PRZEGLĄD BIBLIOTECZNY 2025
e-ISSN 2545-2487

HANNA BATOROWSKA
Faculty of National Security
War Studies University in Warsaw
e-mail: h.batorowska@akademia.mil.pl
ORCID 0000-0001-6759-5094

INFORMATION SECURITY AWARENESS – BETWEEN IGNORANCE AND CONSCIOUSNESS OF THREATS

Hanna Batorowska – habilitated doctor of humanities, since 2022 a university professor at the Faculty of National Security of the War Studies University in Warsaw, previously an extraordinary professor at the Institute of Security Sciences and the Institute of Information Sciences at the University of the National Education Commission, Krakow. Member of the International Society for Knowledge Organization ISKO.

Her research interests include: issues of information security, analysis and information processes, security culture, information and knowledge management, as well as information culture and scientific information. She is the author or co-author of several monographs such as*: Kultura bezpieczeństwa informacyjnego w środowisku walki o przewagę informacyjną* (*The Culture of Information Security in the Environment of the Struggle for Information Advantage*) (Kraków 2021), *Media jako instrument wpływu informacyjnego i manipulacji społeczeństwem* (*Media as an Instrument of Informational Influence and Manipulation of Society*) (Kraków 2019*), Od alfabetyzacji informacyjnej do kultury informacyjnej. Rozważania o dojrzałości informacyjnej* (*From Information Literacy to Information Culture. Reflections on Information Maturity*) (Warsaw 2013), *Kultura informacyjna w perspektywie zmian w edukacji* (*Information Culture in the Perspective of Educational Changes*) (Warsaw 2009), among others, and the editor of monographs dedicated to security from the series Man in the World of Information, such as*: Bezpieczeństwo informacyjne i medialne w czasach nadprodukcji informacji* (*Information and Media Security in Times of Information*

Overproduction) (Warsaw 2022), *Bezpieczeństwo informacyjne w dyskursie naukowym* (*Information Security in Scientific Discourse*) (Kraków 2017), *Walka informacyjna. Uwarunkowania – Incydenty – Wyzwania* (*Information warfare. Conditions - Incidents – Challenges*) (Kraków 2017), *Kultura informacyjna w ujeciu interdyscyplinarnym. Teoria i praktyka.* Tom II (*Information culture in an interdisciplinary perspective. Theory and practice,* Volume II) (Kraków 2016), Volume I (Kraków 2015), as well as numerous scientific articles dedicated to media and information education, information architecture, information technology, and publishing issues. She is the author of over 260 scientific publications and has actively participated in over 200 international and national scientific conferences.

KEYWORDS: Information security awareness. Information security culture. Resilience to threats. Information awareness. Education for security.

ABSTRACT: **Thesis/Purpose** – The article reflects on the impact of the information security culture on the development of a subject's information security awareness. It highlights the factors influencing this awareness. It attempts to justify the thesis that neglecting the task of cultivating a security culture among youth in security education may lead them to experience information security in an irrational manner. It is also assumed that society's ability to respond to threats in the information environment requires it to be intellectually and mentally prepared, as well as to undergo institutional education in the field of security culture. **Method** – The method of critical analysis of the literature on the subject was used, based on materials also derived from scientific debates conducted by experts in information security and cybersecurity during the current year's national scientific conferences. **Results/conclusions** – education for information security positively influences the shaping of the information security awareness of a subject by developing mature information attitudes and behaviors. Therefore, if we do not consider the need to shape a culture of information security in education for security, this strengthens a sense of information security in society built by omitting the sphere of mental culture including values, principles, norms, knowledge, ways of thinking, and wisdom, and is therefore mainly limited to the sphere of material culture.

INTRODUCTION

"Awareness" is a psychological category indicating a person's consciousness of the facts that have occurred, phenomena happening in the surrounding world, and internal states, allowing them to express a subjective evaluation of the current situation and recognize it as meeting expectations or not. It is a type of subjective experience, e.g., of self-worth, the meaning of life, belonging, and a sense of security (Marciniak, 2009, pp. 56-65). In the case of actions that are inconsistent with one's own value system, the individual may feel guilt, and when they conform to it, they usually feel satisfaction. Security awareness as an emotional state related to fear for the individual's safety pertains to the sphere of his individual and collective consciousness and the way of perceiving and assessing phenomena that may pose a threat to them. It is felt individually by each person, depending on their psychological predispositions or differing perceptions of risk (Polończyk, 2018, p.284).

Awareness can also refer to the comfort of an individual's functioning in an information environment, and it is influenced by legal, economic, political, social, and cultural conditions related to information management in that environment. The sense of informational security largely depends on the knowledge possessed about the mechanisms governing the flow of information, the possibilities of accessing information and its quality, the quality of information services, the reliability of telecommunication systems and guarantees of safe use of them, one's own effectiveness in navigating the infosphere thanks to possessed technological and intellectual skills, as well as the possibility of receiving support in case of various types of threats arising in that environment. In scientific publications, awareness of security is often the subject of discussions among researchers representing various disciplines (psychology, pedagogy, sociology, security sciences), but it rarely refers specifically to information security. Although it is generating increasing interest among students and doctoral candidates in fields related to security, this does not translate into their undertaking interdisciplinary research in this area. The technological perspective is often preferred, which leads to the treatment of information security awareness as a concept reflecting sufficient technological competencies that ensure a person the desired level of security for their information resources as well as the technology and equipment processing the data contained therein.

Meanwhile, information security awareness related to the subjective assessment of the level of this security by a subject depends not only on their knowledge and technological skills but also on many other factors, such as age, level of education, activities undertaken in cyberspace and the real world, professional work performed, acceptance of uncertainty and adaptation to change, and willingness to take risks. It also depends on the intellectual and mental preparation of the individual and the level of their security culture, including information security culture.

The last, as a component of security culture, creates an environment of human security and determines the sensitivity and 'heightened awareness' to threats stemming from the infection of the information environment. It reflects the society's preparedness to identify such situations in its surroundings and the development of the need for appropriate responses to them, the resilience of society to informational attacks, and its level of awareness regarding contemporary information warfare.

Information security culture can be defined as the sphere of human activity shaped by information awareness and the way of thinking about information security; values, norms, and rules indicating the legitimacy of a security culture that allows one to perceive challenges, opportunities, and threats in the local and global information space; attitudes that influence the sensitization of society to the importance of information security and the shaping of behaviors characteristic of mature information users who are co-responsible for this security (H. Batorowska, 2021, pp. 15-16). This culture requires training in awareness of threats, which is dependent on the level of informational maturity achieved by the individual. One cannot be aware of threats without developing situational awareness that allows for perceiving elements of the environment and understanding their significance for the development of upcoming events, without developing the ability to forecast threats, without showing the need to act with reason, without maintaining professionalism, wisdom, and directed intelligence, and without being able to manage information and risk as well as to act and communicate effectively.

Unfortunately, the sense of information security is often based on incomplete knowledge and stems from declarative rather than actual readiness for individual information management; it characterizes individuals who do not understand the mechanisms threatening information security or who ignore them (H. Batorowska, 2016, pp. 61-89; H. Batorowska, 2017, pp. 177-191). Information security awareness formed on the basis of objective premises should be the result of education and upbringing for security that takes into account the education of information security culture for the entire society in its programs (Fehler, 2023, pp. 212-213).

SUBJECT AND AIM

The aim of the undertaken research is to show the factors on which the awareness of information security of a society depend, which is why the analysis focuses on this very awareness. The main research problem is formulated as a question: does the information security culture of a subject have an objective influence on shaping its sense of information security?

This requires clarification through detailed problems expressed in these subsequent questions:

- Are concepts such as information security culture, information awareness, information security awareness, and information security differentiated or treated synonymously?
- Does the quality of life of modern man depend on his awareness of information security?

- Does security culture influence the strengthening of the individual's and group's awareness of information security?
- Does awareness of the risks associated with immature information behaviors influence their elimination?
- What competencies must a subject possess to objectively perceive information security?
- How does information security education impact the shaping of information security awareness based on rational and objective premises?

In reference to the above, a research hypothesis was formulated, which relates to the assumption of neglecting the need to shape a culture of safety in security education, which contributes to experiencing information security in an irrational way, not taking into account objective criteria for its assessment. It was also assumed that such an awareness is an effect of subjects functioning in their closed information worlds; that information-immature societies characterized by a sense of security not based on critical analysis of facts become an easy target for info-aggressors; that effective communication is the most important element in shaping information security awareness and building resilience to threats in the infosphere; that the ability of a society to respond to threats in the information environment requires intellectual and mental preparation; and that the evaluation of information security awareness among members of various organizations should also be subject to information security audits.

IRRATIONAL AND CRITICAL APPROACHES TO INFORMATION SECURITY AWARENESS

Information security awareness is most often understood in a way similar to the common definition of security: as a state of consciousness in which a person feels free from threats generated by the information society and by digital civilization; as a sense of comfort from functioning in harmony with the information environment and in a state without fear for the infosphere and for the safety and quality of the information resources they use; as the absence of threats to health, property, and life resulting from information attacks; as mental comfort enabling the realization of life goals; and above all, confidence that in sudden and unforeseen circumstances they can count on the help and support of other entities and institutions established for this purpose, e.g. those arising from equipment failures, network issues, cyberattacks, and cybercrimes (Pieczywok, 2012, pp. 22-23). Identifying these threats can occur as a result of an objective, fact-based approach to the problem of security and its scientific analysis, or an emotional, stereotypical interpretation of incomplete and selectively chosen information. The effect of these actions may be an illusory sense of security arising, for example, from ignoring objective facts, or a sense based on the awareness of the existence of a threat that results from critically perceiving elements of the environment, understanding their significance, and predicting the development of the situation, meaning having a well-developed situational awareness.

Indicating the differences between these two approaches to the concept of information security awareness requires, first and foremost, answering the question: are concepts such as information security culture, information/informatic awareness, information security feeling, and information security distinct or treated interchangeably? Treating these concepts synonymously would mean that the scale of arbitrariness in experiencing information security could oscillate between a purely technical way of identifying threats and a humanistic interpretation of difficult situations occurring in reality. Moreover, treating components of a whole (e.g., information awareness) on par with the whole (in this case with safety culture) introduces chaos in understanding the relationships between them. Such imprecision in terminology would further hinder the subject's assessment of threats and result in an extreme perception of them as either a complete lack of threat or a state of real danger.

In the subject literature these concepts often appear as substitutes, e.g., information security culture, despite its precise definition (Cieślarczyk, 2022, pp. 136-137), is still being replaced by the concept of informatics security culture, information awareness or informatics, and informatics competencies (skills), less frequently information-related skills. According to this nomenclature, it should be acknowledged that proficiency in using information and communication technologies reflects a person's culture in this area. They achieve a satisfactory level of their own information security awareness due to the belief that they possess sufficient technical knowledge and an understanding of their own role in data protection, equipment, and technologies they use, as well as the effectiveness of the security measures they employ (K. Batorowska, 2023). From this perspective, they also assess the professional and private informational environment in which they operate as being information-secure.

Information security audits conducted systematically in various companies by both internal and external auditors raise the awareness among members of the organization and their management that the declarative knowledge and skills of employees, as well as their attitudes towards securing information systems and protecting information, do not always align with actual competencies and responsible behaviors aimed at protecting information and are not always necessarily related to real, objectively existing threats (Feliński, 2024). As studies indicate, people tend to exaggerate threats or to marginalize them, thereby explaining their fears of them or justifying their incompetence in identifying them or their disengagement in combating them, thus avoiding responsibility for their consequences (Łabędź, 2018, pp. 46-47). Ignoring this observation contributes to the management team's establishment of an illusory sense of information security (K. Batorowska, 2024, pp. 287, 290, 304-306), especially since the recorded problems related to information security are not analyzed within the organization along with a diagnosis of the information security awareness of employees.

A simplified definition of the concept of information security awareness has been formulated as "a state in which the information user does not feel threats resulting from: a) contact with low-quality information and b) loss of all or part of the accumulated information resources. Instead, they are accompanied by a sense of calm, security, and satisfaction with the experienced level of information security, as well as a belief in having the resources (e.g., knowledge and skills related to assessing the quality of information) necessary to take appropriate actions in the face of a crisis situation" (Motylińska & Pieczka, 2022, p. 128).

This feeling can be considered from the perspective of the intentional, active functioning of the subject in the informational space, and thus its responsible, mature informational behaviors, which are identified as pro-information ecological (an objective perspective). They directly or indirectly influence the informational security of the subject and the environment in which the subject operates. They are a concern for those who raise and educate the young generation, who strive to shape a culture of security, including elements such as informational awareness and a system of values, attitudes, and behaviors on which societal resilience to security threats can be built.

The question posed at the outset about how the sense of security can affect the building of a person's resilience to threats requires clarifying the concept of resilience and linking it to the subject who properly perceives the state of threat, thus objectively analyzing the crisis situation they find themselves in. Such a subject utilizes the knowledge gained to overcome obstacles, and the awareness of the availability of resources that support them in this endeavor increases their motivation to strive for regaining balance and returning to the state enjoyed prior to the crisis. In a monograph dedicated to the resilience of cities to threats, the main concept is defined as a process of "reducing vulnerability, that is, weaknesses arising from the occurrence of events related to a wide range of threats [including informational], in such a way that one can quickly and efficiently return to normal functioning. (...) resilience should not only encompass recovery and restoration to the original state but also an entry into a new, higher level characterized by stronger resilience to new, often unpredictable crises or changes" (Kowalkowski et al., 2025, p. 8).

This means that the critically built (objective) information security awareness is associated with the individual experiencing a sense of security as a result of their activities and the actions taken by their social and cultural environment for safety. This awareness comes from the subject's belonging to socially, professionally, and digitally included groups, from the state's guarantee of a social information order, from a satisfactory level of information services, from accessible support in situations of cyber threats, and from an overall sense of stability in functioning within the information society. Therefore, the presence and activity of organizations supporting local governments in diagnosing social needs, including informational ones, creating solutions, and implementing public policies such as a transparent information policy, are crucial for the desired quality of life of residents in the infosphere. The correct relationship between the real state of security and the sense of security felt by people depends on their access to information, specifically the actions taken by authorities to build social information security based on a system of social norms, processes, systems, and information resources that are capable of meeting the informational needs of society. The implemented model of social information order must take into account:

- the actual hierarchy of social functions of information implemented by state bodies;
- the scope of mutual rights and obligations regarding information for citizens and other state entities and the manner of their implementation;
- the scope and manner of implementing the economic functions of information;
- the information asymmetry between citizens and organizational units, its magnitude, structure, and the consequences arising from the information gap as well as the state's policy concerning the information gap;
- policy in the field of information quality control;
- policy in the field of creating and developing the information infrastructure of society and the economy, including the scope of information available as a public good (Oleński, 2015, p. 37).

Understanding the importance of social information governance by society is the starting point for shaping information security awareness in a rational manner.

FACTORS INFLUENCING THE FORMATION OF INFORMATION SECURITY AWARENESS

Information security awareness is a variable category. A subject may experience an awareness of security at different levels on a scale that they adjusts according to their needs and understanding of security. The factors influencing this awareness are particularly important, as they depend on the assessment of the quality of one's own life and the fulfillment of material and spiritual needs. Justifying the relationship between the quality of life of contemporary individuals and their security awareness is not straightforward, as security is not only a comfort but a basic human need, and thus lacking a sense of security makes it difficult for a person to engage in various activities that enable them to achieve life goals. A subject who can meet their needs feels safe and fulfilled, and is satisfied with the situation they find themselves in. If these needs are related to ensuring existence for themselves and their family, access to healthcare, stability and professional fulfillment, opportunities for social and intellectual development, self-education, and hobbies, they identify achieving these assets with quality of life and simultaneously a high level of security.

The type of threat influencing this sense is also important, as not all threats evoke the same level of anxiety and fear in the subject. In terms of the subjective feeling of safety, four states of security are possible: when there are no threats or when a real threat exists, and these states are accurately perceived by the subject; when there is a real threat, but it is not noticed or is ignored by the person; or when there are objectively no threats, but they are subjectively perceived by people and classified as actually existing (Frei, 1997, p. 133). The author, analyzing objective and subjective states of threat, distinguishes states of: security, lack of security, false security, and a state of obsession.

Examples of threats affecting the sense of information security include threats related to random hazards (equipment failure, lack of internet access), traditional information threats (information overload, manipulated content on the internet and in traditional media), technological threats (account hacking, receiving unwanted messages – phishing, internet fraud), and threats related to the civil rights of individuals or social groups (personalized content on the internet, including advertisements based on the user's previous actions) (Motylińska & Pieczka, 2022, p. 138).

Increasingly, when analyzing information security threats, the area of threats arising from the information revolution related to information manipulation, surveillance of individuals, loss of privacy and identity is being included. According to Daniel Solove's taxonomy of the right to privacy, violations can be analyzed in relation to processes associated with information gathering (surveillance, interrogation), information processing (collection, attribution, uncertainty, reuse, denial of access), information dissemination (breach of confidentiality, disclosure, exposure, facilitating access to others, blackmail, appropriation, distortion), and the process of invasion (physical intrusion, decision-making influence) (Solove 2006, p. 490). Diagnosing these threats requires the subject to possess competencies that have only been minimally developed so far and are related to building a culture of threat awareness. They enable efficient and prudent navigation in the information environment, thanks to:

- educated situational awareness,
- ability to forecast threats,
- informational maturity,
- skills in reasoning (understanding the need for reason),
- professionalism and effectiveness of actions,
- wisdom and directed intelligence,
- high morale of individuals, institutions, organizations,
- knowledge and proficiency in information and knowledge management,
- skills in effective communication.

New threats are closely related to the consequences of the information revolution, which on one hand contributed to the dynamic development of humanity and the increased awareness of the importance of knowledge and science, but on the other hand led to the emergence of threats resulting from a crisis in the intellectual sphere. The discourse undertaken in this area (Auleytner & Kleer, 2015) has revealed problems related to a superficial understanding of the threats associated with surveillance, privacy, information warfare, and the pursuit of informational advantage, as well as the paradox arising from mass education and the simultaneous superficiality of the knowledge of educated individuals, the coexistence of knowledge and ignorance on equal terms, and the abdication of wisdom in favor of mediocrity and pragmatism. The revaluation of the most desired life goals has led to intelligence no longer being a cardinal value for the majority of subjects, and the information revolution drives information users to a state of internal dispersion, diminishes their need for deeper reflection on the information they acquire, and leads to intellectual limitations. At the same time, a new class of people known as the precariat is emerging, well-educated but with an unstable professional situation, threatened by exclusion, and with a very low sense of security. The social layer that should face these problems is the intelligentsia, which guarantees survival in a fluid, changing, unpredictable environment, and should be a safeguard for people's survival in times of turmoil and post-truth (Auleytner & Kleer, 2015, pp. 9, 13-23), but it belongs to a layer that is being gradually eliminated from the landscape of the modern world and replaced by its caricatured formation.

All these issues are significant in building an individual's sense of security in the new information space. Facing threats that undermine a sense of informational security requires informational maturity, which means responsible behavior. However, merely being aware of the harmfulness of immature informational behaviors is insufficient for an individual to avoid them or engage in preventing them. The relationship between engaging in activities that do not sufficiently protect personal data, one's identity, or privacy, and that manifest in other risky behaviors, and knowledge about the consequences of such behaviors is very complex. It is difficult to explain the mechanism of this complexity without referring to the so-called "privacy dilemma or paradox" (the simultaneous rationality and irrationality of attitudes), the security dilemma (the choice between protection and consent to surveillance and the restriction of freedom), or the discrepancy between the declarative approach to knowing and adhering to security procedures and irrational behaviors that result in real threats to security. The analysis conducted by C. Hoffmann, C. Lutz, G. Ranzini of the phenomenon of behaviors threatening individual privacy resulting from the discrepancy between the declared attitude of a rational approach to privacy issues and "carefree" behaviors that indulge in the widespread practice of self-disclosure in cyberspace can also be related to behaviors associated with information protection and the informational environment, e.g., in the context of consumer surveillance or the culture of digital narcissism (Hoffmann, Lutz & Ranzini, 2016; Bauman & Lyon, 2013; Szpunar, 2016). In this environment, we also deal with the phenomenon of so-called "cynicism about privacy", where the individual sees no necessity in scrupulously adhering to procedures, since they are unable to protect their privacy anyway. "Privacy cynicism" reflects "an attitude of uncertainty, helplessness, and distrust towards data processing by online services, which makes privacy-related behaviors subjective and futile" (Hoffmann, Lutz & Ranzini, 2016, pp. 1-4). And this threatens the information security of people accepting such an attitude. According to A. Westin, a subject's attitude towards privacy protection can take the form of a carefree attitude characterized by a low level of concern for their own privacy (information security). It can also have a fundamentalist dimension when the subject decides to defend privacy at all costs, even at the expense of forgoing potential gain. The most desirable attitude is a pragmatic one, where the subject realistically assesses their own actions and their surroundings related to privacy protection (Westin, 1996, pp. 272-275) and ensures the information security of the environment in which they operate.

The discussion on the irrational attitudes of contemporary consumers towards the phenomenon of consent to the loss of privacy and information security was undertaken by Z. Bauman and D. Lyon (Bauman & Lyon, 2013, pp. 53-54). Noticing the trend of treating privacy as a commodity that needs to be well sold in order to ensure self-promotion and approval from the digital audience, they concluded that surveillance is not currently seen in terms of a security threat. Being watched and monitored does not bother most young people; rather, it becomes a goal of their activities online, as they consider exclusion to be the true danger, while surveillance is seen as an antidote to that exclusion. The voluntary consent leading to a loss of informational security arises from such a creation and management of reality, where consumers of new information and communication technologies perceive their state of subordination as an expansion of their freedom, self-determination, autonomy, and empowerment (Bauman & Lyon, 2013). The widespread ignorance of this problem can lead to a situation where individual control and privacy protection become impossible. This is especially so as the two previously opposing spheres – private and public – have started to overlap, generating new threats in the area of information security (Młynarska-Sobaczewska, 2013, p. 50).

The above issue seems particularly interesting in the context of having a specialized education which individuals engaging in risky behaviors in both private and professional information environments possess. It seems that the knowledge they have should exert a significant influence on their lifestyle, serving as a warning system against the consequences of cyber threats and various information diseases. Engaging in behaviors that threaten the loss of data, identity, or system infection, despite having a sufficient amount of knowledge about possible threats, boils down to the necessity of choosing between convenience, ease, profit, desirable immediacy, and security, especially in the long term.

That is why it is so important to build a culture of risk awareness in society. It requires strengthening desirable attitudes and behaviors towards safety and understanding one's own psychology to identify personal weak points. However, one can lack the traits mentioned above and yet have a high sense of security, evaluating one's quality of life based on the ability to access information, technology, and information services in an unlimited and immediate manner, the quality of those services and their low costs, flexible regulations and rules, a diverse range of offerings, etc. The overwhelming need for information consumption breaks the barriers that protect the community in virtual worlds from surveillance and the loss of privacy, identity, personal data, and sensitive information. The obsessive demand for immediate access to informational goods and being in the media spotlight causes a person to consciously give up security in this world in favor of technological conveniences and the ability to arouse interest from a strictly undefined audience. They sell their intimacy and privacy in exchange for illusory popularity. The culture of digital narcissism destroys this community's sensitivity to threats in cyberspace, but in return, it offers an illusion of happiness, popularity, and a sense of community with other anonymous internet users yearning for fame and publicity. At that point the boundary shifts between what has hitherto been meant by the private sphere and the public sphere, and between what is safe and what is dangerous. The sense of security shifts its place on this scale, meaning that the subject has more freedom and less certainty whether that freedom will ultimately be beneficial for them. Contemporary media, in providing the desired freedom, do not warn about the dangers. It is important to maintain people's security awareness at a high level, regardless of the real situation of the individual, and for the individual to subjectively evaluate that sense positively.

If access to reliable information is hindered and the subject is unaware of the threats arising in their environment, they may still feel safe and fulfilled, even though this sense of security is illusory. Moreover, information (in) security can sometimes be imperceptible, and the initiated information attacks can go unnoticed by the victim for a longer period, in which case they will not be aware that their information security awareness is false, as in reality only their information assets have been attacked.

The culture of threat awareness is therefore an important component of the security culture. It focuses on sensitizing and strengthening people's resilience to danger and their ability to counter threats, constituting in this context a capital of national security.

BUILDING A SOCIETY OF INFORMATION SECURITY CULTURE

Information security culture can be seen as the "characteristic relationship of a given physical or legal subject to data, information, knowledge, and wisdom, among other values, as well as the ability to use them for worthy purposes with the safety of oneself and other subjects with the more immediate (in terms of time and space) or more remote environment in mind" (Cieślarczyk, 2022, p. 230). It consists of elements such as the awareness of the security subject, values and attitudes that enable the building of a security environment, and behaviors that guarantee the maintenance of security, all of which influence information management security and relate to the way information is perceived, created, and used (H. Batorowska, 2021, pp. 15-16).

Information security culture – supporting the construction of a social order of information, preparing management staff to practice transparent information policy, directing the organizational culture towards respecting information security procedures and policies – strengthens social information security, becoming one of the guarantors of national security. It can be considered the foundation for building a society with a culture of information security that is knowledgeable about disinformation techniques and methods, understands the nature of social engineering attacks, and recognizes manifestations of manipulation by individuals and groups spreading destruction. This is a society composed of users of the infosphere who are aware, experts in identifying discreditation, degradation, and deprecation of post-truth, capable of limiting surveillance activities and participating in building a national culture of security and power. It is a society that monitors and holds decision-makers accountable, represented by citizen journalism, online journalism, support groups exposing hidden goals of technological development, think tanks, etc. (H. Batorowska, 2021, p. 98).

The society of information security culture consists of security subjects that serve as a model of civic attitudes and social responsibility, particularly through taking care of cultural security and understanding its importance for achieving victory in the ongoing information war. In this sense, this culture is a value that should be associated with the informational maturity of the security subject. An informationally mature individual acts in accordance with a value system that requires responsibility for actions taken in the informational environment.

Information security culture thus characterizes individuals who are able to think and act in a transcendental dimension, to ask questions, to create forecasts of the development of phenomena, situations, events, and to build visions, scenarios of a future in which there will still be room for humanity despite the unimaginable advancement of information technology and the tendency to trust systems based on artificial intelligence and algorithms (H. Batorowska, 2021, p. 98).

Preparing society to build a sense of information security based on rational premises is a task mainly placed before education for security, taking into account the information security culture for both youths and adults in its programs, as well as the way they are raised in information. The functions of this culture correlate with the tasks facing education for security, such as:

- shaping desired informational behaviors characterizing maturely informed citizens,
- supporting activities aimed at building social order and social informational security,
- adapting entities for sustainable functioning in a hybrid informational environment and overcoming threats generated by the informational society,
- raising societal awareness of threats generated by the informational environment and maintaining the desired level of resilience in conditions of informational warfare directed against the nation,

- building a strong culture of national security, including a culture of awareness of informational threats,
- preventing informational diseases, promoting cyber hygiene,
- respecting the principles and procedures of information security and codes of information ethics by the entity,
- inclusion in activities related to information verification and monitoring threats arising from disinformation transmissions.

The society of information security culture should operate based on a model of an action system, in which elements such as information security culture, morale, wisdom, and legal culture are its main components. Such models were developed by Marian Cieślarczyk, but in the context of considerations regarding information security awareness one deserves special attention. This is an ideal model of an action system that reflects the characteristic attitudes, behaviors, values, and actions of security subjects in a given situation.

The model shown here illustrates the significance of wisdom, courage, responsibility, freedom, knowledge, and friendship as elements that influence safety awareness among group members, their way of thinking about safety, and the behaviors that allow for the construction of a shared security environment. In the case of a high level of information security culture, the situational assessment of the environment by the subject is accurate, based on rational behaviors and focused on action or collaboration, with attitudes being appropriate to the situation because there are no perceptual or reception disturbances, all of which fosters forecasting and predicting situations. This model correlates with the reflective-action model of functioning proposed by M. Cieślarczyk, characterized by a high level of security culture, and indicates that an appropriate level of information security culture affects all spheres of life and society's safety, and is a prerequisite for ensuring information security. The subject positioned within it maintains a relative balance between the emotional sphere of attitudes and the rational sphere, thanks to the knowledge and wisdom possessed, as well as the ability to reflect and anticipate, and by adhering to principles (norms and values) that serve as regulators in difficult situations. Functioning rationally in the environment, based on accepted norms, values, and attitudes, they can effectively utilize data, information, knowledge, and wisdom, which fosters the development of prospective thinking, anticipating changes in situations and the consequences (or lack thereof) of their activity, making appropriate decisions, and taking preventive and preparatory actions. However, before situational information prompts the subject to take action, it passes through a "filter" of wisdom, and within it through a system of norms and values (principles, rules) which guide the subject in various situations by skillfully combining individual and collective good. Such actions, according to Cieślarczyk, promote the adequacy of situational assessments and lead to making accurate, long-term decisions as well as efficient, effective actions and fostering collaborations of individuals and organizational structures in accordance with established procedures (Cieślarczyk, 2022, p. 233). The negative effects of a low level of information security culture lead to:

- difficulties in handling data, information, and knowledge, resulting in disruptions in perception and thinking, as well as difficulties in assessing situations,
- emotional behaviors that hinder collaboration and generate unpredictability,
- a deficit of reflection, foresight, and preparation for current or future situations,
- a deficit of empathy, a prevalence of selfish attitudes, and cunning behaviors aimed at short-term gains (Cieślarczyk, 2022, p. 234).

Comparing all the models of information security culture presented by the researcher, it is important to note the central positioning of wisdom as an element, highlighting its critical role in all spheres of security (spiritual, organizational, and material) and the important functions that wisdom fulfills in relation to these spheres: stimulating, regulatory, and integrative.

CONCLUSIONS

As shown, achieving a satisfactory level of information security awareness by an individual depends not only on having appropriate material, organizational, legislative, political, and cultural assets but also on their intellectual competencies that allow for monitoring the information space and identifying emerging threats through developed situational awareness, as well as on their perception of the world and response to threats, and on the cultivated culture of information security. Building this sense of security is a process that requires effective communication between society and decision-makers, based on verified information from credible sources, its critical interpretation free from persuasion, and awareness of any manifestations of manipulation of public opinion in conditions of ongoing informational warfare and the rising influence of post-truth.

Research on the analysis of the sense of information security within society should also be extended to analyze this state among company employees and incorporated into audit programs related to information security within the organization. This would highlight that not only technology and IT can ensure information security within a company, and that achieving compliance with security standards and regulations should not be treated as a goal in itself, as it leads to a false assessment of the level of security.

The assessment of the level of security awareness is closely related to the process of education and upbringing for information security. Increasing the information awareness of students, developing their risk awareness and skills to manage that risk, as well as situational awareness that enables coping with risk, is carried out through education for security and information in the process of shaping a security culture. As A. Pieczywok emphasizes, it is not possible to counteract threats without citizens' awareness of security regarding the adherence to the culture of being, culture of security, and essential universal and social values, because inculcating values allows for the assessment of the overall life situation in which the subject currently operates (Pieczywok, 2012, pp. 319, 320).

It can therefore be stated that education for information security positively influences the shaping of the information security awareness of a subject by developing mature information attitudes and behaviors. Therefore, if we do not consider the need to shape a culture of information security in education for security, this strengthens a sense of information security in society built by omitting the sphere of mental culture including values, principles, norms, knowledge, ways of thinking, and wisdom, and is therefore mainly limited to the sphere of material culture (infrastructure, technology, technologies, workplaces) (Cieślarczyk, 2022, p. 285). Moreover, a lack of knowledge and information skills makes societies information-immature and leads to their ignorance regarding the perception, assessment, and need to counter threats, resulting in an irrational sense of security, which makes them an easy target for info-aggressors.

BIBLIOGRAPHY

Auleytner, J. (2015). Zagrożenia cyberprzestrzeni. In J. Auleytner & J. Kleer (Eds), *Rewolucja informacyjna a kryzys intelektualny* (pp. 95-106). Polska Akademia Nauk.

Auleytner, J. & Kleer J. (Eds). (2015). *Rewolucja informacyjna a kryzys intelektualny*. Polska Akademia Nauk, Komitet Prognoz „Polska 2000 Plus".

Babik, W. (2024). *Logistyka informacji.* Wydawnictwo Uniwersytetu Jagiellońskiego.

Batorowska, H. (2025). Deficyt kultury bezpieczeństwa informacyjnego w prognozowaniu stanu środowiska informacyjnego. In S. Kowalkowski et al. (Ed.), *Odporność miast na kryzysy i zagrożenia* Vol.1 (pp. 95-106). Presscom Sp. z o.o.

Batorowska, H. (2021). *Kultura bezpieczeństwa informacyjnego w środowisku walki o przewagę informacyjną.* Wydawnictwo Libron.

Batorowska, H. (2016). Perceived self-efficacy vs. actual level of training in personal information and knowledge management. A research report. *Bibliotheca Nostra*, 2, 61-89.

Batorowska, H. (2017). Przetwarzanie informacji w środowisku jej nadmiarowości i przyspieszenia technologicznego w świetle badań własnych. *Edukacja-Technika-Informatyka,* 1(19), 177-191.

Batorowska, K. (2023). *Poczucie bezpieczeństwa informacyjnego społeczności lokalnych w aspekcie wybranych zagrożeń cywilizacyjnych*. Uniwersytet w Siedlcach, Instytut Nauk o Bezpieczeństwie [doctoral thesis].

Bauman, Z. & Lyon, D. (2013). *Płynna inwigilacja. Rozmowy*. Wydawnictwo Literackie.

Chabielski, P. (2025). Strategia odporności miasta w budowaniu zdolności społeczeństwa do reagowania na zagrożenia. In S. Kowalkowski et al. (Ed.), *Odporność miast na kryzysy i zagrożenia,* T.1 (pp. 69-85). Presscom Sp. z o.o.

Cieślarczyk, M. (2022). *Znaczenie kultury bezpieczeństwa w procesach logistycznych na przykładzie pandemii COVID-19 i innych elementów kaskadowej sytuacji kryzysowej.* Wydawnictwo WAT.

Fehler, W. (Ed.). (2023). *Leksykon bezpieczeństwa informac*yjnego. Wydawnictwo Naukowe UP-H w Siedlcach.

Feliński, J. (2024). *Doskonalenie jakości zarządzania bezpieczeństwem informacji w organizacjach*. Akademia Sztuki Wojennej, Wydział Zarządzania i Dowodzenia [doctoral thesis].

Galar, R. (2015). Rozsądek gapia. In J. Auleytner & J. Kleer (Eds) *Rewolucja informacyjna a kryzys intelektualny* (pp. 107-118). Polska Akademia Nauk.

Hoffmann C., Lutz C. & Ranzini G. (2016). Privacy Cynicism: A new approach to the privacy paradox. *Journal of Psychosocial Research on Cyberspace,* 10 (4).

Łabędź, K. (2018). Poczucie bezpieczeństwa we współczesnym społeczeństwie polskim. *Facta Simonidis,* 11(1), 45-64.

Marciniak, E. M. (2009). Psychologiczne aspekty poczucia bezpieczeństwa. In S. Sulowski & M. Brzeziński (Ed.), *Bezpieczeństwo wewnętrzne państwa. Wybrane zagadnienia* (pp. 56-65). Wydawnictwo Elipsa.

Młynarska-Sobaczewska, A. (2013). Trzy wymiary prywatności. Sfera prywatna i publiczna we współczesnym prawie i teorii społecznej. *Przegląd Prawa Konstytucyjnego,* 1, 33-52.

Motylińska, P. & Pieczka A. (2022). Zagrożenia wpływające na poczucie bezpieczeństwa informacyjnego – perspektywa studentów. *Annales Universitatis Paedagogicae Cracoviensis,* 368, *Studia de Securitate,*12 (2), 127-140.

Olejnik, A. (2015). Media społecznościowe i ich rola w kreowaniu poczucia bezpieczeństwa społeczności lokalnych. In J. Auleytner & J. Kleer (Eds) *Rewolucja informacyjna a kryzys intelektualny* (pp. 123-131). Polska Akademia Nauk.

Oleński, J. (2015). Społeczne bezpieczeństwo informacyjne podstawą demokratycznego państwa. *Rocznik Kolegium Analiz Ekonomicznych,* 36, 13–49.

Pieczywok, A. (2012). *Edukacja dla bezpieczeństwa wobec zagrożeń i wyzwań współczesności*. AON.

Polończyk, A. (2018). Poczucie bezpieczeństwa. In O. Wasiuta, R. Klepka & R. Kopeć (Eds.), *Vademecum bezpieczeństwa* (p. 284). Libron.

Solove, D. J. (2006). A Taxonomy of Privacy. *University of Pennsylvania Law Review,* 154(3), 477-560.

Szpunar, M. (2016). *Kultura cyfrowego narcyzmu*. Wydawnictwo AGH.

Wasiuta, O. & Klepka R. (Eds.). (2019). *Vademecum bezpieczeństwa informacyjnego*. Libron.

Wasiuta, O., Klepka, R. & Kopeć R. (Eds.). (2018). *Vademecum bezpieczeństwa.* Libron.

Westin, A. F. (1996). Privacy in the Workplace. *Chicago-Kent LawbrEVIEV,* 72, 272-275.