

HANNA BATOROWSKA
Institute of Security Sciences
The Pedagogical University of Cracow
e-mail: hanna.batorowska@up.krakow.pl
ORCID: 0000-0001-6759-5094

THE INFORMATION SCIENCE CONTEXT OF SAFETY CULTURE



HANNA BATOROWSKA – habilitated doctor of humanities, associate professor at the Institute of Security Sciences of the Pedagogical University of the National Council on Education in Krakow, Head of the Department of Information and Media Security. Member of the International Society for Knowledge Organization ISKO and the Polish Society of Scientific Information and the Polish Society of Educational Technology and Media. Her scientific interests include: information culture, security culture, information technology, information ecology, information and knowledge management. Author or co-author of such monographs as: *Media jako instrument wpływu informacyjnego i manipulacji społeczeństwem* (*Media as an instrument of information influence and society manipulation*) (Kraków, 2019), *Od alfabetyzacji informacyjnej do kultury informacyjnej. Rozważania o dojrzałości informacyjnej* (*From information literacy to information culture. Reflections on information maturity*) (Warszawa, 2013), *Kultura informacyjna w perspektywie zmian w edukacji* (*Information culture in the perspective of changes in education*) (Warszawa, 2009), *Technologia informacyjna w kształceniu ogólnym* (*Information technology in general education*) (Kraków, 2002), *Wybrane zagadnienia nauki o informacji i technologii informacyjnej* (*Selected issues of information science and information technology*) (Kraków, 2000), *Jan Nepomucen Bobrowicz – polski wydawca i księgarz w Saksonii w czasach Wielkiej Emigracji* (*Jan Nepomucen Bobrowicz – Polish publisher and bookseller in Saxony during the Great Emigration*) (Kraków 1998); editor of monographs on security from the series „Man in the world of information”, e.g.: *Bezpieczeństwo informacyjne w dyskursie naukowym* (*Information security in scientific discourse*) (Kraków, 2017), *Walka informacyjna. Uwarunkowania – Incydenty – Wyzwania* (*Information struggle. Conditions – Incidents – Challenges*) (Kraków, 2017), *Kultura informacyjna*

w ujęciu interdyscyplinarnym. *Teoria i praktyka*, Tom II (*Information culture in an interdisciplinary approach. Theory and Practice*, Vol. II) (Kraków, 2016), Tom I (Vol I) (Kraków, 2015); and of monographs devoted to information literacy, education, information architecture, book history, and numerous scientific matters, among others: *Information retrieval support: visualization of the information space of a document* (Würzburg, 2014), *Perceived self-efficacy vs. actual level of training in personal information and knowledge management. A research report* (2016). Author of over 200 scientific publications actively participating in over 160 international and national scientific conferences.

KEYWORDS: Information ecology. Information science. Interdisciplinarity. Security culture. Information security culture. Information culture. Methodology. Security sciences.

ABSTRACT: **Objective** – The aim of the article is to show the interdisciplinary nature of security and information sciences and the relationships that exist between them in the area of threats generated by digital civilisation. Attention was paid to the importance of selected components of the information security culture in shaping the security culture. It has been pointed out that these components are a permanent subject of information science research. **Method** – A method of analysis and criticism of the literature was used. **Results** – Information technology as a discipline dealing, among others, with the functioning of people in the world of information (e.g. individual and group information management, information literacy obligations, information needs and behaviour – also in everyday life, information culture) supports research in the field of security sciences (especially human safety) conducted in the context of the development of technical civilisation and communication. Threats that the information society generates require studies, e.g. in the field of personal, social, health and ecological security (protection of the infosphere against information overload and humans against information stress). As part of these problems, theoretical and empirical research is undertaken, which is also dealt with by information science researchers. The combination of scientific reflection undertaken by specialists in both areas is indispensable in order to be able to see in the information security culture a common research subject enabling the diagnosis of various aspects of the broadly understood information culture.

INTRODUCTION

The subject of information science research comprises objects, processes, events and information phenomena in society seen in the perspective of mediation (between information and its user). According to the literature analysis carried out by Sabina Cisek, the research field of information science is described differently, mainly because “mediation in the social world of information is multifaceted and has an educational, institutional, communicative, cultural, organizational, political, legal, psychological, social, technological, IT, and utilitarian dimension” (Cisek, 2009, pp. 47-56), and because it is possible to define objects, processes, events and information phenomena differently; it is difficult to specify what are fixed information resources, information needs, and behaviours; be-

cause information science integrates what is material (carriers, technology), psychological (information users), ideal (information as such, knowledge of humanity); and also because it uses various concepts and paradigms of science, e.g. cognitive currents. Therefore, in the latter part of the argument, the author states that the formulation of the subject of information science research is not easy, because it is associated with all areas of science, professional activity, everyday and social life. Hence, the connections between IT in other disciplines are very broad. Examples of research directions in information science (Sosińska-Kalata, 2013, pp. 9-14; Sosińska-Kalata 2015, pp. 115-137; Woźniak-Kasperek, 2015, pp. 139-157) conducted at the “interface” with other disciplines are: domain analysis, information architecture, Big Data, information ecology, information economics, philosophical aspects of information science, digital humanities, personal information management (PIM), infobrokering, social informatics, informetry, webometry, cybermetry, cognitivism, information culture, information education, information competences, digital data curating, knowledge organisation, meta-theoretical reflection on information technology, information behaviour, information management in organisations, including information audit, and the domain of information security culture that I propose.

SUBJECT MATTER AND OBJECTIVE

The subject of the article is the issue of information security culture treated as a new area of information science research related to human functioning in a hybrid information environment (infosphere), in which the entity is exposed to dangers resulting, among others, from information overproduction and information stress. The aim of the article is to show the interdisciplinary nature of both domains and relationships that exist between them in the area of research on threats generated by technological civilisation. The specific objective was considered to indicate the importance of selected components of the information security culture in shaping the sense of security of citizens and sensitizing them to activities in which information is used as an element of influence. These components include:

- information culture of members of the society,
- information ecology,
- media security,
- information security management and information audit,
- information policy and shaping the social information order,
- organizational culture and informational behaviour in the organization,
- information, media, intercultural and civic education.

METHOD

The method of analysis and criticism of literature from both fields was used, which allowed, among other things, the comparison of concepts with the same names but different meanings.

THE RELATIONSHIP OF SAFETY CULTURE WITH INFORMATION SCIENCE

While writing a monograph on the basics of security sciences, Leszek F. Korzeniowski assumed that security is multi and interdisciplinary, which results in the need to “cross the boundaries between fields of science and scientific disciplines and the opportunity to use the methodological toolkit and the theoretical output of other sciences” (Korzeniowski, 2012, p. 71) (philosophy, psychology, sociology, history, economics, political and legal sciences, physical culture sciences, in some issues also natural, agricultural, forestry, mining, medical, military, pedagogical and even theological and artistic sciences). Further in the discussion, it is concluded that the adoption of interdisciplinary or monodisciplinary perspectives by security researchers “constitutes a distinction between what is and what is not practicing securitology”, therefore “the programmatic methodological basis of securitology is crossing borders between scientific disciplines and the transdisciplinary approach becomes the determinant of the identity of securitology.” (Korzeniowski, 2008, pp. 47-48). Among the disciplines mentioned by L.F. Korzeniowski, there was no information science, although another researcher in security and defence problems, a specialist in military information operations, Ryszard Szczyra, clearly indicates the importance of information science in analysing phenomena related to information operations¹, which cannot be limited to a physical and cybernetic interpretation of information theory, but should incorporate the psychological context within the implementation of information processes. This context which allows the study of how people relate to information, search for it, process it, and use it, is associated with emotions and cognitive processes (perception) that affect the decision making of individual entities. Hence the interest within security science in the information behaviour of recipients of broadcast messages, and especially in the ways

¹ Information operations are “coordinated and synchronized actions taken to achieve the desired impact on the will, thinking and ability of the opposing party (...) by influencing its information, systems and processes based on information, using and protecting their own” (Z. Modrzejewski, *Operacje informacyjne*. AON, Warszawa, 2015, p. 11). Information operations (states) are also defined as organized state activity leading to the achievement of specific political goals, directed at external and internal information communication systems or information flowing through them.

people who are the target of information operations mentally process and receive information.

The inclusion of the social concept of information theory in research conducted within military sciences allows “treating information science as studying information flow in society” and recognizing that “the act of information transfer presented as a system: source – channel – recipient” is the essence of this concept. As emphasized by Szpyra, the content of social information theory implies the possibility of influencing both “information transmitted through the flow channel and the source generating it, as well as the recipient”, which means that there is a potential area of possible influence on information and information processes, because “all elements of the information process are susceptible to some form of influencing the information they transfer” (Szpyra, 2002, pp. 37-38).

COMMON OBJECTIVES FOR SAFETY AND INFORMATION SCIENCES

Security sciences in many environments are identified with the terms security culture, defence culture, security climate, or securitology (Korzeniowski 2012, p. 55). The consequence of this practice is to define a safety culture either in a broad or narrow perspective (Cieślarczyk, 2014, p. 23). Securitology as an emerging scientific discipline undertakes research on threats to the existence, development, and normal functioning of human and social organizations, taking into account the security of the subject (human), the security of a small social group, the security of society (a large social group) and the security of humanity (Korzeniowski, 2008, pp. 53, 55). The security of each of these entities concerns “the ability to be creatively active and means an objective state of non-threat, felt subjectively by individuals or groups”. Therefore, it covers the context of economic dependence, ecology, social and humanitarian issues, issues related to maintaining national identity, and ensuring proper participation in the civilisation development of the modern world, thus entering the field of research on the information society, information culture, information ecology, information economics, information policy, information behaviour, information needs, information barriers, information processes and systems, information organization, information and communication technologies, information management, digital information and media competences, information communication, information security culture, in other words areas of interest in information science.

The common goals of security and information sciences are related to providing entities with the possibility of creative activity, freedom of intellectual development, identity, and cooperation within the framework

of positive cooperation. Not without reason, in one of the concepts of *information literacy* developed by Jeremy J. Shapiro and Shelley K. Hughes, it is treated as a modern liberal art and an independent scientific discipline (Shapiro & Hughes Shelley). The subject of this discipline is a human functioning in the world of information and a critical reflection on the nature of information in itself and its social, cultural, technical and philosophical contexts. This approach to *information literacy* guarantees preparation of people for functioning in the information society and is the basis of their humanistic upbringing. It also serves social progress and counteracts the process of social exclusion by preparing for lifelong learning because it equips a person with the knowledge that dictates his freedom in the cyber world and active participation in shaping the information society (Batorowska, 2013, pp. 3-10; Jasiewicz, 2012, pp. 107; 108). The subjective dimension of security also applies to "an individual as a citizen and the guarantees of personal safety expected by him as the starting point for stable development, implementation of professional ambitions and aspirations, and creation of conditions for building family happiness" (Buczyński, 2011, p. 54).

Therefore, the common goals of these sciences are related to:

- counteracting exclusion and global social division,
- striving for sustainable development in the infosphere,
- shaping awareness of threats in society,
- shaping social order, including information order,
- protecting against manipulation and distortion of information,
- providing access to information and knowledge,
- shaping pro-infoecological and civic attitudes,
- taking advantage of the challenges and opportunities that digital civilisation creates for the development of the common good of humanity,
- creating transparent information policy,
- disapproving of turning the infosphere into a training ground for information war,
- counteracting the negative effects of globalization processes.

Identification of threats that may interfere with the proper functioning of the entity or the loss of certain values, e.g. potential, determines the subjective scope of security. This means that security should be perceived as a factor that develops and enriches an individual's personality, and is the basis for his intellectual development, the lack of which causes the temporary or relatively permanent loss of the individual's ability to develop widely in the ICT environment. Technological civilisation is subjected to empirical analysis as a source of threats both from the perspective of information science and security sciences, especially in the context of in-

formation ecology (Kamińska-Czubała, 2017, pp. 54-68; Januszko-Szakiel, 2017, pp. 391-414).

Regarding threats generated by technological civilisation in the context of information science, Wiesław Babik refers to the tasks set for information ecology aimed at eliminating these threats. The means of implementing this task are:

- introducing a state of balance and harmony in the anthropoinfosphere,
- ensuring secure and well-organized access to knowledge and information,
- protecting the public against threats arising from overproduction of information,
- constant care for the quality of information,
- preventing the generation of poor quality information,
- removing useless information or its utilization,
- promoting the ethical use of information and ICT,
- shaping the human information environment, including cultural continuity,
- developing appropriate methodologies to improve human functioning in the environment (Babik, 2014, p. 114).

Brunon Hołyst approaches the issues of human security in the context of the development of technical and communication civilisation (Hołyst, 2014, pp. 278-307).

The state of social security level combines:

- treating science and technology institutions as open interactive networks caring to ensure the quality and reliability of the information they produce and disseminate,
- civic valuation of techniques focused on informing users of new media about current events and initiating reactions to them in the form of protests, public debates, social experiments, participation in expert opinions and forecasting,
- counteracting alienation processes in which the products of human action begin to function independently of a person and against him, in order to enslave its creator and destroy him, e.g. technopol, internet of things, big data, virtual reality,
- industrialisation, the consequence of which is “breaking with the past” and gradual loss of identity as “a phenomenon imposed on society, disorganising its organisation and causing a sense of danger”,
- increasing factors of social helplessness, such as social anxiety, low self-esteem, lack of self-confidence, shyness, dependence on others, limited trust in others, detachment from family, lack of friends, ta-

- king the form of social pathologies that result from network addiction, the media, from professing the “philosophy of ease”, from striving for “freedom from” all obligations and responsibilities, giving up skills that can be replaced by artificial intelligence systems, etc.,
- the ability to link public communication with the science sector, hindered due to the different goals adopted by both parties, and the ability to eliminate the lack of connections between them, e.g. in the area of shaping the awareness of the “non-knowledge society” in terms of the consequences from side effects of technological civilisation development for human development,
 - the development of telecommunications, which creates communities with specific interests, standards, and rules of the game, over which politics increasingly loses control, as it does as well over the flow of information,
 - recognising the phenomenon of the superiority of technique over culture, the processes of dehumanisation of interpersonal contacts, “collectivisation of minds” and counteracting these threats,
 - human information awareness, the ability to make choices, make decisions and the intensity and ways of using ICT,
 - dealing with information redundancy and information stress,
 - overcoming infostress, technostress, netoholism, Internet addiction, etc.,
 - the ability to analyse media messages containing elements of persuasion, manipulation and propaganda as well as adherence to media disposers’ codes of journalistic ethics,
 - shaping responsible attitudes of media users, educating them as to information and shaping users’ information culture and their maturity in dealing with the media,
 - information, media and IT education allowing an increase in the level of personal data security and rational management of information and its security.

Both disciplines struggle with the exclusion of the individual from social life, and both disciplines treat mental aspects (spiritual, immaterial, ethical, conscious, axiological) as determining whether human development will properly serve the security and development of humanity, requiring them to be reflective and to “cultivate the human spirit” (Piwoński, 2015, p. 185) and information maturity.

INTERDISCIPLINARITY A COMMON FEATURE OF BOTH DOMAINS

Reading a series of books published by PWN on security by Bruno Hołyst² reveals the domain of securitology from the perspective of various scientific disciplines and subdisciplines, such as anthropology, sociology, psychology, law, economics, biology, technology, philosophy, and ethics. Although in each of these research areas there are different theoretical and methodological approaches, security is treated by the author very broadly as “a set of conditions that allows an individual to achieve their intended goals without interference”, i.e. includes not only his “mental but also biological, social, cultural and legal state, in which a person has a feeling of complete certainty that he or she has support in another person or in a well functioning legal system” (Hołyst, 2014, p. 10). Similarly, IT, in creating the circumstances to ensure optimal conditions for the implementation of the information process, eliminates barriers preventing the fulfilment of information needs and achievement of satisfaction by the entity that expects of information providers a product that meets quality standards, and of intermediaries high-quality information services.

The research area of security sciences, like information sciences, is interdisciplinary. In information science, the subject of considerations is “the entirety of issues related to the flow of information from the source to the user, detection of disturbances occurring at individual stages of this process, and indication of ways to remove these disturbances” (Pindłowa, 1984, pp. 35-38), and it is associated with “objects, processes, events and information phenomena in society in the human world, seen in the perspective of mediation between fixed information resources and people who need it” (Cisek, 2009, pp. 47-56). The connections between information science and other disciplines mainly concern information technology (IT), social communication (journalism, editing, media), management sciences (business intelligence, knowledge management), pedagogical sciences (information literacy, information education), social sciences (information society, social computing, information culture), as well as the study of document collections (GLAM, archival science, library science) (Bawden & Robinson, 2012).

These relationships, which were noticed by David Bawden and Lyn Robinson, were described in the textbook *Introduction to Information Science* and were reflected in the monograph *Diagnostics in information management: information perspective* (*Diagnostyka*, 2017) prepared and edited by Remigiusz Sapa. This publication is a multifaceted discussion of

² B. Hołyst, *Bezpieczeństwo: programy promocji* (2017), *Bezpieczeństwo gatunku ludzkiego* (2016), *Bezpieczeństwo społeczeństwa* (2015), *Bezpieczeństwo jednostki* (2014), *Bezpieczeństwo. Ogólne problemy badawcze* (Warszawa 2014), *Zagrożenia ładu społecznego*. Vol.1-2 (2013, 2014).

problems related to activities that are aimed at formulating a diagnosis in various areas of information management, including both information resources and information processes (formulation of information needs, collections, resources, their development, processing, organizing, sharing, storage, protection). The adopted information technology perspective has made it possible to focus attention on solving practical problems arising in human-information interaction, mainly related to scientific, economic, and educational projects. The interdisciplinary approach to information science reduces the phenomenon of fragmentation of scientific reflection taken in isolation from the achievements built in various areas of knowledge. In this context, the editor of this volume continues the work of Wanda Pindlowa, who drew attention to the opening of information technology to cooperation with more and more new sciences and who stated that “the impact of information science on other disciplines is not visible, because representatives of most disciplines identify information science with computer science, or unconsciously use the experience developed by information science theorists” (Pindlowa, 2013, p. 55). Reading this monograph should make researchers outside of the field of information science, especially those dealing with security sciences, aware of the significance of the potential inherent in the discipline presented here, among others, for diagnostic tests undertaken in the field of information and knowledge management, including information security management.

INFORMATION MANAGEMENT IN SECURITY SCIENCES AND IN INFORMATION SCIENCE

Information management is a cycle of systematic and interrelated activities related to information, the purpose of which is to be effectively used both on an individual, organizational and social level. It concerns the methods, principles and tools for effective information retrieval, collection, development, processing, generation, storage, sharing, use and creation of new information. Therefore, the advantage is not only in gaining access to specific information resources, but mainly in gaining the ability to manage their content. This advantage can create a “conflict situation, in which one of the parties has more effective information systems guaranteeing the possibility of creating better conditions than the other party to achieve their goals”. Uneven access to information creates a threat to the information security of the “uninformed” party (Szpyra, 2002, p. 251).

Following Katarzyna Materska’s modern approach to information management, it becomes necessary to include in her research area the following issues:

- information security management (creating company information security),

- information culture of the organization, the development of which contributes to the improvement of information and communication competencies and information awareness of employees, thereby increasing the level of information security,
- information quality management, which is reflected in the information security management system, and in creating information strategies that are a reflection of the organization's specific information policy, translating into building its own personalized information security policy,
- strategic information management resulting from treating the information resource as a strategic resource of the organization, nation, corporation, or group, from which it gains an informational advantage over the rival side,
- information audit, including also information security audit based on norms and legal acts setting the levels of information validity and types of secrets (state, official, personal, tax, banking, etc.),
- management of the information environment, which is the environment of information struggle, wherein the entities operating in it initiate decision-making processes in which "people and systems observe, analyse, decide and act according to the information entered" (Materska, 2016, pp. 371-372).

The ability to manage information is indispensable in managing information security. From this perspective, one can reflect on the domain of security management, set boundaries between securing information and information security, and indicate the relationship between information management and security management and information security management. In this analysis, it is very important to distinguish information security regarding an entity that is threatened by a lack of information or the possibility of losing information resources, from information security understood as the protection of data held by that entity (Janczak & Nowak, 2013, p. 18). The securing of information is only one of the components of an entity's information security. In turn, information security management comes down mainly to the problems of creating and enforcing the so-called information security policies, where information security management also refers to information itself, systems in which information is subject to information processes, the environment in which these systems operate, the personnel who use these systems, and the legal environment. As Agnieszka Filipek points out, security management cannot be linked only with choosing between safety or risk, but with the ability to take risks, deal with them and manage them wisely in order to introduce change that enables development and, consequently, guarantees the entity's long-term security (Filipek, 2017, p. 176).

Effective safety management requires understanding of the essence of security, knowledge of the specifics of contemporary challenges and threats, preparing society for effective problem solving and acting in situations that threaten human security, and perceiving the scope of changes that allow increasing the quality of activities to shape the environment and safety culture. Prevention safety should include all educational activities aimed at preparing a person to effectively resist threats and supporting his predispositions, interests, abilities, self-esteem, respect, empathy and bonding with society so that he feels like an important link in building a culture of security within his surroundings. Prevention understood in this way requires a reliable diagnosis of a person's sense of security, enabling him/her to participate in designing educational initiatives.

INFLUENCE OF INFORMATION CULTURE ON THE SECURITY CULTURE LEVEL

Marian Cieślarczyk includes information culture among the basic components of security culture (Cieślarczyk, 2011, pp. 13-32), in which he attaches particular importance to the information competencies of modern man, which guarantees the conscious and therefore secure functioning of the subject within the digital civilisation and determines the shape of the subject's defence in this dimension. In an article combining elements of security culture with information ecology and information culture, he writes that "an appropriate level of information culture and information security culture of a given entity is one of the main conditions for shaping the relative balance between objective and subjective security. Without this, there is no security in the long term" (Cieślarczyk, 2017, pp. 144-145; Cieślarczyk, 2015, pp. 16-28). To this end, it is necessary to shape the information awareness of citizens and their civic attitudes, thanks to which it will be possible to shape the social information order, creating a coherent system in which Józef Oleński includes social norms, processes and information systems, and information resources (Oleński, 2006, pp. 19, 27). Each political system of the state creates its own specific social information order, which should ensure the functioning and stability of the state, and thus the security of its citizens.

The research field of security culture therefore covers the problem of education in the field of information security culture. It can be defined as "the sphere of human activity shaped by information awareness and ways of thinking about security; values, norms and rules supporting the need to increase the level of security culture allowing one to see challenges, opportunities and threats in the local and global information space; attitudes affecting the sensitivity of the public to the importance of security and

shaping the behaviour of information-mature users of the infosphere who are jointly responsible for this security” (Batorowska, 2018, pp. 70-85). These behaviours result from the interaction of the cultural components mentioned above. They relate to objects and other products related to information security and the participation of entities in the information process. People who have low education and represent low human capital because they are socially and economically disadvantaged do not think about a culture of security (Batorowska, 2018, pp. 92-100) and investing in the future. Zygmunt Bauman warns that consciously maintaining society in a state of ignorance leads to paralysis of its will, and “a man who does not know what to expect and is unable to assess the situation properly, manifests pathological political ignorance” (Bauman, 2007, pp. 201, 202). Hence the need for education to ensure information and media security. By the latter, Rafał Klepka understands “the state of uninterrupted functioning of the media system in a given country” and combines this with “preparing recipients to consume media content, in particular regarding the most important social and political processes” (Klepka, 2018, pp. 120, 122). However, media and information security requires information and media competence from citizens. Their development supports the sensitivity of their perception of any negative phenomenon related to the information process and the ability to assess its impact on the proper functioning of the infosphere, whose security has a direct impact on the security of the individual and of the group (Batorowska, 2017, p. 26).

Protection against manipulation in the environment of liquid surveillance requires mass media information maturity, which cannot be achieved without constantly “renewable” information competencies, among which PIM occupies a key place. The ability to create and use individual information collections requires metacompetencies, which have to be cultivated. As the research conducted by Marzena Świgoń shows, “society should demand such courses [to] be able to function properly in a group and in society”, and to know how to verify information to preserve a culture based on openness and democracy (Świgoń, 2012, pp. 284, 285).

Continuous and widespread public education is needed about the threats generated by digital civilisation and about information security issues. Education for information security is therefore a response to the appeal of Brig. Gen. Prof Dr hab. Stanisław Koziej for shaping the resistance of Polish society to information attacks and raising its awareness of the modern information war. The document *the Doctrine of Cybersecurity of the Republic of Poland (Doktryna, 2015)*, draws attention to the need to include the public, private, and civil sectors in activities to create an information security environment for the country and to involve representatives of these sectors in the process of continuous education and of raising

awareness of information threats. Education in the field of information security is treated as an important link in supporting the cybersecurity system, and the skills and awareness of individual users is one of the pillars of cybersecurity (Batorowska, 2018, pp. 163-172).

That is why shaping pro-ecological and civic attitudes is an important element of Wiesław Babik's security of the human information environment. Recognizing information as a common research problem of information scientists and representatives of security sciences, he points to the need to integrate and synthesise various ways of recognizing it within the humanities and social sciences in order to "enrich the knowledge of both the information itself and the areas of its creation and use" (Babik, 2018, p. 111; Babik, 2017, pp. 165-166).

CONCLUSIONS

In conclusion, information science, as a discipline that deals with – among other things – people in the world of information, supports research in the field of security sciences, especially human security in the context of the development of technical civilisation and communication. The information behaviours of security entities resulting from the attitudes they accept towards information indicate how to deal with:

- data redundancy and information stimuli, especially with their selection,
- acceleration in the sphere of ICT development, causing the phenomenon of technostress and infostress,
- the need to choose between "freedom from" and "freedom to", which raises axiological dilemmas arising at each stage of the information process,
- rebellion or acceptance of disinformation activities, information and media manipulation, with technological surveillance,
- functioning in an environment of permanent struggle for information advantage.

The subject's susceptibility to manipulation depends on the type of information behaviour and personality traits. The type of information behaviour instilled in an individual or group makes it easier to control them through appropriately selected tools and techniques of exerting influence. Information users include groups seeking to increase the demand for information in the process of its use, as well as those not interested in acquiring, updating, or authenticating information and who don't care about its quality parameters. Both groups of users are extreme and generate many threats to the efficient flow of information. Their behaviours are controlled by the culture of a given society and fall within the area of

information behaviours defined by information science specialists as “all activities, actions, and reactions of people related to information sources and channels, including, among others, how individuals perceive, need, search, manage, convey, and use information in various life contexts” (Cisek, 2017, p. 2).

A new issue in this area, which is not the subject of direct scientific penetration of information scientists, and related to ongoing changes in contemporary reality, is the analysis of information behaviours in the context of threats related to the broadly understood security culture. Thus behaviours that as a component of information culture have an impact on cultural security consisting in “consolidating and strengthening the components that determine the continuity of cultural identity” (Piwowarski, 2016, pp. 335-337). Without cultural security, it is difficult to build information security related to the conditions and actions taken to sensitize and immunize the public to information attacks by the aggressor, who, through disinformation and information and media manipulation, weakens the victim’s cultural identity, imposes his own view of reality (foreign to them), and thus controls their behaviour and influences decision-making processes (Batorowska & Klepka & Wasiuta, 2019, p. 72). Information behaviours and their formation (the controlling of them) may be an area of interest to researchers in problems of information struggle, in particular information operations undertaken in the sphere of psychological activities. All the more so since Natalya Godbold also includes, among information behaviours, actions aimed at avoiding or ignoring information as well as hiding and destroying it (Godbold, 2006), i.e. actions directed against the integrity, authenticity, and availability of information, in other words selected attributes of information security. Including information security culture problems in the area of security research, understood as “the ability to focus on and seek answers to questions of whether the exploitation and handling of information, and the reliance on it, will serve the security of this entity and other entities and will have a positive impact on their environment, or whether it will cause their degradation, especially in relation to the area of values, norms and principles” (Filipek, 2017, p. 176), therefore seems fully justified.

BIBLIOGRAPHY

- Babik, Wiesław (2018). Bezpieczeństwo informacji wyzwaniem dla bezpieczeństwa lokalnego. In: *Elementy teorii i praktyki transdyscyplinarnych badań problemów bezpieczeństwa. Teoretyczne i formalne aspekty bezpieczeństwa w wymiarze lokalnym*. Eds. A. Filipek, D. Krzewniak. Siedlce: UPH, pp. 109-120.
- Babik, Wiesław (2014). *Ekologia informacji*. Wydaw. Uniwersytetu Jagiellońskiego, Kraków.

- Babik, Wiesław (2017). Ekologia informacji a bezpieczeństwo człowieka i informacji we współczesnym świecie. In: *Walka informacyjna. Uwarunkowania – Incydenty – Wyzwania*. Ed. H. Batorowska. Kraków: Uniwersytet Pedagogiczny, pp. 160-169.
- Batorowska, Hanna (2017). Information and Media Literacy (IML) w edukacji dla bezpieczeństwa. In: *Człowiek-Media-Edukacja*. Eds. Janusz Morbitzer, Danuta Morańska, Emilia Musiał. Dąbrowa Górnicza: Wydawnictwo Naukowe Wyższej Szkoły Biznesu, pp. 21-28.
- Batorowska, Hanna (2018a). Kształcenie w obszarze bezpieczeństwa informacyjnego. In: *Edukacja XXI wieku*, Nr 42; *Procesy edukacyjne w dobie globalizacji, społeczeństwa informacyjnego i zmian na rynku pracy*. Eds. Maria Kozielska, Andrzej Zduniak. Poznań: Wyższa Szkoła Bezpieczeństwa, pp. 163-172.
- Batorowska, Hanna (2018b). Kultura bezpieczeństwa informacyjnego. *Edukacja – Technika-Informatyka*, no. 1(23), pp. 92-100.
- Batorowska, Hanna (2013). Obecność koncepcji information literacy jako sztuki wyzwolonej w wychowaniu do roztropnego funkcjonowania jednostki w środowisku społecznym. *Praktyka i Teoria Informacji Naukowej i Technicznej*, no. 1-2, pp. 3-10.
- Batorowska, Hanna (2018c). Potrzeba edukacji w zakresie kultury bezpieczeństwa informacyjnego. *Bibliotheca Nostra*, no. 2 (52), pp. 70-85.
- Batorowska, Hanna; Klepka, Rafał; Wasiuta, Olga (2019). *Media jako instrument wpływu informacyjnego i manipulacji społeczeństwem*. Kraków: Libron.
- Bauman, Zygmunt (2007). *Płynne życie*. Kraków: Wydaw. Literackie.
- Bawden, David; Robinson, Lyn (2012). *Introduction to Information Science*. London: Facet Publishing.
- Buczyński, Józef (2011). Teoria bezpieczeństwa: procedury i metody badawcze. *Przegląd Naukowo-Metodyczny. Edukacja dla Bezpieczeństwa*, no. 2, pp. 53-63.
- Cieślarczyk, Marian (2017). Ekologia informacji, kultura informacyjna i kultura bezpieczeństwa informacyjnego w teorii i praktyce. In: *Walka informacyjna. Uwarunkowania – Incydenty – Wyzwania*. Ed. H. Batorowska. Kraków: Uniwersytet Pedagogiczny, pp. 144-159.
- Cieślarczyk, Marian (2006). *Kultura bezpieczeństwa i obronności*. Siedlce: Akademia Podlaska.
- Cieślarczyk, Marian (2015). *Kultura informacyjna jako element kultury bezpieczeństwa*. In: *Kultura informacyjna w ujęciu interdyscyplinarnym. Teoria i praktyka*. vol. 1. Ed. H. Batorowska. Kraków: Uniwersytet Pedagogiczny, pp. 16-28.
- Cieślarczyk, Marian (2011). Kultura informacyjno-komunikacyjna a funkcjonowanie człowieka i grup społecznych w sytuacjach kryzysowych. In: *Bezpieczeństwo człowieka a komunikacja społeczna*. Tom 2. *Aspekty filozoficzne i polityczne*. Red. E. Jarmocha, A. Świderski, I. A. Trzpił. Siedlce: Wyd. UP-H, pp. 13-32;
- Cisek, Sabina (2009). *Nauka o informacji na świecie w XXI wieku: badania metanaukowe*. In: *Od książki dawnej do biblioteki wirtualnej. Przeobrażenia bibliologii polskiej*. Toruń: Wydaw. Naukowe UMK, pp. 47-56.
- Cisek, Sabina (2017). Zachowania informacyjne – wybrane aspekty. *Biuletyn EBIB*, no. 3 (173), pp. 1-11.
- Diagnostyka w zarządzaniu informacją: perspektywa informatologiczna* (2017). Ed. R. Sapa. Kraków: Biblioteka Jagiellońska.
- Doktryna Cyberbezpieczeństwa Rzeczypospolitej Polskiej* (2015). Warszawa: Biuro Bezpieczeństwa Narodowego.

- Filipek, Agnieszka (2017). Rola edukacji w kształtowaniu kultury bezpieczeństwa informacyjnego. In: *Walka informacyjna. Uwarunkowania – Incydenty – Wyzwania*. Ed. H. Batorowska. Kraków: Uniwersytet Pedagogiczny, pp. 170-180.
- Godbold, Natalya (2006). Beyond information seeking. Towards a general model of information behaviour [online]. *Information Research*, vol. 11, no. 4 [accessed on: 20.06.2019]. Available on: <<https://files.eric.ed.gov/fulltext/EJ1104640.pdf>>.
- Hołys, Brunon (2014). *Bezpieczeństwo. Ogólne problemy badawcze*. Warszawa: PWN.
- Jasiewicz, Justyna (2012). *Kompetencje informacyjne młodzieży. Analiza – stan faktyczny – kształcenie na przykładzie Polski, Niemiec i Wielkiej Brytanii*. Warszawa: Wydaw. SBP.
- Janczak, Józef, Nowak, Andrzej (2013). *Bezpieczeństwo informacyjne. Wybrane problemy*. Warszawa: AON.
- Januszko-Szakiel, Aneta (2017). Zarządzanie bezpieczeństwem informacji w sektorze MŚP - diagnoza i rekomendacje. In: *Diagnostyka w zarządzaniu informacją: perspektywa informatologiczna*. Ed. R. Sapa. Kraków: Biblioteka Jagiellońska, pp. 391-414.
- Kamińska-Czubała, Barbara (2017). Efektywność wybranych metod ewaluacji bezpieczeństwa informacyjnego. In: *Bezpieczeństwo informacyjne w dyskursie naukowym*. Eds. H. Batorowska, E. Musiał. Kraków: Uniwersytet Pedagogiczny, pp. 54-68.
- Klepka, Rafał (2018). Bezpieczeństwo medialne. In: *Vademecum bezpieczeństwa* Eds. O. Wasziuta, R. Klepka, R. Kopeć. Kraków: Libron, pp. 120-124.
- Korzeniowski, Leszek F. (2012). *Podstawy nauk o bezpieczeństwie. Zarządzanie bezpieczeństwem*. Warszawa: Difin.
- Korzeniowski, Leszek F. (2008). *Securitologia. Nauka o bezpieczeństwie człowieka i organizacji społecznych*. Kraków: EAS.
- Kuc, Bolesław; Ściborek, Zbigniew (2018). *Zarys metodologii nauk o bezpieczeństwie*. Toruń: Wydaw. Adam Marszałek.
- Laskowski, Lawiusz (2014). *Koncepcja rozwoju nauki o bezpieczeństwie*. In: *Metodologia badań bezpieczeństwa narodowego*. Vol. VII. Eds. P. Sienkiewicz, H. Świeboda. Warszawa: AON, pp. 20-28.
- Materska, Katarzyna (2016). Zarządzanie informacją i wiedzą. In: *Nauka o informacji*. Ed. W. Babik. Warszawa: Wydaw. SBP, pp. 359-385.
- Modrzejewski, Zbigniew (2015). *Operacje informacyjne*. Warszawa: AON.
- Oleński J. (2006), *Infrastruktura informacyjna państwa w globalnej gospodarce*. Warszawa: Uniwersytet Warszawski.
- Pindłowa, Wanda (1984). *Kształcenie studentów jako użytkowników informacji naukowej. Z pogranicza informatologii i pedagogiki*. Kraków: Uniwersytet Jagielloński, pp. 25-72.
- Pindłowa, Wanda (2013). Pole badań informacji naukowej – problemy zmienne i niezmiennie. In: *Nauka o informacji w okresie zmian*. Eds. B. Sosińska-Kalata, E. Chuchro, M. Lutek. Warszawa: Wydaw. SBP, pp. 53-61.
- Piwowski, Juliusz (2016). *Transdyscyplinarna istota kultury bezpieczeństwa narodowego*. Słupsk: Wydaw. Akademii Pomorskiej w Słupsku.
- Piwowski, Juliusz (2015). Podstawowe kategorie nauk o bezpieczeństwie. In: *Elementy teorii i praktyki transdyscyplinarnych badań problemów bezpieczeństwa* vol. IV. Ed. A. Filipek. *Odkrywanie znaczeń w naukach o bezpieczeństwie*. Siedlce: Wydaw. Uniwersytetu Przyrodniczo-Humanistycznego, pp. 185-204.
- Shapiro Jeremy, Hughes Shelley K. (2019): *Information Literacy as a Liberal Art. Enlightenment proposals for a new curriculum* [online]. [accessed on: 29.09.2019], Available on: <<https://teaching.uncc.edu/sites/teaching.uncc.edu/files/media/article-books/InformationLiteracy.pdf>>.

-
- Sosińska-Kalata, Barbara (2015). Ewolucja koncepcji informatologii (nauki o informacji). In: *Teoretyczne zagadnienia bibliologii i informatologii. Studia i szkice*. Ed. E. Gondek. Katowice: Wydaw. UŚ, pp. 115-137.
- Sosińska-Kalata, Barbara (2013). Obszary badań współczesnej informatologii (nauki o informacji). *Zagadnienia Informatologii – Studia Informacyjne*, no. 2, pp. 9-41.
- Szpyra, Ryszard (2002). Operacje informacyjne państwa w działaniach sił powietrznych [rozprawa habilitacyjna]. *Zeszyty Naukowe. Dodatek*. Warszawa: AON.
- Świgoń M. (2012), *Zarządzanie wiedzą i informacją*. Olsztyn: Wydaw. UWM, pp. 284, 285.
- Woźniak-Kasperek, Jadwiga (2015). Z głównych problemów samoświadomości informatologii. In: *Teoretyczne zagadnienia bibliologii i informatologii. Studia i szkice*. Ed. E. Gondek. Wydaw. Katowice: UŚ, pp. 139-157.