SECURITY DIMENSIONS
NO. 30; 2019 (66–95)
DOI 10.5604/01.3001.0013.7777

Dangers and Attacks on Digital Information in the Public Safety Space

Joanna Grubicka*

Krzysztof Rogowski**

Grzegorz Diemientiew***

ABSTRACT

The need for security is one of the most fundamental human needs. The scale of the threats posed by cybercrime to IT systems is large. It is mostly the result of the high vulnerability of IT systems to threats, the high risk of data theft, a very high occurrence of Internet frauds, the low efficiency of the systems protecting computers and networks, and an inadequately low level, as related to the existing threats, of security measures utilized by the users of IT systems. In this article, the authors discuss the underestimated problem of crime on the Internet and its nature in today's reality.

* Joanna Grubicka, Ph.D., Pomeranian University in Slupsk; correspondence address: Pomeranian University in Slupsk, ul. Arciszewskiego 22A, 76-200 Słupsk, Poland; e-mail: joanna.grubicka@apsl.edu.pl
** Krzysztof Rogowski, Ph.D., Pomeranian University in Slupsk, Słupsk, Poland.
*** Grzegorz Diemientiew, M.Sc., Pomeranian University in Slupsk, Słupsk, Poland.

ARTICLE INFO

Article history
Received: 11.06.2019 Accepted: 27.06.2019

Keywords
threats of Internet crime, cyberspace, ICT systems

1. Introduction

In the era of globalization, there is a growing need to protect cyberspace. Two spheres of cyberspace protection can be distinguished: one relates to the functioning of states and societies in cyberspace, both internally and externally, and the other is the sphere of the activity of cybercriminals. Regarding the first sphere, one can observe the global increase in the number and intensity of attacks on critical infrastructures in specific countries. In particular, it concerns the attempts to block the operation of systems and devices, and to disable the provision of key services to the operation.[1] Increasingly, these types of attacks target state entities or other structures with adequate financial resources and access to information and relevant people. While there are often no large financial or human resources required to carry out a successful attack, the magnitude of the damage caused as a result of the attack is terrifying. Such situations often result in enormous material and immaterial losses for countries. One can easily defend the assumption that state strategies concerning activities in cyberspace are closely related to strategies concerning the areas beyond cyberspace, i.e. land, sea, air and space. Activities in the digital space are complementary to activities in the abovementioned areas, and they also serve to strengthen the country's position on the world stage by implementing the country's strategy.[2]

It is not disputable that the state's functioning totally depends on information. This means that cutting off information may not only paralyze

[1] J. Grubicka, *Globalna przestrzeń bezpieczeństwa społeczeństwa informacyjnego wobec zagrożeń cyberterroryzmu*, [in:] *Bezpieczeństwo – wielorakie perspektywy. Człowiek – społeczeństwo – państwo w sytuacjach kryzysu*, M. Kuć, T. Węglarz (eds), Poznań 2014, p. 327.

[2] W. Jakubczak, M. Szyłkowska, *Wyzwania i koncepcje ochrony cyberprzestrzeni w erze globalizacji*, [in:] *Cyberprzestrzeń. Uzależnienia – zahamowania – zagrożenia*, M. Koziński, J. Grubicka, S. Kosznik-Biernacka (eds), Słupsk 2016, pp. 69–99.

ICT systems, but also prevent access to devices that control conventional protection and defense measures, including combat measures.

2. Attacks on information security systems

Terrorist groups using cyberspace operate in an increasingly complex and sophisticated manner, which is more and more often unpredictable. The almost unlimited economic and technical potential of these groups means that they have access to the most modern tools and technologies. The high level of dependence of contemporary civilization on Internet technologies is a great facilitation for modern terrorists. The Internet stores all the most important information in the world. Government agencies, airlines, defense systems, hospitals, criminal services, tax offices, banks, or even energy management companies[3] have their data servers. Depending upon the place of the attack, one can distinguish external attacks, i.e. those that are conducted from systems outside the targeted network, and internal attacks that take place locally and are carried out from systems in the targeted network.

Another way of dividing attacks is into active and passive ones. An active attack leads to the loss of the integrity of the computer system, e.g. a hacker's attack that removes a certain amount of important data and changes the operation of programs. An active attack can also be modifying a data stream or creating false data. A passive attack is based on entering the system without making any changes, e.g. an attack of a hacker who copies a certain amount of relevant data without causing any changes in the operation of the programs. A passive attack can also be about eavesdropping or the monitoring of transmitted data. In this case, the attacker's goal is to discover the content of the message.

Depending on the type of information flow in the system being attacked, four types of attack are distinguished: signal interruption, signal capture, signal modification and signal counterfeit. Signal capture is a form of confidentiality breach and occurs when an unauthorized person accesses the resources of someone else's computer system. An example here can be eavesdropping of packets to capture data on the network and illegal copying of files or programs. Signal modification is gaining access to resources by an unauthorized person who introduces changes to these resources in order

[3] A. Bógdał-Brzezińska, M. Gawrycki, *Cyberterroryzm i problemy bezpieczeństwa informacyjnego we współczesnym świecie*, Warszawa 2003, p. 45.

to obtain rights or maintain access to a given system. An example here can be a change in the value in a data file, making changes to the program in order to invoke another way of working or modifying messages sent on the network. Signal counterfeit is an attack aimed at authenticity. When transferring data from one computer to another, the third computer blocks it from further transmission, and introduces false objects to the second computer system. ARP Spoofing is an example of a method related to the modification of captured MAC and IP address pairs in a local network. The operation of the address differentiation protocol (ARP) is based on sending Ethernet broadcast packets containing the wanted IP address. The station being the wanted recipient sends a packet in which there is a pair of addresses: IP and an Ethernet address. The system from which the attack is being carried out, transmits false ARP queries or responses, directing all traffic towards itself and presenting itself as an authorized recipient.

One of the most dangerous cyberattacks is the Man in the Middle attack (MITM). This attack is based on putting the attacking system between the victim system and the local gate so that the aggressor's system can monitor everything that the victim sends and receives. The attacker first cheats the victim system due to an incorrectly addressed Ethernet frame in their packet. This results in the victim's data being sent to the system belonging to the attacker. From this moment, it is possible for the attacker to monitor the victim's connections. To allow the victim to send and receive data, the attacker sends another modified ARP broadcast frame. The crafted message misleads the victim's system, saying that information intended for remote systems should be sent to the attacking MAC address before it is sent by the local gate. At this moment, the attacker system intercepts input and output data. The final step of the MITM attack is to transfer traffic to the machine for which it was originally intended. As a result, the attacker turns into a temporary gate between the victim's system and the real LAN gate. The victim is still able to send and receive data to and from remote systems, but all data is transported by the aggressor system. At this point, any information sent, such as passwords or e-mail addresses, can be monitored, or even modified, by the attacker. The ability to edit victim's network data while sending them allows the attacker to change the direction of communication of the victim's system, perform a MITM attack while exchanging the cryptographic key and threat many other security aspects. When modifying traffic during key exchange initialization in an encrypted

Web session, the attacker can intercept and decrypt the victim's network traffic, even when the session still appears to be encrypted.

DNS spoofing is an attack on a DNS server that maps hostnames to IP numbers and vice versa. This attack involves interference in the DNS table and modification of individual entries so that the client is directed to the attacker's computer instead of the target computer.

Interception of a session, or hijacking, is one of the most dangerous attacks on a computer system. Hijacking is a combination of two methods: sniffing and IP-spoofing. In this cyberattack technique the attacker breaks the connection established between the client and the server, then impersonates the client and sends the server packets with their own sequence numbers. The TCP connection requires a synchronized packet exchange, so if for any reason the packet sequence numbers do not match the values expected by the computer, they will be rejected and the waiting phase for the correctly numbered packet will be re-established. The hacker can use the requirements for TCP protocol sequence numbers and capture the connection. In order to be able to view packets sent, it is necessary to use a sniffer.

Blocking or denial of service (DoS) attacks involve pushing software, hardware or network links beyond the limits of their assumed performance. The purpose of such an attack is to block the operation of a service or to deteriorate its quality. Such attacks can be detected in a fairly simple way, but it is much more difficult to determine the source of these attacks. They can take place in various forms – from backfilling emails (mail bombing or spam), to sending specially crafted packets to crash the program in the targeted system. The effect of this action can be, for example, disk overflow, CPU overload, operating system crash or simply the overloading of the link. In order for the link to be cut, it is enough to generate more packets than the recipient can handle.

SYN packaged attacks are another dangerous attack. Attacks based on flooding with SYN packets do not block the link, but are directed against the TCP / IP stack.

Distributed Denial of Service (DDoS) is a special variation of the classic overflow attack. Many computers connected to the Internet are used in the DDoS attack, and these computers participate in the attack without the users' knowledge. The attacker installs the attack software on as many computers (called "zombies") as possible. The program on the "zombie" computer involves one of the ports and waits for further instructions. Then, the attacker installs the main program on one of the computers on the Internet, which

has a list of all computers prepared for the attack. When the attack time comes, the attacker sends the main message to the main program, in which all the "zombie" computers simultaneously carry out a DoS attack, sending towards the target such a number of packets that is able to overpower it.

The types of attacks mentioned above are just a few out of many attack types that pose a threat to the critical infrastructure of the state. Potential targets of cyberterrorist attacks should be considered in two ways. On the one hand, the goal may be the destruction of information technology, and on the other, the technology itself is only a tool for terrorist acts on the web.[4]If terrorists choose the first option and attack IT systems, their goal is to carry out a sabotage in an electronic and physical form.[5] They care about the most serious damage to the entire ICT infrastructure. In the second variant, the situation is more complicated, because terrorists do not intend to destroy the infrastructure but to commit an impudent and unobtrusive theft of important data that they will be able to manipulate and use for their own purposes.

Cyberspace is an ideal theater of war – it provides discretion, carrying out a fast or deliberately delayed attack, performing operations in a synchronized manner. Due to the fact that the target may be hidden, the attacked entity finds it difficult to take appropriate action. At the same time, the contemporary cyberdefense system must be capable not only of responding to every attack – in the present era without proper anticipation and counteracting attacks, functioning in the international arena is a miracle.

According to Article 1 of the Martial Law Act and the competences of the Supreme Commander of the Armed Forces and the principles of its subordination to the organs of the Republic of Poland, cyberspace is a space for processing and exchanging information created by tele-information systems, within the meaning of Article 3 Point 3 of the Act of February 17, 2005 on computerization of the activities of entities performing public tasks and of the relations between themselves and between them and the users.[6] It can therefore be assumed that cyberspace is an area (including external and internal networks, computers, systems) in which digital information is

[4] T. Szubrycht, *Cyberterroryzm jako nowa forma zagrożenia terrorystycznego*, "Zeszyty Naukowe AMW", 2005, no. 1 (160)/2005, p. 183.

[5] J. Grubicka, *Konwergencja technologiczna a system bezpieczeństwa informacji*, [in:] *Nowoczesne technologie na rzecz bezpieczeństwa. Zagadnienia dual-use*, W. Filipkowski (ed.), Gdynia 2015, p. 54.

[6] Journal of Law 2005 no. 64, item 565.

created in any form (sound, image, etc.). In this area, the information can thus be: generated, processed, stored, archived and/or transmitted, determining further links and actions to bring about a specific effect.

In the area of cyberspace, one of the first official classifications of threats was included in the Communication from the Commission to the European Parliament, the Council and the Committee of the Regions COM/2007/0267[7] on the overall strategy for combating cybercrime. Three basic types of crimes are distinguished there:

- group I – traditional forms, i.e. fraud and falsification using electronic IT networks and information systems (communication networks). Among them the most common include: mass scale fraud (e.g. identity theft, spam), phishing, including phishing of confidential information by impersonating a trustworthy person or institution, and illegal international trade (drugs, weapons);
- group II – publication of illegal content in electronic media (websites inciting to racial hatred and acts of terrorism, or containing content related to sexual exploitation of children);
- group III – so-called "typical" crimes in the network, i.e. hacker attacks, attacks against information systems or DDoS attacks.

It is rightly noted that attacks typical of the network may be directed against critical infrastructures of European countries, which is the greatest threat due to potentially dramatic consequences for society. In addition, it was emphasized that in case of illegal content, such offenses are difficult to prosecute, mainly due to the fact that the owners and/or the administrators of the websites are often citizens of other countries (from outside the EU), where the definitions of illegal content are different. In addition, in practical terms, moving the site content to another server in another country is not difficult and can take place within a few minutes. The fact of combining technologies and creating links between IT systems, which in turn facilitates the susceptibility to such attacks, is not without significance to the scale of threats. The content of the Communication shows that the most common purpose of attacks is extortion, and the statistical number remains underestimated due to potential losses that could be caused to entities if information about security problems were made public.

[7] *Communication from the Commission to the European Parliament, the Council and the Committee of the Regions – Towards a general strategy against cybercrime* (COM/2007/0267 final), http://eulex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52007DC0267 (accessed: 19.12.2018).

ICT-related threats with failures or natural and technical disasters significantly affect the security of the state. The main activities of unauthorized persons are: remote interference in ICT systems, their paralysis or disruption of their proper operation, taking control over them, or data theft. The aim of this type of attacks may be the complete failure of ICT systems belonging to e.g. state services, public administration, people running business as well as ordinary users. These systems play an important role not only in the economic and financial condition but also in the proper functioning of critical infrastructure. In terms of state security, the degree of threat of a given cyberattack depends on the system. There are different consequences depending on whether one means hacking a single or administrative website, or nationwide networks, payment systems or the central office network. The motivation, character and skills of the perpetrator also play an important role, and the impact of cyber attacks on the security of the state depends mainly on them. A different threat is posed by the actions of individuals who only want to test their skills and a different one – by the actions that are political in nature, such as the actions of terrorist groups.[8] As a result, new types of threats have appeared, such as cybercrime, cyberterrorism, cyber espionage or cyberwar, in the sense of a clash between countries in cyberspace and other types of cyber conflicts. Today's trends in the emergence of cyber threats point the impact of security in cyberspace on the general security of the state. The growing dependence on technology means that conflicts in the virtual world can be a serious source of ill-functioning of societies and countries.[9] One of the types of cyber conflicts is the information fight. The information campaign's subject is information, while the tools are all means that enable it to be obtained, defended or interfered with. Information in this case may be a target, a weapon, a means, but also a medium with which an attack is carried out. The information fight can be limited only to activities in cyberspace, but sometimes it is only one of the elements to carry out broader activities that take place in the physical world, in case of which one can talk about cyberwar.[10] The information war is all the actions of the actors

[8] *Bezpieczeństwo teleinformatyczne państwa*, M. Madej, M. Terlikowski (eds), Warszawa 2009, pp. 95–96.

[9] *Strategia bezpieczeństwa narodowego Rzeczypospolitej Polskiej [National Security Strategy of the Republic of Poland]*, Warszawa 2014, p. 19.

[10] *Wybrane problemy bezpieczeństwa. Dziedziny bezpieczeństwa*, A. Urbanek (ed.), Słupsk 2013, p. 172.

of a conflict, aimed at taking control, managing the flow and availability of important information. These activities are carried out with the intention of removing, modifying, obtaining and using all information resources, taking over the systems which the opponent has at their disposal, while protecting their own systems and resources[11]. Two types of information wars that take place in cyberspace can be distinguished. The first of these is the so-called net-war, i.e. a dispute between states, communities or nations. It is based on removing or interfering with information, with a view to presenting the attacked state, its society or surroundings in a different light.[12] The net-war has a socio-cultural character and is usually played only in cyberspace. These wars can be carried out between the governments of the conflicting states, between the government of the state and the participants outside the state, or between the government and the protesting groups of citizens who have reservations about government policy. The second type of information wars is cyberwar. Military activities are carried out, in which information is a decisive element in gaining advantage. There are also different technologies that can have an impact on cyberspace, and the consequence of this type of activity may be a hampered flow of information in cyberspace, and physical consequences in the real world. In cyberwar, an opponent may want to perform various tasks, such as spreading propaganda, causing panic in society, but also damaging important objects, e.g. power plants or communication systems. These types of attacks can be used by foreign intelligence to obtain protected and sensitive information resources.[13] Cyberterrorism includes both terrorist activities within ICT systems (the consequence may be destruction or modification of data in sensitive systems, e.g. those responsible for energy or water supply), and any terrorist activity related to cyberspace (ICT systems), from physical attacks on systems to activity propaganda[14] (including also obtaining information useful for the implementation of "classic" terrorist actions). It involves the use of terrorist means in the virtual space, with all elements constituting terrorist activities, such as: the psychological and political impact, fear, violence, sense of threat

[11] M. Madej, *Zagrożenia asymetryczne państw obszaru transatlantyckiego*, Warszawa 2007, p. 320.

[12] J. Gierszewski, *Bezpieczeństwo wewnętrzne. Zarys systemu*, Warszawa 2013, p. 134.

[13] A. Urbanek, *Wybrane problemy bezpieczeństwa. Rozważania o przestrzeni bezpieczeństwa*, Słupsk 2014, pp. 33–36.

[14] According to estimates, the number of websites devoted to jihad is about 300. In addition, there are also pages containing instructions on how to carry out a terrorist attack or construct a bomb. Volunteer recruitment actions are also carried out via the Internet.

etc. Communication in cyberspace is often used by terrorist groups in order to provide communication, free information exchange and coordination of activities between some parts of the structure while performing everyday activities, but also at moments of most important activities, such as the last stages of preparations for attacks or during their implementation. Cyber-terrorism can take various forms. It can be used as a support for physical terrorist activities using cyberspace. These activities can use cyberspace to conduct cyber attacks that cause losses, as well as destruction in the physical world that are at least so big so as to cause fear in the affected population. Nevertheless, cyberterrorism is only attacks in cyberspace combined with the actual use or the threat of physical violence against people and property.[15]

The catalogue of online crime threats is an open list as new ones are still being created. In order to visualize the scale of threats and their particular types, it is worth mentioning the most frequent ones here. These are:

– hazards where the network is only used as a means:
  - online financial services, e.g. proposals for participation in virtual gambling, invitations to virtual casino games, Nigerian fraud or money laundering referred to as cyberbullying,
  - illicit trafficking (e.g. arms, works of art, endangered or dying species),
  - trading in a live commodity (fake online job offers),
  - distribution of banned content and materials (e.g. those spreading racial hatred);

– "proper" cybercrime,[16] which in particular includes: hacking, piracy, cyber fraud, cyber espionage, cyberbanking, cyber lightning, cyberbullying, cyber-stalking, phishing, spamming, illegal eavesdropping, fraud, falsification.

It is worth mentioning fraud and Internet counterfeit here. In both cases, their goal is to get money. The most common types are currently:

- Nigerian fraud – contact is usually made in the form of an e-mail, allegedly from a person who wants to recover money from a specific country (the first fraud indicated Nigeria – hence the name) and offers high financial compensation for the help in the procedure. A potential victim is asked to transfer a certain amount – usually about 1,000 US dollars – to cover bank charges. When the victim transfers money, the contact disappears;

[15] M. Madej, *Zagrożenia,* …, op. cit., pp. 296–297 and 353–357.

[16] I.e. the use of cyberspace for criminal purposes.

- lotteries – the news is also usually spread in the form of an e-mail. The potential victim receives a message about winning the lottery with a request to send their personal data in order to collect the prize. As in the case of Nigerian scams, the victim is additionally asked to transfer the sum to cover alleged bank charges;
- matrimonial fraud;
- fake attractive job offers;
- rental offers for real estate, the viewing of which requires payment (after which a message about the alleged booking of a specific property is shown);
- money extortion via social networks (capturing login data and extorting money from the user's friends).

In turn, Internet counterfeit crimes can be divided into:

- crimes committed with the help of malicious software,
- crimes committed by means of false messages (e-mails),
- hybrid (fake e-mails containing malicious programs or links to such programs).

In case of digital forgery, its tools include both commercial programs whose regular use is legal, e.g. graphic programs (used for counterfeiting and re-processing of documents), and so-called malicious programs – precisely and purposefully designed to perform specific illegal operations in victim systems.

With the help of a graphic program, one can copy any document (e.g. copy a stamp, a signature, etc.). The collective term *malicious software* refers to any software (applications, scripts, etc.) that has harmful or dangerous effect on victim operating systems, on the data collected in them, and/or on computer users – including providing access to the victim's IT system. This type of software can be spread via infected external devices, websites, programs, etc.

There are various divisions and classifications of malicious software. The most common types are: viruses, worms, so-called Trojan horses or logic bombs. A *computer virus* is defined as a self-replicating (malicious) program placed in another program (carrier) with malicious activity. A *computer worm* is a program similar to a virus, however, it differs in the fact that it can generate its own copies, without the need for a host program, by exploiting a software vulnerability, which causes it to spread across all networks connected to the infected computer. In turn, the Trojan horse

is a program that pretends to be useful or interesting for the user, but it additionally has an undesirable, hidden functionality.

There are also other entities that can cause serious problems in the proper functioning of cyberspace and for the stability of countries who operate in cyberspace. These people are called *hackers*, and their activities are called hacking. Hackers have extensive knowledge of computer science and computer support, which allows them to break into computers and networks. Such actions are usually harmful to the victim or to the functioning of cyberspace. Hackers' motives can be different: political, economic, or psychological. Hackers acting only for profit are called *cybercriminals*. Another group is the so-called *hacktivists* acting out of political motives. The hacker's knowledge plays a key role because it determines their harmfulness in cyberspace. Such persons usually act individually or in small groups, and their activities are usually non-terrorist[17] in character.

3. The vulnerability of IT networks to threats

Vulnerability is weakness or a security fault It can be exploited by threat agents, resulting in losses.[18] Vulnerability is also "weakness of the information system or its security, which can be used by attackers".[19] One of the most popular threats in cyberspace are:

- use of malicious software (viruses, worms, Trojan horses, back entries, spyware, procedures using known or hidden vulnerabilities in commercial programs);
- theft and use of other people's personal data;
- extortion, theft, falsification or destruction of data;
- blocking access to services (postal bombs, overloading applications and websites, massive appropriation of computer systems in order to use them for such overloads);
- sending unnecessary or unwanted information;
- social engineering attacks (phishing by impersonating the institution or a trusted person);

[17] M. Madej, *Zagrożenia…*, op. cit., pp. 367–371.

[18] *Bezpieczeństwo informacji*, "Centrum.Bezpieczeństwa.pl", http://www.centrum.bezpieczenstwa.pl/index.php/bezpieczenstwo-informacji/slownik-bezpieczenstwo-informacji (accessed: 18.09.2017).

[19] NIK, *Realizacja przez podmioty państwowe zadań w zakresie ochrony cyberprzestrzeni. Informacja o wynikach kontroli*, p. 5, https://www.nik.gov.pl/plik/id,8764,vp,10895.pdf (accessed: 18.12.2018).

- advanced targeted attacks (conducted with the help of many coordinated and individualized methods targeted precisely against a specific person, organization or company)"[20].

The following indicators are used to determine the risk of cybercrime threats:

- threats resulting from the use of Internet resources;
- threats resulting from using the network of public institutions;
- threats resulting from the use of social networks;
- threats resulting from the use of new technologies.

Table 1. Comparison of the number of incidents handled by CERT Polska in the years 2014–2016 in Poland, according to types

	2014[21]		**2015**[22]		**2016**[23]	
Type of incident	**Number of incidents**	**%**	**Number of incidents**	**%**	**Number of incidents**	**%**
Offensive and illegal content	370	28,86	146	10,03	237	12,31
Malicious software	98	7,64	142	9,75	211	10,96
Gathering information	98	7,64	270	18,54	65	18,54
Attempts to break in	36	2,81	76	5,22	76	3,37

[20] *Ibidem*, p. 20.

[21] *Krajobraz bezpieczeństwa polskiego Internetu 2014: Raport roczny z działalności CERT Polska [Overview of security in the Polish Internet 2014. Annual report on the activity of CERT Polska]*, p. 44, https://www.cert.pl/wp-content/uploads/2015/11/Raport_CP_2014.pdf (accessed: 2.11.2018).

[22] *Krajobraz bezpieczeństwa polskiego Internetu 2015: Raport roczny z działalności CERT Polska [Overview of security in the Polish Internet 2015. Annual report on the activity of CERT Polska]*, pp. 10–11, https://www.cert.pl/PDF/Raport_CP_2015.pdf (accessed: 4.11.2018).

[23] *Krajobraz bezpieczeństwa polskiego Internetu 2016: Raport roczny z działalności CERT Polska [Overview of security in the Polish Internet 2016. Annual report on the activity of CERT Polska]*, https://www.cert.pl/PDF/Raport_CP_2016.pdf (accessed: 2.09.2018).

Hacking	13	1,01	10	0,69	10	0,69
Availability of resources	69	5,38	35	2,4	35	2,4
Attack on information security	25	1,95	89	6,11	89	6,11
Computer fraud	613	47,82	611	41,96	611	41,96
Others	40	3,12	77	5,29	77	5,29

Source: Own elaboration based on: *Krajobraz bezpieczeństwa polskiego Internetu 2016: Raport roczny z działalności CERT Polska* [*Overview of security in the Polish Internet 2016. Report on the activity of CERT Polska*], https://www.cert.pl/PDF/Raport_CP_2016.pdf (accessed: 2.09.2018).

Table 1 shows the comparison of the number of incidents, divided into basic groups, between 2014 and 2016. The huge number of incidents that were handled in 2012–2016 results from the emergence of new data sources that help in detecting incidents related to ICT security. It cannot be unnoticed that the number of incidents related to information processing was increasing significantly and concerned the collection of information. In 2014, there were 98 cases of attacks on general information security and a year later as many as 270 attacks of this kind took place. In terms of attacks on information security, data from 2014 indicate 25 incidents, and data from 2016 – 89 incidents. This rise is associated with increased awareness of the attackers of the value and price of information.

It is also worth emphasizing the types of threats whose values have decreased over the years discussed. In 2014, 370 cases of offensive content were handled in Poland. In the following year, they decreased by more than half, as 146 incidents were reported in 2015, though in 2016 there was an increase again and they totaled 237. The number of attacks on the availability of resources also decreased.[24]

It must be noticed that the number of incidents related to information processing increased significantly and concerned the collection of information. In 2014, it was 98 cases, and a year later, as many as 270 attacks on general information security. Data from 2014 indicate 25 incidents, and

[24] *Krajobraz bezpieczeństwa polskiego Internetu 2015…, op. cit.*, pp. 10–11.

from 2016 – 89. This jump is associated with increased awareness of the attackers as to the value and price of information.

Table 2. Threats resulting from using the Internet in 2010–2015 – data from Poland

Type of crime:	2010	2011	2012	2013	2014	2015
Offenses related to pedophilia	6	62	74	132	151	286
Attack on resources or IT devices of state or local government institutions	0	5	5	9	7	4
Attack on a computer system or a teleinformation network	18	30	30	34	52	111
Providing devices, programs or data to commit crimes	71	29	27	28	43	44

Source: The General Police Headquarters of Poland.

The next factor which affects the vulnerability of ICT networks are threats resulting from using the networks of public institutions. When using public administration services over the Internet, the main threat is the already mentioned *phishing*. This is the so-called catching of passwords – or of confidential information of other kinds, such as logins, bank account numbers or credit card details. Due to phishing, personal information is fraudulently obtained by a perpetrator who impersonates a trustworthy person or institution.[25]

Table 3. Phishing according to industry

Industry:	Phishing rate (1 in):
Agriculture, Forestry, & Fishing	1815
Finance, Insurance, & Real Estate	1918
Mining	2254
Public Administration	2329

[25] J. Kosiński, *Paradygmaty cyberprzestępczości*, Słupsk 2015, p. 126.

Retail Trade	2419
Nonclassifiable establishments	2498
Services	3091
Manufacturing	3171
Wholesale Trade	4742
Construction	4917
Transportation & Public Utilities	6176

Source: *Symantec Internet Security Threat Report*, April 2017, vol. 22, https://www.symantec.com/content/dam/symantec/docs/reports/istr-22-2017-en.pdf

Public administration is one of the leading industries threatened by phishing. On average, 1 out of 2329 e-mails addressed to public institutions were a phishing attempt.

Other threats appear when using social networks. One of these threats is spam, i.e. unwanted information that is sent via email.[26] Another threat appearing on social networks is loss of privacy and personal data. Social networking sites have appeared relatively recently, therefore there is no official data on the threats that occur there. As a result of the development of new internet technologies, new threats appear every year.

As the 2016 report from the activity of CERT Polska indicates, one of the biggest threats in 2016 was encryption software, the so-called ransomware. That year, 193 new ransomware families were discovered. Compared to 2015, the number of attacks of this malware has increased by as much as 550 percent.[27]

[26] *Spam,* "Słownik języka polskiego PWN", http://sjp.pwn.pl/slowniki/spam.html (accessed: 20.03.2018).

[27] *Krajobraz bezpieczeństwa polskiego Internetu 2016: Raport roczny z działalności CERT Polska [Overview of security in the Polish Internet 2016. Annual report on the activity of CERT Polska]*, https://www.cert.pl/PDF/Raport_CP_2016.pdf (accessed: 2.09.2018), p. 43.

Over the last few years, there has been a threat coming from hackers' devices connected to the Internet of Things. *Internet of Things* (IoT), a concept created by Kevin Ashton, in simplified terms means an ecosystem in which objects equipped with sensors communicate with computers. The dynamic development of devices with access to the network caused that this idea has become not only real, but is even indicated by consulting companies as one of the key development engines of the global economy of the future. The scale of application of IoT solutions is huge: from miniature accessories to clothing, through intelligent home appliances, building automation and smart cities, to water management and defense systems. For this reason, the acquired devices can be used for a massive DDoS attack. An example was the Mirai botnet operating in 2016.[28]

Official data indicate that there are at least several serious sources of threats on the Internet, hence protection from each of them can be difficult, to say the least.

4. Risk of data theft threats

The theft of data occurs when someone unlawfully gains access to a person's personal data and uses it against the will of that person. In other words, it is impersonation of someone else, often with the intention of getting money. The scope of the acquisition and use of data stolen this way can vary significantly. Sometimes it is a nickname and password to an Internet account, and sometimes it is the entire package of personal data that is used to take a loan in someone else's name.[29]

The threat to confidentiality and integrity of data in ICT networks is mainly caused by easy access to the transmitted data by unauthorized persons. This is mainly facilitated by the public access to the Internet and the type of network infrastructure used. The TCP / IP protocol, used for data exchange in the network, does not contain any mechanisms protecting against accessing unencrypted data packets (in the open form) by unauthorized persons. Also, the use of public networks can increase the risk of data theft, as different entities often share network devices, such as routers and relays.

[28] *Ibidem*, p. 23.

[29] *Czym jest kradzież tożsamości?*, "Biuro Informacji Kredytowej", https://www.bik.pl/poradnik-bik/czym-jest-kradziez-tozsamosci (accessed: 20.03.2018).

Another factor that increases the threat of data theft is the increasingly common use of wireless networks, which by default have no encryption set. Moreover, their physical security is inefficient and they transmit in the band of radio waves, due to which it is enough to be in range of the network to be able to eavesdrop on transmitted data packets. In addition, wireless networks are often used in public places, in so-called Hotspots, which are convenient places for network attacks to be carried out.[30]

The main types of data theft are: eavesdropping, manipulation, substitution, and combinations of these methods. Eavesdropping is a non-invasive method because packets flowing through the network are transmitted in parallel to the attacker, without interfering with data transmission. Manipulation aims at interfering with the data on computers. Substitution is based on obtaining the rights to the data in the ICT system by impersonating a device in the network that has access to the system.[31]

Table 4. Violation of the secrecy of correspondence

Year	Number of proceedings initiated	Number of offenses identified
2016	3401	2718
2015	3515	2452
2014	2868	1901
2013	2203	1655
2012	1657	1513
2011	1583	948
2010	1194	1102
2009	982	645
2008	694	505

[30] GIODO. Generalny Inspektor Ochrony Danych Osobowych, *ABC zagrożeń bezpieczeństwa danych osobowych w systemach teleinformatycznych*, Warszawa 2009, pp. 27–32, www.giodo.gov.pl/plik/id_p/1560/j/pl/ (accessed: 20.03.2017).

[31] *Ibidem*, pp. 9–11.

2007	616	384
2006	538	370
2005	430	260
2004	378	248
2003	362	232
2002	294	215
2001	259	175
2000	249	240
1999	182	113

Source: KMP.

As it can be seen from Table 4, the number of offenses concerning the violation of the secrecy of correspondence is growing. The highest rate was seen in 2016 – the number of offenses amounted to 2718, and the lowest was observed in 1999, as it was 113.

The effects of data theft may be, for example:

- shopping at the victim's expense;
- opening a bank account in the name of the victim;
- various types of extortion (loans, tax refund, etc.);
- running a fake business;
- entering into contracts in the name of the victim;
- getting the victim involved in money laundering;
- setting up false accounts on the Internet;[32]
- taking a loan in the name of the victim;
- renting an apartment in the name of the victim;
- conducting telephone conversation in the name of the victim;
- blackmail;
- unlawful trade in data.[33]

[32] *Jakie mogą być konsekwencje kradzieży tożsamości?*, "Biuro Informacji Kredytowej", https://www.bik.pl/poradnik-bik/jakie-moga-byc-konsekwencje-kradziezy-to-zsamosci (accessed: 11.12.2018).

[33] *Co złodziej może zrobić z Twoimi danymi*, "Nieskradzione.pl", https://nieskradzione.pl/co-zlodziej-moze-zrobic-z-twoimi-danymi (accessed: 11.12.2018).

The data presented above suggest that Polish users' data are more and more at risk from year to year, which is worrying.

5. Risk of illicit trafficking

E-commerce, i.e. buying or selling goods using the Internet, are transactions carried out via networks based on the IP protocol as well as via other computer networks. Goods and services are ordered via these networks, while payment and delivery of goods or services can take place either online or in reality. Transactions may occur between individuals, enterprises, government institutions, and other private as well as public entities.[34]
The perpetrators of crimes in this area often use anonymizing software that blurs the traces of their activity on the Internet. The software is, among others, TOR (The Onion Router). It is a virtual computer network, based on the so-called third generation onion routing. Network traffic analysis is almost impossible in this case, which in turn allows users of such networks to browse online resources anonymously.[35]

Illegal trade may include the following types of crime:

- "trading in licensed goods without possession of appropriate documents, in this respect or goods whose circulation remains illegal (including drugs and precursors to their production, weapons, explosives and chemical agents used to produce them, protected species of animals);
- trafficking in human beings and human organs;
- illicit trade in excise goods, including in particular tobacco products;
- trade of goods coming from crimes and trade in national heritage property".[36]

[34] *Handel elektroniczny*, [in:] *Pojęcia stosowane w statystyce publicznej*, "Główny Urząd Statystyczny", http://stat.gov.pl/metainformacje/slownik-pojec/pojecia-stosowane-w-statystyce-publicznej/1778,pojecie.html (accessed: 11.12.2018).

[35] *Krajobraz bezpieczeństwa polskiego Internetu 2016…*, op. cit., p. 261.

[36] *Ibidem*.

Table 5. Investigations regarding the illegal circulation of materials

Investigations carried out:	**2010**	**2011**	**2012**	**2013**	**2014**	**2015**
Trading in strategic goods without authorization	20	14	12	7	12	7
Production, processing, storage, possession, use or trade without permission of a substance of strategic importance	0	1	1	1	1	2
Total	20	15	13	8	13	9

Source: ABW.

As it can be seen from Table 5, upward trends are seen for incidents related to the manufacture, processing, accumulation, possession, use or trade without permission of substances of strategic importance: in 2015 there were two cases, while in 2010 such incidents did not occur at all. On the other hand, incidents of trading without authorization of goods of strategic importance do not show either a rising or a falling tendency, although in 2010 and 2011 there were more such incidents than in the following years.

6. The risk of online fraud threats

According to the definition in Polish language dictionary, *fraud* [Polish: *oszustwo*] is the act of misleading someone consciously, or of making use of someone's mistake for one's own benefit.[37] Article 286 of the Polish Penal Code states that whoever, with the purpose of gaining a material benefit, causes another person to disadvantageously dispose of their own or someone else's property by misleading them, or by taking advantage of a mistake or inability to adequately understand the action undertaken, commits a fraud. Fraud is also committed by anyone who demands a material benefit in return for an unlawfully acquired item.[38]

[37] *Oszustwo*, "Słownik języka polskiego PWN", http://sjp.pwn.pl/sjp/oszustwo;2496853.html (accessed: 11.12.2018).

[38] *Ustawa z dnia 6 czerwca 1997 r. Kodeks karny, Dz.U. nr 88, poz. 553 ze zm. [The Act of June 6, 1997. Penal Code]*, Journal of Laws no. 88, item 553, as amended, art. 286 § 1–2.

Victims of *online frauds* may, for instance, be people who do not check the credibility of the seller on an auction portal, even though there are numerous warning signs. For example, a very large number of positive comments about a product may arouse suspicions that they have not been posted deliberately. The risk of cheating is also higher in the offers which suggest "great deals", where items are sold at a heavily discounted price. Another characteristic of a dishonest online auction may be pictures of items from the producer, which may mean that the seller does not, in fact, have the item shown in the picture. Yet another threat is prepayments into the seller's account, which do not guarantee the delivery of the purchased items. Purchasing channels other than online auctions can also pose threats because fraudsters often propose selling goods at a lower price to avoid paying taxes and to skip the security mechanisms of websites. Often buyers sign the confirmation of delivery without checking whether the shipment which the courier has delivered to them is in the desired condition.[39]

Table 6. Computer frauds in Poland, 1999–2016

Year	Number of proceedings initiated	Number of proceedings found
2016	4103	4207
2015	4105	3282
2014	2567	2154
2013	1768	1573
2012	1285	1351
2011	1012	1364
2010	838	623
2009	673	978
2008	472	404
2007	322	492

[39] *Oszustwa internetowe*, "KPP Kępno", http://www.kepno.policja.gov.pl/wl8/aktualnosci/40559,Oszustwa-internetowe.html (accessed: 11.12.2018).

2006	285	444
2005	326	568
2004	229	390
2003	219	168
2002	114	368
2001	59	171
2000	127	247
1999	52	164

Source: KGP.

Frauds on the Internet can occur as:

- "false job offers;
- false offers to buy and sell;
- Nigerian fraud (message asking for financial support);
- fraud with the use of text message confirmation;
- extortion of money (e.g. by means of disk encryption software, the so-called. ransomware)";[40]
- "scams with the use of scareware software (e.g. fake anti-virus, displaying a message about the need to remove the malware, by purchasing the right tool);
- fee-related fraud (e.g., offering paid access to free services or non-existent services);
- fraud associated with the transfer of funds (insidious access to the account of the victim and theft of funds);
- investment fraud (false websites that affect the amount of shares of companies);
- identity theft (impersonating someone to commit a fraud)".[41]

As visible in Table 6 above, the number of computer frauds is constantly increasing year by year in Poland. The highest number of crimes of this kind

[40] *Wydział do walki z przestępczością*, "Komenda Stołeczna Policji", http://www.policja.waw.pl/pl/stoleczna-policja/wydzialy-ksp/wydzial-do-walki-z-cybe/31385,Wydzial-do-walki-z-Cyberprzestepczoscia.html (accessed: 11.12.2018).

[41] M. Siwicki, *Cyberprzestępczość*, Warszawa 2013, pp. 242–243..

was recorded in 2016, their number was 4207, while the lowest number of such crimes was recorded in 1999 – 164.

Internet frauds may result in financial losses on the part of their victims. Their personal data and other sensitive information can also leak out. Such people are also often exposed to blackmail. Virus infections of their computers may occur, as well as loss of data from their hard disks. Internet frauds are punishable by imprisonment. According to the official statistics of fraud, the number of frauds increases rapidly from year to year, which may pose a serious threat to Internet users.

7. The effectiveness of computer and network protection system

In Poland, initiatives are constantly being taken to protect cyberspace. Organizational and legal frameworks are created along with coordination systems, as well as sharing information with public administration. Cooperation in the protection of cyberspace also includes other entities, including individual Internet users, private entities and entrepreneurs.[42] While in the area of protecting cyberspace the initiative is borne by the state, in case of protection against threats on the Internet everyone has to take care of themselves. The level of security plays a major role in networks of Internet service providers. However, as it can be seen from the statistics in Table 7 below, the level of security provided is diversified.

Table 7. Ranking of autonomous systems in Poland as of 2016 in terms of the number of bots

No.	Name	Daily average	Daily maximum
1.	Orange	4141	9252
2.	Netia	934	1852
3.	Plus/Cyf. Polsat	218	336
4.	Multimedia	211	347
5.	T-Mobile	164	503

[42] *Rządowy program ochrony cyberprzestrzeni RP na lata 2011–2016 [Government program for the protection of cyberspace of the Republic of Poland for 2011–2016]*, Warszawa 2010, p. 7.

6.	Vectra	110	169
7.	Internetia	71	108
8.	TK Telkom	64	119
9.	Toya	48	76
10.	ASTA-NET	46	75

Source: *Krajobraz bezpieczeństwa polskiego Internetu 2016: Raport roczny z działalności CERT Polska* [*Overview of security in the Polish Internet 2019. Report on the activity of CERT Polska*], https://www.cert.pl/PDF/Raport_CP_2016.pdf (accessed: 2.09.2018).

As Table 7 shows, the level of botnet infection is highly diverse in the networks of individual Internet service providers. The largest average number of daily connections from botnet network has been observed in Orange network, amounting to 4141 calls, while the smallest average number of such connections has been observed in Asta-NET network, amounting to 46 connections. The next step to protect the computer system is the installation of anti-virus software, a firewall, as well as anti-malware and antispyware programs. In Poland, most operating systems used in both public and private administration are those from the Microsoft Windows family. Microsoft periodically publishes configuration recommendations in the form of the Windows security guide in order to protect their clients' systems appropriately. An important factor is also the fact that as new operating systems are launched on the market, technical support and the provision of updates for older systems is terminated in order to minimize the risk of infecting them with malware and incorporate them into the botnet network.

The popularity of Windows encourages attackers, and other parties seeking errors in the software, to find loopholes that allow them to gain control over operating systems. Often, such vulnerabilities can be found in anti-virus software or firewalls because they have their own drivers and strongly interfere with the operating system. Finding a vulnerability in such software may result in obtaining maximum rights to the system. Producers of equipment (among others Cisco, Apple, Samsung, TP-Link or HP) offer periodic software updates to seal the software for their devices (like

webcams, DSL modems, printers, smartphones, tablets) in the network infrastructure.[43]

The quality of security against online threats, according to the Polish Supreme Chamber of Control, is low. In 2015, the main state entities responsible were inspected for protecting cyberspace, and the level of security in state administration units was examined. The main problem turned out to be lack of an integrated system of protection against cyber threats. Other adversities include lack of adequate resources, underestimation of risks, as well as lack of procedures and methods of operation in crisis situations. According to the Supreme Chamber of Control, in 2015 the greatest cyber threats in Poland were the following: theft of personal data; malware;falsification, destruction, theft and phishing of data; massive DDoS attacks using botnets; spam; and phishing.[44]

As the official data show, the level of protection in the networks of individual operators is very different. It is worrying that the highest level of infection is shown by networks of some of the largest Internet service providers.

8. Conclusion

At the state level, cyber threats may have negative effects on all spheres of the state's activity, both civilian and military ones. It is particularly true in the context of critical infrastructure, including dedicated transport solutions, communication systems, or energy and computer networks. It is assumed that the degree of this type of threats is directly proportional to the technical and technological advancement of the state and to the degree of the dependence of the state's functioning on the flow of information in the entire area of the information economy.

The authors' conclusion is that challenges related to cyber threats not only determine the necessity for state authorities to develop strategic and legislative documents that will acknowledge the dynamically changing security environment and define state strategies of responding to digital threats; they also imply the necessity for the state to acquire effective tools that will protect citizens and systems against attacks of this type and counter-reaction.

[43] *Ibidem*, p. 23–38.

[44] *Realizacja przez podmioty państwowe zadań w zakresie ochrony cyberprzestrzeni RP w 2015 roku [Implementation by state entities of tasks in the field of protection of the cyberspace of the Republic of Poland in 2015]*, pp. 9–21.

A possible remedy for cyber threats on the state level is entering by a state into cybersecurity alliances with other states. Each security system is as strong as its weakest link. Shaping a stable, international cybersecurity environment both in the regional and global dimension depends not only on shared visions and common goals but also on the potential of each member. The efficiency of an alliance – this mostly applies to military alliances – is based on the strategic credibility and deterrence potential of all the members. In the area of defense, which is directly related to cybersecurity, the current trend is building military cooperation by creating and tightening alliances, and thus building the potential to defend cyberspace by means of common systems of alerting and information exchange and by developing the ability to cooperate not only during peace, but also during crisis or war. In order to thoroughly investigate the subject, further research and analysis in this field should be undertaken.

Due to the growing importance of cyberspace defense, it is necessary to increase resource allocation, technological development, staff training, and to raise public awareness of threats in cyberspace.

References

Literature:

1. *Bezpieczeństwo teleinformatyczne państwa*, M. Madej, M. Terlikowski (eds), Warszawa 2009.
2. Bógdał-Brzezińska A., Gawrycki M., *Cyberterroryzm i problemy bezpieczeństwa informacyjnego we współczesnym świecie*, Warszawa 2003.
3. Gierszewski J., *Bezpieczeństwo wewnętrzne. Zarys systemu*, Warszawa 2013.
4. Grubicka J., *Globalna przestrzeń bezpieczeństwa społeczeństwa informacyjnego wobec zagrożeń cyberterroryzmu*, [in:] *Bezpieczeństwo – wielorakie perspektywy. Człowiek – społeczeństwo – państwo w sytuacjach kryzysu*, M. Kuć, T. Węglarz (eds), Poznań 2014.
5. Grubicka J., *Konwergencja technologiczna a system bezpieczeństwa informacji*, [in:] *Nowoczesne technologie na rzecz bezpieczeństwa. Zagadnienia dual-use*, W. Filipkowski (ed.), Gdynia 2015, pp. 53–70.
6. Jakubczak W., Szyłkowska M., *Wyzwania i koncepcje ochrony cyberprzestrzeni w erze globalizacji*, [in:] *Cyberprzestrzeń. Uzależnienia – zahamowania – zagrożenia*, M. Koziński, J. Grubicka, S. Kosznik-Biernacka (eds), Słupsk 2016.

7. Kosiński J., *Paradygmaty cyberprzestępczości*, Słupsk 2015.
8. Madej M., *Zagrożenia asymetryczne państw obszaru transatlantyckiego*, Warszawa 2007.
9. Siwicki M., *Cyberprzestępczość*, Warszawa 2013.
10. Szubrycht T., *Cyberterroryzm jako nowa forma zagrożenia terrorystycznego*, "Zeszyty Naukowe AMW", 2005, no. 1 (160)/2005, pp. 173–187.
11. *Wybrane problemy bezpieczeństwa. Dziedziny bezpieczeństwa*, A. Urbanek (ed.), Słupsk 2013.
12. Urbanek A., *Wybrane problemy bezpieczeństwa. Rozważania o przestrzeni bezpieczeństwa*, Słupsk 2014.

Legal acts:

1. *Ustawa z dnia 6 czerwca 1997 r. Kodeks karny*, Dz.U. nr 88, poz. 553 ze zm. [*The Act of June 6, 1997. Penal Code*, Journal of Laws no. 88, item 553, as amended].
2. *Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne*, Dz.U. 2005 nr 64 poz. 565 [*Act of February 17, 2005 on computerization of the activities of entities performing public tasks and of the relations between themselves and between them and the users*, Journal of Law 2005 no. 64, item 565].

Documents and reports:

1. *Communication from the Commission to the European Parliament, the Council and the Committee of the Regions – Towards a general strategy against cybercrime* (COM/2007/0267 final), http://eulex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52007DC0267 (accessed: 19.12.2018).
2. *Krajobraz bezpieczeństwa polskiego Internetu 2014: Raport roczny z działalności CERT Polska [Overview of security in the Polish Internet 2014. Annual report on the activity of CERT Polska]*, https://www.cert.pl/wp-content/uploads/2015/11/Raport_CP_2014.pdf (accessed: 2.11.2018).
3. *Krajobraz bezpieczeństwa polskiego Internetu 2015: Raport roczny z działalności CERT Polska [Overview of security in the Polish Internet 2015. Annual report on the activity of CERT Polska]*, https://www.cert.pl/PDF/Raport_CP_2015.pdf (accessed: 4.11.2018).
4. *Krajobraz bezpieczeństwa polskiego Internetu 2016: Raport roczny z działalności CERT Polska [Overview of security in the Polish Internet*

2016. Annual report on the activity of CERT Polska], https://www.cert.pl/PDF/Raport_CP_2016.pdf (accessed: 2.09.2018).
5. *Realizacja przez podmioty państwowe zadań w zakresie ochrony cyberprzestrzeni RP w 2015 roku [Implementation by state entities of tasks in the field of protection of the cyberspace of the Republic of Poland in 2015].*
6. *Rządowy program ochrony cyberprzestrzeni RP na lata 2011–2016 [Government program for the protection of cyberspace of the Republic of Poland for 2011–2016]*, Warszawa 2010.
7. *Strategia bezpieczeństwa narodowego Rzeczypospolitej Polskiej [National Security Strategy of the Republic of Poland]*, Warszawa 2014.

Internet sources:
1. *Bezpieczeństwo informacji*, "Centrum.Bezpieczeństwa.pl", http://www.centrum.bezpieczenstwa.pl/index.php/bezpieczenstwo-informacji/slownik-bezpieczenstwo-informacji (accessed: 18.09.2017).
2. *Co złodziej może zrobić z Twoimi danymi*, "Nieskradzione.pl", https://nieskradzione.pl/co-zlodziej-moze-zrobic-z-twoimi-danymi (accessed: 11.12.2018).
3. *Czym jest kradzież tożsamości?*, "Biuro Informacji Kredytowej", https://www.bik.pl/poradnik-bik/czym-jest-kradziez-tozsamosci (accessed: 20.03.2018).
4. GIODO. Generalny Inspektor Ochrony Danych Osobowych, *ABC zagrożeń bezpieczeństwa danych osobowych w systemach teleinformatycznych*, Warszawa 2009 www.giodo.gov.pl/plik/id_p/1560/j/pl/ (accessed: 20.03.2017).
5. *Handel elektroniczny*, [in:] *Pojęcia stosowane w statystyce publicznej*, "Główny Urząd Statystyczny", http://stat.gov.pl/metainformacje/slownik-pojec/pojecia-stosowane-w-statystyce-publicznej/1778,pojecie.html (accessed: 11.12.2018).
6. *Jakie mogą być konsekwencje kradzieży tożsamości?*, "Biuro Informacji Kredytowej", https://www.bik.pl/poradnik-bik/jakie-moga-byc-konsekwencje-kradziezy-tozsamosci (accessed: 11.12.2018).
7. NIK, *Realizacja przez podmioty państwowe zadań w zakresie ochrony cyberprzestrzeni. Informacja o wynikach kontroli*, https://www.nik.gov.pl/plik/id,8764,vp,10895.pdf (accessed: 18.12.2018).
8. *Oszustwa internetowe*, "KPP Kępno", http://www.kepno.policja.gov.pl/wl8/aktualnosci/40559,Oszustwa-internetowe.html

9. *Oszustwo*, "Słownik języka polskiego PWN", http://sjp.pwn.pl/sjp/oszustwo;2496853.html, (accessed: 11.12.2018).
10. *Spam*, "Słownik języka polskiego PWN", http://sjp.pwn.pl/slowniki/spam.html (accessed: 20.03.2018).
11. *Symantec Internet Security Threat Report*, April 2017, vol. 22, https://www.symantec.com/content/dam/symantec/docs/reports/istr-22-2017-en.pdf
12. *Wydział do walki z przestępczością*, "Komenda Stołeczna Policji", http://www.policja.waw.pl/pl/stoleczna-policja/wydzialy-ksp/wydzial-do-walki-z-cybe/31385,Wydzial-do-walki-z-Cyber-przestepczoscia.html (accessed: 11.12.2018).

Cite this article as:
J. Grubicka, K. Rogowski, G. Diemientiew, *Dangers and Attacks on Digital Information in the Public Safety Space*, "Security Dimensions", 2019, no. 30, pp. 66–95, DOI 10.5604/01.3001.0013.7777.