DOI: 10.4467/27204383TER.22.014.15430

ORCID: 0000-0003-4649-589X

ANNA ROŻEJ

The role and importance of information from open sources in increasing vulnerability to security threats in cyberspace, with particular reference to cyberterrorism

Abstract

The aim of the article is to present how the role and importance of open source information has increased in recent years as a significant part of the functioning of societies has moved to the world of Internet. Unfortunately, along with this trend, new threats have emerged, including those of a cyberterrorist nature, which require immediate action to limit their impact on information security.

Keywords:

information security, open source, infosphere, threats, information warfare, critical infrastructure

Over the past decade or so, the dynamically changing environment in which people function has led to radical changes in almost every environment, including the security environment. The memorable attacks on the World Trade Center in New York and the Pentagon in Washington, D.C., over 20 years ago, should be considered a marker of change in the perception of security on a global scale. Immediately after the attacks, most NATO member states, including Poland, were forced to implement elements of their national defence preparedness systems. This tragedy also became a source of deep reflection for the international community, encompassing both the causes and consequences of this event, which, in terms of international relations, can be considered a watershed. The attacks on the World Trade Center and the Pentagon caused a thorough reorientation of all the national systems of Western countries, especially in terms of cooperation with other states and international organisations, including NATO. It can be said that this was a kind of breakthrough since the Cold War. It was not until the attacks of 2001 that the need for reform of the national security systems, which were stuck with 20th century solutions and were unsuited to the challenges of the post-millennium world, was recognised.

The assassination of the symbols of American power proved unequivocally that "(...) today's threats are of a different nature and scale than before, and the contemporary response to these threats is inadequate. Weapons designed to counter threats at the end of the last millennium will not be able to meet them in the first decades of the 21st century. New, often asymmetric, threats to global security require new thinking"[1].

At the same time, legitimate organisations operating across state lines are also gaining in power and influence, with the technical capabilities to adapt to the new security environment. Stock speculators, traders, multinational corporations, and Internet service companies now have the potential to have a significant global impact on the daily lives of citizens in many countries. Globalisation and the revolution in information technology have given these institutions an advantage. Their control is exercised more through financial markets than through

[1] Hall R., Fox C., *Ponownie przemyśleć bezpieczeństwo* (Eng. Rethinking security), „Przegląd NATO" zima 2001/2002, p. 8.

global structures, and distortions arise along the same lines. It should therefore come as no surprise that the traditional mechanisms of the state based on the idea of borders, order, authority, police, and force structures are under threat. They also seem inherently incapable of countering contemporary security challenges. As this incapacity becomes more apparent, disillusionment with the previous system grows and a belief can arise that everything in the security field is heading for the worse, which of course cannot be allowed to happen.

More often than not, it is very difficult to identify a leader or region on which to focus attention to counter threats. Moreover, the scale of these threats is so large that it is becoming dangerous for many countries. Indeed, these threats know no national or continental boundaries. There is also a fundamental difficulty in properly identifying phenomena (organisations, leaders) in order to counter them effectively. These threats can undermine the essence and foundations of the functioning of national and international institutions, and destroy the economies of many countries.

The need for a new approach to security was pressing, as terrorism is only one of many non-traditional security challenges. Ethnic and religious conflicts, drug trafficking, mass migration, regional instability, money laundering, the activities of various extremist groups, information theft, and disinformation itself also pose them. Meanwhile, the cybersphere has just emerged, and it has reached a tremendous growth rate, causing selected powers to recognise the need to reform their defence systems. As a result, separate types of army - cyber armies, among others - began to emerge. The cybersphere has shifted the focus of security from physical warfare to response and the development of resources to counter cyber attacks, as well as pre-emptive action in cyberspace.

Taking into account the considered issue, it was assumed that the subject of research conducted within the framework of this article will be the information from open sources analysed in the context of potential threats. The presented object of research is a determinant of the goals of the research process, which are seen in theoretical and practical terms. The theoretical objective is to develop and complement the content relating to both the theory and practice of cyber security in the specific case of using online open sources. The achievement of the theoretical goal is to contribute to the practical

goal, which will provide useful solutions for ensuring and maintaining information security. The presented problem situation, the subject of the research and its goal clearly define the main research problem, which boils down to answering the following question: has the global publicity and general accessibility for all Internet users at the same time of information from open sources concerning state security increased their vulnerability to cyber attacks? The solution to the research problem will depend on the solution to specific problems, which boil down to answering the following questions:

1. What changes have occurred in the security environment?
2. How have attitudes towards the Internet changed over the last few years?
3. What is open source and what are its specificities?
4. What are the potential risks of using information from open sources?
5. What preventive measures are possible to prevent information security risks?

Preliminary conclusions from observations and analysis of available documents and literature on the subject, as well as the stated aim of the research and research problems determined the working hypothesis, thanks to which it will be possible to carry out the research process: the development of the Internet and the increased interest in open sources are connected with the increase in threats of a cyberterrorist nature.

As Henry Kissinger - prominent American politician and diplomat, national security advisor to President Richard Nixon - used to say: "Security is the foundation of everything we do"[2] and it is hard not to agree with this argument. However, in the era of enormous technological development, access to advanced processes and equipment, it may seem that security concerns are receding into the background. It is the tools and capabilities that are important, rather than one of the most important values - safety. As almost every aspect of life has moved to the internet, we are exposed to many cyber threats, and the level of feeling of security, especially ICT security, has decreased significantly. There is a huge risk that the data we collect and the information we process will become the target of cybercriminals.

[2] Kissinger H., *Dyplomacja* (Eng. Diplomacy), Warszawa 2016.

One of the first theorists of the art of war, Sun Tzu, who lived 25 centuries ago in China, in his treatise *The Art of War,* states that "(...) the highest skill in the art of war is to subdue the enemy without a fight"[3]. At the same time, he gives many tips on how to achieve this desired state. Aiming to achieve success in war, one should, among other things, discredit everything that is good in the enemy's country, involve the representatives of the enemy's ruling classes in criminal enterprises, tear up their good name and, at the right moment, throw them into the mercy of the compatriots' contempt. It is also legitimate to disorganise the activities of the adversary government and to cause feuds and discord among the citizens of the enemy country. The Indian treatise *Arthashastra* by Chanakya Kauṭilya should also be noted. This Indian philosopher and war theorist, apart from assigning a major role in foreign policy to spies and traitors, introduced a rule of warfare according to which it should be permissible to start a war only when comparative analysis of both sides shows that victory is certain. Factors such as wisdom, plan, a strong and well-trained army, high morale and overall potential are the guarantors of success. Kautilya also pointed out that the conquered population must be treated gently in order to have lasting control over them.

In the information security environment, the underlying cause of change can be traced in particular to the information revolution, which introduced various technologies that allowed for the acquisition and distribution of information on a mass scale. This phenomenon had a breakthrough character, due to the global scale of influence of these technologies. The above-mentioned consequences of the information revolution causing immense changes made the infosphere, understood as a synonym of information space and information environment, a subject of security sciences[4]. In the scientific environment the infosphere is understood as the entirety of information resources to which a given entity has access. The analysis of the information society in the aspect of cybernetic system indicates that the infosphere is divided into a local layer, which corresponds to local information resources created along with the development of the local community,

[3] Sun Tzu, *Sztuka wojny* (Eng. Art Of War), Gliwice 2004.

[4] Sosińska-Kalata B., *Obszary badań współczesnej informatologii* (*nauki o informacji*) (Eng. Research areas of contemporary informatology (information science)), „Zagadnienia Informacji Naukowej" 2013, no. 2, pp. 9–41.

and a global layer composed of global resources, which is much more than the information sum of local resources[5]. The beginning of the information society is seen in the 1960s and 1970s. It emerged as a result of the industrial revolution, during which computers were introduced and computerisation developed[6]. For the first time the term "information society" (Jap. *johoka shakai*) was first used by Tadao Umesao, a Japanese scientist, to describe a society that started using computers for communication in the era of digital and microelectronic development. The concept was later developed by Daniel Bell, who believed that for the society of that time the strategic resources were knowledge and information rather than labour and capital[7].

In recent years the infosphere, apart from becoming a permanent feature of globalisation, has become enormously more important by encompassing a much greater amount of available information of a universal nature than just a few years ago. The challenge has become not only the mass and excess of information, but above all its characteristics, such as unreliability, irrelevancy and untruthfulness. The multiplicity of information channels and sources means that the aforementioned characteristics are now intensifying.

Moreover, the information revolution and the accompanying intensely developing technology, the dynamics of life, and more recently the pandemic caused by the SARS-CoV-2 virus have meant that almost all of everyday life has been transferred to the world of the Internet, which on the one hand offers great opportunities, but on the other generates many security risks, on a national and international scale. "As soon as new information techniques spread and were adopted by different countries, different cultures, different organisations and different purposes, there was an explosion of different types of behaviour and uses, which in turn contributed

---

[5] Sienkiewicz P., *Społeczeństwo informacyjne jako system cybernetyczny*, w: *Społeczeństwo informacyjne. Wizja czy rzeczywistość?* (Eng. Information society as a cybernetic system, in: Information Society. Vision or Reality?), vol. 1, L.H. Haber (ed.), Kraków 2004, s. 79.

[6] Nowak J.S., *Społeczeństwo informacyjne – geneza i definicje*, w: *Społeczeństwo informacyjne. Krok naprzód, dwa kroki wstecz* (Eng. Information society - origins and definitions, in: Information Society. One step forward, two steps back), P. Sienkiewicz, J.S. Nowak (ed.), Katowice 2008, p. 25.

[7] http://www.bbc.uw.edu.pl/Content/20/08.pdf [accessed: 25 XI 2021].

to technological innovation, accelerating the pace and extending the reach of technological change, as well as diversifying its sources"[8]. The quoted statement of the Spanish sociologist Manuel Castells proves that the contemporary society is indeed an information society, which has been almost entirely dominated by telecommunication systems used for sending, receiving and processing information. Information is now an integral part of social and economic life and is present in every area of human functioning.

It should be noted that the manifestations of social life are most intense in large spaces, such as, for example, urban centres, airports or transport routes. Modern societies, on the other hand, prove that these places do not have to exist in reality, because it is enough that they are only an infrastructure or a communication platform that creates the conditions for organisations or various other entities to connect with each other in real time. Communication theorist Marshall McLuhan also recognised the changes in society during the information revolution. He believed that thanks to close online relationships, the world is becoming a global village where people can connect and communicate in real time[9]. We did not have to wait long, and the era of personal computers, the Internet and smartphones arrived, without which no one can imagine functioning today. Thanks to the technological solutions that have emerged, it is possible to communicate with anyone regardless of their location.

As a result of the enormous dynamism of the processes which have taken place over the last few decades, the Internet is now the largest source of information, which consists of an open part - publicly accessible, and a dark part - the so-called Darknet, access to which is somewhat limited, but with the use of appropriate technologies also possible.

The desirability of the Internet as a source of information is demonstrated by data froma report published in 2018 by the ITU (International Telecommunication Union)[10]. Well, already then, more than half of the world's population had access to the Internet.

[8] Elliott A., Castells M., *Społeczeństwo sieci,* w: Elliott A., *Współczesna teoria społeczna. Wprowadzenie* (Eng. Network society, in: Contemporary social theory. Introduction), Warszawa 2011.

[9] Ibid, pp. 311–319.

[10] *Measuring the Information Society Report,* t. 1, Geneva 2018.

At the end of 2018, almost 51.2 per cent, or 3.9 billion people, were using it. This represented a significant step towards even greater development of the global information society. It was estimated that in developed countries, 4 out of 5 people had direct and unlimited access to the web. In developing countries, about 45% of the population had access to the Internet, and in the least developed countries only 20%. However, according to ITU predictions, there is a continuous upward trend in access to the Internet. This is confirmed by the data given in the Global Digital Report[11] on the state of digitisation of society in January 2021, which is presented in Figure 1.

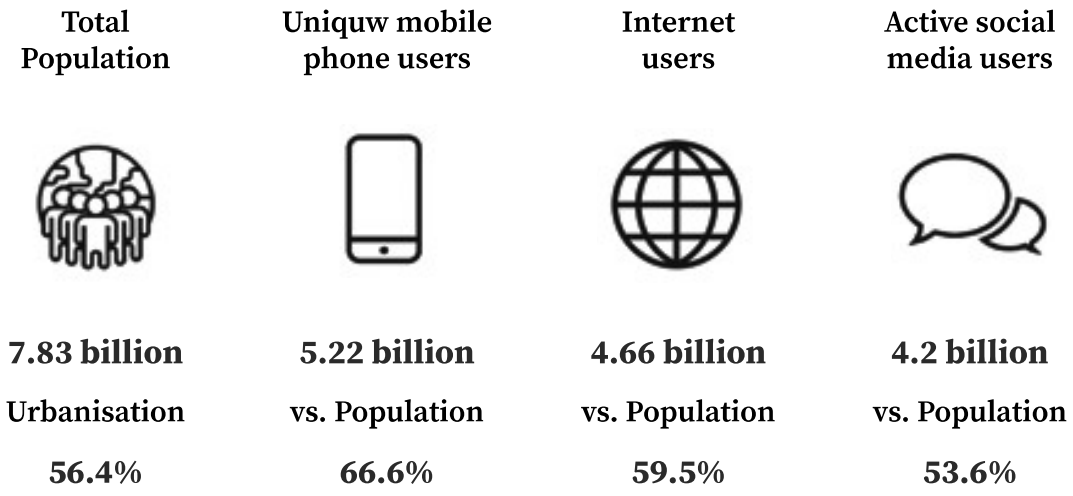

Fig. 1. Global digitalization in January 2021.

Source: DataReportal - Global Digital Insights.

Characterizing the data presented in Figure 1, it is important to note that:

- **Population**: the global population was 7.83 billion.
- **Mobile**: 5.22 billion people used a mobile phone, representing 66.6 per cent of the global population. The number of mobile users increased by 1.8 per cent since January 2020. The total number of mobile connections increased by 72 million to reach 8.02 billion by early 2021.

[11] https://datareportal.com/reports/digital-2021-global-overview-report [accessed: 26 XI 2021].

- **Internet**: 4.66 billion people worldwide used the Internet, accounting for 59.5 per cent of the global population. This represents an increase of 316 million over the year.
- **Social media**: there were 4.2 billion social media users worldwide. This number has increased by 490 million since January 2020. The number of social media users accounted for more than 53 per cent of the global population.

Furthermore, the following facts also prove that the Internet is one of the most common sources of data:

- The number of social media users is constantly increasing. It currently stands at around 4.48 billion (Figure 2).
- The platforms belonging to the Facebook family (Facebook, WhatsApp, Instagram, Messenger) are hugely popular (Figure 3).
- The time spent using the Internet is increasing (Figure 4).
- The time spent using social media is increasing (Figure 5).

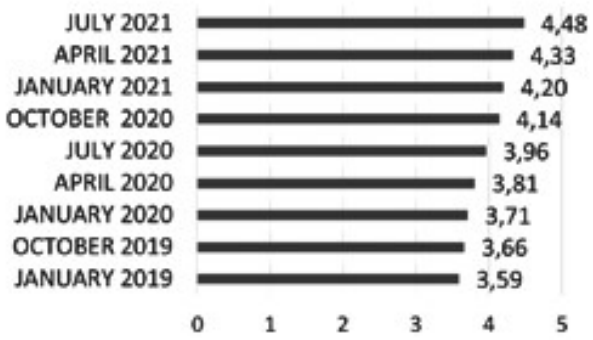

Fig. 2. The increase of social media users between 2019 and 2021 (in billions).

Source: DataReportal, DataReportal - Global Digital Insights.

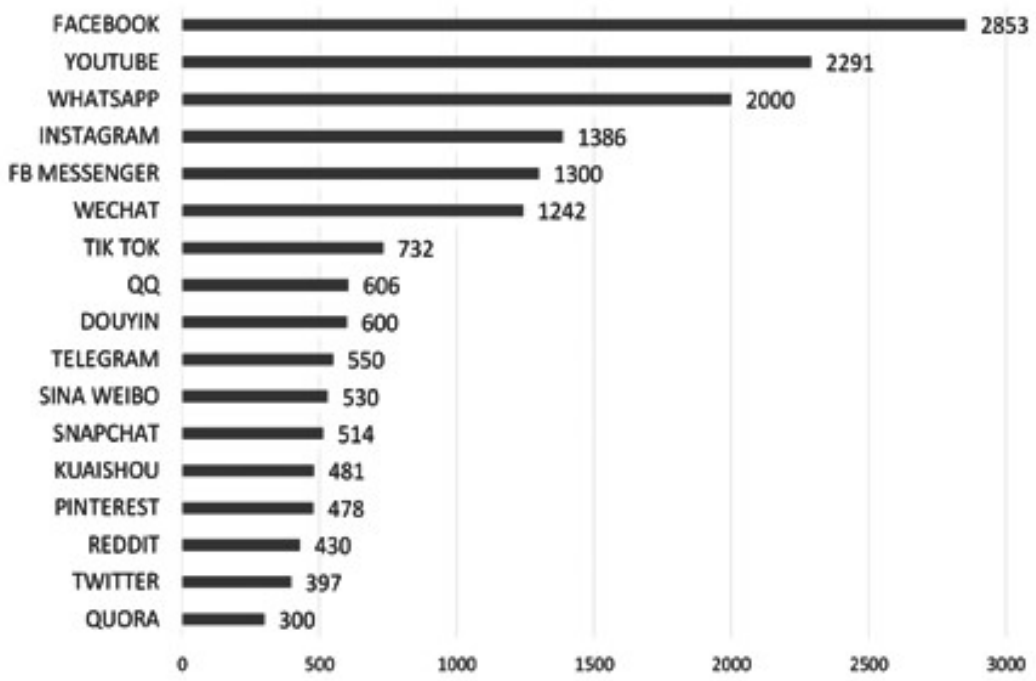

Fig. 3. Users of most popular social media in millions (updatet in July 2021).

Source: DataReportal, DataReportal - Global Digital Insights.

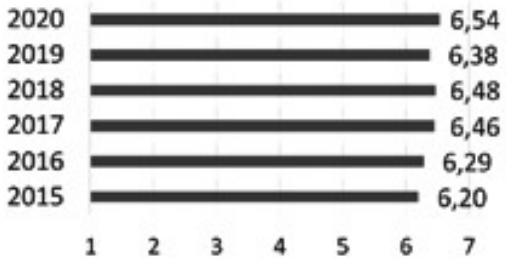

Fig. 4. The increase of time spent daily on using the Internet (in hours) by users at the age of 16–64 in the years 2015-2020.

Source: DataReportal, DataReportal - Global Digital Insights

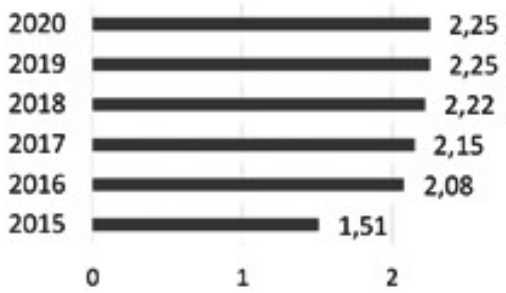

Fig. 5. The increase of time spent daily on using social media (in hours) by users at the age of 16–64 in the years 2015-2020.

Source: DataReportal, DataReportal - Global Digital Insights.

The most popular reasons why people go online include:
- seeking information;
- staying in touch with friends and family
- having up-to-date data and information;
- looking for tips on how to perform certain activities;
- watching movies, television.

Detailed data is shown in Figure 6.

Fig. 6. Primary reasons for using the Internet by users at the age of 16–64.

Source: DataReportal - Global Digital Insights.

On the basis of the data presented above indicating the enormous activity of the global society on the Internet and its constant growth, it should be stated that the aforementioned network is the largest collection of information, often of a strategic nature. No wonder that information has become the most important resource determining the functioning and success of almost every organisation or enterprise. It is a resource that constitutes the basis of activity, ensures competitive advantage and gives a sense of security. The universality of information and its almost unlimited availability result, among other things, from the fact that its source is often open. Researchers and experts in the area of intelligence activities define open source as an entity or object characterised by qualities that enable it to generate information

allowing for its legal processing, including its recording, transmission or collection[12]. Information from open sources is of primary or secondary nature, which may also generate certain limitations. Information originating from a primary source may have limitations related to the possibilities of its dissemination, if, for example, it is classified or private information. However, if the information is obtained from secondary sources - publicly available, its openness is no longer a problem[13]. It should be noted that although information from open sources is available, the recipient rarely has full knowledge of its sources and characteristics. Another definition points out that open sources are all written, audiovisual or IT means of disseminating information[14]. Open information sources can be classified in several ways, taking into account the relationship between the importance of the information and the value of the source. In practice, however, what is most often taken into account is the type of medium used to convey the information, which may be due to the fact that media vary in quality and titles are published in different ways. For example, on the Internet the user may find information that appeared on television or in newspapers, and vice versa. However, this information may appear in articles with different titles.

Technological development, as well as increased access to the Internet, has meant that open sources of information have also evolved. Examples of open sources are presented in the table.

Table. Examples of open sources.

OPEN SOURCES			
Domains (e.g. registers, lists, WHOIS)	Maps (e.g. Provincial Spatial Information Systems)	Individuals (e.g. surnames - surnames-polskie.pl, Public Information Bulletin)	Users/logins (e.g. Albicla, Allegro, Fotka)

[12] Saramak B., *Wykorzystanie otwartych źródeł informacji w działalności wywiadowczej: historia, praktyka, perspektywy* (Eng. The use of open sources of information in intelligence activities: history, practice, perspectives), Warszawa 2015 pp. 22–23.

[13] West Ch., *Competitive intelligence*, New York 2001, p. 50.

[14] Oleński J., *Ekonomika informacji* (Eng. Economics of information), Warszawa 2001, p. 49.

Social networking sites (e.g. Facebook, Albicla, Fotka)	Dating sites (e.g. Sympatia, eDarling)	Companies/organisations (e.g. CEIDG, eKRS, Rejestr.io)	Society (e.g. Local Data Bank - CSO, Demography Database - CSO)
Business/economy (e.g. Allegro, WSE)	Archives (e.g. IPN Archive Inventory, National Digital Archive)	Translation (e.g. Electronic Dictionary of the Polish Language)	Public registers (e.g. Data Bank, Public Procurement Bulletin)
Law (e.g. Official Journals, Internet System of Legal Acts)	Universities (e.g. POL-on, RAD-on)	Transport (e.g. CEPiK API, EPKT Spotters)	Dark web (Active TOR Sites)
Documents (e.g. chomikuj.pl)	Video (e.g. Kamery.edu.pl)	Photos (e.g. Fotosik.pl)	Telephone numbers
Phone books (e.g. Service provider, Who called)	SIGNIT (e.g. WebSDR)	OpSec (e.g. IT Generators, GenApps)	Knowledge base (e.g. blogs, courses, presentations)

Source: Own elaboration.

Each of the above sources can be divided into individual subcategories, and the element which links them all is the Internet. However, when looking for reliable information on the Internet, one should approach it with great caution and not forget about other sources from the printed categories, such as books, newspapers or magazines. Moreover, it is worth noting that the Internet is not only information services, but also very popular and widespread social networking sites that ensure the functioning of various thematic environments, interest groups, as well as dictionaries, encyclopedias, forums or blogs. All these sources contain a wide variety of information. In addition, open sources allow access to private photos, satellite images and geolocation data. Although these sources are primarily open, accessible and public, it is prudent to keep a reasonable distance from them and to verify them.

It is worth being aware that search services, one of the most popular functionalities of the Internet, are based on the use of specialised software, which is responsible for exploring Internet databases. The most popular mechanisms include:

- mechanical indexing of words and phrases – AltaVista/Yahoo, Google, HotBot;

- arbitrary cataloguing of documents according to an accepted thematic classification - Yahoo;
- services that search documents from discussion groups - AltaVista Usenet;
- metasearch - a tool using individual search engines - MetaCrawler, MetaFIND;
- search using specialised databases - Alphasearch;
- others.

Despite the existence of such specialised technology, when reviewing open sources, including websites, it is important to assess them each time for credibility. To do this, it is useful to ask yourself five basic questions: who?, what?, where?, when?, why?

In order to find the answer to "who?" - you can analyse the site to look for authors, specific names or detailed information. It is also good practice to check domain types - .com/.org/.gov/country code - and assess whether the type is appropriate for the content presented. If the site from which the information is taken is a personal site or a user's social networking site, it would be useful to identify who is responsible for entering the content and, if possible, analyse the source code of the site, where the author's name is often written. Then, in order to verify the reliability of the information, it would be necessary to check who owns the server on which the page is hosted and whether the information gathered is consistent. A good method to check the credibility of the given content is to look for opinions of other users, as well as to trace the distribution of the information, for example by verifying the number of shares.

When checking a given website, you should pay attention to the content it contains, i.e. try to answer the question "what?". In order to be able to assess the truthfulness of the posted content, it is necessary to verify sources, dates, and whether the content is not changed with respect to, for example, quoted sources. A very important feature of information is its timeliness, i.e. answering the question "when?". Therefore, one should check when the information was posted, when it was updated or how often it is updated. Gathering answers to the above questions will make it possible to assess whether the information coming from open sources is, above all, true, reliable and up-to-date.

The statistical data presented in the first part of the article show that with the growing number of population with access to the Internet, it is a tool for posting, searching and exchanging information. Moreover, Internet resources are easily and quickly supplemented by Internet users. Therefore, anyone can be both a recipient of information and its author. In order to identify the attributes of open sources, it is necessary to indicate:

- availability,
- low cost of acquisition,
- uncertain reliability,
- lack of dependence,
- low risk,
- openness.

The above features, in a way, answer the questions about the number of open sources and, above all, the amount of information collected and processed in them. One example is the social networking site Facebook.com, which currently has around 2.8 billion active users monthly, with around 1.84 billion daily visitors. Since the beginning of 2021, the number of Facebook users has increased by around 12 per cent. This scale illustrates how much information appears on the portal at the same time.

The information presented so far indicates that the reach and accessibility of open sources is enormous. Today, more than half of the world's population has access to the Internet through computers, smartphones or other devices. The technological revolution that has taken place in this field has undoubtedly increased the quality of life and thus also the digital competences of international society. It is now difficult to imagine professional or private life without access to the web. Looking from the perspective of development in the economic and social area, the current situation should only be a reason for satisfaction and pride. After all, access to so much information is the basis for further development, new opportunities and chances.

Unfortunately, the development of cyberspace, in which a huge amount of information is processed, also brings with it the development of cyberterrorism. Just as cyberspace has no borders, terrorism has an unlimited range, which allows cybercriminals to undertake and successfully carry out cyber-terrorist activities on the Internet. A permanent feature of cyberterrorism is the invisibility of its actions

and, to some extent, its effects, which cannot be said of terrorism in its conventional form. Most often, the Internet user does not notice the cyber attack and is not aware of it. An attack becomes apparent when, for example, the ICT systems of strategic facilities responsible for critical infrastructure are blocked. Unfortunately, these threats are very poorly measured or not measured at all. The problem also lies in the fact that cyber-terrorists are adversaries against whom it is difficult to apply any international conventions on military action by states, as it is not really clear who the adversary is. The need for legislation in this area is certainly a priority for every state, as well as international organisations. The development of cyberspace has meant that states have lost the ability to fight this invisible adversary, and there is no legal basis to trigger international cooperation to identify the enemy and their status.

Only a dozen or so years ago, we as a society were very impressed by ICT developments and the digitisation of many areas. However, new threats to 21st century security, such as cybercrime as well as cyberterrorism, among others, have led to a review of such an enthusiastic attitude. 'Cybercrime' is defined as any illegal behaviour carried out by means of electronic activities targeting the security of computer systems and the data they contain. It also includes illegal activities carried out on or in relation to a computer system or network, including crimes such as illegal possession, offering or distribution of information via a computer system or network. Such crimes may include, but are not limited to, fraud, forgery, industrial espionage, sabotage and extortion through computer piracy and other intellectual property crimes. Cyberterrorism, on the other hand, includes attacks on public safety, life and electronic warfare against critical infrastructure. Cyberterrorism also uses new information technologies or cyberspace for traditional activities[15].

Previously, cyberterrorism was more associated with banking systems, identity theft or computer system viruses. An example of the scale of cyberterrorism at the time can be seen in the events that took place in Estonia in 2007. A cold war of a cyber nature was fought over the attempt to move a monument to the so-called Bronze Soldier, which commemorated Soviet servicemen. At the time, it was not the conflicts

[15] http://unicjin.org/documents/congr10/10e.pdf [accessed: 27 XI 2021].

in the streets that were the major threat, but the massive attacks on government and private servers. They caused widespread paralysis by blocking banking systems, information services and government websites. The scale of these events is reflected in the words of former Estonian President Toomas Hendrik Ilves, who stated that: "These days you don't need missiles to destroy infrastructure. You can do it online". Estonian society learnt then that the Internet offers many opportunities, but it can also take away the ability to function properly. The transfer of life to the world of the Internet means that cyberterrorism is constantly evolving and extending its reach into new areas of operation. According to the literature on the subject, "cyberterrorism" "(...) is a politically motivated attack or threat of attack aimed at an information system, specific data. The purpose of an attack can vary from destroying information to, for example, making it available to achieve political or social goals. Nowadays, cyberterrorism is not only typical terrorist attacks in cyberspace, nowadays it also includes such activities as propaganda, disinformation, espionage, online surveillance, manipulation of information, called soft cyberterrorism"[16].

It should be noted that all the negative phenomena that can be encountered every day in "real life" can occur in cyberspace. Theft, fraud, manipulation, espionage are just examples of the threats that can be faced in cyberspace. Physical destruction of servers contributing to disruption of systems can be an example. Hackers can achieve a similar goal by introducing malware. This malware can be a virus, Trojan horse, ransomware, exploit, rootkit, keylogger or backdoor. All of these examples of malware are capable of blocking ICT systems, depriving users of access to information. At the same time, their mode of action is secret, which makes them very difficult, and in some situations even impossible to detect.

It is worth noting that information and data in open sources, often made available on a mass scale, remain in cyberspace forever and cannot be permanently deleted. This also applies to data about ourselves posted on various social networking sites, offices that make

[16] Grzelak M., *Szpiegostwo i inwigilacja w Internecie*, w: *Sieciocentryczne bezpieczeństwo. Wojna, pokój i terroryzm w epoce informacji* (Eng. Espionage and surveillance on the Internet, in: Network-centric security. War, peace and terrorism in the information age), K. Liedel, P. Piasecka, T. Aleksandrowicz (ed.), Warszawa 2014, pp. 164–181.

public data available, or any other organisations. This set of data is later publicly accessible, easy to obtain without leaving virtually any traces. This means that it can take criminals literally no time at all to obtain the information they need to carry out attacks. In a way, people have already got used to posting information on the Internet without thinking about the impact on their private security. In addition, social networks, but also websites, have accustomed web users to express their reactions and emotions under posts or articles. However, not many people check whether the post they have liked has not been transformed into a post with negative or criminal content and whether it is not being used to commit criminal acts. Charity campaigns, for example, are used to convince the user that for every "like" a certain amount of money is donated for the treatment of a particular person. In this way, massive fraud takes place and the money gained is used for completely different purposes.

Another threat to information is the flow of information generated by particular social networks or open source information retrieval tools. The available documentation of some portals indicates that the requests sent are not directed to the target data sources, but to intermediary servers. Very often these servers are located in the United States, which, for legislative reasons, may have a negative impact on the information security attribute of confidentiality. Furthermore, sending requests to proxies raises the question of whether requests are inadvertently directed to undesirable locations. Due to the possible existence of proxies, the user has no assurance that the results returned are not modified or partially filtered. The transmission of information in text form also creates the risk of it being easily intercepted by hackers. This is especially dangerous if the leak concerns strategic information or information processed by entities responsible for ensuring national security[17].

Social networking sites have become one of the primary channels for exchanging information. We are often even assured of encrypted communication, otherwise known as secure communication. However, it should be noted that this is not the safest way to exchange information. It is not a secret that the administration of Internet, social networking sites reviews and uses them according to their needs. An example is Cambridge Analytica, which used the data of about 87 million Facebook users. This action consisted of transferring photos

[17] Documentation review conducted by analysts at Inseqr sp. z o.o.

and private conversations to a department that deals with personality analysis and strategies for influencing mass population behaviour.

Unfortunately, the disclosure of private messages even by the unknown administration of websites or social networks is not a positive prospect. An additional threat is the possibility of transmitting information, messages to various institutions, including governmental ones, or to foreign services.

It is worth being aware that in case of actions of cyber criminals or, what is worse, cyber terrorists, they may have access to the following data:

- telephone numbers
- bank account numbers;
- logins and passwords to computers, bank accounts, domains;
- private information;
- information on industrial and intellectual property rights;
- knowledge of planned projects.

In the least harmful case, the data obtained, originating from private conversations on communication platforms, information from social networks or various other websites, are used to prepare and then present the most varied products in the form of advertisements appearing on the websites viewed. These actions are obviously aimed at stimulating the user's interest and, consequently, persuading him to make a purchase. Artificial intelligence mechanisms now allow various Internet assistants to eavesdrop on our conversations in order, for example, to tailor advertisements for products that may be of interest to us. It is therefore worth paying attention to the confidentiality of our conversations and considering securing smartphones during important meetings. An example of a product that can ensure the confidentiality of our conversations are the so-called 'hummers' already available on the market. These are acoustic boxes that act as a safe depository for devices that can capture or transmit sound. Such solutions very often prevent eavesdropping by means of electronic devices equipped with a voice recorder function. In addition, they also prevent eavesdropping that may be carried out by assistants embedded in mobile systems.

A serious interdisciplinary threat to open-source information is the spread of disinformation, primarily because of the extent of its impact. When the terms 'disinformation', 'fake news' appear, people

usually think of social media posts with rather fantastic, improbable stories. However, fake news is much more than exaggerated social media article titles. Disinformation may seem like a new phenomenon, but the only novelty is the platform used and the environment in which it is spread. In fact, it has been around for centuries and the internet is just a newer means of communication that can be used to spread lies and disinformation.

The essence of disinformation is a way of communicating information - true or false - in such a way as to mislead an opponent or competitor and induce them to behave as we expect and in our favour. Disinformation is not a simple lie, i.e. the communication of false information, but a real deception. Typically, a disinformation campaign involves the transmission of multiple pieces of information, most of which are true, while only one - the key piece of information to produce the intended effect - is false. It is also sometimes the case that a disinformation campaign is conducted on the basis of information that is true but presented in such a way that a competitor believes it to be false. In addition, several independent sources and channels of information are used to increase the effectiveness of disinformation. Although, as mentioned above, disinformation is not a new phenomenon, its importance has undoubtedly increased with the emergence of mass media. As Tomasz Aleksandrowicz rightly pointed out, there has been a weaponisation of information, which has contributed to the creation of weapons of mass manipulation[18]. A perfect example of the use of this weapon was the leak of confidential information via the WikiLeaks website. This case shows perfectly well that keeping data secure on the Internet is a real challenge.

Similarly to the fire triangle, which assumes that three factors - oxygen, fuel and energy - are required for a building fire to spread, disinformation also requires three different elements to succeed. Together they form the fake news triangle, and the absence of at least one of them will result in fake news not being able to spread and reach its intended audience.

[18] Aleksandrowicz T. R., *Zagrożenia dla bezpieczeństwa informacyjnego państwa w ujęciu systemowym. Budowanie zdolności defensywnych i ofensywnych w infosferze* (Eng. Threats to the state's information security from a systemic perspective. Building defensive and offensive capabilities in the infosphere), Warszawa, 2021, pp. 32 – 49.

Fig. 7. Fake news triangle.

Source: https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/fake-news-cyber-propaganda-the-abuse-of-social-media [accessed: 26 November 2021].

The first element is the tools and services for manipulating and spreading news in the relevant social networks. There is a wide range of tools and services available in the world, some of them are relatively simple (paid likes/observers etc.), others are more complicated - some services promise to provide online surveys, others force site owners to delete stories.

Of course, for these tools to be useful, social networks must exist as a platform for spreading propaganda. Since people spend a lot of time in them to get the latest news and information, their importance in spreading fake news cannot be underestimated. However, there is a difference between simply publishing propaganda and turning it into something that the target audience consumes. The study of social media also gives an idea of the relationship between bots and recipients of social media promotions, such as Twitter, and thus gives an idea of the scope and organisation of campaigns attempting to manipulate public opinion.

Finally, a propaganda campaign always brings with it the question: why? The motives of those spreading fake news vary: sometimes it is simply to gain money through advertising, but it can also be for criminal or political purposes. Whatever the motive, the success of any propaganda campaign is ultimately measured by how much it affects the real world.

In summary, disinformation can be said to exist when the information disseminated:

- is totally or partially false, manipulated or misleading;
- concerns a matter of public interest;
- is intended to create uncertainty or hostility, polarisation or disruption of democratic processes;
- is disseminated or amplified through automated and aggressive techniques such as social bots, artificial intelligence (AI), microtargeting or trolling.

Disinformation can destabilise a country, exert a destructive influence on its administrative and decision-making structures, and undermine its social, economic and cultural foundations. According to the report Freedom on the Net 2017: Manipulating Social Media to Undermine Democracy[19], more and more countries around the world are using social media for disinformation activities - both to shape their internal policies and to influence other countries. Countering disinformation is becoming a challenge facing not only individual states, but also international institutions and organisations. The need to counter disinformation campaigns in Europe was first highlighted by the European Council in March 2015. Since then, several teams have been established within the structures of the European External Action Service to analyse disinformation in the European Union and neighbouring countries.

The problem of disinformation - on the state-wide and strategic level - was raised in the National Security Bureau (BBN) during work on recommendations to the new National Security Strategy. It was also discussed on the international forum and during numerous expert meetings organised at the BBN. From the discussions held, the biggest challenges in the information environment at present are:

- lack of understanding of the importance and nature of the problem;
- lack of an efficient system of strategic communication and coordination of activities in combating disinformation at the national level;
- low levels of media literacy among selected social groups;

[19] https://freedomhouse.org/article/new-report-freedom-net-2017-manipulating-social-media-undermine-democracy [accessed: 28 XI 2021].

- striking a balance between freedom of expression and countering disinformation;
- building a positive narrative and promoting the state externally.

All these challenges are universal and to a large extent also concern Poland as a country belonging to the community of Western civilisation, which shares democratic values. Internationally, disinformation most often targets democratic procedures and seeks to undermine citizens' trust in the state. Such action also threatens national security. Disinformation activities mislead citizens and often create uncertainty in them. Among other things, this prevents them from making sovereign electoral decisions based on reliable information.

Countering disinformation requires first and foremost:

- raising citizens' awareness of disinformation threats;
- building institutional capacity;
- undertaking cooperation between various institutions and strategic communication units in EU and NATO countries and institutions;
- designing and implementing active measures, i.e. conducting projects and information campaigns;
- supporting Polish NGOs and undertaking cooperation with them.

To identify disinformation, one should:

1. Get to know the source of information (understand its goals and intentions), find out who is responsible for this source, who owns it, etc.
2. Read the whole article, not just the headline (to understand the whole material).
3. Check the authors to verify that they are credible. This is not always possible because not all articles are signed by name and not all authors - even in credible content - are signed. If it is possible, it is a good idea to search for the name of the author or authors and see other content that this person creates.
4. Check this information with other sources (make sure they give the same information).
5. Find the date of publication (to check that the information is up to date).
6. Think about your own biases (to see if they affect your judgement).

7. Ask experts (to get confirmation from independent people with knowledge of the subject).

Faced with the huge amount of information that is processed in open sources on a daily basis, there is a problem in distinguishing truth from falsehood. Very often we are dealing with the creation of certain visions, especially by the media, instead of presenting reliable information. In addition, the dynamic pace of life means that the information life cycle is very short. The information which appeared today and moved the public opinion will be replaced the next day by another, equally important one. Additionally, the overabundance of various information makes decision-making processes extremely complicated, and people are guided not by the real state of affairs, but rather by the social perception of given facts. In addition, information is manipulated to achieve certain benefits. The spread of disinformation by Russia during the 2016 US presidential election can serve as an example. This state of affairs is a huge problem in modern societies. Currently, it is very difficult to control the circulation of public information, there are many manipulative tools that greatly undermine the credibility of the information presented. Additionally, the situation in which information attacks become recognisable only at the moment when the attacker reaches his goal or are not recognised at all is very worrying. The words of Sławomir Zalewski, who said: "(...) the statement of the absence of threats does not eliminate them in the future, but also does not exclude the possibility that actions constituting a threat are undertaken here and now, only that they have not yet been recognised"[20].

Considering the numerous threats to information in cyberspace, it should be noted that the largest countries in the world have introduced special legal regulations to protect ICT resources and counter threats in this area. Among others, Russia in the Law on the Protection of Personal Data and its subsequent supplements introduced the order to store personal data of Russians only on the territory of their country[21]. The United States has enacted the CLOUD Act[22], which compels US providers of electronic services to disclose, upon request

[20] Zalewski S., *Bezpieczeństwo polityczne. Zarys problematyki* (Eng. Political security. Outline of issues), Siedlce 2013.

[21] https://gdpr.pl/panstwa-spoza-ue-a-rodo-czesc-i-rosja [accessed: 28 XI 2021].

[22] https://epic.org/wp-content/uploads/privacy/cloud-act/cloud-act-text.pdf [accessed: 28 XI 2021].

by a US court, information on users of those services, regardless of whether it is processed in the States or in any other country in the world. It is also worth noting the Cyber Security Law introduced in China and the law setting the National Information Security Standard. These documents sanction the principle that all hardware and software supplied to government entities or critical infrastructure entities must be audited by designated and prepared entities. The source code of any software purchased for the needs of the above entities must also be checked.

In 2014, the process of effectively establishing a cyber security system began in Ukraine. The most important impetus for such measures was the cyber attacks on the electricity grid, which led to temporary disruptions in electricity supply. In 2016, the Cyber Security Strategy of Ukraine was approved, which stressed the need for legislative work on the national cyber security system[23]. It was recognised that the above activities are the basis of national security. In addition, it focused on the interaction between actions taken by state bodies, local authorities, military formations, scientific institutions, as well as commercial entities. However, despite the introduction of legislative documents, there are huge problems with the development of cyber security strategies in Ukraine. These are due to, among other things, the lack of effective implementation of cyber security policy, lack of awareness of cyber threats and insufficient human potential. Problems are also created by: lack of legal and organisational framework for the protection of critical infrastructure, lack of up-to-date cyber security standards and weak national legislation on cybercrime[24].

Noteworthy is the action taken in Estonia, which can be a model for other countries. Estonia should be regarded as a pioneer of digitalisation in Europe, as evidenced by the introduction of a cyber security strategy back in 2008[25]. This was the first document of its kind in the world.

[23] Semeniy J., Glushchenko S., Makarevich O., *Ukraine*, [w:] *Cybersecurity* 2018, B.A. Powell, J.C. Chipman (ed.), Law Business Research, London, p. 99.

[24] Boiko V., *Comparison of the Polish and Ukrainian cybersecurity system*, „Teka of Political Science and International Relations" 2019, t. 14, no. 2, pp. 119–137.

[25] Narodowa Strategia Cyberprzestrzeni Estonii (Eng. Estonia's National Cyberspace Strategy), https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map?selected=Estonia, [accessed: 28 XI 2021].

Estonia is constantly working to increase the level of cyber security. This is primarily due to highly developed e-services, and preventive measures are aimed at countering online crime. Estonia is in favour of a single digital market within the European Union, which is expected to translate into tangible benefits in terms of the development of the e-economy. In addition, it is pushing the Member States to take joint action for digitalisation and security in cyberspace. The protection of personal data in mobile networks and on websites, the free movement of non-personal data and the taxation of Internet services are among the areas of interest. Estonia's cybersecurity policy primarily seeks to clean up existing regulations and adapt them to dynamically changing circumstances. It also continues to improve the technology supporting the response to cyber incidents by, among other things, improving the network infrastructure, coordinating the administration of IT systems and strengthening the IT department in the administration[26].

A tangible action within the European Union in the field of cyber security was the adoption of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation)[27], the so-called GDPR, which is binding on all processors of personal data in connection with their business activities. By means of the aforementioned regulation, many changes and increased obligations for data controllers and processors have been introduced.

As cyber security is currently one of the biggest challenges facing ICT network administrators and users, the EU's response to it is also Directive 2016/1148 of the European Parliament and of the Council of 6 July 2016 on measures for a high common level of security of IT networks

[26] Raś K., *Estonia jako lider w zwiększeniu cyberbezpieczeństwa* (Eng. Estonia as a leader in increasing cyber security), „Biuletyn – Polski Instytut Spraw Międzynarodowych" 2018, no. 68, pp. 20 – 22.

[27] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation). Official Journal of the EU L of 2016, No. 119/1 of 27 April 2016.

and systems within the Union[28]. In Poland, this Directive was implemented by the Act of 5 July 2018 on the National Cyber Security System. The Act imposed new obligations on entities that have an impact on state security. Among other things, internal audits of ICT systems, the development of relevant documentation, the implementation of security management systems, as well as carrying out activities to detect, record, analyse and classify incidents became a requirement. Poland also enacted the Act of 10 June 2016 on anti-terrorist activities[29]. By virtue of this document, the tasks of the Internal Security Agency (ABW) include, among others: the identification and detection of threats to the security of the ICT systems of public administration bodies or the system of ICT networks included in the uniform list of objects, installations, devices and services constituting critical infrastructure, as well as the ICT systems of the owners and holders of objects, installations or devices of critical infrastructure, which are important for the continuity of the state's functioning, and the prevention of such threats. The Head of ABW is responsible for keeping a central register of terrorist incidents which breach the security of ICT systems of particular importance to the state security or ICT networks. Moreover, in order to prevent and counter terrorist incidents in cyberspace, the Internal Security Agency may assess the security of ICT systems by conducting security tests in order to identify vulnerabilities. A vulnerability is understood as a weakness of a resource or security of an ICT system, which can be exploited and threaten the integrity, confidentiality, accountability and availability of that system.

The presented examples show how important it is to protect information resources in the international arena and which security measures will allow to counteract any threats related to the flow of information.

It is also worth noting that the actions of cyber criminals have a major impact on critical infrastructure facilities. Their aim is primarily to undermine public confidence in civil society and the foundations of democracy. It is also a threat to sovereignty, which gives terrorist organisations and criminals the opportunity to operate anonymously using techniques and effective methods to influence the policies

[28] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 on measures for a high common level of security of networks and information systems within the Union. OJ. EU. L. 2016.194.1 of 6 July 2016.

[29] Act of 10 June 2016 on anti-terrorist activities. Journal of Laws of 2021, item 2234.

and strategies of other states. An example is the actions of Russia, which is one of the most active perpetrators of cyber attacks, during the illegal annexation of Crimea in 2014. Another example is China, which has actively engaged in carrying out cyber attacks and disinformation campaigns against members of the NATO alliance and poses a very serious threat to critical energy infrastructure, as highlighted in the NATO 2030 expert report[30].

The cyber attacks carried out in the last 15 years prove that they affect both those who carry them out - the cyber criminals - and the environments that try to defend the network. Today, the cybersecurity defence environment requires many tools and solutions, which are usually very expensive. Attacks conducted on a smaller scale are just a bridgehead to larger attacks and, going forward, to the development of cyber defences. The development of cyber attacks has led cybersecurity professionals to consider them as an everyday phenomenon and to focus their efforts on network defence. The methods of ensuring cyber security, as well as the way to respond to attacks, must evolve in line with the development of intrusions. As the commercial sector is mostly responsible for the Internet environment, state organisations and private entities should consider cooperation in network security. However, this requires broad legislative changes in terms of proactive and reactive measures against cyber threats.

It seems reasonable to develop an operational doctrine implemented by national cyber forces, which should be developed, tested and modified depending on threats. The organisation of bilateral exercises seems to be a good introduction to further cooperation. Subsequently, representatives of the commercial community responsible for protective measures should also take part in the exercises. Representatives of individual countries should not be afraid of cyber experts from the private environment, as they have already taken the initiative and are conducting pre-emptive actions. Moreover, the global nature of the Internet requires international cooperation. Individual state solutions to cyber threats will not be effective, as combating these threats requires a coherent and flexible approach. NATO as an international organisation has years of experience

[30] https://nato.int [accessed: 29 XI 2021].

in developing policies and operations against conventional threats. However, the time has now come to apply the experience and expertise gained to ensure and maintain cyber security[31].

In conclusion, it should be stated that the assumed hypothesis has been verified. Well, in the last few decades there has been a huge technological progress related to the development of modern technologies, and above all the emergence of an advanced information society. Currently, no one can imagine life without access to the Internet, and thus to information from open sources. Their universality, accessibility and low cost make them the first source of information to be used. However, along with their development, new threats have emerged, often of a cyberterrorist nature, which pose a great danger to people as individuals, all organisations and state structures. Information security is an area that requires radical and immediate action, as cybercriminals are able to secretly access any system to achieve their planned goal. The situation is not helped by a dynamically changing environment, the coronavirus pandemic and the transfer of life to the world of the Internet, as well as by conflicts between states aimed at gaining an advantage in the international arena. Implemented legal regulations appear to be insufficient in protecting information. It is necessary to create a synergy effect by combining international actions, as well as actions at the level of individual states, in order to permanently ensure network security, both at national and international level. It is important to be aware that cyber-terrorist attacks will occur and even increase. They can range in scale from the manipulation of information and the spreading of disinformation to attacks on critical infrastructure ICT systems. Although the complete eradication of cyber terrorism is not feasible, preventive measures should be taken, as well as measures aimed at detecting attacks of a cyber terrorist nature as soon as possible and minimising the losses caused by them.

[31] W.E. Leigher, *Cyber conflict in a hybrid threat environment: Death by a thousand cuts*, Helsinki 2021.

Bibliography

Aleksandrowicz T. R., *Zagrożenia dla bezpieczeństwa informacyjnego państwa w ujęciu systemowym. Budowanie zdolności defensywnych i ofensywnych w infosferze* (Eng. Threats to the state's information security from a systemic perspective. Building defensive and offensive capabilities in the infosphere), Warszawa, 2021, pp. 32 – 49.

Boiko V., *Comparison of the polish and Ukrainian cybersecurity system*, „Teka of Political Science and International Relations" 2019, vol. 14, no. 2, pp. 119–137.

Elliott A., Castells M., *Społeczeństwo sieci,* w: Elliott A., *Współczesna teoria społeczna. Wprowadzenie* (Eng. Network society, in: Contemporary social theory. Introduction), Warszawa 2011.

Grzelak M., *Szpiegostwo i inwigilacja w Internecie,* w: *Sieciocentryczne bezpieczeństwo. Wojna, pokój i terroryzm w epoce informacji* (Eng. Espionage and surveillance on the Internet, in: Network-centric security. War, peace and terrorism in the information age), K. Liedel, P. Piasecka, T. Aleksandrowicz (ed.), Warszawa 2014, pp. 164–181.

Hall R., Fox C., *Ponownie przemyśleć bezpieczeństwo* (Eng. Rethinking security), „Przegląd NATO" zima 2001/2002, p. 8.

Kissinger H., *Dyplomacja* (Eng. Diplomacy), Warszawa 2016.

Leigher W.E., *Cyber conflict in a hybrid threat environment: Death by a thousand cuts,* Helsinki 2021.

Measuring the Information Society Report, vol. 1, 2018.

Nowak J.S., *Społeczeństwo informacyjne – geneza i definicje,* w: *Społeczeństwo informacyjne. Krok naprzód, dwa kroki wstecz* (Eng. Information society - origins and definitions, in: Information Society. One step forward, two steps back), P. Sienkiewicz, J.S. Nowak (ed.), Katowice 2008, p. 25.

Oleński J., *Ekonomika informacji* (Eng. Economics of information), Warszawa 2001.

Raś K., *Estonia jako lider w zwiększeniu cyberbezpieczeństwa* (Eng. Estonia as a leader in increasing cyber security), „Biuletyn – Polski Instytut Spraw Międzynarodowych" 2018, nr 68, pp. 20 – 22.

Saramak B., *Wykorzystanie otwartych źródeł informacji w działalności wywiadowczej: historia, praktyka, perspektywy* (Eng. The use of open sources of information in intelligence activities: history, practice, perspectives), Warszawa 2015.

Sienkiewicz P., *Społeczeństwo informacyjne jako system cybernetyczny*, w: *Społeczeństwo informacyjne. Wizja czy rzeczywistość?* (Eng. Information society as a cybernetic system, in: Information Society. Vision or Reality?), vol. 1, L.H. Haber (ed.), Kraków 2004, p. 79.

Semeniy J., Glushchenko S., Makarevich O., *Ukraine*, [w:] *Cybersecurity* 2018, B.A. Powell, J.C. Chipman (ed.), Law Business Research, London, p. 99.

Sosińska-Kalata B., *Obszary badań współczesnej informatologii (nauki o informacji)* (Eng. Research areas of contemporary informatology (information science)), „Zagadnienia Informacji Naukowej" 2013, no. 2, pp. 9–41.

Sun Tzu, *Sztuka wojny* (Eng. Art Of War), Gliwice 2004.

West Ch., *Competitive intelligence*, New York 2001.

Zalewski S., *Bezpieczeństwo polityczne. Zarys problematyki* (Eng. Political security. Outline of issues), Siedlce 2013.

Internet sources

https://datareportal.com/reports/digital-2021-global-overview-report [accessed: 26 XI 2021].

https://epic.org/wp-content/uploads/privacy/cloud-act/cloud-act-text.pdf [accessed: 28 XI 2021].

https://freedomhouse.org/article/new-report-freedom-net-2017-manipulating-social-media-undermine-democracy [accessed: 28 XI 2021].

https://gdpr.pl/panstwa-spoza-ue-a-rodo-czesc-i-rosja [accessed: 28 XI 2021].

https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map?selected=Estonia, [accessed: 28 XI 2021].

https://nato.int [accessed: 29 XI 2021].

http://unicjin.org/documents/congr10/10e.pdf [accessed: 27 XI 2021].

http://www.bbc.uw.edu.pl/Content/20/08.pdf [accessed: 25 XI 2021].

Legal acts

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation). Official Journal of the EU L of 2016, No. 119/1 of 27 April 2016.

Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 on measures for a high common level of security of networks and information systems within the Union. OJ. EU. L. 2016.194.1 of 6 July 2016.

Act of 10 June 2016 on anti-terrorist activities. Journal of Laws of 2021, item 2234.