Appendix 2

SUMMARY OF PROFESSIONAL ACCOMPLISHMENTS

1. Name and Surname

Monika Szyłkowska

2. Diplomas and scientific degrees

- *Doctor of security sciences* – Ph.D. in social sciences in the discipline of security sciences awarded by the resolution of the Council of the Faculty of Internal Security of the Police Academy in Szczytno on 18th November, 2014 on the basis of the presented dissertation entitled *The protection of cyberspace in the national security system of the Republic of Poland,* November, Szczytno 2014;
- *M.Sc. in law* – Diploma of completion of the second-degree studies in the field of law at the University of Administration and Law in Warsaw. Subject of the master's thesis: *Evidence problems in cases of computer crimes,* Warsaw 2004;
- The diploma of completion of post-graduate studies, Academy of National Defence, Strategic and Defence Department, field of study: *national security,* Warsaw. Subject of the diploma thesis: *Capabilities and needs of using the mass media in creation of national security,* Warsaw 2006.

3. Information on previous employment in scientific units

3.1. Contracts of employment and equivalent agreements- positions held:

- 2015 – adjunct at the Department of Strategies and Defence Systems of the Institute of Security and Defence Systems, the Faculty of Logistics at the Military University of Technology in Warsaw;
- 2016 till now - Head of the Department of Strategies and Defence Systems – Institute of Security and Defence Systems, the Faculty of Logistics at the Military University of Technology in Warsaw;
- 2012-2013 r. – the Military University of Technology in Warsaw, Faculty of Mechanical Engineering (civil law contract for lecturing and exercises);
- 2015 -2016 - Helena Chodkowska University of Technology and Economics (civil law contract for lecturing and exercises).

3.2. Functions performed:

- 2016 till now - Head of the Department of Strategies and Defence Systems of the Institute of Security and Defence Systems, the Faculty of Logistics at the Military University of Technology in Warsaw;
- 2016 till now - Member of the Senate Committee for Development and Cooperation at the Military University of Technology;
- 2017 till now - Member of the Council of the Logistics Department;
- 2017 till now - Member of the Department of Finance and Property of the Faculty of Logistics;
- 2015-2016 - Member of the Faculty Electoral Commission of the Logistics Department;
- Supervisor of first-degree students' adaptation internship as part of the practical profile at the Faculty of Logistics of the Military University of Technology (2015-2016),
- Supervisor of first-degree students' improving internship as part of the practical profile at the Faculty of Logistics of the Military University of Technology (2015-2016),
- Supervisor of first-degree students' adaptation internship as part of the practical profile at the Faculty of Logistics of the Military University of Technology (2016-2017),
- Supervisor of first-degree students' improving internship as part of the practical profile at the Faculty of Logistics of the Military University of Technology (2016-2017),
- Supervisor of second-degree students' internship as part of the practical profile at the Faculty of Logistics of the Military University of Technology (2018-2019),
- Member of the editorial board: Defence Science Review, the Faculty of Logistics of the Military University of Technology.

3.3. Completion to the minimum staff resources:

- First cycle degree programme in the field of *Defence of the State* at the Faculty of Logistics at the Military University of Technology of Jarosław Dąbrowski in Warsaw in the academic year 2018/2019.
- Second cycle degree programme studies in the field of *Defence of the State* at the Faculty of Logistics at the Military University of Technology of Jarosław Dąbrowski in Warsaw in the academic year 2018/2019.

4. Indication of the achievements resulting from art. 16 sec. 2 of the Act of 14 March 2003 on *academic degrees and academic title, and on degrees and title in the field of art* (i.e. Journal of Laws of 2017, item 1789).

a) title of scientific achievement

The fifth dimension of security – cyberspace. Challenges, threats, implications.

[Polish: Piąty wymiar bezpieczeństwa – cyberprzestrzeń. Wyzwania, zagrożenia, implikacje]

b) author / authors, *title of the publication*, name of the publishing house, place and year of publication, number of pages

M. Szyłkowska, *The fifth dimension of security – cyberspace. Challenges, threats, implications.* Pub. *Sine qua non,* Kraków 2019, ss. 218. ISBN: 978-83-8129-557-4.

c) discussion of the scientific purpose of the abovementioned work and the results achieved, together with a discussion of their possible use

First: security. In this brief statement, is included the main idea of my research interests, in which I identify the entire complexity of the essence of security science. A science, which is understood as: *the theory of the real.* The constant concern for the raison d'état and fundamental national interests - existence, sovereignty, inviolability of survival and development - is the subject, object, aim and aspiration of the state and the nation. A manifestation of this care in the scientific field is reflected in the area of constant, interdisciplinary science research. A strongly and firmly established theory in the field of security science gives not only the basis for further scientific explorations, but also fulfils a key function - the possibility of pragmatic application in creating the security system.

The reference to the essence of considerations over security and safety, expressed by F. Hölderlin: *But where the danger is, also grows the saving power*, has allowed for the deeper deliberations from a different perspective. The thesis stating that threats have the most creative function to minimize the risk of their materialization and more broadly creating a security system can be accepted. The basic criterion is, therefore, constant search and identification of dangers. In this respect, cyberspace has basically unlimited explorations, perfectly exemplifying the classical cognitive paradox. However, identifying and analysing threats is an incomplete spectrum of activities for improving the security system, because this process requires searching for connections and relationship of phenomena.

The indicated guiding ideas, accompanying me through years of scientific exploration, were the key inspiration and impetus to undertake research on matter outlined in the subject of the indicated and presented achievement. My deeper exploration of this scope resulted from: my interests in the impact of broadly understood *cyberspace* on the security of the individual and the state; empirical research, which started in 2000; and other research programme carried out at a later time, in which I participated as a team member and the coordinator. The presented subject is an attempt of comprehensive reference to a problem that in the national scientific literature has not had a wide range of interest yet in the proposed approach presented in the monograph.

The subject matter of my research finds a reference in national studies; however, it is still significantly dispersed in various fields and disciplines of science. The importance of acquiring new knowledge about the phenomena and mechanisms occurring in the digital sphere affecting the level of security and the possibilities of improving the state's security system ultimately determined the choice of the object of research presented in the publication. The theme of the monograph became its cognitive and utilitarian purpose - an attempt to show both the deterministic complexity of cyberspace and the analysis of its impact on selected areas of security.

In the cognitive layer, the aim is to identify cyberspace perceived as the fifth dimension of security and identification of mechanisms of creating the dependence of phenomena and processes between the digital space and the security of the state. In the utilitarian layer, the aim was to scientifically define the ranges of common relations between selected phenomena in cyberspace to determine potential of their consequences for the security of the state. With this aim, scientific exploration should have been subject to identification of the areas of state functioning in the digital space and factors determining the creation of the state security system in this dimension.

Another element of the research was the identification of the causes of digital threats, their types, course, range of effects and directions of impact on the security of the state. There was also the need to identify contemporary conflicts in the digital space and determine the possibilities - and legitimacy - of their legal sanctions in the context of the impact on forming the state security environment. An indispensable element of the research was also the identification of the potential of cyberthreats proliferation including the so-called *human factor* and defining development directions, including impact on the state security system. In order to obtain the broadest possible picture of the studied issues, it was necessary to identify and recapitulate areas that implied the need to include in the process of designing

the state security system. These are such issues as: technical and technological sovereignty and digital competence of users (citizens) in terms of creating intangible assets forces of national defence means.

In order to achieve the assumed purpose, it was also necessary to determine the directions of possible changes for a multidimensional security environment along with the assessment of legislative necessities and opportunities as a critical element of actions taken to counteract digital threats. Implementation of the adopted research objective required clarification of the main research problem, which took the form of a question: *In what areas and ranges can the network capabilities of cyberspace (digital space) be effectively used in the creation and functioning of the state security system, with the integral perception of cyberspace as its fifth dimension?*

The assumption made conditioned the necessity to analyse selected phenomena and to adjust the conceptual scope in specific problem areas. For the needs of the conducted research, detailed research problems were formulated in the form of the following questions: *What is the essence of cyberspace in the security dimension? What is the nature of the identified threats in it? What types of cyber threats are crucial to state security? What is the meaning of so-called human factor in the proliferation of digital threats? What challenges does cyberspace bring to the defence system of the state? What are the attributes of the digital conflict compared to classic definitions? What is the legal possibility of declaration of the digital war? What other security areas implies cyberspace? What is the possibility (and legitimacy) of bearing legal responsibility for a digital product? What mechanism causes digital services to force consent from users? What is the importance of unsolicited sending user information by the software? Is it possible to find a balance between cyber-freedom and cyber-safety? What are the implications of cyber-identity? To what extent can the digital competences of citizens be an intangible force in creating national defence in this sphere?*

Conducted, at the stage of the initial research process, analysis showed the interdisciplinary nature of the undertaken problem and therefore the need to apply various, adequate methods, techniques and research tools, identified primarily in the discipline of security sciences, but also in legal sciences. In the research process, I have made extensive use of qualitative research methods, including in the form of analyses (e.g.: legal and institutional analysis, comparative analysis, system analysis and methods: analysis and logical construction), synthesis, abstracting, comparison, generalization and implication.

The analysis method allowed first to establish mutual relationships between the essence and the features of cyberspace and the impact on the functioning of the state and influence of cyberspace on forming the security system. This resulted in a key conclusion, that cyberspace is now another area constituting an inseparable element of the functioning of the state, and thus - affects the environment of its security.

The method of inference has been taken at every stage of the research work, which has led to deeper research (including during the study of materials in the context of the assumptions' validity), in order to enable their formulation in individual stages and in summary. In turn, among quantitative research methods, I intensively used statistical analysis and a diagnostic sounding survey.

In addition to the literature analysis, important support of the research process was the examination of documents (including provisions of national and international law) and available sources of knowledge about the problems studied. The source material included both open access and published studies in specialist journals. The indicated methods allowed to obtain a research material of high complexity. At this stage of the research, I have analysed the applicable legal regulations in the area of security, including cyber security (national and international), strategic documents and selected security policies.

As a result of the above, I verified and presented in the form of theory: the concept, essence and characteristics of cyberspace (1.3.1.); conceptual scope and character of cyber-conflicts (1.2.); the concept, essence and characteristics of cyber threats (2.1); social engineering attacks (2.2.); the possibility of proliferation of digital threats by so-called human factor (2.3); contrasting concepts of cyber-freedom and cyber-security (3.3.); and cyber-identity as determinant of protection (3.4.). Institutional and legal analysis was used to assess national solutions in the area of cyberspace (1.4.1, 2.1.3, 3.2, 3.4) as well as regulations and provisions concluded at the international level (1.3, 3.1, 2.1.2).

System analysis allowed the inclusion of the studied phenomena as elements of the system (1.1.). Comparative analysis, in turn, allowed to compare specific processes and specific phenomena (1.2, 3.2). The synthesis of individual results in the area of research problems. This has allowed for the use of the generalization method at a higher level, and thus the identification of universal determinants. During the research process, I also used the Delphi method, which allowed for the application of generalized expert prognosis evaluations.

The mentioned above, empirical methods included the following: a diagnostic sounding survey - conducted in the form of surveys using the CAWI technique – concerning: a.) *digital competence of users* and b.) *knowledge of citizens in the area of national defence.*

The empirical stage of the research was also comprised in the evaluation of the strategic interpretation that determines the functioning of the state security system and the assessment of the legal, organizational and functional status. The conclusions were confronted with the views presented in the publications of both state institutions and academia. The theoretical analysis has made possible to know the latest science views on security and were a source of comparative analysis - in terms of attributes of cyberconflicts and responsibility for a digital product.

In the whole range of research, I have referred to the analysis of views presented in the literature related to the subject of research. However, the basis of the research process related to this monograph was the theory of social science, particularly security science and legal sciences. In the process of verifying the hypothesis, also important were the conversations and expert consultations, which provided a significant supplement to the indicated research methods.

The cognitive and utilitarian premises of the problems are the implementation of the adopted hypothesis: *The dynamic growth of the importance of the complex problem of cyberspace provides many convincing arguments for its perception as the fifth dimension of state security in a systemic approach, with consider the generated challenges, threats and implications.* This assumption made possible to target selected problem areas. The analysis of the dynamics of constant changes determined by the digital space has become a challenge requiring the adoption of specific research areas, but also to consider their *network of problems* [connections of problems] in a system of innumerable the number of elements and connections. Confirmation of the adopted assumption can be found in the existing documents and strategic concepts, but in-depth, multi-aspect analysis required both issues that are just emerging in the conceptual field, as well as those that have not been the subject of extended research so far.

The adopted assumptions allowed to determine the following research hypotheses: *Cyberspace is an inherent element of the functioning of the state and thus - a component of the security environment requiring complementarity with other in the field of creating a security system. Cyberthreats can have a direct impact on the functioning of the state, which is why they determine the forming of its security system. Cyberspace implies the need to update existing national and international legal solutions. The consequence of cyber-threat interference at the global level should be the right to a digital war. The dynamics of development of forms of functioning created by available technical solutions and new types of threats determine the need to define a new security paradigm. The users (citizens) digital*

competences have an impact on the potential proliferation of threats, but <a contrario> - can also be an important element in the risk minimization process. The knowledge and skills of citizens can be a non-military force in creating national defence in the digital sphere.

The indicated research problems influenced both the order and the selection of areas that were in three dimensions: challenges, threats and implications determined by cyberspace. The structure of the monograph has also been subordinated to the main purpose, which consists of three theoretical chapters corresponding to the selected areas. The research process has been divided into stages, reflecting the pursuit of extensive exploration of the indicated areas and phenomena associated with them. This process was a consequence of the complexity of the research object itself as well as its relation in selected problem areas. The initial stage was devoted to determining the essence of cyberspace, its structure, features and correlations within the state security system.

I assumed that at this stage of research the meaning of such concepts as: cyberspace and cyberconflict will be or is determined and the layers of cyberspace determining the creation of specific processes and threats will be identified. Regarding the conceptual scope, the starting point was the definitional analysis contained in national regulations and strategic documents, based on which the structure of cyberspace (material, logical and cognitive layer) was presented and its individual features were characterized. The conclusions drawn from this part allowed to state that the conceptual scope of cyberspace is wide, because it includes: all means and communications and information resources for a civil and /or military use, including: networks (all types); devices; techniques; technologies; actors (service providers, operators and users) and space (communications).

The logical consequence of the initial part of the study was the theoretical analysis of the state security environment in the digital dimension based on the regulations governing the national cyber security system. The presented organizational model together with a range of competences and tasks should be assessed positively, however, the ideal solution would be to create a comprehensive, uniform IT architecture for all structures based on national solutions (producers), constituting an integration base for modular subsystems. The indicated solution would allow, above all, to become independent from the currently operating, commercial systems of global producers. Technical and technological sovereignty is and will be both a predominance, development opportunities and security level of the entire state information system. An example can be the lack of access to the source codes of the IT commercial solutions used in such sensitive systems as a state systems. The security chain of each information system originates from the technical solutions it possesses and uses,

therefore, the sovereignty mentioned above has a critical importance. In this context, the adoption of a broad definition of cyberspace as: *the processing and information exchange space created by tele-informatic systems* (...) *together with links between them and users' relations* supports the argument for creating a state system based on national solutions. As a result of the developed conclusions, the organization of the state security system in the dimension of cyberspace security of the Republic of Poland (part of the cyber security of the state) includes: forces, resources and a team of organizational, legal, physical, technical and educational undertakings to ensure the efficient functioning of the cyberspace of the Republic of Poland taking into account the security of information resources processed in it.

An additional part of the research process in the area of challenges included a reference to the phenomenon of cyberconflict, to its essence and attributes. The comparative analysis was based on the theory of classical definitions, which in the literature on the subject can be found in numerous studies. Also, international law documents allowed for in-depth considerations in the field of conflict typology and their features. As a result of the conducted research, it was important to show conflicts that were not the subject of numerous analyses earlier and referred to as: *long* (time) and *unresolved* (no agreement concluded) and so-called. *endless wars*, the essence of which is the lack of interest of the sides to resolve the conflict.

The identification of the indicated typology allowed to propose the definition of the concept of cyberconflict as an asymmetric conflict, the characteristics of which are: secretiveness; variability; surprise; dispersion and unlimited range. The analysis made possible to state that: the features that distinguish cyberconflicts from their classic counterparts include: the space of action; form and resources used for combat where purposes, motives and effects are invariable. The developed conclusions also allowed to state that the current challenge is the need to legitimize cyber operations at the international level (*digital conventions*) and the *right to the digital war* in two references: the digital response to the cyber-attack and the possibility of reaction using conventional methods in response to a cyber-attack. Despite the existing technical barriers and those resulting from the very nature and attributes of digital conflicts remaining passive in the face of strategic challenges soon may lead to *unreactive vulnerability.* The next stage of the research was aimed at identifying the determinants of cyberspace in the area of threats. As part of it, I analysed and classified threats according to previously accepted criteria. The starting point were source documents and the proposal to adopt the conceptual scope of cyberspace as: *the area of technical, logical and cognitive infrastructure, in which information systems operate, enabling data handling and information processing and exchange based on user relations and connections.*

The consequence of the assumption adopted in this way has been to propose a cyberthreat according to the technical criterion as: *unlawful action aimed at: modification, taking control or destruction of technical, logical and cognitive infrastructure, particularly in the functioning of information systems.*

Considering the disputable nature of the general scope of the subject, I adopted the technical criterion, because even the unintentional proliferation of this type of threat has a specific purpose located in the binary code. With a very high caution it can be exclude from this group only programming errors and failures, which, however, do not absolve from the need to include them in the design of security systems. The key result of the conducted research was the possibility to state that the catalogue of digital threats is an open set and for objective reasons inexhaustible. However, it became possible to identify the main categories of threats, examples of which may be dichotomous divisions - the need for a user's reaction or no- reaction - to make possible to materialize the threat.

In the further part of the research process, I analysed the source documents in the area of classification of the phenomenon of cybercrimes, namely detailed two forms: counterfeiting and falsification of the document - based on Polish law. Considering the statistics showing the scale of financial losses of both individuals and institutions, the indicated types of crimes in the digital space acquire a key significance. The wider perspective allows to see the directions of possible interactions at the level of the security system, especially in relation to the economic level. As part of the above-mentioned research process, I also subjected the phenomenon of cyber-terrorism to a thorough comparative analysis. As a result of this analysis I proposed a definition assuming that it would be: *all unlawful, independent of motives, intentional actions (use of or the threat of violence or force) taken by a person or group of persons against the applicable legal order of a given country in order to force its authorities to behave in a certain manner (act or omission) using intimidation or threatening methods that do not exhaust the international right to self-defence - covering both activity in ICT systems and all terrorist activities related to cyberspace.*

The following stage of the research was an attempt to identify and analyse digital threats to the security of the state, in which I assumed that it would be *any illegal electronic operations aimed against the resilience (security) of the state's information systems or the data processed by these systems.* These operations may be committed *using systems or networks* or may *involve systems or networks.* The conducted analysis allowed to conclude that in the information dimension of state security, threats may have a negative impact on all spheres and areas of activity - in particular: in the context of critical infrastructure. This fact allowed

for a general diagnosis allowing to assume that: the degree of threats to information systems is proportional to the degree of technical state advancement and the dependence of the functioning of information flows in the whole area of information economy in these systems.

As part of in-depth research, I indicated selected types of threats in the information environment of the state. The accepted criterion - together with the comparative analysis of existing definitions - made possible to propose the scope of an information war [fight] comprising: *comprehensive defensive and offensive actions in order to obtain an information advantage over an opponent using information systems and computer networks together with the possibility of neutralizing or destroying the opponent's network while protecting one's own.*

The next stage of research in the area of threats was devoted to phenomena: social engineering attacks and the proliferation of digital threats, which have not found a wide field of interest in the scientific literature yet. It should be emphasized that currently applicable regulations and strategic documents only signal the need to raise the level of users' awareness, stressing its significance, however, are without precisely defined solutions.

Regarding the specific purpose of the research I deemed it necessary to carry out quantitative research as a specific objective in the area of digital competence of users whose results allowed among others to say that despite the satisfactory level of respondents' knowledge about the existence and types of cyber threats - there is still a lot to do in the field of strengthening knowledge, e.g. in the area of risk minimization methods. In the context of the information war and related phenomena (often an instrument) described as: fake news - interesting results relate to the knowledge of the phenomenon (over 80%) and awareness of the possibility of using social media for propaganda (over 90%) - in regarding the scale of information verification, which is used by just over half of the respondents. However, a key role in this area has another of the distinctive features of cyberspace - the ability to create content by users.

This fact causes a significant spectrum of opportunities to use defensive and offensive measures of information war. The results obtained also allowed to state that the level of risk proliferation will be proportional to the knowledge and skills of digital users. The same ratio applies to the possibility of materializing a social engineering attack. The indicated research results allowed to identify the need for a wider consideration of the so-called human factor in the process of creating the security system, particularly taking into account the fact that users also perform various professional roles, and their habits are transferred simultaneously to the professional sphere.

The last area of research were selected implications defined by cyberspace. For the implementation of the research process, I selected issues related to the basis for the use of electronic devices in the program layer - along with the analysis of key issues, i.e. the apparent consent of users forced by devices and applications, and lack of control over the type, time and scope of information sent by devices without users knowledge. The same process concerned the possibilities, needs and barriers related to the responsibility for digital products.

The empirical process of using the selected electronic device from the moment of the first activation allowed for the discovery of the apparent consent of the user. In the absence of acceptance (by marking) specified by the manufacturer of the controls displayed on the screen of the device, it is not possible to run its full functionality allowing to use it without additional interference in the system software. Another identified *seeking consent* is the lack of accurate information from the manufacturer regarding the type, time and method of data transfer from the user's device. It is critical that the manufacturer reserves the right to send information necessary for the operation of important services through devices even if certain functions are disabled by the user. The conducted analysis allowed to state that currently there are no legal solutions protecting users in this respect - obliging device manufacturers and programs to exercise due diligence and care for comprehensive information in this respect. Among the identified gaps, it should be also pointed out the lack of a clearly defined prohibition on installing hidden program functions (also in the sense of operating systems) and liability in the event of their illegal residing of hidden program functions.

The analysis of normative regulations in the field of data processing allowed to state that the protection principles contained therein do not apply, without exception, to anonymous information (including processing for statistical or scientific purposes), which this exception should be made by mobile devices. The necessity to register each SIM card (subscriber identity module) under Polish law results in unambiguous and precise identification of the owner of the device in which it is installed. The result of the conducted research is a statement confirming the validity of the arguments for the need to adapt legal regulations to real phenomena. Exaggerated general provisions leave too much margin of interpretation to the detriment for the protection of users' rights. In the next research stage, I carried out in-depth research on the nature of the reflective relationship: cyber-freedom and cybersecurity. For the implementation of the research process both phenomena were placed as counterpoints in order to determine the possibility of achieving a balance in this respect.

As a result of my research, I determined that the immanent attributes of cyber-freedom are: the possibility of free use of network resources, including access to information, cultural goods, education, entertainment; the possibility of expressing yourself in any way in the digital space; and lack of control and supervision (the only limitations are the provisions of the regulations of individual services).

The second aspect of digital freedom is the scope and forms of using this space in criminal activities that are also dedicated to this sphere. This fact causes an urgent need to make fundamental changes both in the perception of the freedom to use digital space, and the possibility (necessity) of introducing restrictions for cyber- security. The results of the conducted research allow to state the changes should mainly concern the creation of regulations on the international level together with the establishment of transparency of action and liability in the field of services. A cautious assumption can be made that achieving the desired balance in the relationship between freedom and security in the digital space would be theoretically possible under the condition of changing the mentality and the attitude of the users themselves, who, according to the survey results, are ready to accept specific regulations (e.g. illegal content) to increase the level of security.

These changes take place at a slower pace than the dynamics determined by the ever-new solutions and technical services, but any beginning is the right step towards security. Therefore, there is once again a demand for the need to raise the knowledge and awareness of users already at the level of primary education. Only comprehensive activities in this area have a chance to realize the idea of freedom and security in the digital space in the future. Currently, for some users, the Internet network is still a *world without consequences*, however, noticeable social changes and the challenges that arise with them should constitute a permanent point of analysis, forecasts and pragmatic solutions.

The last selected problem area of the stage of the research process is closed by surveys carried out in the aspect of non-material forces and national defence means connected with social reception and identification of concepts related to state security and national defence in the area of cyberspace. The results of the conducted research confirmed initially that in the digital dimension of the security environment the level of knowledge and digital competences of users, citizens, allow for the possibility of using non-military national defence means in creating a new security model in the state structure. Additionally, research has demonstrated the existence of significant user awareness in this area (e.g. the possibility of an official announcement of a digital war).

The range of challenges facing the use of users' competences in creating national defence is just emerging and requires in-depth research but has already been clearly identified and can be a motor of progress in the way of thinking. The measures taken in this matter should ultimately enable the improvement of the concept of creating the state security system, including such a sensitive element as the non-military means of national defence in cyberspace with a wide spectrum of their application.

The entire research process is completed with generalized conclusions and a summary. Among the reflections ending the deliberations, one of the most important messages is that the understanding of the increasingly complex security environment and the creation of the state security system requires considering the *network of problems* [problems connections] implied by cyberspace. In turn, achieving adaptive flexibility will require changes at the organizational and functional level, which now, can be considered as a significant barrier with the complexity of problems presented only in selected areas of the monograph.

The proposed actions and ultimately legislative work would certainly not only contribute to increased digital social awareness, but above all - it would establish normative grounds for protection in this respect. In addition, the results of the conducted research may become useful for state authorities and institutions and decision makers at the strategic level. In turn, proposals for possible changes, presented with the intention of adapting existing solutions to the dynamics of change and the emergence of new phenomena (in terms of their multifaceted and determinants) determining the emerging challenges, bring the appropriate theoretical concepts to the social sciences and gives the possibility of their pragmatic use, particularly in the area of security science.

Defining concepts and phenomena allows for the possibility of predicting the effects and determining the remedies, but especially for pragmatic preventive actions. The proposed approach to the topic may also outline future research trends, contributing to the creation of a new paradigm in social sciences.

As part of the conclusions, I would like to emphasize that the indicated achievement is a study consuming the results of research on selected issues of cyberspace in the dimension of security together with their continuation. It is an attempt to systematize my research regarding the scientific problem reflected in the title of the monograph. Therefore, selected problems include research, the results of which have been partly published in national and international science journals. This topic not only does not lose its relevance, but it is finding a wider understanding, both in theoretical and practical aspects. The emerging

scientific theories serve to strengthen the level of security of both individuals and states, providing support for practical opportunities to improve the security system, which was also my intention as the author of this monograph. The study probably is not free of imperfections in the problem being solved, but they are not the result of methodological unreliability or carelessness.

Summarizing the indicated achievement, referring to the essence and aspirations of my research to the deterministic complexity of cyberspace, I will use a paraphrase quote: *Everything is possible, but not everything is certain.* For this reason, the analysis of new phenomena at the rate of change dynamics in a systemic five-dimensional approach to state security, can make possible to improve this system, making it effective and more resilient.

5. Discussion of the remaining scientific and research achievements

As part of my scientific and research work, I focus my interests around the subject of security in an interdisciplinary approach, in the area of *cybersecurity and security law.* The inspiration and encouragement to undertake research in the presented area of security was not only the fascination with modern technology, its possibilities and influence on the scope and forms of functioning, but also the passion for learning about it and analysing it in combination with knowledge gained through practice and during studies, which was reflected both in the selected topic of the master's thesis (*Evidence problems in cases related to computer crimes)*, and in the doctoral thesis (*Protection of cyberspace in the national security system of the Republic of Poland).*

Empirical research was initiated as a result of using modern tools at the user level. The results of the first experiments, which became a subsequent inspiration to undertake scientific experimental research ended with the impossibility of further use of electronic devices. Digital tools that have been used for empirical research were: a.) malicious program, downloaded and opened the attachment from an unreliable source; b.) intended infection with a malicious program generated be means of dedicated software; c.) installation of software with a different, than specified purpose, d.) intended installation of software monitoring user activities.

The culmination of the research work was the doctoral dissertation prepared under the supervision of prof. dr hab. Ryszard Jakubczak: *The protection of cyberspace in the national security system of the Republic of Poland* [Police Academy archives, pp. 483. Police Academy, Szczytno 2014,]. The proposals of defining the following concept, presented in the doctoral

dissertation: (1) *cyberspace* – as an *area* (systems, networks, devices), in which *there is a digitized information produced by a human* (creator of information) *in any form* (sound, image, data), in which the *information can be: produced, processed, transmitted and stored – determining the further connections and activities through goals (purpose of creation) and functions (information transfer), to achieve a specific effect (or change) with it;* and (2) *protection of cyberspace, which will be the protection of information functioning in it from the intentional (or unintentional): violation, distortion, modification, damage or destruction, regardless of the circulation (closed or open) and the form in which it functions* – have become a determinant of in-depth research both in functional and normative terms.

The legal possibilities of regulating virtual phenomena are also part of my passion for research in this field, being an inspiration to seek solutions in this sphere above all for security. The argument for the need of their existence is the degree of advancement and the use of technology in each field and the scale, types and the potential consequences of the materialization of digital crimes.

Scientific development and improvement of the research workshop took place from the moment I started to work at the Institute of Security and Defence Systems of the Faculty of Logistics at the Military University of Technology of Jarosław Dąbrowski in Warsaw, in which from 2016, I am also the Head of the Department of Strategies and Defence Systems.

During my current scientific and research activity (apart from lecturing, where I used the results of the research), I was also involved in a fundamental research in this area. The multi-faceted approach to problems in the area of law, security, defence or logistics as well as a scientific internship at the Institute of Motor Transport (2018) allowed me to build a potential of knowledge that enables holistic recognition of many phenomena determined by dynamically changing conditions. In subsequent stages of scientific and research work, I devoted special attention to research on user behaviour and explored the issue of risk proliferation in the structure of information flows, which was reflected, among others, in a joint monograph: B. Wiśniewski, R. Kowalski, J. Kozioł, M. Szyłkowska, *Safety of decision-making processes*, WKA TUM, Wyd. Social Observatory Foundation 2018. ISBN 978-83-7454-445-0, Wrocław 2018, as well as in individual research projects. In particular, the results of empirical research included in the presented monograph were part of the scientific and research work as part of fundamental research, of which I am the coordinator. These include: *Intangible national defence measures* - coordinator of science project, Warsaw 2017-2018 [work code: PBS

881/2018] and: *Proliferation of threats implied by information users as a critical factor of their safety* – coordinator of science project, Warsaw 2019-2020 [work code: PBS 904/2019].

In the last five years of work, since the of the doctoral dissertation, from among the research carried out by myself and as a member of research teams, the achievements include, inter alia, full scientific papers, chapters in monographs and scientific articles in peer-reviewed national and international scientific journals (including in Germany, Bulgaria, Slovakia, and Ukraine), popularizing knowledge in the field of security. These achievements are both: the result of my independent studies and studies carried out jointly with other co-authors.

- ✓ Selected monographs and chapters in monographs:

1. B. Wiśniewski, R. Kowalski, J. Kozioł, M. Szyłkowska, *Safety of decision-making processes*, WKA TUM, Pub. Social Observatory Foundation 2018 (collective work: own contribution: 25%, number of pub. sheets: 9,77 (pp. 210)], ISBN 978-83-7454-445-0, Wrocław 2018.
2. M. Marciniak (red.), B. Ćwik, J. Figurski, J.M. Niepsuj, M. Szyłkowska, S. Wojnarowska-Szpucha, K.E. Świerszcz, *Dilemmas of Contemporary Defence of Poland - Non-military conditions of state defence* (own contribution - Chapter 7, p. 72-82, pp. 270), Pub. Adam Marszałek, ISBN 978-83-8019-839-5, Toruń 2017.
3. L. S. Kościelecki, Z. Trejnis (red.), J. Bil, P. Bryczek-Wróbel, M. Cieślarczyk, M. Szyłkowska (i.in.), *Challenges and threats to the security and defence of the Republic of Poland in the 21st century in the social and technological-environmental dimension.* The monograph is a report on the implementation of the research task entitled "Challenges and threats to security and defence of the Republic of Poland in the 21st century" carried out as part of the Research Grant No. 997/2018 titled "Logistic system as a determinant of the defence capabilities of the Republic of Poland" carried out by the Logistics Department of the Military University of Technology of Jarosław Dąbrowski in Warsaw financed by the Ministry of National Defence of the Republic of Poland. Collective work - participant, participation (chapter, p. 30, all: pp. 381, number of sheets issued: 22.9). Ed. ASPRA-JR publishing house. ISBN 978-83-7545-913-5. Warsaw 2018.

- ✓ Chapters in monographs:

4. B. Wiśniewski, M.Szyłkowska, *Cyberspace security – legal and organizational challenges* [in:] *Cyberspace – addictions, inhibitions, threats,* Foundation PRO POMERANIA Słupsk, p. 51-68, ISBN 978-83-63680-31-2 (my contribution in the study is 50%), Słupsk 2016.
   The publication analyses and diagnoses the organizational and legal status in the area of cyberspace security - including regulations included in particular -in: the Constitution of the Republic of Poland of April 2, 1997, the Act of 29 August 2002 *on martial law and competences of the Supreme Commander of the Armed Forces and the rules of his subordination to the constitutional organs of the Republic of Poland*, the Act of 6

June 1997 - *Penal Code*, The Act of July 18, 2002 *on the provision of electronic services*, the Act of September 12, 2002 *on electronic payment instruments*, the Act of August 29, 1997 - *Banking Law* and the Act of April 26, 2007 *about crisis management.* The scope of regulation included was also indicated in a later Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 *concerning measures for a high common level of security of network and information systems across the Union.*

5. M. Szyłkowska, *State authorities performing administrative police tasks* [in:] Administration of security. Selected problems. Volume I. University of Administration in Bielsko-Biala, p. 201-212; ISBN 978-83-935790-9-9, Bielsko-Biala 2016.
   The chapter includes the systematisation of state organs performing administrative police tasks. Bodies of this kind have a special character - apart from control functions - they also have competences typical for state administration bodies - in particular, imperious (e.g. issuing decisions) and police functions. Forms of functioning and activities are carried out both by inspections and specialized administrative services equipped with supervisory, regulatory and control functions (issuing permits, administering financial administrative penalties). In addition, some of them have competences and prerogatives for investigations (e.g.: prosecution of criminal offenses and tax offenses and e.g. Border Guard, Customs Service - and in the scope of simplified proceedings, among others: Trade Inspection, UKE President, or Forest Guard).

6. M. Szyłkowska, *Legal challenges for digital threats* [in:] Contemporary challenges of social and economic sciences, University of Technology and Trade of Helena Chodkowska, p. 546 – 556. ISBN 9788362250370, Warszawa 2016.

   The key result of the research outlined in the topic of the indicated chapter was the postulate to create a separate the Cyberspace Protection Act, containing consistent definitions from the area of cyberspace; determining competence and tasks taking into account the state structure and division of powers, as well as create of new institutions with separate competences and units at the civil and military level (e.g..: the Cyberspace Protection Agency, the Military Service of Cyberspace Protection). In turn, the creation of the Protection of Cyberspace Security Office, would allow to concentrate efforts, tasks and competences in one institution.

7. M. Szyłkowska, *Contemporary problems of combating cybercrime* [in:] Internal security and the law and management (selected problems). The Main School of Fire Service,
   p. 35-52, ISBN 978-83-88446-62-7, Warszawa 2016.

   The chapter presents the results of research on the issue of combating cybercrime, pointing to their broad and heterogeneous scope - starting with from inaccuracies of conceptual collections in legal regulations to evidential problems in the field of strictly *online crimes*. A comparative analysis of crimes classified as computer-made and against systems was also made - along with reflection on the evidentiary difficulties in such cases.

8. M. Szyłkowska, W. Jakubczak, *Challenges and concepts for the protection of cyberspace in the era of globalization* [in:] Cyberspace – addictions, inhibitions, threats, Pub. Foundation PRO POMERANIA, p. 69-98, ISBN 978-83-63680-31-2 (my contribution in the study is 50%), Słupsk 2016.

   In the matter of the theme of publication were the results of the analysis, which were subjected to existing concepts of cyberspace protection at the international level, as well as the applicable strategic documents and legal regulations. The current (then) trends were also presented along with the discussion of the assumptions and objectives of building military cooperation and the potential of defending cyberspace based on common systems of warning and information exchange, as well as developing the ability to cooperate in all states (state of peace, crisis and war).

9. M. Szyłkowska, R. Socha, *Organizational and Legal Conditions of Command in the Legal System in Poland* [w:] Schriften zu Mittel - und Osteuropa in der Europäischen Integration. Band 21 Management Contexts in Security Institutions, s. 97-108 (my contribution in the study is 50%), ISBN 978-3-8300-9339-8 Hamburg 2017.

   The chapter analyses the legal and organizational determinants of management and command during peace and during the war under the Polish legal system in the light of the amendment of the regulations in this area along with the analysis of the change of the command and control system as part of the reform of the Armed Forces launched in 2011, which at the time was one of *The main directions* of *development of the Armed Forces of the Republic of Poland and their preparations for state defence for 2013-2022.*

10. B. Wiśniewski, M. Szyłkowska, *Emergency and crisis management in cyberspace* [in:] *Management of public and private institutions in the context of uncertainty of threats, crises and risks*, p. 299-316, ISBN 978-83-7462-578-4 (my contribution in the study is 50%), Pub. Police College, Szczytno 2017.
    The publication presents key recommendations related to the organization of the security system in the normative network in the context of emergency states and crisis management, which may be triggered by actions in cyberspace. Attention was drawn to the necessity of legal regulations, regarding administration bodies - in the matter of defining the rules of their operation and decision-making procedures in all phases of crisis management.

11. W. Kaczmarek, M. Szyłkowska, *Legal terms of liability for software – outline of the problem* [in:] Administration of Security – selected problems. Volume IV, Academy of Administration in Bielsko-Biala, 2017, p. 119-130, ISBN 978-83-935790-0-6 (my contribution to the study is 50%), Bielsko-Biala 2017.
    The chapter presents (in outline) the problems of existing and missing legal regulations regarding digital products and electronic devices and conditions of liability for these products. The analysis covered in particular: Council Directive of 14 May 1991 *on the legal protection of computer programs* (91/250 / EEC), Council Directive of 25 July 1985 *on the approximation of the laws, regulations and administrative provisions of the Member States concerning to liability for defective products* (85/374 / EEC), the

Act of 30 June 2000 - *Industrial Property Law* and the Act of December 12, 2003 *on general product safety.*

12. M. Szyłkowska, *Cyber terrorism - threats to the security of the individual and the state* [in:] *Challenges and threats to the security and defence of the Republic of Poland in the 21st century in the social and technological-environmental dimension* [chapter, p. 30, all: pp. 381, number of sheets issued: 22.9). Ed. ASPRA-JR publishing house. ISBN 978-83-7545-913-5. Warsaw 2018.

    The publication presents a conceptual analysis of the phenomenon of cyberterrorism currently assessed as one of the fastest growing threats, with the indication of practical examples - and a proposal for theoretical typology (cyberterrorism proper (only in cyberspace) and quasi-cyberterrorism (cyberspace as an element of activities). In addition have been presented potential types of weapons of technical and electromagnetic cyberterrorism (including using IEMI, HPM and EMP).

13. M. Szyłkowska, *Verification proceedings and security clearance in the context of global forms of contact* [in:] "Contemporary problems of management and security", Pub. UTH, ISBN 978-83-62250-42-4, Warszawa 2019.

    The publication analyses the issues of the existing procedure under Polish law about security clearance in the context of global - digital forms of contact. The main purpose of the considerations was to indicate the need to update the regulations regarding the discussed matter - *Personal Security Surveys* – attached to the Act, in relation to forms of contact with citizens of foreign countries, which currently take place mostly via digital message services.

✓ Selected scientific articles:

14. M. Szyłkowska, *The cyber threats of modern IT solutions supporting logistics* [in:] Material Economy & Logistics, Polish Economic Publishers SA, No. 5/2015, Polskie Wydawnictwo Ekonomiczne S.A., p. 719-730, ID: 620240, ISSN 1231-2037, Warszawa 2015.

15. M. Szyłkowska, J. Murasicki, *Digital globalization as a determinant of modern security* [w:] Scientific Papers of Witelon State University of Applied Sciences in Legnica No. 16(3)/2015, p. 73 - 83, ISSN 1896-8333, eISSN 2449-9013 (my contribution in the study is 50%), Legnica 2015.

16. M. Szyłkowska, *IT threats to national security: description, classification and problems* [w:] Bulletin of the Lviv State University of Life Safety/ Вісник Львівського державного університету безпеки життєдіяльності /Bulletin of Lviv State University of Life Safety, Nr 12/2015, s. 18 – 22, ISSN 2078-4643, Lwów 2015.

17. M. Szyłkowska, M. Kulczycki, *The Armed Forces as the guarantee of the safety and peace on the country's territory and beyond the border`s- legal regulations* [w:] Вісник Львівського державного університету безпеки життєдіяльності / Bulletin of the Lviv State University of Life Safety, s. 6-11, No. 12/2015, ISSN 2078-4643 (my contribution in the study is 50%), Lwów 2015.

18. M. Szyłkowska, *Regulation on State of Exception in Polish Legislation* [w:] Schriften zu Mittel- und Osteuropa in der Europäischen Integration/Legal Context in the Chosen Order and Security Area, Verlag Dr. Kovač, s. 135-148, ISBN 978-3-8300-9140-0, Hamburg 2016.
19. M. Szyłkowska, *Digital extortions and falsifications as the key threats for supply chain companies* [in:] Material Economy & Logistics, Polish Economic Publishers SA, No. 5/2016 (CD), p. 716-727, ISSN 1231-2037, Warszawa 2016.
20. M. Szyłkowska, R. Polak, *Digital logistics challenges* [in:] Material Economy & Logistics, Polish Economic Publishers SA, No. 9/2016, p. 719-729, ISSN 1231-2037 (my contribution in the study is 60%). Warszawa, 2016.
21. M. Szyłkowska, *Digital threats and challenges for a state security - review, classifications, definitions,* Sociálno-psychologické aspekty utvárania osobnosti príslušníkov ozbrojených síl, bezpečnostných a záchranných zborov: zborník vedeckých a odborných prác z medzinárodnej vedecko-odbornej konferencie v Liptovskom Mikuláši, Akadémia Ozbrojených Síl gen. M. R. Štefánika, ISBN 978-80-8040-519-9 Słowacja 2016.
22. M. Szyłkowska, *Cyber threats in logistics - an outline of the problem* [in:] „Vasil Levski" National Military University/ "Scientific Works", p. 130-139, ISBN 978-954-9681-82-6, *Cybersecurity in the information society*, Shumen 2017.
23. M. Szyłkowska, *Human factor in the proliferation of threats* [in:] The Intentional Scientific Journal: "Security & Future" Issue 2/2018, p. 55- 58, ISSN (Print) 2535-0668, ISSN (Online) 2535-082X. Red. Prof. Nikolay Radulov, Sofia 2018.
24. M. Szyłkowska, *Security challenges for cyber identity-outline of the problem* [in:] International Scientific Journal "Industry 4.0." ISSUE 2, P.P. 102-105 (2019), ISSN 2535-0005 (Print), ISSN 2535-0013. Sofia 2019.

The mentioned research activity was presented at national and international conferences and scientific seminars, where in the form of speeches or presentations I presented problem-related issues and the results of science investigations carried out in this area, including:

- ✓ II Coordinating Conference of Poland's participation in the MCDC project 2015-2016, a working meeting: "Concept of military operations in cyberspace", Warszawa 2015.
- ✓ I International Scientific Conference: *Contemporary management and security problems*, UTH, Zakopane 2016.
- ✓ VIII National Scientific Conference: *Participation of modern solutions in ensuring Poland's security in the light of current threats,* WSGE, Józefów 2016.
- ✓ VIII Scientific Conference of Applied Logistics: *Dual-use technologies in civil and military logistics. Theory and practice*, ILOG Department of Logistics of the Military University of Technology, Rynia 2016.

- ✓ III International Scientific Conference: Contemporary Management and Security Issues, UTH, Zakopane 2017.
- ✓ International Scientific conference: Cybersecurity in the information society, "VASIL LEVSKI" National Military University, Shumen, Bulgaria 2017.
- ✓ II International Scientific Conference on Security „CONFSEC 2018", Scientific-Technical Union of Mechanical Engineering, Bulgaria 2018.

In addition, I also participated in the following organizational and scientific committees:

- ✓ I edition of the Conference: *Security of European Borders of the 21st century, "Protection of the European Union's borders in the context of migration processes*, Department of Logistics of the Military University of Technology, Warsaw 2015.
- ✓ I National Scientific and Training Conference: *Non-military defence preparations, crisis management and civil defence in the security and defence system of the Republic of Poland*, ISBiO Military University of Technology, Warsaw 2016.
- ✓ I National Scientific Conference: *Dilemmas of contemporary defence of the Republic of Poland RP*, ISBiO Department of Logistics, Warsaw 2017.
- ✓ II National Conference of Scientific Groups, Warsaw 2017.
- ✓ II International Scientific Conference: *Dilemmas of contemporary defence and security of the Republic of Poland*, ISBiO Department of Logistics of the Military University of Technology, Warsaw 2018.
- ✓ Scientific conference: *ANIMUS BELLI 2017*, Academy of War Art, Warsaw 2017.
- ✓ I National Scientific Conference *GlobState*, 2018: *Challenges for the security of the state in the aspect of the changing geopolitical environment*, CDiS SZ, Bydgoszcz 2018.
- ✓ III National Conference of Scientific Groups of the Faculty of Logistics of the Military University of Technology "New challenges and directions of changes in logistics", ILOG ISBiO Department of Logistics of the Military University of Technology, Warsaw 2018.

In addition, I am the author of the review of:

- ✓ The monograph Gula P.;' Prońko J.; Wiśniewski B.: *Information management in crisis situations (2nd edition supplemented)*, ISBN: 978-83-60430-08-X, WSA Bielsko-Biala 2015;

- ✓ The scientific article: *National critical infrastructure as the target of cyberattacks* [in:] "Student Notebooks PRO PUBLICO BONO", Yearbook of the Main School of Fire Service in Warsaw, Warszawa 2017;
- ✓ The scientific article: *The challenge of the 21st century – war in cyberspace* – II National Conference of Scientific Groups "Logistics and defence in the light of new technologies", Department of Logistics of the Military University of Technology 2017;
- ✓ The scientific article: *Cyberspace as a new dimension of human activity – conceptual analysis*, Teleinformatics Review ISSN 2300-5149, Warszawa 2018.

In the activities in the popularization of security science, I was the author of articles on: *Cyber space - a new field of activities during the modern war* [in:] The Civil Defence and Crisis Management Guide, March 1/2016. ISSN 1733-8417 and *Four sides of information* [in:] The Civil Defence and Crisis Management. ISSN 1733-8417.

In terms of a significant contribution to scientific activity, should be also perceived didactic achievements in which I conducted and still conduct the following lecturer classes (including all forms: lectures, seminars, laboratories and seminars):

- ✓ *Protection of cyberspace in the defence system.*
- ✓ *Information society.*
- ✓ *National and international security standards in cyberspace.*
- ✓ *Security in cyberspace.*
- ✓ *Science about the state and law.*
- ✓ *International logistics.*
- ✓ *Basics of international logistics.*
- ✓ *Cyberspace protection as a part of defence system* – within the ERASMUS+ program.

Issues in the indicated research areas constituted the theoretical basis to develop modules in the educational programs prepared by me - include:

- ✓ *Information society* – master's program in the field of: *Defence of the state* [2017/2018].
- ✓ Development of the concept of classes using the multimedia laboratory – *Laser Trainer Vistula* – in the field of: *Theory and practice of shooting* – master's program in the field of *state defence* [2019/2020].
- ✓ *International logistics* – master's program in the field of logistics [2016/2017; 2017/2018].
- ✓ *National and international standards for the protection of cyberspace* master's program [2016/2017],

- ✓ *Cybercrime* [2017],
- ✓ *Cyberspace and its threats* [2017],
- ✓ Development of a module of classes using the multimedia laboratory – Laser Trainer *Vistula* – in the field of: *Theory and practice of shooting* – bachelor's program, implemented in the academic year [2018/2019].
- ✓ *Protection of cyberspace in the state's defence system*– bachelor's program in the field of *state defence* [2015/2016].
- ✓ *Cyberspace security* – bachelor's program [2015/2016].
- ✓ *Basics of international logistics* – bachelor's program in the field of logistics [2016/2017; 2017/2018].
- ✓ *Cyberspace protection as a part of defence system* – ERASMUS+ program [2018/2019].
- ✓ *Cybersecurity – basics* – development of a training program in the area of cybersecurity – obtaining the Rector's consent for conducting trainings addressed - in particular - to employees of public administration at all levels. The program was developed in accordance with the assumptions adopted in the *Doctrine of cybersecurity of the Republic of Poland:* Chapter 4. The concept of preparation tasks (...) - 4.3. Public and private support links – point 54.

In addition, I managed 43 diploma theses (supervisor of theses: 1st degree 2nd degree and manager of final postgraduate studies) and I was a reviewer of 7. The topics of work include, for example: *The importance of security of information processing systems for the functioning of logistics companies. Cyber threat in the logistic supply chain of digital products. Analysing and creating consumer behaviour by using digital data. Possibilities of achieving a competitive advantage on the market of non-negotiable digital products in the distribution process. Digital surveillance as a measure for creating the security environment. Electronic civil disobedience as a new social phenomenon. The importance of personal data protection for the security environment formation. Possibilities of using digital media in an information war. The potential of the Internet of Things in the formation of state security environment.* In addition, I am currently the promoter of the final work 10. graduates.

In terms of a significant contribution to scientific activity, should be also perceived my other didactic and organizational achievements in which are: implementations of modern solutions supporting didactic processes in the area of security and defence of the state and logistics. The added value of implementations is the possibility to conduct scientific

research, the results of which will then translate into further use in the didactic process. These include:

- ✓ Development, preparation and implementation of the laboratory position – *multimedia training system of the VISTULA TL shooting training.* Field of study: *Defence of the state* [subjects: *Basics of shooting* and *Theory and practice of shooting*]. The system allows for conducting exercises: static, situational and interactive with the use of replicas of weapons equipped with a laser emitter. Generated scenarios allow a very real mapping of simulated conditions, among others, in the scope of ballistics of the projectile – weight, diameter, muzzle velocity and atmospheric conditions.
  An additional, innovative solution are the tactical vests simulating shots with the use of vibrating motors [2017/2018].
- ✓ Development, preparation and implementation: *Laboratory of research on cybersecurity and information security* 2018/2019. Name of the subject: *Cyberspace protection in the defence system* [2018/2019]. The laboratory has separate computer stations, prepared for *malware software* research in the aspect of their impact on the operating systems and positions for conducting research in the field of user behaviour and reactions as part of the Internet activity and the effects of individual activities performed on devices equipped with commercial operating systems.
- ✓ Development, preparation and implementation: *Critical infrastructure protection laboratory* [2019/2020]. Currently, the laboratory equipment – besides the workplace infrastructure – consists of the dedicated software, i.e.: a.) simulation decision games based on techniques enabling faithful representation of the actual course of the selected critical situation, including the necessary elements, i.e.: roles, decisions, phenomena and infrastructure. It allows for effective skills improvement, among others: selection and analysis of information, correct assessment of the situation, making difficult decisions, using the available forces and resources in an optimal manner, proceeding within the limits of the powers set out in the function, communication and cooperation in the team; b.) software for risk management in standardized management systems, among others, support for strategic and operational risk management, including as part of the ISO 31000 and COSO I standards; risk management as part of the management control, and identification and assessment of threats for the continuity of processes.

In addition:

- ✓ Implementation of software including a comprehensive set of advanced analytical procedures [2016/2017].
- ✓ Implementation of software dedicated to risk analysis and analysis of threats to the protection of classified information, serving as practical support of individual subjects in the didactic process based on the methodology consistent with the recommendations of the Department of ICT Security of the Internal Security Agency and the Regulation of the Prime Minister on the *basic requirements of ICT security* [2017/2018].
- ✓ Implementation of software dedicated to risk analysis and analysis of threats to the security of personal data [2019].
- ✓ Implementation of software in the area of international logistics together with the possibility of certification – educational version of a professional application used in the TSL industry. The transport exchange module helps train students' practical skills in the field of broadly understood transport organization [2016/2017].
- ✓ Implementation of software in the area of logistics – educational version of specialist, decision-making software, allowing to acquire practical skills in a wide range, including structure and network planning, distribution optimization and work automation, process efficiency improvement (including KPI quality analysis) [2017/2018].

Additionally, as part of the didactic and popularizing activities:

- ✓ I organized study classes for students in the field of: *State defence* – in the Central Centre for Contamination Analysis [2016/2017].).
- ✓ I conducted the training: *Cybersecurity – basics* – at University of Szczecin, 2017.
- ✓ I conducted the following external and open lectures in the field of cybersecurity:
  - National Defence Academy in Warsaw [Management of internal security systems [2014/2015],
  - Cardinal Stefan Wyszynski University in Warsaw: *Legal basis for cybersecurity* [2016],
  - Centre for Certification and Quality – 2019,
  - The Military University of Technology *Open Day* [2017, 2018 and 2019] and training classes: *Cybersecurity* – as part of the program of the Ministry of National Defence "Legia Akademicka" implemented at the Military University of Technology in Warsaw [2019].

In terms of a significant contribution to the scientific activity should also be perceived other organizational achievements. Among them, actions to promote knowledge about security deserve special attention - as part of the participation in editorial committees and scientific boards of journals, including:

- ✓ *Defence science review* – member of the editorial team, Pub. WAT, Warszawa 2017, ISSN 2450-6869.
- ✓ *Students' Science Papers PRO PUBLICO BONO* No. 1(1) 2017, Main School of Fire Service, Department of Civil Engineering – Member of the editorial board – theme editor of the *Cybersecurity* section. Warszawa 2017 ISSN 2544-2481.
- ✓ *Logistics and defence in the light of new technologies – KNS WAT, E*d. Pub. WAT, Warszawa 2017 – member of the editorial committee.

In addition, I am a member of the following international and national organizations: *Information Systems Security Association* – International Association of Information Systems Security [2018 – now] and the "Safe Children" Foundation [2015-now].

The mentioned above activity, propagation of the achievements of security sciences, has been awarded distinctions by rewarded from:

- ✓ Director of the Department of Security and Crisis Management - Diploma of recognition for *popularization in the field of security in the pages of the "Civil defence information and crisis management guide" for increasing the effectiveness of the governmental field operations* (2015).
- ✓ Commandant of the School of Aspirants of the State Fire Service in Krakow - Diploma of recognition as *a scientific support for educational initiatives for general safety* – School of Aspirant of the State Fire Service in Krakow (2016).

In addition, I received The Bronze Medal of the Armed Forces in the *Service of the Fatherland* (2018) and many times received awards and recognition prizes from my superiors.

As part of other achievements, the following may be indicated: *The Security Certification* in the scope of access to classified information. Noteworthy is also the possession of the international *PRINCE2® Foundation Certificate* - certifying knowledge of process-based project management.

Summarizing my scientific, academic activity and achievements, I would like to emphasize that it stays within the field of social sciences and are closely related to it - above all in the sphere of security sciences. My scientific, didactic and popularizing activities were focused, connected and contained in two main areas: cybersecurity and security law. My scientific activity refers above all to the phenomenon of the deterministic complexity of cyberspace in the context of security and the legal aspects and foundations of security - in a broad sense.