SAFETY&DEFENSE
Scientific and Technical Journal ISSN 2450-551X

The Importance of Military Information Security

Wojciech SŁUGOCKI[1*], Marzena WALKOWIAK[2]

[1] Military University of Technology, Warsaw; slugockywoj@gmail.com,
ORCID: 0000-0003-0275-8096
[2] Military University of Technology, Warsaw; marzena.walkowiak@wat.edu.pl,
ORCID: 0000-0002-3317-562X
* Corresponding author

DOI: https://doi.org/10.37105/sd.93

Abstract

The main goal of the research is to identify the key problems related to information security in the armed forces and to classify the most important factors and aspects necessary to increase security. The implemented research methods include a critical analysis of legal acts, organizational and competence documents, literature on the subject. Synthesis and inference were employed to achieve the formulated goals. The main findings indicate that the armed forces' information security system will play an increasingly important role in shaping the security of modern states and should be treated as a priority. The results of the analyzes indicate that in the coming years, the main challenge of modern armies will be to strengthen the offensive and defensive information capabilities of the state. The general findings of this article present the view that information security is a key task for the armed forces to ensure national security. Therefore, it is necessary to revise, clarify and tighten up the procedures in force for the protection of key information processed in the state - especially in the armed forces – which should have adequate capabilities to conduct complex operations in cyberspace. Moreover, the need for a thorough and comprehensive analysis of this topic is confirmed.

Keywords

information security, national security, military security, safety.

Submited: 26.01.2021. Accepted: 23.02.2021. Published: 11.03.2021.

1. Introduction

The need to ensure the security of important information is becoming a growing challenge for state institutions, mainly due to the emergence of new threats resulting from the progressive computerization, globalization and digitization of the modern world. It could be argued that "for a modern state community, the threats of information crimes, i.e. cybercrime, will be particularly significant. The increase in the importance of information, the development of IT infrastructure and technologies has created a completely new sphere of social activity, and at the same time a platform for competition and possible abuse and crime cyberspace" (Szczurek, Walkowiak & Bryczek-Wróbel, 2020, p. 86). Moreover, there are a number of categories of information whose protection seems particularly important from the point of view of the state's interest. Such data includes messages processed in the armed forces of modern countries.

The concept of state information security began to appear in literature in the second half of the 20th century. However, this does not mean that information was not previously viewed as a security factor. Reliable, accurate and up-to-date information has always been important for state decisions, especially in the field of security – both external and internal. Following the history of this topic, it can be concluded that, traditionally, information security was understood as a conglomerate of several elements. First, it was to ensure access to information about the environment, potential enemies and allies. Secondly, it is the protection of state information, the disclosure of which would violate the interests of a given entity (Aleksandrowicz, 2018).

The main research problem is contained in the following question: What are the challenges in the area of information security in the armed forces of modern countries resulting from the need to ensure the security of the state and its citizens? This main problem was divided into two more specific questions:

- What is the significance of information security for the security of the state and its citizens?
- What are the challenges facing the modern armed forces in the area of information security?

Based on the analyzes conducted so far and after a preliminary study of the literature on the subject related to the research problem formulated above, the following hypothesis was adopted: the information security of the modern armed forces requires further strengthening and improvement with a particular emphasis on classified information and personal data.

The aim of the research was to identify key problems related to the organization of data security in the armed forces and identify the most important elements requiring change or improvement. Therefore, the factors that have an impact on the analyzed issues have been specified, performing conceptual work on improving data protection in the armed forces.

Research methods and techniques used in the research process are mainly based on a critical analysis of the literature on the subject, legal acts, organizational and competence documents, and synthesis and inference.

2. Terminology-related arrangements

The concept of security is understood in many ways. Therefore, when attempting to define and redefine (extend) the contemporary understanding of security (Mathews, 1989), it should be taken into account that it is a social phenomenon that covers many disciplines and scientific specialties. As Koziej (2006, p.7) analyzes: "security in the static sense is a state of no threats to the subject, a state of peace, certainty, an objective and subjective state: conscious and unconscious. Security in the dynamic sense (acting for the benefit of security) [is] the process of achieving and maintaining the state of no threats and freedom of action". The concept of security in the most general terms should be classified into a group of subjective needs and the need for security should be included in existential needs. Zięba (2008a), on the other hand, identified security with the certainty of existence and survival, possession, functioning and development of the subject, which arises as a result of the creative activity of a given subject and is variable over time, i.e. it has the nature of a social process. The concept of security refers to an extremely complex phenomenon, including not only the state of securing the vital interests of society (individuals, social groups, nation) against direct threats but also ensuring conditions conducive to the undisturbed functioning of all the processes ensuring the sustainable development of protected entities or at least ensuring their stability and sovereignty (Nowakowski, 2009).

As Zięba (2008b, pp.17-18) claims, the safety classification can be adapted according to the following criteria:

- "Subjective: national security and international security.
- Subject: political, military, economic, social, cultural, ideological, ecological, information security etc.
- Spatial: personal security (concerning individual people), local (state-national), subregional, regional (coalition), supra-regional and global (global, universal).
- Time: the state of security and the safety process".

From the point of view of this publication, it seems particularly important to define the term 'national security', which has been defined in various ways over the years:

- A nation is secure when it does not have to sacrifice its legitimate interests to avoid war, and is able, if challenged, to maintain them by war (Lippmann, 1943).
- "National security, however, has a more extensive meaning than protection from physical harm; it also implies protection, though a variety of means, of vital economic and political interests, the loss of which could threaten fundamental values and the vitality of the state" (Jordan & Taylor, 1981, p. 3).

J. Marczak described national security as the overall preparation and organization of the state for the continuous creation of national security, including:

- The legal basis of security.
- National security policy and strategy.
- Civil and military protection and national defense organizations.
- Security infrastructure.
- Education for safety.
- Alliances and international cooperation in the field of security (Marczak, 2008, p. 13).

For the scientific considerations outlined in the title of this article, it seems crucial to define the notions of information and information security. The concept of information is defined in many ways:

- "Information: facts, data, or instructions in any medium or form" (Department of Defense, 2011, p. 175).

- “Preservation of confidentiality, integrity and availability of information. Note: In addition, other properties, such as authenticity, accountability, non-repudiation and reliability can also be involved” (ISO/IEC 27000:2009).
- “The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability” (CNSS, 2010).
- “Information Security is the process of protecting the intellectual property of an organization” (Pipkin, 2000, p. 53).
- ”...information security is a risk management discipline, whose job is to manage the cost of information risk to the business” (McDermott & Geer, 2001, p. 97).
- “A well-informed sense of assurance that information risks and controls are in balance” (Anderson, 2003, p. 309).
- “Information security is the protection of information and minimizes the risk of exposing information to unauthorized parties” (Venter & Eloff, 2003, p. 300).
- “Information Security is a multidisciplinary area of study and professional activity which is concerned with the development and implementation of security mechanisms of all available types (technical, organizational, human-oriented and legal) in order to keep information in all its locations (within and outside the organization's perimeter) and, consequently, information systems, where information is created, processed, stored, transmitted and destroyed, free from threats. Threats to information and information systems may be categorized and a corresponding security goal may be defined for each category of threats. A set of security goals, identified as a result of a threat analysis, should be revised periodically to ensure its adequacy and conformance with the evolving environment. The currently relevant set of security goals may include: confidentiality, integrity, availability, privacy, authenticity & trustworthiness, non-repudiation, accountability and auditability” (Cherdantseva & Hilton, 2013, p. 21).

To define the essence of information security, it should be remembered that there is currently no universal general definition of information security and concepts related to it. However, it is important not to lose its essence at individual stages of gathering and verifying knowledge on information security.

The discussion and analysis of the issues are aimed at organizing the basic conceptual apparatus necessary to carry out research covering the broadly defined realm of security related to the activity, which involves information. It includes:

- Information security.
- Information safety.
- Information security policy.
- Information security threats.
- Information struggle (e.g. between organizations)
- Information warfare (Fehler, 2016, p. 25).

In this context, the definition of cyber security is also important. It can be defined as the application of security measures for the protection of communication, information, and other electronic systems, and the information that is stored, processed or transmitted in these systems with respect to confidentiality, integrity, availability, authentication and nonrepudiation (AJP-3.20).

Information security is very often understood as protecting information against undesirable destruction or preventing its processing. According to Allied Joint Doctrine For Information Operations, information security is the protection of information (stored, processed, or transmitted), and the host systems, against a loss of confidentiality, integrity and availability through a variety of procedural, technical and administrative controls (AJP-3.10).

3. The significance of information security

In recent years, we have had the opportunity to observe an extraordinary increase in the importance of computer science. As a result, it becomes a value, which allows for gaining power, money, security, but also when skillfully used, it may pose a threat to opponents. Nowadays, it is evident how much information influences the functioning of the economic, social and cultural life of today's nations. In modern times, which can be called the "electronic age", what decides and ultimately determines the success of people, organizations, states and communities in almost all spheres of their functioning is information and the ability to use it (e.g., to communicate). Communication is the interconnection of spoken and written words or messages (Cutlip, Center & Broom, 2006).

Information itself is obviously nothing new and people have always processed all kinds of messages. It should be noted, however, that the role of information has changed dramatically compared to previous eras – the agrarian and industrial society. It could be said that "with the globalization and dissemination of modern information technologies, the traditional values of many societies began to change gradually" (Górnikiewicz & Szczurek, 2017, p. 472). According to the same authors, in the modern world, the influence of information on human behavior is decisive: "successful information activities are those that will be tailored to the thinking patterns, behaviors, emotional reactions and perceptions of affected people" (Górnikiewicz & Szczurek, 2018, p. 116). Information has become a kind of raw material, i.e. technologies are used to process it, and information is not used to modify technology. Importantly, since information is an integral part of most of the processes taking place in society, it is already possible to speak of the ubiquitous impact of information-based technologies (Castells, 2008).

The development of technology, homogeneous tele-information networks (Internet), the universality of access devices, and the emergence of social networks makes information a key factor determining knowledge, power, and, importantly, the security of citizens, organizations and entire countries (Liderman, 2012). As a consequence, new dangers closely related to the use of information networks and information systems, e.g. related to computer hacking, espionage, sabotage, vandalism have emerged (Liderman, 2012). The growing role of information in the modern world causes an increase in threats to its security (Nowak & Scheffs, 2010). Apart from traditional information threats, such as espionage, the contemporary era has produced new threats resulting from the development of technology, i.e. computer crimes, cyberterrorism, and subsequent challenges related to technological progress may become a source of previously unknown dangers (Bączek, 2006).

In the near future, along with the further development of new technologies and cyberspace, one should expect a progressive increase in threats to information security and personal data. As a result, the extent to which st/ate institutions interfere in the privacy of an individual will continue to increase. This is evidenced by the words of T. Szczurek: "The technological and information revolution caused by artificial intelligence will change our everyday and professional environment to an unimaginable degree. It is possible to imagine that people will start living in interconnected homes and contact each other on a level that is difficult to understand today. Privacy will disappear completely, and the interference of public safety systems in private life will become a generally accepted norm" (Szczurek, 2019, p. 196). In his paper Hatch (2019, p.84) analyzes that: "to prepare for future challenges across the continuum of conflict, the United States must be postured to manage and exploit the effects of information by conducting and defending against strategic information operations. Toward this end, the United States will need to engage in operations through multiple domains to capture data and process intelligence to identify malign actors and understand their intentions…". This indicates the direction threats to national security may develop. It also shows the importance of information security in modern armies.

In the international aspect, information security issues begin to be regulated in international legal acts. The NIS Directive is the first horizontal legislation undertaken at the EU level to protect network and information systems across the Union. Directive 2016/11481 on security of network and information systems (the "NIS Directive") is the first horizontal legislation that has been undertaken at European Union (EU) level for the protection of network and information systems across the Union. The NIS Directive could be considered a late response to an already exacerbated and well-known problem (Carrapico & Barrinha, 2017). By now, cybersecurity incidents, in the form of cyber-attacks and even cyber warfare, have not only been identified at the expert level but have also frequently captured public attention and been featured on the front pages of the press (Markopouloua, Papakonstantinoua & Hert, 2019).

It is worth mentioning the international organizations responsible for ensuring information security e.g. ENISA - the European Union Agency for Network and Information Security. It is located in Greece (Heraclion Crete) and has an operational office in Athens. ENISA was founded by Regulation (EC) No 460/2004,53 whereas its current regulatory framework consists of Regulation (EU) No 526/2013.54. Since 2004, ENISA has been actively contributing towards warranting a high level of network and information security within the EU (Markopouloua, Papakonstantinoua & Hert, 2019).

4. Information security threats

Information security is often understood as a safe state. The proper identification of threats is now the basis for determining the right strategy not only for survival, but also for the development of each organizational entity. The dangers of information processing are often associated with the development of new technologies. However, threats to information security, cannot be related only to the area of cyberspace and ICT, and thus confuse it with ICT security, which is also referred to as "network security", "network security", "computer security" or "telecommunications security" (Polończyk, 2017, p. 81). The concept of ICT security is narrower than information security, as it only concerns the processing of information in electronic form through computer systems and ICT systems. This concept does not apply to all kinds of data found in the resources of the institution (e.g. library, archives, official collections, etc.).

Information security threats can be divided according to the following criteria:

- Random threats: natural disasters, catastrophes, accidents that affect the information security of the organization (fire in the building where information media are stored).
- Traditional information threats: espionage, subversive or sabotage activities (aimed at obtaining information or offensive disinformation carried out by other people, entities and organizations).
- Technological threats: threats related to the collection, storage and processing of information in ICT networks (e.g. computer crime, cyber terrorism, information warfare).
- Threats related to the civil rights of individuals or social groups (e.g. selling information, providing information to unauthorized entities, violating privacy by the authorities, unlawful interference by secret services, restricting the transparency of public life) (Bączek, 2006, pp. 72-73).

Due to the location of their sources, threats can be divided into:

- Internal (arising within the organization), which include the risk of data loss, damage or modification due to unintentional (erroneous or accidental) or deliberate actions by dishonest users (employees).
- External (generated outside the organization), which include the risk of data loss, data corruption or the inability to be operated by accidental or intentional actions by third parties.
- Physical, where data loss, corruption or the inability to service occurs as a result of an accident, breakdown, catastrophe or other unforeseen event affecting the information system or network device (Żebrowski & Kwiatkowski, 2000, p. 65).

Human activity is the greatest threat to information security. Deliberate threats to the information security system may result from the accumulation of three elements: motive, means of breaking into the system and opportunity, which is access to a computer disk or network. Various methods of hacking into information systems can be used:

- Collusion of several perpetrators.
- Deliberate failure initiation.
- Triggering false alarms.
- Blackmail, corruption.
- Sending surveys, inquiries, proposals to companies.
- Decoding the access password.
- Dictionary attack.
- Network wiretapping.
- Viruses, Trojan horses, logic bombs and other dangerous applications destabilizing the system's efficiency.
- Exploiting security gaps in access to e-mail and information service,
- Security circumvention techniques, e.g. programs that exploit bugs in operating systems and application software.
- Interception of open network connections (Polończyk, 2017, p.83).

These threats will certainly be accompanied with new threats and the methods of breaking into information systems. Therefore, the task of every organization is to constantly monitor threats in the external environment, especially when disseminated data and information can potentially be used to undermine its security. The early identification of potential threats will enable the modification of the existing software so as to eliminate or reduce the likelihood of one of them occurring in the future, thus strengthening the security system of the entire organization.

5. Military information security

Nowadays, in the military sphere, information is seen as a strategic resource. As a consequence, the technologies used for acquiring, processing and protecting important information have become an important part of the potential of the armed forces. It can be concluded that competition for information has become an important part of the armed forces' activities. The advantage gained in this respect may protect against the negative consequences of ‘‘information warfare" and, consequently, ensure the security of the state. Therefore, the challenge for the modern armed forces is to ensure the efficiency and security of information systems, to prevent the effects of crimes against information infrastructure and maintain the ability to obtain key information. Thus, it has become a standard to develop the concept of information operations, create and maintain structures for their implementation. (Nowacki, 2013). Information security is one of the most important military issues of the 21st century. Heavy reliance on computers by the U.S. and its allies for communications, vehicle control, surveillance, and signal processing makes it imperative for U.S. military forces to keep data secure from nations and groups hostile to our national interests (Keller, 2007). The dynamic development of ICT technologies and their effective use on the real battlefield is a highly relevant factor in terms of the functioning of contemporary and future armies (Rybak & Dudczyk, 2019). According to Gerasimov (2019), information technology is in fact becoming one of the most promising weapons. According to Karaman (et al., 2016, p. 6), "the military organizations need to prepare for the worst by establishing resilient and cyber command structure, interoperable and synchronized planning efforts with electronic warfare command. Due to the changing character of wars from conventional to unconventional, symmetric to asymmetric and hybrid wars, cyber operations need to be designed to defense and sustain the military assets”.

An important reason for the expansive growth of the importance of information in the armed forces was the change in the nature of contemporary conflicts in the world from a symmetrical asymmetric, i.e., where the parties have different legal and international status and asymmetrical military potential (Górnikiewicz & Szczurek, 2018). Its feature is the recognition of the superior techniques of violence (Ciszewski, 2010). Notably, the armed forces are confronted with an enemy whose goals, organization, means, and combat methods do not fall into conventional categories. The aim of the entity waging an asymmetric fight is to maximize the effects while minimizing costs through spectacular terrorist actions to cause psychological impact on society (Nowacki, 2013). An asymmetric struggle is often waged with clandestine groups that share an ideological and ethnic bond. Their distinguishing feature is the unconventional use of the available means of destructive influence. Apart from the cheapest weapons and ammunition, they can use a different type of means of influence (Bujak, 2005). As Nowacki (2013, p. 118) notes: "In addition to the significant development of electronic means (microprocessors, electromagnetic pulse generators" logical "bombs, computer viruses) and mass media (Internet, television, radio, press), new possibilities of influencing have appeared, such as beam weapons (energy directed), strobe lights inducing nausea or infrasound causing depression, tension, fear, artificial cheerfulness, slower reaction, heart ailments and imbalances. Moreover, various psychotronic techniques can be used, which induce subjective and objective behavior of people under the influence of suggestions or self-suggestions”.

Information security and information itself are of particular importance when it comes to conducting of hostilities. The ubiquitous role of the mass media in social life is a factor that could significantly contribute to a greater sense of responsibility for the manner of warfare in the future. Thanks to the inquisitiveness of journalists seeking sensationalism, it is increasingly difficult to hide war crimes or other acts prohibited in hostilities. The media also have a major impact on the assessment of war, both in countries directly involved in a given conflict and among the international community. With the development of the mass media and access to information (satellite TV, Internet), the role of psychological activities in future wars will also increase, fostered by the ever-increasing demand for immediate access to information from the battlefield, often in the form of a live report or near real-time. Live coverage and almost unlimited media access to information do not necessarily entail a lack of censorship and manipulation. An example of manipulating information from the battlefield may be the actions of the American services responsible for contacts with the media during the Gulf War. At that time, journalists had to remain in the background, and they were only taken for short, organized trips to the stations where troops were stationed (often far from the front). Furthermore, only carefully selected information was provided. The contemporary recipient is looking for current and interesting information. Therefore, in order to meet these expectations, the media present the most spectacular, often shocking images from the battlefield. Therefore, the parties to the conflicts protect and will protect any information that affects their image in the future (Szczurek, 2009).

The modern armed forces must be ready to face new threats in the information sphere, such as penetrating databases or conducting disinformation activities aimed at paralyzing the state security system. Due to the significant increase in security threats in the information sphere, the armed forces are gradually adjusting their structures to new challenges, focusing more and more on the need to protect cyberspace.

In order to ensure the security of key information, from the point of view of the state's interest and national security, the armed forces focus on: creating the information environment, acquiring new technologies (including especially information technologies), expanding the information structure, which should ensure the safe flow of data in almost real time. This may contribute to strengthening one's own potential to influence and protect more effectively against the undesirable influence of external entities. The infrastructure should be composed of systems and subsystems of obtaining source information, management and control of electronic devices.

Currently, in the armed forces, key information that is subject to special protection is classified information and constitutes a state secret. These are data and messages, the loss of which or transfer to the wrong hands would endanger the security of the state. A wide range of forces are commonly used to protect this type of data and measures ranging from specially designed procedures for accessing and processing these data through physical security. The most important security measures used to protect classified information include: security personnel, physical barriers (lockers and lockers), and a system for controlling people and objects. Of course, all kinds of ICT systems are also subject to special protection, the security of which is becoming an increasing challenge in the era of the development of new technologies.

In recent years, another category of data that is specially protected in the armed forces is the personal data of soldiers, whose personal data may be used at any time for purposes incompatible with the interests of a given state. The protection of these data is therefore a task and a challenge for state institutions, which should select the means and methods of strengthening the protection of soldiers' personalities adequately to contemporary threats. However, recent years have proved that in the era of new threats in the areas of ICT and cyberspace and disinformation activities increasingly used by secret services of many countries, improper data protection may pose a threat to the interest of the state. A breakthrough in the perception of the importance of personal data was the adoption in April 2016 of the Regulation of the European Parliament and of the Council (EU) on the protection of individuals with regard to the processing of personal data and on the free movement of such data, commonly referred to as GDPR (Journal of Laws UE L 119 of 4 May 2016, item 1).

With regard to international examples of the use of information in security aspects, Russia should be mentioned. As Szpyra (2020) analyzes: “Studies have revealed that the Russian Federation, aware of the importance of using “information weapons”, is working on concepts of intensive introduction of foreign information technologies into the sphere of activity of the individual, society and the state”. Since Russia has a natural predisposition to playing the role of a superpower in the face of the dynamic growth of globalization and contemporary geopolitical competition, the use of aggressive forms of information warfare is inevitable (Manoylo, 2003). Meanwhile, both theorists and representatives of the Russian authorities are convinced that the modern information war should also be waged in peacetime in all spheres of social life (Rogozin, 2011). According to Frida Ghitis (2020, p. 1): “Russia was engaging in an incendiary and divisive disinformation campaign in Latin America waged over social media similar to Russia's political interference in the 2016 elections in the US". What is more, Russia has deployed a range of hybrid threats against the energy assets, policies or supplies of NATO allies, and other countries. It has used political and economic leverage, combined with disinformation campaigns, against Bulgaria and Romania to undermine efforts to reduce their dependence on Russian energy sources (Dupuy, et al., 2021).

Therefore, EU countries should strengthen the defense capabilities of information security in times of peace and war.

6. Conclusion

One of the significant consequences of the emergence and dynamic development of modern information technologies is the extension of the objective scope of state security by the category of information security.

In the extensive literature on the subject in the field of security sciences, information security is classified within the subject criterion next to political, military, economic, social, cultural, environmental, ideological and universal security. However, derives directly from public security, perceived as a process involving activities provide protection against prohibited activities. Most often, it is defined as the entirety of activities undertaken to ensure the integrity of the collected, stored and processed information resources, by securing them against unwanted, unauthorized disclosure, modification or destruction (Potejko, 2009).

In today's reality, one of the key challenges facing various states is ensuring information security as one of the most essential elements of national security. Information security plays a special role in the armed forces of modern countries. The protection of important information in military entities has even become a priority. Information began to be treated as a strategic resource of the state; therefore, information resources are a critical element for its functioning. Currently, information is protected at every stage of processing: from obtaining information, through its transmission, storage, analysis and use, to keeping it confidential.

The modern army's dependence on an efficient system of obtaining, processing and distributing information, also in a digitized form, is a fact. The main challenges for the armed forces include expanding the ability to obtain information, analyze it, distribute it, protect its own information resources, as well as the ability to identify and effectively counteract the effects of hostile information operations. The protection of information functioning in cyberspace becomes the greatest challenge. The information security of modern armies is therefore inseparable from information warfare, in which information is both a weapon and a target of attack. It is connected with the armed forces' need to develop their information capabilities in the defensive area (protection of their own information resources and information systems) and in the offensive area (the ability to conduct their own information and disinformation operations).

Declaration of interest – The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this article.

References

1. AJP-3.10 (2009) Allied Joint Doctrine For Information Operations, Nato Standard, NATO/PfP UNCLASSIFIED publication. The agreement of NATO nations to use this publication is recorded in STANAG 2518.
2. AJP-3.20 (2020) Allied Joint Doctrine for Cyberspace Operations, Nato Standard, AJP-3.20, Edition A, Version 1.
3. Aleksandrowicz, T. R. (2018). Bezpieczeństwo informacyjne państwa. *Studia Politologiczne, Volume 49*, pp. 33-50. http://www.studiapolitologiczne.pl/Teoretyczne-i-praktyczne-aspektybezpieczenstwa-panstwa,115397,0,2.html
4. Anderson, J. M. (2003). Why we need a new definition of information security. *Computers & Security*, *Volume 22*, pp. 308-313. https://doi.org/10.1016/S0167-4048(03)00407-3
5. Bączek, P. (2006). *Zagrożenia informacyjne a bezpieczeństwo państwa polskiego*, Wydawnictwo Adam Marszałek.
6. Bujak, A. (2005). Możliwe kierunki zmian w reagowaniu kryzysowym (part I), *Zeszyty Naukowe WSOWLąd*, Volume 2, pp. 85-93.
7. Carrapico, H., & Barrinha, A. (2017). The EU as a Coherent (Cyber) Security Actor? *Journal of Common Market Studies, Volume 55* (6), pp. 1254–1272. https://doi.org/10.1111/jcms.12575
8. Castells, M. (2006). The Network Society: From Knowledge to Policy. In M. Castells, & G. Cardoso (Eds.), *The Network Society: From Knowledge to Policy* (pp. 3-22). Center for Transatlantic Relations.
9. Cherdantseva, Y., & Hilton, J. (2013). Information Security and Information Assurance. The Discussion about the Meaning, Scope and Goals. In F. Almeida, *Organizational, Legal, and Technological Dimensions of Information System Administrator* (pp. 167-169). IGI Global Publishing.
10. Ciszewski, T. (2010). Zarządzanie sytuacją kryzysową w środowisku zagrożonym IED. *Zeszyty Naukowe WSOWLąd*, *Volume 3*, (pp. 205-224).
11. Committee on National Security Systems. (2010). Information value. *In National Information Assurance (IA) Glossary*. (CNSS Instruction No. 4009, p. 38).
12. Cutlip, S. M., Center, A. H., & Broom, G. M. (2006). *Effective Public relation*, Pearson.
13. Department of Defense. (2011). Information. In *Department of Defense Dictionary of Military and Associated Terms* (The Joint Publication 1-02, p. 173).
14. Dupuy, A., Nussbaum, D., Butrimas, V., & Granitsas, A. (2021, January 13). *Energy security in the era of hybrid warfare*. NATO Review. https://www.nato.int/docu/review/articles/2021/01/13/energy-security-in-the-era-of-hybrid-warfare/index.html?fbclid=IwAR2rPTR6fzYPOJIshYO06um9u01-TBhgk4h3bdfbg_UJhgXG4hdkBHEPxDY
15. Fehler, W. (2016). O pojęciu bezpieczeństwa informacyjnego. In M. Kubiak, & S. Topolewski, *Bezpieczeństwo informacyjne XXI wieku* (pp. 24-43). Pracowania Wydawnicza Wydziału Humanistycznego.
16. Gerasimov, V. (2019, March 04). *Vektory razvitiya voyennoy strategii*. Krasnaya Zvezda. http://redstar.ru/vektory-razvitiya-voennoj-strategii/?attempt=1
17. Ghitis, F. (2020, January 23). *Russia's Disinformation War Reaches Latin America, Challenging U.S. Influence*. World Politics Review. https://www.worldpoliticsreview.com/articles/28489/for-putin-venezuela-and-latin-america-are-key-to-challenging-u-s-influence

18. Górnikiewicz, M., & Szczurek, T. (2017). Wschodnioazjatycka, a europejska perspektywa bezpieczeństwa międzynarodowego: wpływ różnic kulturowych na projektowanie polityki bezpieczeństwa ma przykładzie wybranych społeczeństw. In M. Gębska, *Współczesne bezpieczeństwo ekonomiczne i społeczno-kulturowe, Wymiar Międzynarodowy*. Akademia Sztuki Wojennej.
19. Górnikiewicz, M., & Szczurek, T. (2018). *Social Media Wars – The Revolution Has Just Begun*. Military University of Technology.
20. Hatch, B. (2019). The Future of Strategic Information and Cyber-Enabled Information Operations. *Journal of Strategic Security, Volume 12* (4), pp. 69-89. https://doi.org/10.5038/1944-0472.12.4.1735
21. International Organization for Standardization. (2009). *Information technology – Security techniques – Information security management systems* – Overview and vocabulary. ISO Standard No. 27000:2009 (E).
22. Jordan, A. A., & Taylor, W. J. Jr. (1981). *American National Security*, John Hopkins University Press.
23. Karaman, M., Çatalkaya, H., & Aybar, C. (2016). Institutional Cybersecurity from Military Perspective, *International Journal Of Information Security Science, Volume 5* (1), https://www.ijiss.org/ijiss/index.php/ijiss/article/view/174/pdf_33
24. Keller, J. (2007, October 01). *The importance of military information security*. Military Aerospace Electronics. https://www.militaryaerospace.com/communications/article/16706235/the-importance-of-military-information-security
25. Koziej, S. (2006). *Między piekłem a rajem, Szare bezpieczeństwo na progu XXI w*. Wydawnictwo Adam Marszałek.
26. Liderman, K. (2012). *Bezpieczeństwo informacyjne*, Wydawnictwo Naukowe PWN.
27. Lippmann, W. (1943). U.S. Foreign Policy: Shield of the Republic. In S.E. Corwin (Ed.), *American Political Science Review* (pp. 259-262). Cambridge University Press. https://doi.org/10.1177/000405736440010021
28. Manoylo, A. (2003). *Gosudarstvennaya informatsionnaya politika v osobykh usloviyakh: Monografiya*. MIFI. http://www.klex.ru/jlj
29. Marczak, J. (2008). Powszechna ochrona i obrona narodowa. In R. Jakubczak (Ed.), *Podstawy bezpieczeństwa narodowego Polski w erze globalizacji* (pp. 37-48). AON.
30. Markopoulou, D., Papakonstantinou, V., & Hert, P. (2019). The new EU cybersecurity framework: The NIS Directive, ENISA's role and the General Data Protection Regulation, *Computer Law & Security Review, Volume 35* (6). https://doi.org/10.1016/j.clsr.2019.06.007
31. Mathews, J. (1989). Redefining Security. *Foreign Affairs, Volume 68* (2), (pp. 167-177).
32. McDermott, E., & Geer, D. (2001). Information security is information risk management. In B. Blakley, McDermott, & D. Geer, *Proceedings of the 2001 Workshop on New Security Paradigms* (pp. 97-104). Association for Computing Machinery. https://doi.org/10.1145/508171.508187
33. NIS Directive - Directive 2016/1148 of the European Parliament and the Council concerning measures for a high common level of security of network and information systems across the Union.
34. Nowacki, G. (2013). Znaczenie informacji w obszarze bezpieczeństwa narodowego. *Nierówności społeczne a wzrost gospodarczy, Volume 36*, pp. 107-123.
35. Nowak, A., & Scheffs, W. (2010). *Zarządzanie bezpieczeństwem informacyjnym*, AON.
36. Nowakowski, Z. (2009). *Bezpieczeństwo państwa w koncepcjach programowych partii parlamentarnych w Polsce po 1989 roku*. Towarzystwo Naukowe Powszechne.
37. Pipkin, D. (2000). *Information security: Protecting the global enterprise.* Hewlett-Packard Company.

38. Polończyk, A. (2017). Zagrożenia bezpieczeństwa informacyjnego na przykładzie Krajowej Mapy Zagrożeń Bezpieczeństwa. In H. Batorowska, & E. Musiał, *Bezpieczeństwo informacyjne w dyskursie naukowym* (pp. 79-94). Uniwersytet Pedagogiczny w Krakowie.
39. Potejko, P. (2009). Bezpieczeństwo informacyjne. In K. A. Wojtaszczyk, & A. Materska-Sosnowska (eds.), *Bezpieczeństwo państwa* (pp. 209-220). Oficyna Wydawnicza ASPRA-JR.
40. Rogozin, D. (2011*) Voyna i mir v terminakh i opredeleniyakh.* Voyenno-politicheskiy slovar. Veche.
41. Rybak, Ł., & Dudczyk, J. (2019). Increasing the information superiority on the modern battlefield through the use of virtual reality systems. *Security and Defence Quarterly, Volume 25* (3), pp. 86-98. https://doi.org/10.35467/sdq/105998
42. Szczurek, T. (2009). *Konflikty zbrojne.* Wojskowa Akademia Techniczna.
43. Szczurek, T. (2019). *Wyzwania dla bezpieczeństwa – niepewna przyszłość między zagrożeniami a szansami*. Wojskowa Akademia Techniczna.
44. Szczurek, T., Walkowiak, M., & Bryczek-Wróbel, P. (2020). *Military, non-military and paramilitary threats*. Military University of Technology.
45. Szpyra, R. (2020). Russian information offensive in the international relations, *Security and Defence Quarterly, Volume 30* (3), pp. 31–48. https://doi.org/10.35467/sdq/124436
46. Venter, H. S., & Eloff, J. H. P. (2003). A taxonomy for information security technologies. *Computers & Security*, *Volume 22* (4), pp. 299-307. https://doi.org/10.1016/S0167-4048(03)00406-1
47. Zięba, R. (2008a). *Bezpieczeństwo międzynarodowe po zimnej wojnie*, Wydawnictwa Akademickie i Profesjonalne.
48. Zięba, R. (2008b). Pozimnowojenny paradygmat bezpieczeństwa międzynarodowego, In R. Zięba, *Bezpieczeństwo międzynarodowe po zimnej wojnie*. Wydawnictwo Akademickie i profesjonalne.
49. Żebrowski, A., & Kwiatkowski, M. (2000). *Bezpieczeństwo informacji* III Rzeczypospolitej. Oficyna Wydawnicza Abrys.