institutions, bodies, offices and agencies of the European Union, and relevant stakeholders from the public and private sectors on issues related to cybersecurity,
— providing support for capacity-building and preparedness throughout the European Union by helping its institutions, bodies, offices and agencies, as well as Member States and public and private stakeholders, to enhance the protection of their networks and information systems, create and improve cyber resilience and response capacities, and develop skills and competences in the field of cybersecurity.

The objectives of ENISA include[92]:

— analysing emerging technologies and providing thematic assessments of the expected social, legal, economic and regulatory impact of technological innovations on cybersecurity,
— supporting Member States in implementing specific cybersecurity aspects of European Union policy and law related to data protection and privacy, and by providing advice to the European Data Protection Board at its request,
— assisting Member States in developing national strategies on the security of network and information systems, if such assistance is re-

[88] *See:* European Parliament resolution of 12 September 2013 on the European Union's cybersecurity strategy: an open, secure and protected cyberspace (Official Journal EU C 93 of 2013, p. 112).

[89] *See*: Gerwatowski J, Bezpieczeństwo..., *op. cit.*, p. 94.

[90] OJ L 151, 2013, p. 15; ibid., pp.94-95.

[91] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (European Union Agency for Cybersecurity) and cybersecurity certification in the field of information and communication technologies and repealing Regulation (EU) No 526/2013 (act on cybersecurity) (Official Journal L 151 of 2013, p. 15).

[92] *Ibid*.

quested under Article 7(2) of Directive 2016/1148, and promoting the dissemination of these strategies and recording progress in their implementation throughout the European Union in order to promote best practices.

Conclusions

Development of new technologies undoubtedly brings us many positive changes, which greatly improves our everyday life. Certainly, as examples, we can mention: wide access to information and knowledge, the ability to develop our interests (passions, hobbies), and the speed of information transfer. On the plus side, we should also notice the impact of technological innovations on the development of medicine and science. Undoubtedly, new technologies also save our time and money.

But, on the other hand, we cannot forget or underestimate the fact that one of the effects of the development of new technologies is the appearance of new kinds of threats. One of such threats is probably a false sense of anonymity and safety in cyberspace. Unfortunately, the level of users' awareness and knowledge about potential dangers in cyberspace is still definitely too low. We also have to accept the fact that some of us approach the issue in a disrespectful way, which can facilitate the dealings of those involved in cybercrime. An example of threats that all of us may have to deal with in everyday life is phishing[93] and pharming[94]. The next kind of threats, which we definitely have to mention are disorders of interpersonal relations, addiction to the use of new technologies (for example social networks, smartphones, and computers)[95], fake news and psychological violence on the Internet, and information overload[96].

[93] *See*: Wasilewska-Śpioch A, Pharming — na czym polega i jak się przed nim zabezpieczyć. *Electronic source*: https://biznes.gazetaprawna.pl/artykuly/462036,pharming-na-czym-polega-i-jak-sie-przed-nim-zabezpieczyc.html, *accessed*: 28 February 2020.

[94] *See*: Phishing — czy jest dla nas realnym zagrożeniem? Jak się przed nim chronić? *Electronic source*: https://www.parkiet.com/Finanse/180739993-Phishing--czy-jest-dla-nas-realnym-zagrozeniem-Jak-sie-przed-nim-chronic.html, *accessed*: 27 february 2020 r.; Gawin M, Uwaga na atak phishingowy na klientów Alior Bank. *Electronic source*: https://www.bankier.pl/wiadomosc/Uwaga-na-atak-phishingowy-na-klientow-Alior-Banku-7560214.html, *accessed*: 27 February 2020.

[95] For more information, *see:* Ciszewska K, Ryzyko uzależnienia od Facebooka jako jedna z kategorii zagrożeń związanych z użytkowaniem portali społecznościowych. *World Journal of Theoretical And Applied Sciences*, 2016, No. 1(4), Bezpieczeństwo dzieci i młodzieży w przestrzeni wirtualnej — teoria i praktyka, p. 27–36; Fałdowska M, Filipek A, Ważniewska J, Społeczne i zdrowotne aspekty bezpieczeństwa w cyberprzestrzeni, [in:] Koziński M, Kosznik-Biernacka S, Grubicka J (Eds), Cyberprzestrzeń. Zagrożenia w Sieci. Słupsk, 2017, pp. 153–174.

[96] Information overload, which makes it difficult to extract true and relevant information.

Based on many examples, we should say that cyberterrorism is a phenomenon that poses a real threat both to the functioning of societies and states, and to world safety. Due to the dynamics of the development of cyberterrorism, in order to effectively counteract this problem, it is necessary to conduct interdisciplinary and transdisciplinary research. Also, no less important in this situation is effective cooperation between countries and international organisations and the creation of appropriate tools, standards and legal regulations.

However, we must remember that even the most effective tools and comprehensive regulations will not guarantee the security of "ordinary users" of the Internet if we continue to perceive the indicated threats as something that have an abstract nature.

References

Bielski K, Cyberterroryzm — nowe zagrożenie bezpieczeństwa państwa w XXI wieku. *Acta Politica*, 2015, No. 34.

Binczycka-Anholcer M, Imiołek A, Bioterroryzm jako jedna z form współczesnego terroryzmu. *Hygeia Public Health*, 2011, No. 46.

Biuro Bezpieczeństwa Narodowego, Biała Księga Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej. Warsaw, 2013.

Bolechów B, Terroryzm. Aktorzy, statyści, widownie. Warsaw, 2010.

Borkowski R, Terroryzm, [in:] tenże (Ed.), Konflikty współczesnego świata. Krakow, 2001.

Ciszewska K, Ryzyko uzależnienia od Facebooka jako jedna z kategorii zagrożeń związanych z użytkowaniem portali społecznościowych. *World Journal of Theoretical And Applied Sciences*, 2016, No. 1(4), Bezpieczeństwo dzieci i młodzieży w przestrzeni wirtualnej — teoria i praktyka.

Denning D, Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy, [in:] Arquilla J, Ronfeldt D (Eds), Networks and Netwars: The Future of Terror, Crime, and Militancy. Santa Monica, 2001.

Fałdowska M, Filipek A, Ważniewska J, Społeczne i zdrowotne aspekty bezpieczeństwa w cyberprzestrzeni, [in:] Koziński M, Kosznik-Biernacka S, Grubicka J (Eds), Cyberprzestrzeń. Zagrożenia w Sieci. Słupsk, 2017.

Fiszer J, Terroryzm jako zagrożenie dla bezpieczeństwa euroatlantyckiego i nowego ładu międzynarodowego, [in:] Fiszer J, Olszewski P (Eds), System euroatlantycki w wielobiegunowym ładzie międzynarodowym. Warsaw, 2013.

Fordoński R, Kasprzak W, WannaCry ransomware cyberattack as violation of international law. *Studia Prawnoustrojowe*, 2019, No. 44.

Gerwatowski J, Bezpieczeństwo informacyjne w jednostkach samorządu terytorialnego. Studia Prawnoustrojowe, 2019, No. 44.

Ghamari M.E, Ochrona cyberprzestrzeni — wyzwanie naszych czasów? *Bezpieczeństwo i Technika Pożarnicza*, 2018, No. 49.

Grotowicz V, Terroryzm w Europie zachodniej. Warsaw–Wrocław 2000.
Gruza E, Goc M, Moszczyński J, Kryminalistyka — czyli rzecz o metodach śledczych. Warsaw, 2008.
Hołyst B, Cyberterroryzm. *Zabezpieczenia,* 2010, No. 3.
Hołyst B, Kryminologia. Warsaw, 1986.
Hołyst B, Terroryzm. Tom 1. Warsaw, 2011.
Indecki K, Prawo karne wobec terroryzmu i aktu terrorystycznego. Łódź, 1998.
Izak K, Townshend C, Terroryzm. *Przegląd Bezpieczeństwa Wewnętrznego*, 2018, No. 18.
Izak K, Zagrożenie terroryzmem i ekstremizmem w Europie na podstawie wybranych przykładów. Teraźniejszość, prognoza ewolucji i kierunki rozwoju. *Przegląd Bezpieczeństwa Wewnętrznego*, 2011, No. 5.
Jankowski P, Cyberterroryzm jako współczesne zagrożenie dla administracji publicznej. *Młody Jurysta*, 2018, No. 4.
Janowska A, Cyberterroryzm — rzeczywistość czy fikcja?, [in:] Haber L.H (Ed.), Społeczeństwo informacyjne — wizja czy rzeczywistość? Tom 1, Krakow, 2003.
Karatysz M, *Zjawisko cyberprzestępczości a polityka cyberbezpieczeństwa w regulacjach prawnych Rady Europy, Unii Europejskiej i Polski. Refleksje*, 2013, No. 7.
Lewis J.A, Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats. Washington, 2002.
Lichocki E, Cyberterroryzm państwowy i niepaństwowy — początki, skutki i formy. Gdynia, 2011.
Lisiak-Felicka D, Szmit M, Cyberbezpieczeństwo administracji publicznej w Polsce. Wybrane zagadnienia. Krakow, 2016.
Makarski A, Centrum Antyterrorystyczne Agencji Bezpieczeństwa Wewnętrznego. Geneza, zasady działania oraz doświadczenia po pierwszym roku funkcjonowania. *Przegląd Bezpieczeństwa Wewnętrznego*, 2010, No. 2.
Ministerstwo Cyfryzacji, Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017–2022. Warsaw, 2017.
Moskiewski M, ks. Socha J, Terroryzm jako problem etyczny. Studia Gdańskie, 2005–2006, Vol. XVIII–XIX.
MSWiA, Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2015 roku. Warsaw, 2016.
NASK, CERT Polska, Krajobraz bezpieczeństwa polskiego Internetu. Raport roczny z działalności CERT Polska, 2018. Warsaw, 2019.
NASK/CERT Polska, System bezpieczeństwa cyberprzestrzeni RP. Ekspertyza dotycząca rekomendowanego modelu organizacji systemu bezpieczeństwa cyberprzestrzeni w Polsce, wykonana na zlecenie Ministerstwa Administracji i Cyfryzacji. Warsaw, 2015.
Olak A, Krauz A, Zjawisko terroryzmu we współczesnym świecie. *Kultura bezpieczeństwa*, 2014, No. 15.
Oleksiewicz I, Cyberterroryzm jako realne zagrożenie dla Polski. *Rocznik Bezpieczeństwa Międzynarodowego*, 2018, Vol. 12, No. 1.

Oleksiewicz I, Rola służb specjalnych w polityce zwalczania cyberterroryzmu RP. *Humanities and Social Sciences*, 2017, Vol. XXII.
Pawłowski A, Typologia terroryzmu politycznego, [in:] Muszyński J (Ed.), Terroryzm polityczny. Warsaw, 1991.
Resztak I, Pojęcie, historia i typologia zjawiska terroryzmu. *Науковий вісник*, 2011, No. 4.
Resztak I, Zjawisko terroryzmu. Prokuratura i Prawo, 2012, No. 7/8.
Sadowski J, Cybernetyczny wymiar współczesnych zagrożeń. *Studia nad Bezpieczeństwem*, 2017, No. 2.
Schmid A.P, Jongman A.J, Political Terrorism. A New Guide to Actors, Authors, Concepts, Data Bases, Theories & Literature. New Brunswick–London, 2005.
Stefanowicz B, Informacja, wiedza, mądrość, Vol. 66. Warsaw, 2013.
Szalaty M, Współczesne organizacje terrorystyczne, [in:] Kwiatkowska-Darul V (Ed.), Terroryzm. Materiały z sesji naukowej. Toruń, 11 April 2002, Toruń 2002.
Szubrycht T, Cyberterroryzm jako nowa forma zagrożenia terrorystycznego. *Zeszyty Naukowe Akademii Marynarki Wojennej*, 2005, No. 1.
Wałek T, Pojęcie, geneza i klasyfikacja zjawisk terrorystycznych. *Securitologia*, 2018, No. 2.
Wasilewski J, Cyberprzestępczość. Wybrane aspekty prawnokarne i kryminalistyczne. praca doktorska, Uniwersytet w Białymstoku, Wydział Prawa, Katedra Prawa Karnego. Białystok, 2017.
Weinberg L, Pedahzur A, Hirsch-Hoefler S, The Challenges of conceptualizing terrorism, "Terrorism and Political Violence" 2004, Vol. 16, No. 4.
Wiak K, Prawnokarne środki przeciwdziałania terroryzmowi. Lublin, 2009.
Wilkinson P, Stewart A.M (Eds), Contemporary Research on Terrorism. Aberdeen, 1987.
Wojciechowski S, Terroryzm. Analiza pojęcia. *Przegląd Bezpieczeństwa Wewnętrznego*, 2009, No. 1.
Zajda M, Teoretyczne aspekty terroryzmu. *Security, Economy & Law*, 2015, No. 8.
Zur-Mühlen R von, Computerkriminalität. Gefahren und Abwehr. Neuwied–Berlin, 1973.

Legal acts

Ustawa z 24 maja 2002 o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (Dz.U., 2002. No. 74, item 676).
Ustawa z 26 kwietnia 2007 o zarządzaniu kryzysowym (Dz.U., 2007, No. 89, item 590 as amended).
Council of Europe Convention on Cybercrime, adopted in Budapest on 23 November 2001 (Dz.U., 2015, item 728).
Regulation (EU) of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity and repealing Regulation (EU) No. 526/2013 (Cybersecurity Act) (OJ L 151 of 2013).

Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (OJ L 194 of 2016).
Council Decision (CFSP) 2017/2073 of 13 November 2017 amending Common Position 2001/931/CFSP on the application of specific measures to combat terrorism (OJ L 295 of 2017).
Council Decision (CFSP) 2021/142 of 5 February 2021 updating the list of persons, groups and entities subject to Articles 2, 3 and 4 of Common Position 2001/931/CFSP on the application of specific measures to combat terrorism, and repealing Decision (CFSP) 2020/1132 (OJ L 43 of 2021).
Council Common Position 2001/931/CFSP of 27 December 2001 on the application of specific measures to combat terrorism (OJ L EU 344 of 2001).
Council Common Position 2009/468/CFSP of 15 June 2009 updating Common Position 2001/931/CFSP on the application of specific measures to combar terrorism and repealing Common Position 2009/67/CFSP (OJ EU L 151 of 2009).
European Parliament Resolution of 12 September 2013 on Cybersecurity Strategy of the European Union: An Open,Safe and Secure Cyberspace (OJ UE C 93 of 2013).

Other sources

AO, Hakerzy przejęli oficjalną stronę internetową Urzędu Miasta w Toruniu. *Electronic source*: https://nowosci.com.pl/hakerzy-przejeli-oficjalna-strone-internetowa-urzedu-miasta-w-toruniu/ar/10835662, *accessed*: 31 January 2020.
Baranowska J, Atak hakerski kosztował UMŁ 43 tys. zł. *Electronic source*: https://lodz.naszemiasto.pl/atak-hakerski-kosztowal-uml-43-tys-zl/ar/c1-1950650, *accessed*: 30 January 2020.
Cichocka A, Ofensywa urzędu po ataku hakerskim. Będą kolejne zabezpieczenia strony. "Nowości. Dziennik Toruński" z 3 września 2015 r. *Electronic source*: https://nowosci.com.pl/ofensywa-urzedu-po-ataku-hakerskim-beda-kolejne-zabezpieczenia-strony/ar/10835408, *accessed*: 31 January 2020.
Dajana, Czym są robaki komputerowe i jak je usunąć? *Electronic source*: https://www.omegasoft.pl/Robak-komputerowy, *accessed*: 21 January 2020.
Datareportal, All the numbers you need. *Electronic source*: https://datareportal.com/reports/digital-2019-poland, *accessed*: 3 February 2021.
Digital 2019: Poland. *Electronic source*: https://datareportal.com/reports/digital-2019-poland, *accessed*: 20 January 2020.
Długołęcki S, Ewolucja telefonii komórkowej i mobilnego internetu. *Electronic source*: https://www.pcworld.pl/news/Ewolucja-telefonii-komorkowej-i-mobilnego-iternetu,375151.html, *accessed*: 21 January 2020.

Encyklopedia PWN online, hasło: terroryzm. *Electronic source*: https://encyklopedia.pwn.pl/haslo/terroryzm;3986796.html, *accessed:* 14 January 2020.

Gawin M, Uwaga na atak phishingowy na klientów Alior Banku. *Electronic source*: https://www.bankier.pl/wiadomosc/Uwaga-na-atak-phishingowy-na-klientow-Alior-Banku-7560214.html, *accessed*: 27 February 2020.

Haertle A, Hasło do systemu wyborczego na stronie urzędu — Ty też mogłeś testować. *Electronic source*: https://zaufanatrzeciastrona.pl/post/haslo-do-systemu-wyborczego-na-stronie-urzedu-ty-tez-mogles-testowac/, *accessed*: 30 January 2020.

IKMJ Cyberbezpieczeństwo w Polsce — statystyki. *Electronic source*: https://ikmj.com/cyberbezpieczenstwo-w-polsce-statystyki/, *accessed*: 31 January 2020.

Kajut P, Samorządy toczą nierówną walkę z przestępcami. *Electronic source*: https://www.prawo.pl/samorzad/samorzady-tocza-nierowna-walke-z-cyberprzestepcami,100471.html, *accessed*: 31 January 2020.

Kemp Simon, Digital 2019: Global Digital Overview, 31 January 2019. *Electronic source*: datareportal.com/reports/digital-2019-global-digital-overview, *accessed*: 20 January 2020.

Kuzdraliński A, Bioterroryzm. *Electronic source*: http://www.e-biotechnologia.pl/Artykuly/bioterroryzm, *accessed*: 20 January 2020.

kw, Dane osobowe wyciekły z urzędu miasta w Piotrkowie. Prokuratura wszczęła śledztwo po donosie GIODO. *Electronic source*: https://piotrkowtrybunalski.naszemiasto.pl/dane-osobowe-wyciekly-z-urzedu-miasta-w-piotrkowie/ar/c1-3299451, *accessed*: 30 January 2020.

Liedel K, Współczesne zamachy terrorystyczne: forma, metoda, cel. *Electronic source*: http://rcb.gov.pl/wspolczesne-zamachy-terrorystyczne-forma-metoda-cel/, accessed: 15 January 2020.

Łosińska-Okoniewska E, W gminie Kościerzyna udało się odzyskać dane po ataku hakera, "Dziennik Bałtycki" z 18 grudnia 2019 r. *Electronic source*: https://dziennikbaltycki.pl/w-gminie-koscierzyna-udalo-sie-odzyskac-dane-po-ataku-hakera/ar/c1-14664883, *accessed*: 29 January 2020.

Malicki P, Meltdown i Spectre i ich wpływ na użytkowników komputerów osobistych. *Electronic source*: https://www.cyberdefence24.pl/kryptologia-wiadomosci/meltdown-i-spectre-i-ich-wplyw-na-uzytkownikow-komputerow-osobistych, *accessed*: 13 March 2020.

Maroszek W, Niewiedza groźniejsza od hakerów. *Electronic source*: https://regiony.rp.pl/trendy/23136-niewiedza-grozniejsza-od-hakerow, *accessed*: 1 February 2020.

Atak na serwer Urzędu Wojewódzkiego. *Electronic source*: https://echodnia.eu/swietokrzyskie/atak-na-serwer-urzedu-wojewodzkiego/ar/8645979, *accessed*: 30 January 2020.

Mocek K, Największe cyberataki i wycieki danych ostatnich lat. *Electronic source*: https://www.pcformat.pl/News-Najwieksze-cyberataki-i-wycieki-danych-osttnich-lat,n,20127, *accessed*: 28 January 2020.

Największe cyberataki i wycieki ostatnich lat. *Electronic source*: https://mobileclick.pl/najwieksze-cyberataki-i-wycieki-danych-ostatnich-lat/, *accessed*: 28 January 2020.

Nowak M, Zatrzymano przestępców, którzy ukradli 2 mln zł. Wśród nich najbardziej poszukiwany polski haker. *Electronic source*: https://www.spidersweb.pl/2015/10/policja-polsilver-torepublic.html, *accessed*: 31 January 2020.

Nowak P, Miliardy dolarów strat oraz skradzionych kont — największe cyberataki i wycieki danych ostatnich lat. *Electronic source*: https://wavepc.pl/miliardy-dolarow-strat-oraz-skradzionych-kont-najwieksze-cyberataki-i-wycieki-danych-ostatnich-lat/, *accessed*: 30 January 2020.

Palczewski S, Największe cyberataki na sektor finansowy 2018 roku. *Electronic source*: https://www.cyberdefence24.pl/najwieksze-cyberataki-na-sektor-finansowy-2018r, *accessed*: 29 January 2020.

Phishing — czy jest dla nas realnym zagrożeniem? Jak się przed nim chronić? *Electronic source*: https://www.parkiet.com/Finanse/180739993-Phishing--czy-jest-dla-nas-realnym-zagrozeniem-Jak-sie-przed-nim-chronic.html, *accessed*: 27 February 2020.

Pudzianowski J, System wczesnego ostrzegania o zagrożeniach w sieci Internet. *Electronic source*: https://rcb.gov.pl/system-wczesnego-ostrzegania-o-zagrozeniach-w-sieci-internet/, *accessed*: 12 February 2020.

Rada Europejska, Unijna lista terrorystów. *Electronic source*: https://www.consilium.europa.eu/pl/policies/fight-against-terrorism/terrorist-list/, *accessed*: 21 January 2020.

Redakcja DailyWeb, 4G, LTE, 3G, 2G — czym różnią się od siebie poszczególne technologie? *Electronic source*: https://dailyweb.pl/4g-lte-3g-2g-czym-roznia-sie-od-siebie-poszczegolne-technologie/, *accessed*: 21 January 2020.

Redakcja koscierzyna24.info, Atak hakerski w Gminie Kościerzyna. Sprawę przejmuje prokuratura. *Electronic source*: https://www.koscierzyna24.info/wiadomosci/3657,atak-hakerski-w-gminie-koscierzyna-sprawe-przejmuje-prokuratura, *accessed*: 30 January 2020.

Redakcja Niebezpiecznik.pl, Zatrzymała go policja, bo zgłosił dziurę urzędnikowi. *Electronic source*: https://niebezpiecznik.pl/post/zatrzymala-go-policja-bo-zglosil-blad-na-stronie-urzedu-wojewodzkiego/, *accessed*: 30 January 2020.

Redakcja Orange.pl, Największe ataki hakerskie w historii. *Electronic source*: https://www.orange.pl/poradnik/twoj-internet/najwieksze-ataki-hakerskie-w-historii/, *accessed*: 28 January 2020.

Struzik A, Miliardy dolarów strat oraz skradzionych kont — największe cyberataki i wycieki danych ostatnich lat. *Electronic source*: https://sarota.pl/biuro-prasowe/miliardy-dolarow-strat-oraz-skradzionych-kont-najwieksze-cyberataki-i-wycieki-danych-ostatnich-lat/, *accessed:* 27 February 2021.

Surażyńska J, Urząd Gminy Kościerzyna opublikował oświadczenie na temat ataku hakera. *Electronic source*: https://koscierzyna.naszemiasto.pl/urzad-gminy-koscierzyna-opublikowal-oswiadczenie-na-temat/ar/c1-7468085, *accessed*: 30 January 2020.

Wasilewska-Śpioch A, Pharming — na czym polega i jak się przed nim zabezpieczyć. *Electronic source*: https://biznes.gazetaprawna.pl/artykuly/462036,pharming-na-czym-polega-i-jak-sie-przed-nim-zabezpieczyc.html, *accessed*: 28 February 2020.

Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego, System ARAKIS-GOV. *Electronic source*: https://csirt.gov.pl/cer/system-arakis-gov/310,System-ARAKIS-GOV.html, *accessed*: 12 February 2020.

Electronic source: https://www.state.gov/foreign-terrorist-organizations/>, *accessed*: 21 January 2020.

Keywords: terrorism, cyberterrorism, cybercrime, threats in cyberspace

Summary: The article is about the threats that result from the evolution of new technologies. Problems such as terrorism and cyberterrorism have been discussed in detail. The article presents examples of cybercrimes. Selected law regulations are also described in terms of cyberterrorism and cybersecurity. The author also presents cyberthreats which we may be exposed to in our everyday life, including phishing and pharming. Finally, Polish and global cybercrime statistics are presented in the article.