Information Protection in Cyberspace a Factor in National Security

KRZYSZTOF BOJARSKI

Abstract National security is a very broad issue and includes a number of factors that may affect the security situation. In addition to the traditionally considered, especially of a military nature, nowadays attention is also drawn to other elements, among which those related to national security in cyberspace are of particular importance, and in this respect, especially the security of information, in particular, of classified information. Ensuring national security in this regard is currently becoming a key challenge for the state's functioning and development. Therefore, mechanisms, procedures and structures are being put in place to safeguard this security at different levels of state function.

Keywords: • national security • cyberspace • cybersecurity • classified information

CORRESPONDENCE ADDRESS: Krzysztof Bojarski, Ph.D., Faculty of Security, Marshall Józef Piłsudski Higher School of Safety and Security in Warsaw, Zakroczymska Street 13, 00-225 Warsaw, Poland, e-mail: k.bojarski@wsbio.waw.pl, ORCID: 0000-0002-0729-5759.

https://doi.org/10.4335/2022.1.5 ISBN 978-961-7124-10-1 (PDF)
Available online at http://www.lex-localis.press.

1 Introduction

Security, in its broad sense, is nowadays a ubiquitous notion, considered in various scopes and in relation to various values. One of the key issues of security is national security. This is because in any country, its national security affects the security of every citizen of that state, their lives and development. Hence it must be taken seriously. Indeed, Article 5 of the Constitution of the Republic of Poland of 2 April 1997 (consolidated text, Polish Journal of Laws 1997, No. 78, item 483, as amended) states that "the Republic of Poland shall safeguard the independence and integrity of its territory and ensure the freedoms and rights of persons and citizens, the security of the citizens (...)."

Thus, in one of the first articles of the Constitution, the legislators emphasise issues relating to territorial independence and integrity, and the security of citizens. Independence means, of course, the separate state existence of the Republic, as well as the existence of the Polish state within its present boundaries, while sovereignty is understood as the ability of the state to decide and act independently about all matters concerning it. However, national security is not only about independence and the associated aspect of defending that independence alone, as the concept of national security has evolved considerably over the years. It is true that the traditional approach pays particular attention to the military aspect, and to the absence of threats in this respect. Therefore, in this sense, the fundamental values to be protected include territorial integrity, political independence or even the survival of the state or nation. Of course, these are extremely important aspects of national security, but they are not of sole significance. Today, many other factors are also indicated which influence this security, and at the same time often pose a serious threat to it. These factors include, for example, the destabilisation of the state system, poorly functioning economic and social mechanisms, social conflicts, natural disasters, illegal migration, organised crime, terrorism, and, in recent times in particular, special attention should be paid to threats to the state occurring in cyberspace and the related information domain. Thus, national security is shaped by a number of often interrelated factors that can lead, when significantly intensified, to the destabilisation of the state and, consequently, to the collapse of the state understood as the inability of the central government to perform its basic functions over the entire territory of the state (Bojarski, 2017: 26-27).

2 Cyberspace and cybersecurity – definitional attempt

The starting point for further consideration of the subject in question is cyberspace and its definition, which is provided in Article 2(1b) of the Act of 29 August 2002 on Martial Law and the Competences of the Commander-in-Chief of the Army and the Rules of the Commander-in-Chief's Subordination to the Constitutional Authorities of the Republic of Poland (consolidated text, Polish Journal of Laws of 2017, item 1932) in the wording which determines that cyberspace is understood as space for the processing and exchanging of information created by ICT systems, as defined in Article 3(3) of the Act of 17 February 2005 on the Computerisation of the Operations of Entities Performing

Public Tasks (consolidated text, Polish Journal of Laws of 2021, item 670), including the links between them and relations with the users. Thus, cyberspace is the information space where the processing and distributing of information and messages is carried out. It consists of both ICT networks and systems, and the relationships between them and users (Kowalewski, 2014: 24). Cyberspace can be at the same time identified as an area – an electronic domain – used for the distribution of information, which has an interstate form and consists of the sum of activities carried out by the user (Wasilewski, 2013: 231). Analysing the term itself in even more detail, it should be noted that the prefix "cyber" refers to the use of new information and communication technologies, as well as to the development of e.g. economy, culture or knowledge based on these technologies in a broad sense. The basic element of the term indicates a space that is constantly expanding and evolving as a result of continuous changes based on the ingenuity and participation of users themselves. Therefore, cyberspace obviously requires hardware, software and information systems, but it is also co-created by human behaviour captured through digital networks. All these interactions are a rich set reflecting the positive as well as the negative sides of human nature, ranging from cyberautocreation to criminal activities, also leading to terrorist acts and possible cyber conflicts. It can therefore be concluded that the main characteristics of cyberspace are the absence of borders, dynamic processes and phenomena and the anonymity of users. This situation makes public institutions with their domain in cyberspace vulnerable to intrusion, whether by individuals, organised groups or hostile states (Górka, 2018: 33-34).

This therefore raises the question of cybersecurity – what it is and how it is understood. The definition of cybersecurity is contained in the Act on the National Cybersecurity System of 5 July 2018 (consolidated text, Polish Journal of Laws of 2020, item 1369) – the Act is hereinafter referred to as the NCSA – according to which cybersecurity is the resilience of information systems against actions which compromise the confidentiality, integrity, availability and authenticity of processed data, or the related services provided by those information systems (Article 2(4) of the NCSA). This definition is linked to the definition of the concept of an incident and its various types, which are also defined in the NCSA (Article 2(5-9) and according to which: incident – means an event which has, or may have, an adverse impact on cybersecurity; critical incident – means an incident resulting in significant damage to public security or order, international interests, economic interests, operation of public institutions, civil rights and freedoms or human life and health, classified by the competent CSIRT MON (Computer Security Incident Response Team operating on a national level, managed by the Minister of National Defence), CSIRT NASK (Computer Security Incident Response Team operating on a national level, managed by the Research and Academic Computer Network – National Research Institute) or CSIRT GOV (Computer Security Incident Response Team operating on a national level, managed by the Head of the Internal Security Agency); serious incident – is defined as an incident which causes, or may cause, a serious reduction in the quality, or an interruption of the continuity, of a critical service; significant incident – means an incident which has a significant impact on the provision of a digital service within the meaning of Article 4 of Commission Implementing Regulation (EU) 2018/151 of 30 January 2018 laying down rules for application of Directive (EU) 2016/1148 of the European Parliament and of the Council as regards further specification of the elements to be taken into account by digital service providers for managing the risks posed to the security of network and information systems and of the parameters for determining whether an incident has a substantial impact (OJ EU L 26, p. 48); incident in a public entity – is an incident which causes, or may cause, a reduction in the quality of, or an interruption to, the performance of a public task carried out by a public entity, as referred to in Article 4(7) to (15) of the NCSA.

Cybersecurity is also addressed by the Cybersecurity Strategy for 2019-2024 (Official Gazette of 2019, item 1037), hereinafter referred to as the Cybersecurity Strategy. First of all, it is worth mentioning a few words about the document itself – namely, that it replaced the National Framework of Cybersecurity Policy of the Republic of Poland for 2017-2022, and was introduced by a resolution of the Council of Ministers. Moreover, it directly affects government administration bodies, and indirectly, after the adoption of generally applicable laws on the initiative of the Council of Ministers, other public authority bodies, as well as entrepreneurs and citizens. The main motive of this document is to define strategic objectives and appropriate political and regulatory measures aimed at achieving a high level of cybersecurity, i.e. primarily to ensure the resilience of the information systems of operators of essential services, critical infrastructure operators, digital service providers and public administration to cyberthreats, as well as to increase the level of information protection in information systems through standardisation of security features. As a result, the implementation of the strategic objectives is expected to influence the improvement of national security, increase the effectiveness of law enforcement agencies and judicial authorities in detecting and combating cybercrimes, as well as hybrid (including terrorist activities) and espionage activities in cyberspace. Therefore, we can conclude that the main objective of this strategy is to increase the level of resilience to cyberthreats and to enhance the level of information protection in the public, military and private sectors, as well as to promote knowledge and good practices to enable citizens to better protect their information (Cybersecurity Strategy: 8-10).

It must be stressed that cyberspace has been shaped primarily by the process of integration of basic forms of information transmission and interpretation (Marczyk, 2018: 60), which emphasizes the importance of user behaviour from a cybersecurity perspective. Therefore, it seems that activities related to the promotion of knowledge and education in the field of cybersecurity are a prerequisite for the success of information protection in cyberspace, because it is well-known that humans are the weakest link here. For this reason, according to this strategy, education about cybersecurity should be available at the earliest possible stage of access to digital services – preferably before entering the digital world. In practice it is often required at the stage of early childhood education. In this respect, it is advisable that, in cooperation with non-governmental organisations, the private sector and academic centres, the public administration carry out systemic actions to sensitise society to the risks of cyberspace, as well as educational actions in the field of rights and freedoms in the digital environment and the rights of persons who are victims of cyberattacks and suffer damage as a result of violations of network security.

In the context of the growing number of threats aimed at exerting a specific influence on society, as well as bearing in mind the consequences of the deliberate use of social engineering tools for manipulative activities in the form of, among others, disinformation campaigns or inspiration or disintegration activities, it is necessary to implement systemic actions enabling the development of citizens' awareness in the context of verifying the authenticity of information and responding to attempts to disrupt it (Cybersecurity Strategy, 2019: 26). Indeed, it is not without a reason that the 21st century is called the century of the information society, which emphasises the important role of information and communication systems existing within a given society and determining its specific features as compared to other types of societies. Such a society consists not only of information and ICT means, but also of humans and their needs, the economy, the state and the environment. It is the development of ICT means in processing and collecting information, as well as communication means in sending and receiving information that is responsible for the establishment of the information society (Krztoń, 2015: 101-102) and the related key role of information and its protection.

3 Information and information security

Information is a term which is ambiguous and difficult to define. Although many different definitions can be found in the literature on the subject, it can be assumed, according to the Polish language dictionary, that information is, among other notions, what has been said or written about someone or something, also the communication of something, as well as data processed by a computer (https://sjp.pwn.pl/sjp/informacja;2466189.html). Information is a key factor influencing decision-making in all areas of life. The basis of information is data, which must be understandable and, moreover, should contain an element of novelty for the recipient. However, when defining information in the context of an information system, it is emphasised that information is what changes and supports understanding, while data is the input of the communication channel, as data is tangible and consists of numbers, words, phone calls, etc. Data becomes information when people use it to better understand specific issues. As a result, information systems should provide information rather than data. Information in any organisation, including the state, is the basis for building the knowledge of all people involved in the process of acquiring and using it. By shaping the awareness of the phenomena occurring in the organisation itself and in its environment, information makes it possible to adapt to the changing reality, as well as to transform it to facilitate the more efficient functioning, for example, of the state as the most universal organisation. Furthermore, it is due to information that it is possible to become aware of existing problems and then to begin the search for solutions (Grabowski, Zając, 2009: 104).

Nowadays, information in the virtual world is of particular importance. This is because it is the most important element of cyberspace, being generated from data which, when processed, commented and disseminated, creates a new dimension of reality.

Today more than ever, a new facet of information is revealed – namely, in the modern world information it is treated as a commodity, which, like any other good, can be bought and sold. As a result, the growing importance and significance of information in both the economic and national security fields is gradually but continuously increasing its price. It is already a truism today to say that those who have information have power. Therefore, it is not surprising that adequate cybersecurity has become a priority for many governments in recent years (Cyfrowa Polska, 2019: 3), since thanks to the global Internet, all who are interested have access to almost the entire world. In addition to the obvious benefits, however, this also has its dark side, because it entails a new threat to national security, which takes the form of uncontrolled leakage of information of not only economic, political, but even strategic importance.

Such a threat requires effective action to eliminate or minimise it. Therefore, there is a need for constant monitoring of the situation, and thus for the establishment of services, institutions or organisations which, on the basis of appropriate legal regulations, will ensure the security of the state in this field of its functioning. Similarly to other countries, Poland is also susceptible to the threat of information leakage, which may be the result of improper management of information resources or deliberate action by intelligence and special services of other countries, or even terrorist organisations hostile to Poland and its domestic and foreign policy. Particularly important and sought-after is not only military and national defence data, but also data relating to business activity, technology and scientific research, and in fact any information that may contribute to the competitive advantage of another country or organisation. Therefore, in response to a new threat, in order to ensure the security of information that is particularly important to the state, all countries establish properly prepared and trained services whose task is to constantly monitor information security and eliminate or limit its leakage. In the functioning of the state, the efficiency of governing bodies is of utmost importance, which is mainly related to the speed and accuracy of decisions, and this in turn depends on the availability of a large amount of reliable and detailed information in a given area, so security management must be organised in such a way that information is easily accessible to authorised persons and at the same time protected from unauthorised use by outsiders who may act to the detriment of the state (Machura, 2013: 156-157). This, of course, also, and perhaps above all, requires appropriate legal regulations.

The principal legal act relating to this issue is the Act of 5 August 2010 on the Protection of Classified Information (Polish Journal of Laws of 2019, item 742) – the Act is hereinafter referred to as the APCI. The provisions set out in this Act govern the standards for the protection of classified information, the classification of classified information, the preparation of its protection, as well as the standards for the use of physical, personnel and ICT security measures (Wojciechowska-Filipek, Ciekanowski, 2019: 195).

According to this legal act, classified information is considered to be information, the unauthorised disclosure of which would or could cause damage to the Republic of Poland, or would be detrimental from the point of view of its interests, also in the course of its preparation and regardless of the form and manner of its expression (Article 1(1) of the APCI). Classified information may be made available only to a person providing a guarantee of confidentiality and only to the extent necessary for the performance of their work or service at the position held or for the performance of commissioned activities (Article 4(1) of the APCI).

Proper management of access to classified information requires its appropriate classification, and in accordance with the APCI, it may be assigned one of four secrecy clauses, the common denominator of which is the fact that its disclosure may have negative consequences for national security. Therefore, according to Article 5(1) of the APCI, classified information shall be marked as “top secret” if its unauthorised disclosure causes exceptionally serious damage to the Republic of Poland by: 1) threatening the independence, sovereignty or territorial integrity of the Republic of Poland; 2) posing a threat to the internal security or constitutional order of the Republic of Poland; 3) posing a threat to the alliances or the international position of the Republic of Poland; 4) weakening the defence readiness of the Republic of Poland; 5) that fact that it will or may lead to the identification of officers, soldiers or employees of the services responsible for the performance of intelligence or counterintelligence tasks, and who perform operational and exploratory activities, if this endangers the security of the activities performed or may lead to the identification of persons assisting them in this respect; 6) the fact that it will or may endanger the life or health of officers, soldiers or employees who perform operational and exploratory activities, or persons assisting them in this respect; 7) the fact that it will or may endanger the life or health of crown witnesses or persons closest to them, persons who have been granted protection and assistance measures provided for in the Act of 28 November 2014 on the protection and assistance for the victim and the witness (Polish Journal of Laws of 2015, item 21), or witnesses referred to in Article 184 of the Act of 6 June 1997 of the Code of Criminal Proceedings, (consolidated text, Polish Journal of Laws of 2021, item 534), or persons closest to them.

In turn, classified information is classified as “secret” if its unauthorised disclosure causes serious damage to the Republic of Poland by: 1) making it impossible to perform tasks related to the protection of the sovereignty or constitutional order of the Republic of Poland; 2) deteriorating the relations of the Republic of Poland with other states or international organisations; 3) disrupting the defence preparations of the state or the functioning of the Armed Forces of the Republic of Poland; 4) hindering the performance of operational and exploratory activities carried out in order to ensure the security of the state or the pursuit of perpetrators of crimes by services or institutions authorised to do so; 5) significantly disrupting the functioning of law enforcement agencies and judicial authorities; 6) bringing about a considerable loss to the economic interests of the Republic of Poland.

Classified information may also be classified as “confidential” if its unauthorised disclosure causes damage to the Republic of Poland by: 1) hindering the current foreign policy of the Republic of Poland; 2) hindering the implementation of defence undertakings or adversely affecting the combat capability of the Armed Forces of the Republic of Poland; 3) disrupting public order or endangering the security of citizens; 4) hindering the performance of tasks by services or institutions responsible for protecting the security or fundamental interests of the Republic of Poland; 5) hindering the performance of tasks by services or institutions responsible for the protection of public order, security of citizens or prosecution of perpetrators of crimes and fiscal offences, as well as judicial authorities; 6) threatening the stability of the financial system of the Republic of Poland; 7) adversely affecting the functioning of the national economy.

Finally, classified information is classified as “proprietary” if it has not been assigned a higher security classification, and its unauthorised disclosure may have a harmful effect on the performance of tasks in the field of national defence, foreign policy, public security, observance of citizens’ rights and freedoms, judicial authorities or the economic interests of the Republic of Poland by public authorities or other organisational units.

Classified information assigned a specific security classification should be protected in accordance with the criteria specified in a given classification. The security classification of documents should be assigned by the person authorised to sign them. Classified information with a security classification may be disclosed only to an authorised person holding an appropriate security clearance, and who had undergone training on the protection of classified information. Information is made available only to the extent necessary for the performance of duties on a given position. The processing of classified information obligatorily takes place in conditions that prevent its unlawful disclosure, e.g. in classified registry offices or other places that can meet the requirements set out in the Act, as well as in secondary legislation, related to the physical protection and security of ICT systems (Wojciechowska-Filipek, Ciekanowski, 2019: 200). The issue of security of ICT systems, which is key from the point of view of information security in cyberspace, will be discussed further below.

At this point, however, it is worth presenting the conditions for marking materials with specific classifications, which are set out in the Regulation of the Prime Minister of 22 December 2011 on the manner of marking materials and affixing security classifications on them (Polish Journal of Laws of 2011, No. 288, item 1692) – the Regulation is hereinafter referred to as the RMMCL. Without going into too much detail, it is necessary to mention several basic principles related to marking materials with security classifications. First of all, in accordance with § 3 of the RMMCL, the material must be marked clearly and in full with the security classification. Where different parts of the material have been given different security classifications, or where some parts are unclassified, the separate parts must be marked with the relevant security classification indicated in full or with the word “unclassified”. The parts of the material containing text or images shall be separated by appropriate marking before and after the text or images.

If different parts of the material have been given different security classifications, the material shall be marked with a security classification at least equal to the highest security classification given to that part of the material.

Regarding the symbols used for the individual security classifications, in accordance with § 4 of the RMMCL, the following symbols for security classifications apply: 1) "00" – for "top secret" classification; 2) "0" – for "secret" classification; 3) "C" – for "confidential" classification; 4) "P" – for "proprietary" classification. From a cybersecurity point of view, the handling of electronic documents is particularly important, so, for example, according to § 6 (1) of the RMMCL, an electronic document must be marked in such a way that its specification contains the following information: 1) the security classification; 2) the letter and number reference; 3) the name of the unit or organisational unit; 4) the document registration date; 5) in the case of a document processed as correspondence, the indication of the addressees by stating their full names or the names of their positions; 6) the security classifications of any annexes, together with their registration numbers; 7) the position, full name or other indication of the person authorised to sign the document; 8) the full name or other indication of the person preparing the document; 9) the name given to the document or the indication of what the document relates to.

In addition, in relation to threats to the security of classified information in cyberspace, ICT security is extremely important. The basic requirements in this respect are set out in the Regulation of the Prime Minister of 20 July 2011 on basic requirements for ICT security (Polish Journal of Laws of 2011, No. 159, item 948) – the Regulation is hereinafter referred to as the RRIS. § 5 of the RRIS states that the security of classified information processed in an ICT system shall be ensured by implementing a consistent set of safeguards to ensure the confidentiality, integrity and availability of that information. This objective shall be achieved by: 1) subjecting an ICT system to the risk management process for the security of classified information processed in the ICT system; 2) limiting trust, consisting in treating other ICT systems as potential sources of threats and implementing in the ICT system safeguards controlling the exchange of information with those ICT systems; 3) implementing multi-level protection within the ICT system, consisting in the application of safeguards on as many different levels of organisation of protection of the ICT system as possible - in order to limit the occurrence of cases in which a breach of a single safeguard results in a violation of the aforementioned objective; 4) performing periodic security tests; 5) limiting authorisations, by way of giving users of an ICT system only the authorisations necessary to perform their work; 6) minimising functionality by way of installing, activating and using in an ICT system only the functions, communication protocols and services necessary for the correct performance of tasks for which the ICT system is intended.

Moreover, § 6 of the RRIS stipulates that in order to ensure protection against unauthorised access to an ICT system: 1) the conditions and manner of assigning users authorisations to work in an ICT system shall be determined; 2) information and materials enabling access to an ICT system shall be protected; 3) elements of an ICT system which are important for its security shall be protected and implemented in a manner ensuring the possibility of detecting unauthorised changes or attempts to introduce them. Also, according to § 7 of the RRIS, before allowing persons to work in an ICT system, the head of an organisational unit shall ensure that they have been trained in the field of ICT security and have been familiarised with procedures for secure operation within the scope applicable to them. In order to prevent the loss of confidentiality of classified information due to electromagnetic compromising emanation from system components, electromagnetic protection measures must be applied in an ICT system processing classified information with the "confidential" classification or above, based on the results of a risk assessment for the security of classified information, taking into account the recommendations.

Beyond the aforementioned, a similar approach is taken in relation to preventing the loss of availability of classified information processed in ICT equipment as a result of interference with its operation by means of emanation or high-power electromagnetic pulses, by employing electromagnetic protection measures selected on the basis of the results of a risk assessment for the security of classified information (§ 8(1) of the RRIS). However, in order to ensure availability of resources in an ICT system, the following shall be established: 1) principles of creating and storing backup copies; 2) procedures for handling crisis situations, including cases of failure of ICT system components; 3) procedures for monitoring the technical condition of an ICT system. Depending on the needs and results of a risk assessment for the security of classified information, alternative telecommunication links, alternative equipment or emergency power supply shall be used in particular to ensure the availability of the resources of an ICT system (§ 9(1) of the RRIS). Depending on the needs and the results of a risk assessment for the security of classified information, data transmissions between ICT system components shall be protected against detection, interception or interference.

Furthermore, the confidentiality of classified information communicated in the form of transmission outside protection zones shall be ensured by the use of encryption devices or tools certified in accordance with Article 50(2) of the APCI or approved under Article 50(7) of the APCI, appropriate to the security classification of the information communicated. In particularly justified cases, taking into account the results of a risk assessment for the security of classified information, the encryption protection measures referred to above may be supplemented or replaced by safeguards other than encryption (§ 10 of the RRIS). To the extent necessary to ensure review, analysis and provision of evidence of actions violating the security of classified information, records of events shall be created and stored for an ICT system processing classified information, and their confidentiality, integrity and availability shall be ensured (§ 11of the RRIS). In addition, an ICT system shall be provided with mechanisms or procedures preventing ICT security incidents, including protection against malicious software, as well as enabling the quickest possible detection of ICT security incidents and ensuring that appropriate persons are immediately informed of a detected incident (§ 12 of the RRIS).

The head of the organisational unit in which classified information is processed is responsible for the protection of classified information. He/she is charged with, in particular, organising and ensuring the functioning of such protection. Therefore, a classified information security officer employed by the head of the organisational unit reports directly to the head of the organisational unit and is tasked with ensuring compliance with the provisions on the protection of classified information. Such officers are required to have: 1) Polish citizenship; 2) higher education; 3) an appropriate security clearance issued by the Internal Security Agency (ISA) or the Military Counterintelligence Service (MCS), as well as by the former Office for State Protection or the former Military Information Services; 4) a certificate of classified information protection training conducted by the ISA or the MCS, as well as by the former Military Information Services. The head of the organisational unit may also employ a deputy or deputies of the security officer, provided that such persons fulfil the conditions referred to above (Article 14(1) to (4) of the APCI).

On the national level, the ISA and the MCS perform a special role in the protection of classified information. As provided for in Article 10(1) of the APCI, the ISA and the MCS supervising the functioning of the classified information protection system in organisational units within their competence set out in the aforementioned act: 1) control the protection of classified information and the observance of the provisions in force in this respect; 2) perform tasks in the field of security of ICT systems; 3) conduct verifying proceedings, control verifying proceedings and industrial security proceedings; 4) ensure the protection of classified information exchanged between the Republic of Poland and other states or international organisations; 5) provide advisory services and conduct training in the protection of classified information. The Head of the ISA performs the function of a national security authority and, to the extent necessary for the performance of this function, the Head of the ISA or officers of the ISA authorised by him, and the Head of the MCS or soldiers or officers of the MCS authorised by him have the right to: 1) inspect documents relating to the protection of international classified information; 2) enter premises and facilities intended for the processing of international classified information; 3) access ICT systems intended for the processing of international classified information; 4) obtain explanations and information relating to the protection of international classified information (Article 11(1) to (4) of the APCI).

4 Conclusion

Cybersecurity, and the security of classified information, becomes all the more important, the more we realise that today actions below the threshold of war are and will continue to be an important policy measure, enabling both state and non-state actors to achieve their objectives. Therefore, information security in cyberspace is now becoming one of the key areas of national security, both in relation to the structures of the state, its citizens and their activities. This is, of course, among others, a consequence of the rapid progress in digital technologies, which is at the same time a challenge for the state, which is forced to join the technological race in this area (National Security Strategy of the Republic of Poland, 2020: 7-8). Accordingly, the importance of cyberspace for the functioning of the state needs to be constantly emphasised, as actions taken in cyberspace have a direct impact on all key components of the state, and threats to the security of classified information are particularly serious in this respect and should be given increased attention (Biernacik, 2018: 13). It seems that awareness of these threats and of the damage that may be caused as a result of the unauthorised disclosure of classified information is growing, among those in power and among public administration employees, but also among average citizens. However, without appropriate knowledge in this area, strict observance of procedures, as well as adequate ICT infrastructure, we will continue to be exposed to a real danger resulting from activities taking place in cyberspace, because nowadays, and probably even more so in the future, both dimensions, the real and the virtual, are and will remain in an even greater and closer relationship.

References:

Biernacik, B. (2018) Nauka i najnowsze narzędzia informatyczne w służbie bezpieczeństwa cyberprzestrzeni – piątego wymiaru walki zbrojnej, In: Roman, Ł., Krassowski, K., Sagan, S. & Wróblewski, D. (eds) *Wykorzystanie nowoczesnych narzędzi informatycznych w identyfikacji zagrożeń* (Józefów: Wydawnictwo Wyższej Szkoły Gospodarki Euroregionalnej im. Alcide De Gasperi w Józefowie), pp. 9-39.

Bojarski, K. (2017) *Współdziałanie administracji publicznej z organizacjami pozarządowymi w sferze bezpieczeństwa wewnętrznego w ujęciu administracyjno-prawnym* (Warszawa-Nisko: Wydawnictwo Wyższej Szkoły Bezpieczeństwa i Ochrony im. Marszałka Józefa Piłsudskiego w Warszawie).

Cyfrowa Polska (2019) *Cyberbezpieczeństwo w Polsce: ochrona urządzeń końcowych przed cyberatakami. Analiza sytuacji i rekomendacje działań* (Warszawa), available at: https://cyfrowapolska.org/wp-content/uploads/2019/01/Raport_cyberbezpiecze%C5%84stwo_2019.pdf (April 12, 2022).

Górka, M. (2018) Cyberbezpieczeństwo jako wyzwania dla państwa i społeczeństwa, In: Dębowski, T. (ed.) *Cyberbezpieczeństwo wyzwaniem XXI wieku* (Łódź-Wrocław: ArchaeAgraph Wydawnictwo Naukowe), pp. 31-50.

Grabowski, M. & Zając, A. (2009) Dane, informacja, wiedza – próba definicji, *Zeszyty Naukowe Uniwersytetu Ekonomicznego w Krakowie*, 798, pp. 99-116.

Kowalewski, J. & Kowalewski, M. (2014) Cyberterroryzm szczególnym zagrożeniem bezpieczeństwa państwa, *Telekomunikacja i Techniki Informacyjne*, 1-2, pp. 24-32.

Krztoń, W. (2015) XXI wiek – wiekiem społeczeństwa informacyjnego, *Modern Management Review*, 3, pp. 101-112.

Machura, E. (2013) Informacja i jej znaczenie we współczesnym świecie w kontekście ochrony informacji niejawnych w Polsce, *Obronność – Zeszyty Naukowe Wydziału Zarządzania i Dowodzenia Akademii Obrony Narodowej*, 1, pp. 155-167.

Marczyk, M. (2018) Cyberprzestrzeń jako nowy wymiar aktywności człowieka – analiza pojęciowa obszaru, *Przegląd Teleinformatyczny*, 1-2, pp. 59-72.

Słownik języka polskiego, available at: https://sjp.pwn.pl/sjp/informacja;2466189.html (April 12, 2022).

Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej (2020), available at: https://www.bbn.gov.pl/ftp/dokumenty/Strategia_Bezpieczenstwa_Narodowego_RP_2020.pdf (April 12, 2022).

Cybersecurity Strategy for 2019-2024 (Official Gazette of 2019, item 1037).

Wasilewski, J. (2013) Zarys definicji cyberprzestrzeni, *Przegląd Bezpieczeństwa Wewnętrznego*, 5, pp. 225-234.

Wojciechowska-Filipek, S. & Ciekanowski, Z. (2019) *Bepieczeństwo funkcjonowania w cyberprzestrzeni: jednostki-organizacji-państwa* (Warszawa: CeDeWu).