Scientific Journal of the Military University of Land Forces
ISSN: 2544-7122 (print), 2545-0719 (online)
2022, Volume 54, Number 4(206), Pages 609-623
DOI: 10.5604/01.3001.0016.1767

Review article

Information security as part of Poland's security

Maciej Marczyk[1], Marek Błachut[2]*

[1] Faculty of Cybernetics, Military University of Technology, Warsaw, Poland, e-mail: maciej.marczyk@wat.edu.pl

[2] Command Institute, General Tadeusz Kościuszko Military University of Land Forces, Wrocław, Poland, e-mail: marek.blachut@awl.edu.pl

INFORMATION

Article history:

Submited: 22 December 2021

Accepted: 21 November 2022

Published: 15 December 2022

ABSTRACT

Dynamic advances in technology as well as information and communication entail many new threats to the functioning of the Polish state, its citizens, as well as to the international community. These are mainly the dangers of using information networks and information systems. For this reason, particular importance is given to ensuring information security which combines procedures and tools for the protection of classified information, data and network systems. Information security has now become one of the most sensitive trans-sectoral areas of national security, having an impact on the efficiency of Poland's entire security system. This is about information security, ICT security and cybersecurity.

The paper aims to analyse the issue of information security as part of the security area of the Republic of Poland. The issue was raised because of its importance and topicality, as recently there has been an increase in cyber-terrorist activity and a growing number of media reports on attacks on information systems, targeting the critical infrastructure of states. Information security risks pose a real threat and loss of information can lead to a violation of the vital interests of various entities and a compromise of people's safety and fundamental values of social life.

KEYWORDS

state security, information security, cybersecurity

* Corresponding author

Introduction

A sense of security is one of the basic needs of each individual and entire communities, which a state can guarantee with an arsenal of measures and techniques necessary for this purpose. Given the role of information in the modern world, great importance is attached to information security which protects the information dimension of the functioning of people and the state.

The 21st century has been described as the age of information, because it is a valuable asset providing people with a better and safer life. It is protected as a material good and critical resource. The increasing value of information becomes a source of advantage, knowledge

and power for individual entities. With the advances in the acquisition, processing and dissemination of information and the development of modern information and communication technologies, new threats have also emerged. Information security is threatened by the forces of nature, human error and organisational shortcomings, but also the dishonesty of people and their deliberate, harmful action in the form of computer crime, espionage, information warfare and cyber-terrorism. Hence the growing role of information security provision and state measures aimed at security in Polish cyberspace.

The paper aims to analyse the issue of information security as part of the security area of the Republic of Poland, presented in the literature and legislation. The issue was raised because of its importance and topicality, as recently there has been an increase in cyber-terrorist activity and a growing number of media reports on attacks on information systems, targeting the critical infrastructure of states. We are witnessing migration crises, used in hybrid operations by one state against another (the border between Poland and Belarus, actions of the government/president of Belarus – not recognised by many countries in Europe and around the world). Information security risks pose a real threat and loss of information can lead to a violation of the vital interests of various entities and a compromise of people's safety and fundamental values of social life.

For the purposes of the study, the authors formulated the following working hypothesis: information security is a very important element of Poland's security system and its provision should become a priority task of the state authorities. Protecting information and countering threats in cyberspace requires the cooperation of all public and private sector entities, state institutions and every citizen. Only a safe cyber world will allow for safe functioning in the real world.

A sense of security is one of the most important needs and the most precious values of every human being, which can be guaranteed by a state that has appropriate technical measures and institutions established to provide it. Security changes over time. It is determined by a number of internal and external factors, which means that it can not be achieved or gained once and for all. It is threatened by many undesirable phenomena, and as civilisation develops, new challenges continue to appear. Therefore, the state should effectively implement the security policy in two main dimensions: internal and external [1, p. 27].

1. The essence of security – theoretical approach

The positive dimension of security is related to the ability to combat threats that exist in the country's environment. This approach also includes certainty of survival and possession [2, p. 59].

In a democratic state, security is a core value affecting both the functioning of that state and its authorities, as well as all members of society, stimulating their proper existence. It is the purpose of the existence of the state, it determines its nature and the nature of the constantly satisfied social needs [3, p. 66]. It is considered a universal value, concerning a vast number of entities, the most significant being the security of the individual, society and the state [4, p. 167-168].

Security is a difficult concept to define clearly, sparking a number of polemics and discussions because of its intuitive and multi-faceted nature [5, p. 15]. In the most general sense, it is the state of being free from any threat [6, p. 26]. In the subjective sense, it denotes a mental state of calm and confidence, whereas in objective terms, a state of absence of real threats

[7, p. 76]. The perception of security in these two dimensions can be explained with Daniel Frei's D model which makes the following distinction:

- state of insecurity, when the actual threat is major and people perceive it correctly,
- state of obsession, when a minor actual threat is perceived as major,
- state of false security, when a major actual threat is perceived as minor (so-called misperception, i.e. false perception),
- state of security, when the actual threat is minor and people perceive it correctly [8, p. 29; 9, p. 91-92].

Security is a core constitutional value, although there is no precise definition of the term in the Basic Law [10, p. 9] nor a comprehensive view of it in the context of the common good, seen as the value that binds all particular goods that exist in the state and social spaces [11, p. 131].

Ensuring the security of citizens consists in countering threats and attacks against their functioning, within the law and with their goodwill, as well as protecting the entire population that is under the jurisdiction of the state. Citizens have the right to security which correlates with the obligation to provide this security on the part of the state. For this reason, restrictions on the rights and freedoms of individuals shall be allowed to ensure the security of the entire state, as stated in the judgment of the Constitutional Tribunal of 25 November 2003 [12]. This is also regulated in the Constitution of the Republic of Poland.

2. Security areas – problem analysis

Security is considered in a number of areas. Most often in the language of politics and diplomacy, as well as in international relations studies and political and legal documents, there is a distinction between national and international security [13, p. 22]. There is feedback between these two types of security, as the security of each state has a direct impact on the security of the international system as a whole, of which the state is a member, while international security conditions national security to a great extent [2, p. 60-61].

International security is implemented in an international environment. It refers to ensuring the security of groups of different countries, regions and international systems. It is the result of complex international interdependencies and is generated by securing the interests of individual states as part of multilateral cooperation. This consists in the joint definition of a catalogue of protected values, cooperation standards and institutions for ensuring international security. These include existence (survival), as the overarching value for which states may sacrifice other values, as well as identity, political autonomy, territorial integrity and development certainty (the quality and standard of the population's living and the level of economic development) [14, p. 56; 15, p. 6].

The internal and external security of the state is described extensively in the Polish Constitution. Ensuring it is the responsibility of the Council of Ministers (Art. 146 sec. 4 point 7 and 8). Pursuant to Art. 126 sec. 2 of the Basic Law, the President of the Republic of Poland safeguards the sovereignty and security of the State while, based on the provisions of Art. 135, he is advised by the National Security Council. Ensuring security is one of the most important tasks of the Armed Forces of the Republic of Poland (Art. 26 sec. 1). Pursuant to Art. 31 sec. 3 of the Constitution, state security is also a general limitation clause on human and civil freedoms and rights [16, p. 26-27].

The central element of security is threat, posing a risk to the existence of the State [17, p. 17]. A threat is an action or sequence of events that threatens the quality of life of the population

of a given state and significantly narrows the range of choices and actions available to the government [18, s. 40].

The term "threaten" means to foretell something bad, intimidate, warn under pain of certain consequences, to be dangerous, menacing. In terms of political science, a threat is a challenge taken on too late or not taken on at all [19, p. 31]. A threat is an indirect or direct destructive impact on the subject. It is subdivided into potential, real, external and internal, subjective and objective, military and non-military [20, p. 269].

Internal threats denote a negative state of affairs and set of circumstances that arise in various areas of the internal activity of the state and disturb its stability and harmonious development, as well as weaken or lead to the loss of the ability to survive in an international environment. By contrast, external threats originate in the international environment. They include wars and armed conflicts.

According to the most common classification, security threats are divided into military and non-military. However, it should be noted that threats are characterised by high volatility. Some phenomena treated as threats in the past are currently no longer regarded as such, while others, previously harmless, become dangerous and are currently a major concern. The intensity of threats also changes over time, because some weaken and others intensify [21, p. 27].

From the point of view of the authors, an important element of the studied areas is information security.

3. The essence of information security – theoretical approach

People have always needed information. Already at the time when the first tribal structures were formed, they acquired it by learning where to find drinking water and food, they assessed it by determining whether the information is useful, and the person providing it credible, and they protected it by creating closed elites that had exclusive access to the information. Over time, at each stage of society's development, information was collected, processed, used and protected more and more effectively. Today, we are dealing with an information society in which information is the most important commodity and one of the most valuable assets [22, p. 95].

Due to technological progress, the development of electronics and the Internet, the ubiquity of mobile devices and the rise of social networks, information has now become a desired good, a key factor determining the level of knowledge, authority, and also the security of individual citizens, organisations and entire countries [23, p. 11-12].

The 21st century known as the age of information has brought about a significant change in the nature and shape of global threats, because these times of universal access to state-of-the-art information technology are conducive to the emergence of new dangers [20, p. 268]. These are dangers closely related to the use of IT networks and information systems (computer-mediated crimes, loss of information due to computer hacking, espionage, sabotage, vandalism [23, p. 24]. For this reason, the identification, achievement, maintenance and improvement of information security have nowadays become necessary for the proper functioning of the state, economic operators, their profitability, financial liquidity and compliance with the law [24, p. 22].

Information security of a state is directly related to its internal and external security. It is not a new security area, as its traces date back to as early as the 6th century BC when Chinese

philosopher Sun Tzu developed the first strategies of information superiority and not necessarily conventional warfare. This allowed him to triumph over the opponent without a fight [25, p. 163]. Today, the issue of information security is of interest to the science known as securitology which studies threats to the existence, development and normal functioning of people and social organisations [22, p. 93].

Information security combines procedures and tools for protecting information, data and systems. This sphere covers concepts such as information security, ICT security and cybersecurity [26, p. 452].

There are many definitions of information security in the literature which mainly come down to the protection of classified information or to the security of ICT systems. This is confirmed by the definition of Krzysztof Liedel, according to whom information security is equated to the protection of information against unwanted, intentional or accidental, disclosure, modification, destruction or denial of processing [27, p. 19].

Information security can be defined as a set of activities, methods and procedures undertaken by authorised entities that aim to ensure the integrity of information resources that are being collected, stored and processed. All of them are adequately protected against unwanted and/or unauthorised disclosure, modification or destruction. The term should also be understood as a state when the risk of a threat to the proper functioning of information resources is reduced to an acceptable level [28, p. 150].

According to S. Kowalkowski, information security ranks right next to political, economic, social, military, cultural and environmental security. It addresses the issues of protection against network attacks and the consequences of physical attacks, as well as includes concern for maintaining the stability of contemporary international economic systems [29, p. 13-15].

In the opinion of K. Liderman, the term "information security" is accompanied by the concept of "information security", encompassing all forms of the exchange, storage and processing of information, also verbal. It determines the subject's (individual, organisation) confidence in the quality and accessibility of information that may be lost or distorted. According to this author, security thus defined shall not be regarded as an object, process or event but as imponderabilia in the field of psychology. Due to the high proportion of technical measures in the transmission, storage and processing of information, information security is becoming increasingly vulnerable to cyber threats, especially cyber-terrorist attacks [23, p. 22-24, 109]. It is not without reason that information security is considered to be part of an IT system, synonymous with telecommunications [30, p. 17], computer or network security [24, p. 22].

The term "information security" is often wrongly equated with IT security. This is incorrect insofar as it would only cover the protection of information in electronic form. Meanwhile, it involves many other processes, leading to the generation, modification and transfer of data in verbal form as well [23, p. 22; 31, p. 141]. IT security (ICT security) has a much narrower semantic scope, drawing attention to technological developments in obtaining, storing, processing and sharing information which are the result of the popularisation of digital forms of data presentation [32, p. 18-19].

The concept of information security is also applicable to information appearing on standard media, i.e. outside of the ICT system (e.g. paper documents or microfilms). The scope of information security policy covers processes of using information without considering the way it is processed. Therefore, it concerns both traditionally operated systems (archives, files, paper documents) and computer systems [24, p. 40].

The issue of information security comprises the process of protecting information and personal data against unwanted interference and ICT systems against the destructive activity of hostile external and internal objects [33, p. 91].

According to P. Bączek, information security is a concept that describes the internal and external state of a country in which nothing threatens the strategic information resources of the state, while the authorities take the most important decisions based on true, verified, reliable and up-to-date information whose flow is not disrupted. The state by virtue of law guarantees the protection of citizens' personal data and ensures the security of public ICT networks and legal information protection systems. Citizens have the right to privacy, and public and private institutions do not violate the applicable legal standards when collecting information on citizens and organisations. Citizens and their representatives, including media, parliamentarians, non-governmental organisations and control bodies, have free access to information on the activities of the authorities [19, p. 74].

M. Madej indicates that information security concerns efforts directed at the protection of information important in terms of security, i.e. having a significant impact on the smooth functioning of both state structures and society as a whole, as well as on providing information advantage by acquiring new or more recent data, and on conducting disinformation campaigns against possible opponents [32, p. 18-19].

In accordance with the provisions of the Information Security Doctrine of the Republic of Poland of 2015, state information security is a trans-sectoral security area, relating to the state's information environment and cyberspace. It is a process aimed at ensuring the secure functioning of the state in the information space by controlling its own national infosphere, as well as focused on the effective protection of national interests in a foreign, i.e. external infosphere. This is possible through adequate protection of available information resources and protection against hostile disinformation and propaganda activities, in terms of defence, while retaining the ability to carry out offensive activities against possible opponents [34, p. 3].

In another view, information security includes ensuring the integrity, completeness and reliability of the information resources of an entity (state) in any form [35, p. 194-197].

An accurate definition of information security was proposed by W. Fehler who regards it as a state and a process that ensures free access, collection, flow and processing of high-quality information following its substantive selection combined with the rational, customary and legal separation of categories that are protected or regulated for the safety of the interested parties [36, p. 29-30].

In turn, a broad definition of the term was put forward by E. Nowak and M. Nowak. According to this definition, information security is a state of external and internal conditions which allow the state to freely develop its information society. Among the conditions that guarantee this state, the authors include:

– unthreatened strategic resources of the state,
– uninterrupted flow of information between state bodies,
– decisions of the authorities based on relevant and reliable information,
– protection of classified information and citizens' personal data guaranteed by the state,
– uninterrupted operation of ICT networks comprising the critical ICT infrastructure of the state,

– free access to public information for all citizens,
– the principle that public institutions shall not infringe upon citizens' right to privacy [37, p. 103].

When considering the term "information security" reference should also be made to the standards PN-EN ISO/IEC 27000:2020-07 [38; 39]. These standards use the concept of information security seen as maintaining the confidentiality, integrity and availability of information. This is illustrated in detail in (Fig. 1).

According to the authors, state information security should refer to security in the technical and personal space. In practice, it is impossible to build a completely secure information protection system, since man is identified as the weakest link in any system.

Therefore, maintaining state information security must be based on several important considerations, which are:

– increasing the protection of information systems,
– continuously assessing weaknesses in the information systems of potential opponents, the possibility of intrusion into their systems,
– preparing possible responses to an attack using informational and conventional means of destruction,
– developing methods of estimating information losses and damage suffered or inflicted.

Such an approach requires consideration of the most important determinants of information security, which include:

– treating information as a resource of strategic importance to the state,
– treating information and resulting knowledge and information technology as primary production factors,
– the information sector producing a significant part of national income,
– treating information technology as an essential element in the functioning of state security, in particular the Armed Forces [38, p. 219].

An information protection system in the area of state security should, according to the authors, be supported by legal and organisational solutions, the whole area of information security policy, thanks to which the state will be able to effectively and efficiently perform its functions: internal and external.

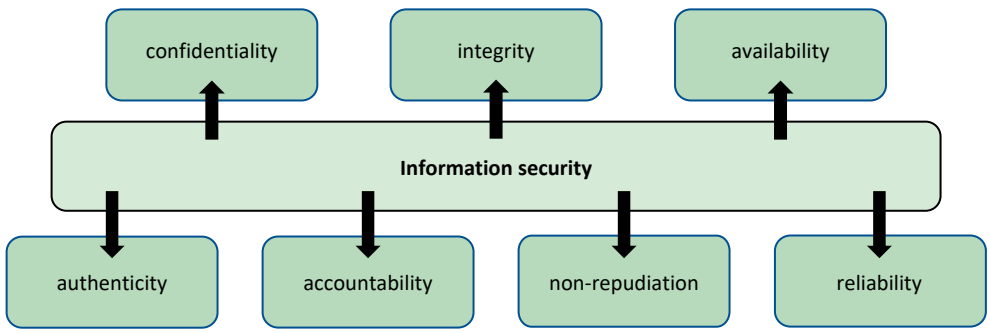

Fig. 1. Information security attributes
Source: Study based on [40].

4. Legal aspects of information security in Poland

Freedom of expression and access to information are the foundation of civilisation standards that apply in democratic countries. Respect for free access to information is the basis for creating a democratic society since the adoption of the Convention for the Protection of Human Rights and Fundamental Freedoms in 1950 [41]. Attempts to restrict this right are considered an attack on fundamental human rights. The universal principle of unrestricted access to information is also expressed in acts of international law, particularly in the UN Universal Declaration of Human Rights (1948) and the International Covenant on Civil and Political Rights (1966) [42, p. 109].

An important document of European law regulating cybersecurity is Regulation 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act). ENISA, by providing advice and assistance as well as by virtue of its scientific and technical independence and transparent operating procedures, has become a centre of expertise in the field of broadly understood cybersecurity [33, p. 94].

Information security also includes a personal data protection system which is part of the protection of the right to privacy. It was based on the provisions of the GDPR and the Polish Act of 10 May 2018 on the protection of personal data. Natural persons' rights with regard to data processing are subject to protection under administrative, medical, financial, press and copyright law, as well as telecommunications and labour law. In connection with the obligations imposed by the GDPR, Polish law was harmonised with European law and regulations contradicting or duplicating the GDPR solutions were removed from the Polish legal order. In February 2019, The Sejm passed a law amending certain acts in order to ensure the application 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, i.e. the General Data Protection Regulation [43, p. 27].

The Polish Constitution grants citizens the right to obtain information on the activities of public information bodies, as well as persons discharging public functions. Furthermore, the Constitution establishes a clause on the possibility of introducing certain restrictions in the event of circumstances set out in the Act. Based on Art. 61 sec. 3 of the Basic Law, two normative acts relevant to economic operators were incorporated into the Polish legal order, namely the Act on the protection of personal data [44] and the Act on the protection of classified information [45].

Information security issues are also included in the Act on access to public information [46], the Act on counteracting unfair competition [47] and the Act on copyright and related rights [48].

The emergence of more and more new threats to information security generated the implementation of various reservations related to the handling of information. It also resulted in solutions related to criminal liability for disclosing information to unauthorised persons. For this reason, provisions relating to the protection of information also appeared in the Penal Code [49, p. 13].

The Penal Code sets out the highest sanctions against the provisions of other acts which regulate matters of protection of state and official secrets, as well as other secrets protected by

law. In addition, it addresses the issue of acts against cybersecurity. The legislator categorised these risks as information warfare, grouping the provisions in Chapter XXXIII "Offences against the Protection of Information in Cyberspace" (they are typified by Art. 267, 268, 268a, 269, 269a i 269b) [50, p. 19].

In recent years, Poland has seen an increase in cyber-terrorism threats. Thus, cybersecurity is currently one of the most important, priority challenges of Poland's security policy. The cybersecurity system of the Polish state is built on the provisions of the Act on the national cybersecurity system [51] which was passed by the Polish Parliament in order to implement in the Polish legal order Directive (EU) 2016/1148 of the European Parliament and of the Council concerning measures for a high common level of security of network and information systems across the Union. The Directive imposed on the EU Member States the obligation to guarantee security at a minimum level of capacity in the area of cybersecurity by appointing competent authorities and a single point of contact for cybersecurity issues, as well as by creating special response teams for all computer incidents (currently, according to the Act on the national cybersecurity system, these are CSIRTs). In addition, it was recommended to adopt national strategies concerning cybersecurity issues. In the light of the Directive, service sectors of key importance for the maintenance of the state's critical socio-economic activities were obliged to ensure the cybersecurity of their information systems. The person responsible for building defence capacity in cyberspace is the Minister of Defence [45, p. 28-29].

Issues concerning information protection in cyberspace are regulated by three types of documents:

- conceptual documents, relating to cybersecurity and information security – the National Security Strategy [52], the Cybersecurity Doctrine of the Republic of Poland [53], the National Framework of Cybersecurity Policy of the Republic of Poland for 2017-2022 [54] and the superseding Cybersecurity Strategy of the Republic of Poland for 2019-2024 [55],
- acts on the protection of ICT systems against cyber-terrorist attacks: the Act on the computerisation of the activities of entities performing public tasks [56] and the Telecommunications Act [57],
- implementing documents having the status of regulations, relating to cybersecurity issues: the Regulation of the Council of Ministers on the National Interoperability Framework, minimum requirements for public registers and exchange of information in electronic form as well as the minimum requirements for ICT systems [58].

The Cybersecurity Strategy of the Republic of Poland for 2019-2024 continues and extends government administration activities aimed at increasing the level of cybersecurity in Poland. The main objective of the strategy is to increase the level of resilience against various cyber threats and the level of information protection in key sectors, i.e. in the public, private and military sectors, as well as promote knowledge and good practices which will allow citizens to better protect information.

Conclusions

The analysis of selected legislation and literature on the subject shows the validity of the addressed topic and the conducted theoretical research. It also proves the importance of the problem in the area of information security on a national scale.

Both the public and private sectors have been assigned relevant tasks to be carried out as described, for example, in the already analysed *Cybersecurity Strategy of the Republic of Poland for 2019-2024*.

The tasks of the public sector are primarily the identification of real and potential sources of danger through the international exchange of information about threats and incidents; participation in the international response to cyber threats within the EU and NATO structures; cryptographic and cryptanalytical activities aimed at securing domestic ICT systems and their information resources; ongoing monitoring of all critical points of the security system, especially those most vulnerable to cyber attacks; development of a risk assessment methodology; responding to any ICT security incidents; conducting audits of cybersecurity measures and mechanisms; preparation and implementation of response scenarios in the event of cyber attacks directly targeting the digitised tasks of the state.

It is important to develop emergency response plans and operational plans in the event of specific threats and war. Active cyber defence must be implemented, including offensive operations in cyberspace, and constant readiness for cyberwar must be maintained. The priority task in terms of information protection is preventing and combating cybercrime, including espionage and events bearing the hallmark of a terrorist attack, as well as informing and educating the public on the safe use of cyberspace and the threats therein.

The main tasks of the private sector in the field of information security include close cooperation with the public sector in the area of countering threats in cyberspace, exchange of information on cyber threats and their sources, and effective protection of available information resources (safeguards, passwords, cryptography).

The civil sector should support the state authorities in ensuring information security by participating in social initiatives aimed at supporting Poland's cybersecurity (volunteering for the cybersecurity and cyber defence of the state), taking care of the computer systems and ICT equipment used, monitoring proposals for legal amendments related to the protection of human rights, particularly the right to privacy on the internet [53].

The trans-sectoral tasks, as described in the *Cybersecurity Doctrine of the Republic of Poland*, are primarily the coordination of cooperation between various public and private sector entities, the creation of mechanisms necessary for the exchange of information, as well as cybersecurity standards and good practices (e.g. cybersecurity testing and audits, certification of ITC products and services, secure hardware and software, supply chain security).

The national-level documents are of crucial importance, meaning the preparation, maintenance and development of operational cyber-security links, rapid response to emergencies, efficient management of cybersecurity measures and the ability to conduct proactive operations in cyberspace. When it comes to the military, these tasks are the responsibility of Ministry of Defence. The armed forces need to have the capacity to defend and protect their own ICT systems and the information resources stored in them, as well as the capacity to take offensive action and conduct defensive and protective operations, i.e. the full spectrum of military activities in cyberspace in the event of a cyber conflict, including a cyber war [53].

It is therefore necessary to implement NATO standards related to cyber defence, in particular in the aspect of defence and operational planning, and to factor in the minimum standards of the North Atlantic Treaty Organisation in the area of protection of the Alliance's own assets and national mission-critical infrastructure assets. In the field of cybersecurity, it is also extremely important to develop the competences and capabilities of intelligence and

counterintelligence services to counteract espionage and effectively neutralise the activity of foreign intelligence services in cyberspace [53].

The acquisition of capabilities and competences in the field of controlling the IT subsystems of foreign-made weapons and equipment used for national security, especially the possession of the necessary source codes, is also considered strategically important. Cryptology also is also of great importance in this respect. The state should work on developing the ICT tools and technologies controlled by authorities and use them to protect and defend mission-critical state systems, while remaining compatible with NATO tools and technologies [53].

Significant technological advances in the information and communication sphere entail a number of new threats to the functioning of the state and its citizens, as well as to the international community. These are mainly dangers associated with the use of IT networks and information systems and access to the global network. For this reason, particular importance is placed on ensuring information security which combines procedures and tools for the protection of classified information, data and network systems. Information security has now become one of the most sensitive trans-sectoral areas of national security, having an impact on the efficiency of Poland's entire security system. This includes information security, including information, ICT security and cybersecurity. The authors believe that these are the most important aspects of the contemporary security area of each state.

Information protection and security in the Polish cyberspace is regulated by a number of legal acts and other documents, both European and national. The most important one in this regard is the Polish Constitution. The act on the protection of classified information and the act on the protection of personal data are also important. The Penal Code penalises acts committed against information security and cybersecurity. As for the Polish cybersecurity system, it is based on the provisions of the National Cybersecurity System Act. Other documents of relevance in this regard include the National Security Strategy, the Cybersecurity Doctrine of the Republic of Poland, the Cybersecurity Strategy of the Republic of Poland for 2019-2024.

The purpose of this paper was to attempt to analyse the matter of information security as an element of the security area of the Republic of Poland, which was conducted by identifying written sources and legal documents concerning these issues. The indicated/cited authors of monographs and articles, but also footnotes from the law and doctrinal documents of the last few years, confirm the authors' assumptions regarding the relevance of this problem and why it is important to write about it.

The aim of the paper, in the view of Authors, was achieved and the hypothesis adopted at the outset was also confirmed. Using the method of critical analysis of the literature, the article characterises the area of Poland's information security demonstrating its enormous role in the overall activities of the state aimed at ensuring a safe and peaceful existence for all citizens and participants of social life, especially those connected to the Internet and storing data in the cloud, i.e. the entire 5.0 community.

Acknowledgement

No acknowledgement and potential founding was reported by the authors.

Conflict of interests

All authors declared no conflict of interests.

Author contributions

All authors contributed to the interpretation of results and writing of the paper. All authors read and approved the final manuscript.

Ethical statement

The research complies with all national and international ethical requirements.

ORCID

Maciej Marczyk https://orcid.org/0000-0002-7991-8126

Marek Błachut https://orcid.org/0000-0001-6974-7493

References

1. Paździor M, Trubalska J. *Pojęcie bezpieczeństwa państwa*. In: Paździor M, Trubalska J, Wojciechowski Ł, Żywicka A (eds.). *Bezpieczeństwo państwa w XXI wieku. Podręcznik akademicki*. Toruń: WSEI; 2015, p. 15-27.
2. Górka-Winter B. *Kryterium bezpieczeństwa międzynarodowego państwa*. In: Dębski S, Górka-Winter B (eds.). *Kryteria bezpieczeństwa międzynarodowego państwa*. Warszawa: PISM; 2003, p. 59-70.
3. Karpiuk M. *Prawne podstawy bezpieczeństwa*. In: Żukowski A, Hartliński M, Modzelewski WT, Więcławski J (eds.). *Podstawowe kategorie bezpieczeństwa narodowego*. Olsztyn: Instytut Nauk Politycznych Uniwersytetu Warmińsko-Mazurskiego w Olsztynie; 2015, p. 64-70.
4. Dudek D. *Bezpieczeństwo Rzeczypospolitej jako wartość konstytucyjna*. In: Antonowicz L (ed.). *Bezpieczeństwo Polski. Historia i współczesność*. Lublin: Wydawnictwo KUL; 2010, p. 167-84.
5. Potrzeszcz J. *Bezpieczeństwo i porządek publiczny w ujęciu filozofii prawa*. In: Lis W (ed.). *Bezpieczeństwo państwa. Zagadnienia podstawowe*. Lublin: Wydawnictwo KUL; 2014, p. 15-34.
6. Ścibiorek Z, Wiśniewski B, Kuc RB, Dawidczyk A. *Bezpieczeństwo wewnętrzne*. Toruń: Wydawnictwo Adam Marszałek; 2015.
7. Korzeniowski LF. *Podstawy nauk o bezpieczeństwie*. Warszawa: Difin; 2012.
8. Zięba R. *Instytucjonalizacja bezpieczeństwa europejskiego*. Warszawa: Scholar; 1999.
9. Jemioł T, Malaka K (eds.). *Bezpieczeństwo zewnętrzne Rzeczypospolitej Polskiej*. Warszawa: AON; 2002.
10. Braniewicz OE. *Podstawy prawne bezpieczeństwa i obronności RP.* In: Skrobotowicz G, Maciąg K. *Wybrane aspekty bezpieczeństwa narodowego*. Lublin: Wydawnictwo Naukowe TYGIEL; 2016, p. 7-27.
11. Bień-Kacała A. *Bezpieczeństwo Rzeczypospolitej Polskiej.* In: Bień-Kacała A, Jirásek J, Cibulka L, Drinóczi T (eds.). *Kategoria bezpieczeństwa w regulacjach konstytucyjnych i praktyce ustrojowej państw Grupy Wyszehradzkiej*. Toruń: Wydawnictwo Naukowe Uniwersytetu Mikołaja Kopernika; 2016, p. 131-42.
12. Wyrok Trybunału Konstytucyjnego z 25 listopada 2003. K 37/02, OTK ZU 2003, Nr 9A, poz. 96.
13. Zięba R. *Instytucjonalizacja Bezpieczeństwa Europejskiego. Koncepcje – struktury – funkcjonowanie*. Warszawa: Wydawnictwo Naukowe SCHOLAR; 2001.
14. Zięba R. *Pojęcie i istota bezpieczeństwa państwa w stosunkach międzynarodowych*. Sprawy Międzynarodowe. 1989;10:1-23.
15. Szmulik B. *Zagadnienia ogólne*. In: Paździor M, Szmulik B (eds.). *Instytucje bezpieczeństwa narodowego*. Warszawa: Wydawnictwo C.H. Beck; 2012, p. 1-11.
16. Czuryk M, Dunaj K, Karpik M, Prokop K (eds.). *Bezpieczeństwo państwa. Zagadnienia prawne i administracyjne*. Olsztyn: Wydział Prawa i Administracji UWM; 2016.

17. Czaputowicz J. *System czy nieład? Bezpieczeństwo europejskie u progu XXI wieku*. Warszawa: Wydawnictwo Naukowe PWN; 1998.
18. Levy MA. *Is the Environment a National Security Issue?* International Security. 1995;20(2):35-62.
19. Bączek P. *Zagrożenia a bezpieczeństwo państwa polskiego*. Toruń: Wydawnictwo Adam Marszałek; 2006.
20. Koziej S. *Teoria sztuki wojennej*. Warszawa: Bellona; 2011.
21. Pokruszyński W. *Bezpieczeństwo narodowe u progu XXI wieku*. Zeszyty Naukowe AON. 2008;70(1): 23-32.
22. Grzebiela K. *Pojęcie i istota bezpieczeństwa informacyjnego*. Kultura Bezpieczeństwa Nauka – Praktyka – Refleksje. 2018;30:87-101.
23. Liderman K. *Bezpieczeństwo informacyjne*. Warszawa: PWN; 2012.
24. Nowak A, Scheffs W. *Zarządzanie bezpieczeństwem informacyjnym.* Warszawa: AON; 2010.
25. Plecka M, Rychły-Lipińska A. *Bezpieczeństwo informacyjne*. In: Urbanek A (eds.). *Wybrane problemy bezpieczeństwa*. Słupsk: Wydawnictwo Społeczno-Prawne; 2013, p. 163-87.
26. Żebrowski A. *Bezpieczeństwo informacyjne Polski a walka informacyjna*. Roczniki Kolegium Analiz Ekonomicznych. Szkoła Główna Handlowa. 2013;29:447-63.
27. Liedel K. *Bezpieczeństwo informacyjne w dobie terrorystycznych i innych zagrożeń bezpieczeństwa narodowego*. Toruń: Wydawnictwo Adam Marszałek; 2008.
28. Wrzosek M. *Procesy informacyjne w zarządzaniu organizacją zhierarchizowaną*. Warszawa: AON; 2010.
29. Kowalkowski S (ed.). *Niemilitarne zagrożenia bezpieczeństwa publicznego.* Warszawa: AON; 2011.
30. Sutton RJ. *Bezpieczeństwo telekomunikacji.* Stawikowski G (transl.). Warszawa: Wydawnictwo Komunikacji i Łączności; 2004.
31. Więcaszek-Kuczyńska L. *Wybrane regulacje prawne w obszarze zagrożeń bezpieczeństwa informacyjnego*. Zeszyty Naukowe Obronność. 2014;3:139-55.
32. Madej M. *Rewolucja informatyczna – istota, przejawy oraz wpływ na postrzeganie bezpieczeństwa państw i systemu międzynarodowego*. In: Madej M, Terlikowski M (eds.). *Bezpieczeństwo teleinformatyczne państwa*. Warszawa: Wydawnictwo PISM; 2009, p. 17-40.
33. Gerwatowski J. *Bezpieczeństwo informacyjne w jednostkach samorządu terytorialnego*. UWM Studia Prawnoustrojowe. 2019;4:89-106.
34. *Doktryna Bezpieczeństwa Informacyjnego RP*. Warszawa: Biuro Bezpieczeństwa Narodowego; 2015.
35. Potejko P. *Bezpieczeństwo informacyjne*. In: Wojtaszczyk KA, Materska-Sosnowska A (eds.). *Bezpieczeństwo państwa*. Warszawa: Oficyna Wydawnicza ASPRA-JR; 2009.
36. Fehler W. *O pojęciu bezpieczeństwa informacyjnego.* In: Kubiak M, Tobolewski S (eds.). *Bezpieczeństwo informacyjne w XXI wieku*. Siedlce: Wydawnictwo UPH; 2016, p. 25-43.
37. Nowak E, Nowak M. *Zarys teorii bezpieczeństwa narodowego*. Warszawa: Difin; 2011.
38. Balcerowicz B. *Siły zbrojne w stanie pokoju, kryzysu, wojny*. Warszawa: Wydawnictwo Naukowe SCHOLAR; 2010.
39. *PN-ISO/IEC 27001:2007. Technika informatyczna – Techniki bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji – Wymagania*. Warszawa: Polski Komitet Normalizacyjny; 2007.
40. Łuczak J, Tyburski M. *Systemowe zarządzanie bezpieczeństwem informacji ISO/IEC 27001*. Poznań: Wydawnictwo Uniwersytetu Ekonomicznego w Poznaniu; 2009.
41. Konwencja o Ochronie Praw Człowieka i Podstawowych Wolności sporządzona w Rzymie dnia 4 listopada 1950 r., zmieniona następnie Protokołami 3, 5 i 8 oraz uzupełniona Protokołem nr 2 (Dz. U. 1993 Nr 61, poz. 284).
42. Ciecierski M, Gajos M (eds.). *Ochrona Informacji niejawnych i biznesowych. Materiały III Kongresu. Krajowe Stowarzyszenie Ochrony Informacji Niejawnych*. Katowice: Uniwersytet Śląski w Katowicach; 2007.

43. Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. z 2019 r., poz. 742).
44. Chrostowska-Malak K. *Bezpieczeństwo informacji a ochrona danych osobowych*. In: Porzeżyński M, Borcuch A (eds.). *Bezpieczeństwo w erze społeczeństwa informacyjnego. Wyzwania w sferach kultury, marketingu i gospodarki*. Kielce: Laboratorium Wiedzy Artur Borcuch; 2019, p. 27-36.
45. Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2019 r., poz. 1781).
46. Ustawa z dnia 6 września 2001 r. o dostępie do informacji publicznej (Dz. U. z 2019 r., poz. 1429).
47. Ustawa z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji (Dz. U. z 2019 r., poz. 1010).
48. Ustawa z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych (Dz. U. z 2019 r., poz. 1231).
49. Żebrowski A, Kwiatkowski M. *Bezpieczeństwo informacji III Rzeczypospolitej*. Kraków: Abrys; 2000.
50. Aleksandrowicz TR. *Bezpieczeństwo w cyberprzestrzeni ze stanowiska prawa międzynarodowego*. Przegląd Bezpieczeństwa Wewnętrznego. 2016;15(8):11-28.
51. Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2020 r., poz. 1369).
52. *Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej*. Warszawa: Biuro Bezpieczeństwa Narodowego; 2020.
53. *Doktryna Cyberbezpieczeństwa Rzeczypospolitej Polskiej*. Warszawa: Biuro Bezpieczeństwa Narodowego; 2015.
54. *Krajowe Ramy Polityki Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017-2022*. Warszawa: Ministerstwo Cyfryzacji; 2017.
55. Uchwała nr 125 Rady Ministrów z dnia 22 października 2019 r. w sprawie Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019-2024 (M.P., poz. 1037).
56. Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2020 r., poz. 346).
57. Ustawa z dnia 16 lipca 2004 r. Prawo telekomunikacyjne (Dz. U. z 2019 r., poz. 2460).
58. Rozporządzenie Rady Ministrów z 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. z 2017 r., poz. 2247).

Biographical note

Maciej Marczyk – Reserve Colonel, D.Sc., professor at WAT, employee of Faculty of Cybernetics, Military University of Technology, and a professor at WSU, employee of Faculty of Military Science, Academy of Military Art. He is in an expert in ICT environment management. His areas of expertise are information security, the operation of communication systems and ICT networks, cybersecurity and the directions of development of command support (ICT) in future operations in a network-centric environment. He has written and co-written dozens of publications and articles (papers) in the field of command support and management of ICT networks in the SZRP and organisation of command and staff structures of military units in times of peace, crisis, war.

Marek Błachut – Captain, M.Sc., graduate of Land Forces Officer Candidate School in Wrocław (2016), the University of Szczecin (2009) and completed postgraduate studies at the Military University of Technology in 2015 and 2021. Since 2016, he has been holding teaching positions at the Land Forces Officer Candidate School and currently at Military University of Land Forces. He has completed more than 15 courses and training sessions in communications, cryptography and radio reconnaissance and combat. He is the Team Leader of the Communications Systems Team. He is the author of publications in the fields of ICT security, radio communications, artificial intelligence.

Bezpieczeństwo informacyjne jako element bezpieczeństwa Polski

STRESZCZENIE

Dynamiczny postęp technologiczny i informacyjno-komunikacyjny niesie wiele nowych zagrożeń dla funkcjonowania państwa polskiego, jego obywateli, a także dla społeczności międzynarodowej. Są to głównie niebezpieczeństwa związane z użytkowaniem sieci informatycznych oraz systemów informacyjnych. Z tego powodu wyjątkowego znaczenia nabiera zapewnianie bezpieczeństwa informacyjnego, które łączy w sobie procedury i narzędzia służące ochronie informacji niejawnych, danych oraz systemów sieciowych. Bezpieczeństwo informacyjne stało się obecnie jednym z najbardziej wrażliwych obszarów bezpieczeństwa narodowego o charakterze transsektorowym, wywierającym wpływ na efektywność funkcjonowania całego systemu bezpieczeństwa Polski. Chodzi o bezpieczeństwo informacji, bezpieczeństwo teleinformatyczne i cyberbezpieczeństwo.

Celem niniejszego artykułu jest próba analizy zagadnienia bezpieczeństwa informacyjnego jako elementu obszaru bezpieczeństwa Rzeczypospolitej Polskiej. Temat podjęto z powodu jego ważności i aktualności, albowiem w ostatnim czasie nasilają się działania cyberterrorystów, coraz częściej media donoszą o atakach na systemy informatyczne, wymierzone w infrastrukturę krytyczną państw. Zagrożenia bezpieczeństwa informacyjnego stają się realne, zaś utrata informacji może prowadzić do naruszenia żywotnych interesów różnych podmiotów, narażenia bezpieczeństwa ludzi oraz podstawowych wartości życia społecznego.

SŁOWA KLUCZOWE bezpieczeństwo państwa, bezpieczeństwo informacyjne, cyberbezpieczeństwo

How to cite this paper

Marczyk M, Błachut M. *Information security as part of Poland's security*. Scientific Journal of the Military University of Land Forces. 2022;54;4(206):609-23. DOI: 10.5604/01.3001.0016.1767.