OPINION

prof. Rus Marinov Dr. Sc.,
New Bulgarian University

The dissertation work for the award of the degree of "Doctor of Sciences"
in the Professional Area 9.1. National Security.

As a member of the Scientific jury to obtain a doctoral degree in professional field 9.1. National Security, with a participant prof. Nikolai Radulov. Based on Order No. 3-RK-165 of 03.20.2020 and Decision AC 07 / 17.03.2020.

The dissertation, written by a professor, Dr. Radulov, is on the topic: "**Technological and digital transformations in security. Security 4.0** ".The dissertation has a total volume of 378 pages. The structure of the work consists of an introduction, five main parts, conclusion and sources used. The volume and structure of the dissertation show that prof. Radulov has done significant research work, in the field of national security and the use of modern information and communication technologies in the transformation of security structures. The various sections and chapters of the dissertation follow chronologically and logically the idea of presenting an overview of the main sources on the role of intelligent technologies in managing important aspects of security 4.0. The content of the dissertation demonstrates that prof. Radulov chose one of the most actual problems as the goal of research work.

The relevance of research

The topic discussed is related to issues that are extremely relevant due to the accelerated development of new technologies, which leads to their daily and ubiquitous use. The fourth industrial revolution underway poses new challenges to security professionals. It is necessary to draw up a complete picture, the result of clarifying the links between the technologies used or with potential to be used in the security system and the changes caused by them both in the system itself and in its individual elements (substructures), as well as so in the overall ecosystem of Security 4.0. Different technologies create both security advantages and problems. This is because security is a complex concept, it is made up of many interconnected and interdependent components, so that wherever thoughtless or malicious innovation (new technology) is used, the overall effect may be reduced, compromised, insufficient security. So far, the problems of high-tech and digital and technological security transformations have not been addressed anywhere in the world. The subject of research is modern security with its advantages and disadvantages, but especially in terms of high technology and digitalization. This site is extremely dynamic but placing it in the light of new features will allow us to provide new and improved levels of security and safety of life. The research is oriented to the current state and prospects of integration into the security of a qualitatively new toolbox, which will bring it to the level of world requirements considered from the perspective of Industry 4.0.

The subject of the study is the current state and prospects of implementation in the security of a qualitatively new toolkit, which will place it at the level of the requirements of the world, considered from the standpoint of Industry 4.0.

Aims and main tasks of the study

The main argument of the thesis is that only the vigorous introduction of high-tech and digital tools and the subsequent restructuring of special services can ensure the security of people in the high-tech environment of Industry 4.0. In view of the above, the purpose of the study is to identify those aspects of high technology and digitalization that would contribute to achieving sufficient security for people in the rapidly evolving technological world – to create a vision for high-tech security. To achieve this ultimate goal, the author sets himself the following tasks: exploring the relationship between the technological revolution, a consequence of Industry 4.0, and security, defining the concept of Security 4.0.; dentification of new technologies that can be used in security; analyzing the threats to citizens' security and national security as a possible result of the use of the latest technological tools and applications by criminal circles. Identification of current technological crimes; modeling existing and future opportunities to build a security ecosystem that meets today's challenges.

Correlation between the chosen methodology and research methodology and the goal and objectives of the dissertation

The dissertation research examines a specific and so far, not covered complex specialized topic. When analyzing security issues in the light of modern, extensively evolving technologies, the focus is on the application and role of technology in two poles – crime-counteraction, with the aim of the work to outline the possibility of proactive behavior by special services. Using single solutions to generate complex capabilities requires the use of logical methods, especially analysis, synthesis and deduction..

However, the inductive method is also widely used, as it seeks to address the topic of security, starting from the individual and moving on to the effect on civil and national security in a gradually expanding circle, similar to the circles forming on the smooth water surface after stone throwing – from the security of one's own home, neighborhood – to the city, region, state, international community.

By analyzing and using the method of comparing and adapting best existing practices and developing perspectives, the current and emerging technological tools that optimize operation performance and high efficiency are derived.

The inductive and deductive method, the analysis, the comparative analysis, the analysis of the analysis and the synthesis are used in all parts of the study and they help to individualize the problems and at the same time to draw summaries and conclusions. The thesis relies heavily on synthesis, presenting an expanded view of all the major issues of introducing a high-tech toolkit to create a modern security ecosystem.

In presenting the problems, the historical method was also used, without going into an extensive narrative form and only where it was considered necessary to put the issues into perspective and to demonstrate the necessary and inevitable link between the past and present – from the First Industrial Revolution to Industry 4.0, in order to guarantee the author's conclusions. Given the need to explore processes in their development over a longer period of time, this method is of limited use at the beginning of work. The inductive and deductive method, analysis, comparative analysis, analysis and synthesis are used in all parts of the study, and they help to individualize problems and at the same time draw summaries and conclusions. The thesis is based on a generalization, presenting an expanded view of all the basic issues of introducing high-tech tools to create a security ecosystem.

Scientific and applied contribution of the dissertation (description and evaluation), including the availability of an original contribution to science

The idea of introducing modern technologies and digitizing security is a contribution to Bulgaria, where there are individual elements that are considered individually and in limiting individual approaches to use. Security 4.0, the ecosystem of security, the ecosystem of individual crime prevention applications is considered for the first time in a comprehensive manner and were first identified by the author in separate articles over the past two years. An analysis of the possibilities of new technologies for generating new types of crimes was considered in separate materials, but never before in a single work that achieves comparative complexity and synergy. The view on digital crime has not yet gone further than cybercrime, which significantly narrows the possibility of considering and discussing the problem from the point of view of the new digital world - the space of big data, the Internet of everything and virtual reality.

In a broader sense, considering the topic of security through the prism of the world of high technology and the digital being, but in a complex aspect and in the theory of intelligence, counterintelligence and security, is a creative and unused approach. She develops a number of problems, only hinted at a number of articles on various issues of security technology, including the author.

Specific contributors to the study are the definitions of Security 4.0, the Security Ecosystem, and their structural and semantic analysis. Another specific contributing element is the creation and description of models for the use of modern technologies in security theory and practice, as well as the creation of conceptual models for new applications and new security products.

The practical relevance of the study

The thesis is that only the vigorous introduction of high-tech and digital tools and the subsequent restructuring of special services can ensure the security of people in the high-tech environment of Industry 4.0. The work proves that the optimal and modern development of special services and the achievement of high quality civil and national security is only possible through the accelerated introduction of high-tech and digital tools. The dissertation confirms that the moment for such changes is appropriate. Not only that, the fact that the security and public order services in the most developed countries are already making their first steps this way is evident.

Currently, the development of the Bulgarian special services is stagnant, in purely organizational and value terms. It is not at all a fundamental technological change for which the world is ripe, and citizens are suffering even from the lack of its beginnings. Unfortunately, though a little better, but not enough in scope, is the state of the European Special Services. It seems that the French special services and the police look a little better, but there has not been a common concept and implementation yet. We are far from the achievements of US and Russian high-tech intelligence and counterintelligence organizations.

Evaluation of publications of the dissertation: the number, nature of publications in which they are published

Cited sources - 176, of which 6 in Bulgarian, the rest from electronic sites and foreign authors. Total footnotes 213. Annotation on 27 pages. Number of dissertation publications –10. Of the publications presented in Bulgarian are-4, the rest in English, published in the materials of scientific conferences by specialized security journals. Also presented is a monograph on the topic "Security 4.0", a monograph edited by. NTS on Industry 4.0 Engineering, Sofia, 2019, ISBN 978-619-7383-15-7. 325 pages. In conclusion, the author notes that success in the field of security is directly measured in terms of the level, quality of life, calmness of the average person. Therefore, the technologies used and applied should not only be humane, but also in the service of society, giving priority to the building, good forces.

Publications in professional magazines

Scientific publications on this topic have been published in prestigious publications with implications for national security. I will give some examples with the article "Modern Security Correlations" published by Ed. NTS Edition, Technics, Technologies, Education, Security, Issue. 10, Volume 3, 2016 Five other publications in English in the national scientific journal "International Scientific Journals", STUME. Safety and the Future, Int. Sci. J., Ed. STUME, ISSN 2603-2945, in 2017-2019, respectively. I will cite as an example the publication "Additive Technologies and Security 4.0 in: Industry 4.0.

Opinions, recommendations and notes

Technologies in recent years have been improved too dynamically for a modern specialist to understand them and quickly put them into practice. In particular, the theoretical framework of modern technologies, such as artificial intelligence, automated machines, Internet of things, was established in the 50s and 60s of the 20th century and is currently used in enterprises and institutions.

For example, the framework of IoT / widely discussed in the dissertation / set up of Kevin Ashton in 1999, he himself says that the concept is conditional and modern experts say that every smart device switch to the Internet should be part of this space. In this case, some of the concepts used in practice is not entirely appropriate as a name. People love change and therefore often come up with different names to indicate new trends, such as 1G, 2G, 3G, 4G, 5G; or web1.0, web 2.0, web3.0, web4.0; and Internet1, Internet 2, the Internet of Things, the Internet of everything. The fourth industrial revolution will be associated with the active use of cybernetic systems, but we all know that the scientific foundations of cybernetics are defined by Norbert Wiener in 1948. This year, the first book was published entitled "Cybernetics: or Management and Communication in the Animal and the Machine" That is, it takes more than 60 years to find practical wide applications in business or in the work of institutions, they begin to actively discuss issues related to this science during the World Economic Forum 2016. Over the past 4-5 years, the number of publications in the field of "Security 4.0" is growing.

Statistics show that their number in the world reaches 9,840 articles. Cordis European projects are under development. In professional magazines in the field of information technology, the publication of Security 4.0 in the information field occurred in 2015. The topics are discussed during specialized seminars and forums on cybersecurity. One platform even claims that Industry 4.0 = Security 4.0. It also shows the relevance of the in-depth issues studied by prof. Radulov. Current trends are expressed not only in the creation of information security capabilities, but also in the widespread use of advances in cognitive technologies. Cognitive computers use a combination of artificial intelligence, neural networks, machine learning, execution of commands in a natural language, analysis of mood and sensitivity to context. In the case of artificial intelligence, the system assumes complete control over the processes and takes actions to complete the task or to avoid one or the other scenario using previously introduced algorithms. Cognitive technologies, in contrast to AI, only helpers and human assistants act, instead of completing the task. In addition to the trends outlined above, it is expected that new trends will be developed related to the development of a post-digital architecture based on a different logic compared to traditional computer systems. Quantum and neuromorphic computations will accelerate these trends, but in a different direction. We are currently witnessing a new era of innovation based on custom computer architectures, genetics and materials science. This requires a transformation of the organizational structure, focusing from vertical hierarchies to horizontal networks. Such trends will also impact security management models for more effective trend analysis. Current trends are expressed not only in the creation of information security capabilities but also in the widespread use of advances in cognitive technologies. Cognitive computers use a combination of artificial intelligence, neural networks, machine learning, execution of commands in a natural language, analysis of mood and sensitivity to context. In the case of artificial intelligence, the system assumes complete control over the processes and takes actions to complete the task or to avoid one or the other scenario using previously introduced algorithms. Cognitive technologies, in contrast to AI, only helpers and human assistants act, instead of completing the task. In addition to the trends outlined above, it is expected that new trends will be developed related to the development of a post-digital architecture based on a different logic compared to traditional computer systems. Quantum and neuromorphic computations will accelerate these trends but in a different direction. We are currently witnessing a new era of innovation based on new computer architectures, genetics and materials science. This requires a transformation of the organizational structure, focusing now on vertical hierarchies, to move on horizontal networks. Such trends will also impact security management models for more effective trend analysis.

A conclusion with a clearly formulated positive or negative assessment of the thesis

Professor Radulov has been giving lectures at the New Bulgarian University since 2009 and is successively elected as an assistant professor for the period 2011-2014 and from 2014. he later became head of the department of national and international security. His extensive experience as a teacher, expert, researcher and scientist allows him to work on the identification of complex security problems and technologies that are clearly demonstrated in the form of competencies in the presented work.

The author and presented it fully meets the requirements for awarding the degree of "doctor sciences." The professionalism of Professor Radulov, combined with the analytical work that he did on an interdisciplinary basis, which, in my opinion, has led to new knowledge in the field of the relationship between security and modern technology.

In conclusion, I believe that prof. Dr. Nikolai Radulov presented a completely independently developed work, with unquestionable qualities, both in the science and the scientific and application fields.

My assessment is positive, and fully I support the Thesis and appeal to my colleagues from the Scientific jury to award the degree “Doctor of sciences” to Nikolai Stefanov Radulov for his work on “Technological and digital transformation in security. Security 4.0 ", in the professional area 9.1. National security.

Date: 06.04.2020 Signature: /R.Marinov/