New Bulgarian University

School of Graduate Studies

Department of National and International Security

Prof. Nikolay Stefanov Radulov, PhD

Technological and digital transformations in security

Security 4.0

ABSTRACT

of dissertation work

for the award of the degree of "Doctor of Sciences"

in the Higher Education Strategies and Policies program 9. Security and Defense, Professional Area 9.1. National Security

Sofia

2019

The dissertation consists of 376 pages including:
Main text – 360 pages

Number of sources – 176

Number of publications on the dissertation – 10.

The author of the thesis is a head of National and International Security Department, School of Graduate Studies of New Bulgarian University and doctoral student in the same department.

Thesis researches are carried out in NBU and the Scientific and Technical Union, Bulgaria.

I. General characteristics of the thesis

1. Volume and structure of the thesis

The thesis is 376 pages. Structurally, the work consists of nine parts, including an introduction, a conclusion, a bibliography and a list of keywords. There are 84 footnotes. The bibliography list contains 176 sources, eight of them in Bulgarian, five in Russian, one in French and 162 in English.

2. Relevance of the study

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. ***This makes this research not only a vital but highly promising strategic product.***

3. Object and subject of the study

The object of the study is modern security with its advantages and disadvantages, but especially in the perspective of high technology and digitalization. This object is extremely dynamic, but placing it in the light of new opportunities will allow for a new level of safety and security of life.

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.

4. 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 digitalisation 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:

1. Exploring the relationship between the technological revolution, a consequence of Industry 4.0, and security, defining the concept of Security 4.0;
2. Identification of new technologies that can be used in security;
3. 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;
4. Modeling existing and future opportunities to build a security ecosystem that meets today's challenges.

In view of the significant falling behind of the country's special services in the area under consideration, comparisons, recommendations and best practices will be used following the example of the most active and highly developed special services in the world.

5. Methodology

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.

As in any study of this kind, a systematic approach is used. The systematic method allows to study the problems in high technologies, universal digitization, universal connectivity and their impact on security as a single system with corresponding interconnections between the different components.

The structure is characteristic of the dissertation research. This is, on the one hand, because of the already mentioned interdisciplinary nature of the topic under discussion – security-high technology-digitization, and, on the other, because of the purpose that the thesis pursues. The aim, as noted above, is to create a strategic base for high-tech security from a security science perspective. This does not preclude a thorough analysis of local good practices. On the contrary, such an analysis is required to confirm the thesis of the many and significant challenges facing high-tech security tools. These challenges are so significant that they can only be addressed by designing and building a new technological-digital and humane security model. And since these challenges are so significant that they lead to profound changes in the security structure itself, it cannot help but concern the special services and their progressive reconstruction.

6. Contributions

The analysis on the topic of incorporation modern technologies and digitalization of security is a contribution for Bulgaria, and I would say on a global scale, as far as my studies have shown that no such visionary product has been produced anywhere. There are separate elements that are considered individually and in limitation of individual application approaches. Security 4.0, Security ecosystem, Ecosystems of individual crime prevention applications are considered for the first time and have been defined for the first time by the author in separate articles within the last two years.

The analysis of the possibilities of new technologies for generating new types of crime has been considered in separate materials, but never before in a ***single work that achieves comparative complexity and synergy***. The study of digital crime so far has not gone further than cybercrime, which greatly narrows the possibility of considering and discussing the problem from the perspective of an infinitely digitized world - a world of big data, the internet of everything and virtual reality.

More broadly, addressing the topic of security through the lens of the high-tech world and the digital being, but ***in a complex aspect also in the theory of intelligence, counterintelligence and security, is a creative and unused approach***. It develops a number of issues, only partially addressed in a number of articles on private security technology issues, including mine.

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***.

7. Practical significance of the study

As I stated above, 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.

There is a lack of knowledge, courage and, above all, a vision for future development. If we look at the legal and theoretical topics in the security field in recent years, we will see stagnation, lack of ideas, indifference and misunderstanding of the modern place of the special services.

From this perspective, the present work provides recipes for exiting the status quo. It gives vision, possible high-tech constructions, adapts and brings together in a single system existing developments, operational applications and conceptual designs.

8. Limitations

The limitations of the analysis are most closely related to the vastness of the high-tech solutions created, the understandable lag in the study of the application of technological and digital instruments in security from their development. By the time this work was done, hundreds of Zbytes of new content were added to the volume of big data, and the processing power of computers was tenfold. The author therefore strives to cover the processes in depth and in principle, giving private examples only for a better understanding and illustration of his theses.

II. Main content of the dissertation

Introduction

The introduction aims to set the framework for dissertation work. It substantiates the relevance, the subject and object of the research, the goals and objectives of the work, the methodology applied. The following chapters logically follow from the frameworks placed therein:

1. Chapter One. Industrial revolutions

In the last 250 years, three industrial revolutions have taken place (Fig. 1). They have changed the process of building and perception of values and the world as a whole. Each of them develops technologies, political systems and social institutions. Production, people's views about themselves, their relationship with the environment changes.

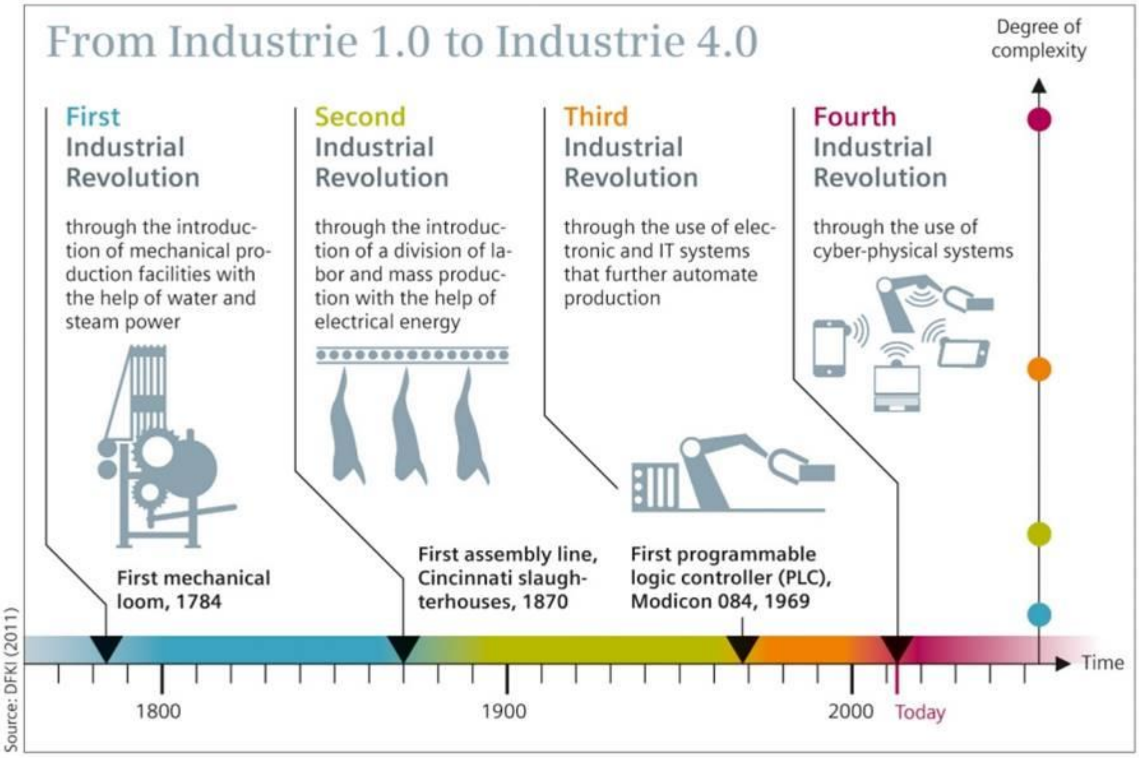

From Industrie 1.0 to Industrie 4.0
Degree of complexity
First Industrial Revolution
through the introduction of mechanical production facilities with the help of water and steam power
Second Industrial Revolution
through the introduction of a division of labor and mass production with the help of electrical energy
Third Industrial Revolution
through the use of electronic and IT systems that further automate production
Fourth Industrial Revolution
through the use of cyber-physical systems
First mechanical loom, 1784
First assembly line, Cincinnati slaughterhouses, 1870
First programmable logic controller (PLC), Modicon 084, 1969
Time
1800
1900
2000
Today
Source: DFKI (2011)

Figure 1. Industrial revolutions in time (after DFKI, 2011)

The development of public order and security systems undoubtedly follows the development of the economy and social relations. Technology development often occurs first in military and security organizations, and subsequently they also emerge as civilian use products. A parallel impact is noted in the development of the criminal environment.

To each stage of industrial development, a stage of development of the security system corresponds. Therefore, when we think about security in the flow of ideas of Industry 4.0, we mean innovative paradigms, technologies, and security techniques that are relevant to the high technology that we should unite under the common name Security 4.0.

2. Chapter Two. The Forth Industrial Revolution and Security. Security and insecurity

The author analyzes and synthesizes in a unified system the ideas of the technologies of the Fourth Industrial Revolution on a large scale, outside the context of a simple toolkit, in close connection and interdependence, in the light of the idea of synergies, looking for opportunities that on the one hand enable the security and public order services to have a positive impact on the quality and level of national and civic security and, on the other, to extract and prioritize these technologies and combinations of them to ensure people that Security sector works only in their favor and protection. Technologies must also be analyzed in terms of the possibilities for their use by criminals in order to create a conceptual counteraction environment.

Based on what has been said so far, the author makes some specific predictions.

Crises in the economy, the complexity of entering the new industrial revolution increase the tensions in the labor market, in international relations, in the migrant environment. This has a negative impact on security, with both traditional and non-traditional crimes increasing. Law enforcement in terms of deficit funding for their existence will have to combat two directions - both traditional and non-traditional crime. Moreover, it is now clear that the law enforcement system will be constantly delayed in its actions to counter the technologicalization of the criminal world. It is known that the loser of the initiative in the fight will probably collect the final loss as well.

In the detection of crimes, the system of using new technical means to obtain objective information about the guilt of one or the other suspect must be completely changed.

It is necessary to eliminate archaic ways of investigating criminal cases, writing and reading hundreds of volumes without machining, especially in economic cases and organized crime. Inflated administration can be successfully replaced in most cases by flexible artificial intelligence computer systems.

A revolution in expertise is needed. Even now, it is necessary to use the latest discoveries in a number of areas of science in the field that we traditionally refer to as forensic expertise.

Soon we may find ourselves in a situation where criminals will use quantum calculations, and we will continue to perforate the paper and tie the folders of criminal files with a cord.

By adding new and new devices, people forget that everything available over the web can be hacked, eventually. No existing technology and security agencies are enough to counter the growing threat. The Internet is developing at times faster than the means for its protection.

A new project is needed to bring together the best scientists and researchers, universities, governmental and non-governmental organizations, corporations, civil society. Entrepreneurs, politicians, lawyers, military, analysts must be attracted to create comprehensive, complete protection, including safer equipment, operating systems and software, at a minimum national level, and even better globally.

In order to outline trends in the necessary security developments in the context of Industrial Revolution 4.0, the author examines the challenges ahead:

- The need for a fair distribution of the benefits of the Fourth Industrial Revolution;
- Control over the negative effects and risks of the Fourth Industrial Revolution;
- Ensuring that the Fourth Industrial Revolution will develop for the benefit of the people and under human control;

From the analysis of the forthcoming tasks, the author formulates four principles that are extremely important for the formation of an adequate way of thinking in security:

- It is important not only to consider and implement security technologies, but to integrate them into a synergistic effect system.
- Technology must expand, not limit, the ability to counter crime.
- Use by design, not by default. System thinking must continually analyze security structures and systems and identify approaches for how new

technologies can effect change that lead to greater positive effects for people;

- Values should be seen as a dignity, not a disadvantage. Technology-driven security values must be sustainable and meaningful, but be flexible in nature so that they can change dynamically without losing their charge and advantages.

These four principles form the basis for evaluating, discussing and controlling the technologies that are already affecting us today and will change the world in the future. The Fourth Industrial Revolution can give birth to systems that are able to make society much more prosperous, increase life expectancy, increase the level of security in its broad and close understanding, and open up new opportunities for existence and development. There is a spiral of technological and technical development, stimulated or impeded by the available security environment.

Therefore, several security management responsibilities – civilian and national – must be derived:

- Identify the values ensuring security associated with certain high technologies;
- Clarifying how new technologies affect people's decisions. How new technologies used by criminals influence decision making related to increasing crime. How new technologies influence decision-making in security and lead to effectively combating crime.
- Determine the most effective ways of influencing technological development with a view to the objectives and interests of the security and public order services subordinated to ensuring national and civil security.

In this regard, the author defines some sensitive points, enabling the study, analysis and influence of values deployed in technology guaranteeing security:

➢ Establishment of security education programs;

- Financing and investment in mandatory and inevitable security resources;
- Establishment of organizational and technological culture in security;
- Priorities are ranked according to security needs, resources, technological capabilities;
- It is necessary to create and use operational methodologies to achieve the required level of security;
- It cannot respond adequately and effectively without economic incentives for proven achievements;
- Designing high-tech security products;
- Creation and maintenance of efficient and modern technical architecture;
- Overcoming public resistance;
- Coverage of all national and civil security stakeholders.

To be able to ensure prosperity, openness and equality for the public and citizens in the Industrial Revolution 4.0, a conscious choice of technological systems is required that will inevitably affect security. This means that modern paradigms and their reformatting are needed to achieve the involvement of all stakeholders.

In the chapter, the author groundedly defines a new concept: **The ecosystem of Security 4.0 represents the unity of people, organizations, high-tech elements and environment, creating, securing and protecting national and civil security.**

The urgent need for digital transformation of the security system implies a complex informatization of security management processes based on the creation and consolidation of national and European computing and information resources, such as:

- Consider and initiate the development and deployment of adjoining pan-European, national, regional and municipal digital security platforms.

- Gradually reduce the total amount of automated security systems based on the transfer of their functions to integrated systems and the formation of a single national digital security ecosystem, with further integration with the European system foreseen at the planning stage.
- Consider and start building standard national, regional and municipal security platforms that will facilitate the creation of an unified security ecosystem. Typical scenarios, protocols, forecasting and counteracting models are required.

The author identifies and examines the key elements that characterize the Ecosystem of Security 4.0: 1. High-tech environment; 2. High-tech modern public order and security services; 3. An opponent with the potential for technological impact.

The classic requirement for successful counteraction to crime and counter-espionage is for the structures that carry it out to act proactively – losing an initiative equals the failure of counteraction. Therefore, the advance reconstruction of special services in line with new technologies is essential for the successful provision of national and civil security.

defining, characteristic and typical for Industry 4.0 technological concepts such as: Big data, Internet of Things, Blockchain technologies, Artificial Intelligence, Additive technologies, Virtual, mixed and augmented reality.

3. Chapter Three. Environment in Security 4.0 Ecosystem

3.1. Technology and security, opportunities and change

In this chapter, the environment is discussed in the focus of new technologies. Of course, other components of the environment are also important, such as social, legal, demographic, environmental, etc., but this will lead to unnecessary complication and aggravation of the material, so this is a consciously accepted restriction on the part of the author..

The subject of analysis in the chapter is the new computing technology in security.

3.1.1. Big Data (Fig. 2)

An analysis of the techniques and methods of processing and analysis of Big Data was carried out, such as: Data Mining; Crowdsourcing; A / B testing; Forecast analysis; Machine learning - artificial intelligence; Network analysis.

The benefits of analyzing Big Data in security are analyzed, as well as some promising implementation options.

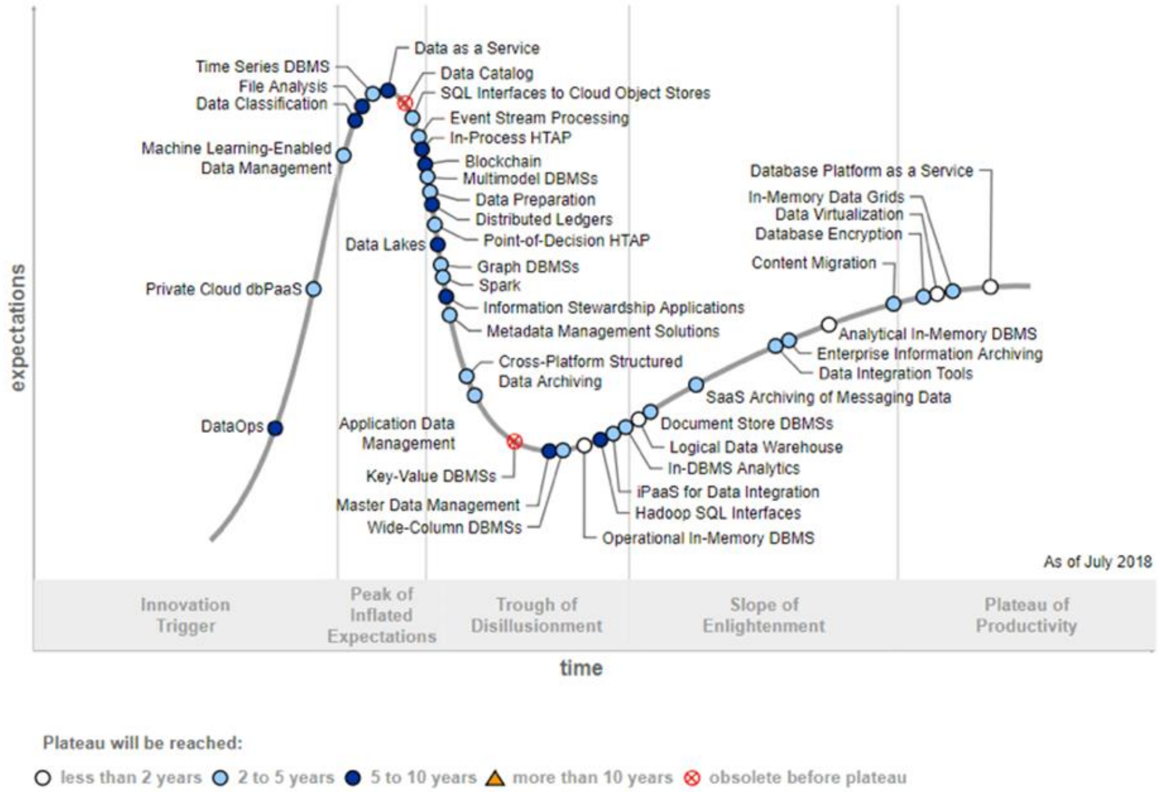
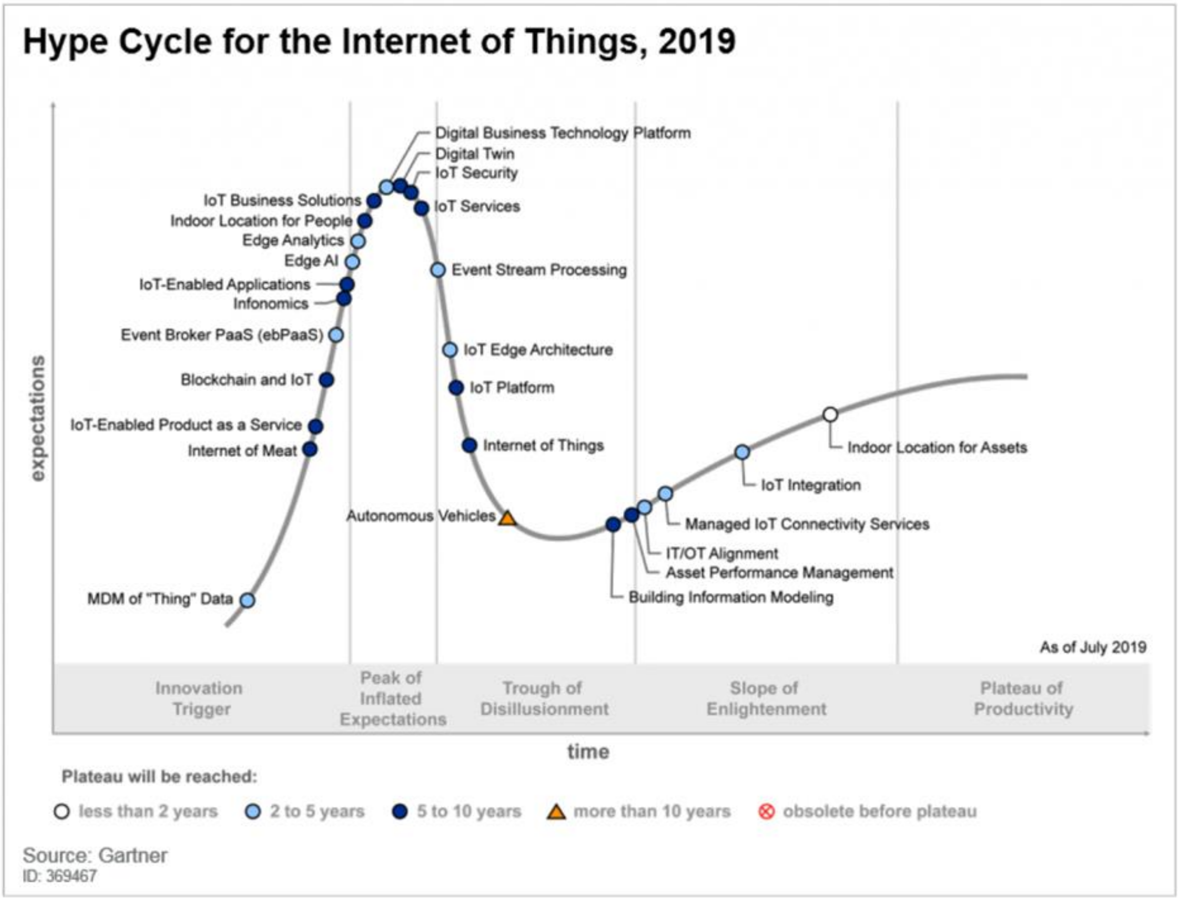


Figure 2. Trend in Big Data Technology Development. Source: https://agileengine.com/megatrends-in-big-data/

3.1.2. Internet of Things (Fig. 3)

IoT can serve as a tool to address systemic issues such as efficient use of energy, traffic management on the roads and increased traffic safety – disaster reduction, environmental pollution. In fact, it is a tool for achieving security, whether in the broad or narrow sense of the term – from infrastructure security, environmental security, energy security – to civil and national security.



Source: Gartner
ID: 369467

Figure 3. Trends in the evolution of the Internet of Things ecosystem

Internet of Battle Things – IoBT. The military (battle) Internet of Things is a logical continuation of the concept of network-oriented warfare, which became popular at the beginning of the century, and the concept of the battle in multiple domains, i.e. combat through operations in various fields: land, sea, air, space, cyberspace and electromagnetic spectrum.

3.1.3. Blockchain and Distributed Registry Technologies

Blockchain technology is based on the use of the distributed digital register, which allows securely exchanging digital records and ensuring the existence of only one unique record without copies, thus preserving the value of the digital object or information. This technology brings exceptional security for the transfer of information and values, thus indirectly affecting the overall system of international, national and civil security, preventing distortion and misuse of information.

In security, the resources of the special services in the various countries are very different – from huge investments of hundreds of billions to the sanitary minimum of tens of millions. However, the innovative nature of security technology must be understood, adapted and prioritized, of course, if there is a political will to do so.

3.1.4. Artificial Intelligence

Artificial intelligence (AI) is already transforming the digital economy and will soon change the economy of the material world. In the early 21st century, AI helps autonomous mechanisms navigate the material world and interact with humans. In the future, artificial intelligence systems will be able to solve complex system tasks. In practice, even today, if the police have quality computer systems with integrated AI, much of the routine clerical work can be done by them, leading to the opening of new reserves for increasing police presence in urban areas. AI already provides monitoring of video streams and data collected from a huge amount of sensors, and can alert security services for suspicious activity. At the same time, police is using robots to conduct search and rescue operations, to disarm explosive devices in terrorist activity and even to destroy armed criminals.

3.1.5. Additive production and multidimensional printing

The growth trend of 3D printing (Fig. 4) shows that it is capable of radically altering the entire production system, including industrial, armaments, transport, logistics, infrastructure, construction, aerospace, shipbuilding and more companies and to have a huge impact on governments, economies, the labor market of both developing and developed countries. It follows that the impact on security in a general and narrow sense will also be enormous. In practice, this means mass production to order – from fashion items to weapons and printed human organs.

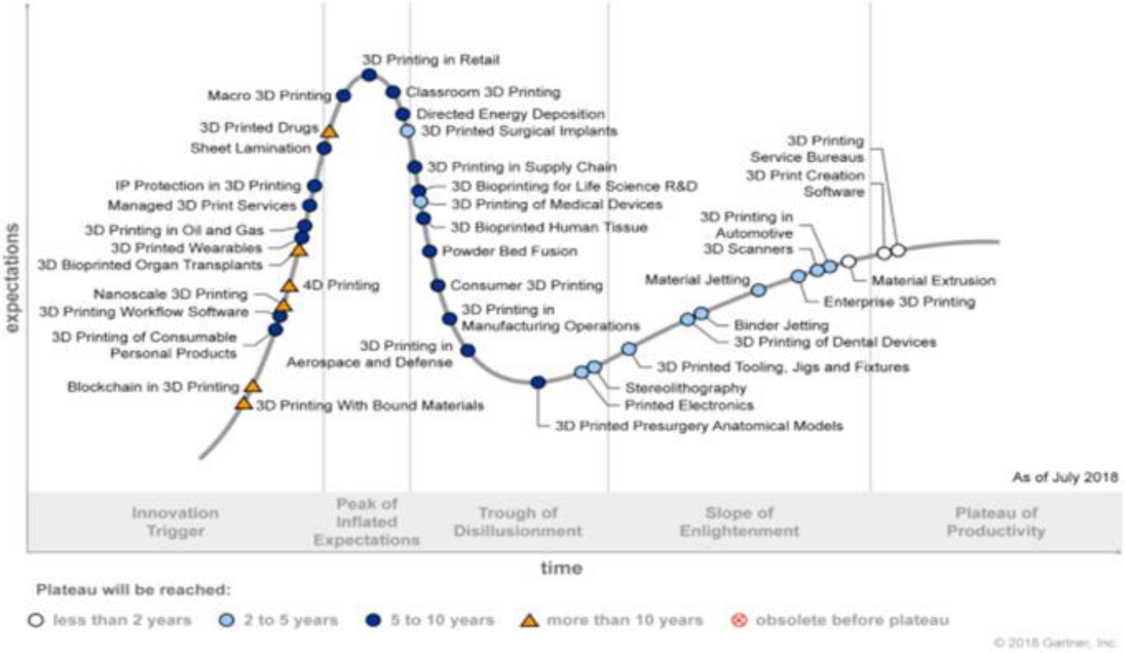


Figure 4. Trend in the development of 3D printing (https://www.3dnatives.com/en/gartner-hype-cycle-3dprintingpredictions-150120194/)

3.1.6. Virtual and Augmented Reality

In the field of security, they can be applied to modeling, interactive force and resources management, training, management of database, information and analysis systems, visualization of intelligence and counterintelligence platforms, etc.

3.1.7. Drones

Drones reduce the cost of intelligence operations, replacing manned aircraft, which cost 10-15 times more expensive. Using them reduces the time it takes to prepare staff and minimizes losses, eliminating the danger for the machine operator.

3.1.8. Security and biotechnology

Biotechnology has three important differences from the digital technologies of Industry 4.0. They elicit a more emotional response from society, appear less predictable because of their organic nature, and also require more investment and regulation, so that the investment horizon is extended. In addition, the acceptability and use of different biotechnologies depend on the profound cultural and historical features that determine the eligibility of scientific requirements..

3.1.9. Neurotechnology

The concept of "neurotechnology" includes a wide range of methodologies that allow deep penetration into the mechanism of work of the human brain and information retrieval, empowerment, change of human behavior and interaction with the world.

3.1.10. New (smart) materials

New materials usually represent strategic raw materials and resources and, as such, enjoy all the safeguards that the state applies to maintain the monopoly of production and use. In the security field, new materials are used for protection, communications, camouflage, monitoring.

3.1.11. Energy and security. New energy sources

Possibilities for the use of innovative energy sources and their relation to security are analyzed. The importance of energy independence for security is emphasized.

3.1.12. Geoengineering

The idea of geoengineering consists in the purposeful effective management of extremely complex processes in the Earth's crust and atmosphere of the Earth. However, many scientists believe that technologies designed to intervene in this field are at best immature and at worst, threaten the existence of humanity and can lead to unpredictable and uncontrollable consequences.

3.1.13. Space technology

Special services and the military use the capabilities of space technology to monitor the surface, gather information about the enemy, trafficking in military equipment, drug trafficking, human trafficking. Major criminal organizations do not fall behind – there are reports that they hire segments of space devices for communications and counter-surveillance. Space technology requires money, and as we said above, organized crime has sufficient liquidity.

4. Chapter Four. Forces, means and methods

The chapter examines theoretical and practical selection of employees, training and preparation, working with secret collaborators and special intelligence means and methods of activity and action typical of special services in the light of innovative technologies analyzed in the previous chapter. Attention is also given to the capabilities of technical intelligence when using high-tech devices.

A new paradigm in the security services is defined as a consequence of new technologies implementation – ***temporal intelligence***. It is not a narrow methodology for collecting specific intelligence that focuses on specific sources, but rather a holistic approach to collecting and analyzing data globally and totally. It suggests that most people and infrastructures will be monitored and that some of the data can be collected, analyzed and stored, generated for intelligence. The ultimate time intelligence platform of what is happening everywhere, of course limited to a specific event, place and interest, allows the event to be scalable, stop, scroll back (like video) at will – with full commentary on the state of the physical and the mental health of each person or structure, details of which have been obtained using portable devices or already gigantic quantities of smart sensors.

The chapter provides a brief analysis of the existing Big Data toolkit actively used by modern special services. These tools can be used both in their original form and as specialized, purpose-modified varieties to practice specific intelligence and analytics. Let's mention them for demonstrating the available possibilities:

Data base: *Apache Hive, DRIL, Impala, Presto.*

Framework Platforms: *Hadoop, Spark, Storm.*

Analytical platforms: *Deductor, Dell EMC Analytic Insights Module, Flume, IBM SPSS Modeler, IBM Watson Analitics, Informatica, KNIME, Microsoft Azure Machine Learning, Oracle Big Data Preparation, Pentaho Data*

Integration, Qlik Analytics Platform, RapidMiner, SAP BusinessObjects PredictiveAnalytics, SAS Enterprise Miner, Statistica, Teradata Aster Analytics, Windows Azure HDInsight, World Programing System, Zookeep.

This shortlist aims to show that a variety of Big Data tools are available that allow analysts in the Special Services to use it with ease. Many of the tools are open source, which allows for further development and use for special purposes in the environment and focus of the special service.

From description and analysis to here, although in a relatively laconic format (due to the impossibility of making a comprehensive presentation, analysis and description of the extremely wide range of high technology problems and opportunities), we can be sure of the continued involvement and interest of special services in the study, implementation and use of high-tech solutions. Moreover - it can be considered that the accelerated implementation and development of modern technologies of high level is vital for security – civil, corporate, national.

At the end of the chapter, the author makes a brief analysis of the security management cycle in the light of high technology as a mandatory element of the security ecosystem..

5. Chapter Five. Crime and high technology

This chapter focuses on the adversary's actions, which concludes the full exploration of the Security Ecosystem 4.0.

A growing number of studies conclude that the advent of the Internet transforms the organizational life of crime. Many articles and reports describing various structures involved in cybercrime as "organized crime" make it clear that a new criminal ecosphere is formed. In the last five years, the world of cybercrime has reached an industrial scale. Hackers, programmers, social engineers and money mules maintain a working business mode and often employ modern targeting techniques against companies and individuals. Over the last few years, the parallel between characterizing organized crime as a serious threat to national security and the evolving character of cybercrime as a serious crime – hence organized by default – has triggered cybercrime securitization, with important implications for police powers and approaches and police resources distribution.

The author defines and classifies opponent in the approaches used and organization of activities – from organized crime groups to individuals, from foreign special services to hackers mercenaries. He analyzes contemporary crimes in the light of the high-tech fields discussed above.

6. Conclusion

It should be noted that lack of vision in the security services leads to a deficiency of creativity, to mismanagement and poor results. Special services are not self-sufficient organizations, but have the noble purpose of effectively combating crime and ensuring a peaceful life and activity for citizens.

The summary of work presented in the abstract shows that the goals and objectives set in advance have been achieved and the work has a great personal charge – a scientific and visionary break in the link between the security sciences and the sciences relating to each of the major elements of Industry 4.0 and Security 4.0.

III. Scientific publications on the subject

1. Радулов, Н., Сигурност 4.0. Сигурността и четвъртата промишлена революция, В: Сб. докл. от Годишна Университетска научна конференция, В. Търново, изд. НВУ, ISSN 2367-7465, 2018, 9-34
2. Радулов, Н., Виртуална реалност и сигурност. Сигурност 4.0, В: Сб. докл. от Годишна Университетска научна конференция, В. Търново, изд. НВУ, ISSN 1314-1937, 2019, т. 4, 86-93
3. Радулов, Н., Проследяване. Сигурност 4.0, В: Сб. научни трудове, НБУ, ISBN 978-619-7383-13-3, 2019, т. 1, 8-14
4. Радулов, Н., Съвременни корелации в сигурността, В: Technics, technology, education, safety, Изд. НТС, ISSN 1310-3946, бр. 10, т. 3, 2016, 28-30

5. Radulov, N., Security today. Current issues, In: CONFSEC, International scientific conference, Dec, 2017, Ed. STUME, ISSN 2603-2945, year 1, issue 1, 37-39
6. Radulov, N., Internet of the things. Security 4.0, In: CONFSEC, International scientific conference, Dec, 2017, Ed. STUME, ISSN 2603-2945, year 2, issue 1(3), 2018, 5-7
7. Radulov, N., Artificial Intelligence and security, In: Security & Future, Int. Sci. J., Ed. STUME, ISSN 2535-0668, 3, 2018, 3-5
8. Radulov, N., Security 4.0. Part one: Security and The Forth Industrial Revolution, In: Security 4.0, Int. Sci. J., Ed. STUME, ISSN 2543-8582, year 4, issue 5, 2019, 265-267
9. Radulov, N., Ecosystem of Security 4.0, In: Security & Future, Int. Sci. J., Ed. STUME, ISSN 2535-0668, year 3, ISSUE 3, 2019, 69-70
10. Radulov, N., Additive Technology and Security 4.0, In: INDUSTRY 4.0, Int. Sci. J., Ed. STUME, ISSN 2534-8582, year 4, ISSUE 6, 2019, 317-318
11. Радулов, Н., „Сигурност 4.0“ монография, Изд. НТС по машиностроене „Индустрия 4.0“, София, 2019, ISBN 978-619-7383-15-7, 325 с.

IV. Sources for the abstract

In Cyrillic

1. Йончев, Д. В търсене на сигурността. Сигурността в концепцията на присъствието, „Изток-Запад“, 2014, 411 с.
2. Радулов, Н., Разузнавателен Анализ, АСИ Принт, София, 2013, 430 с.

In Latin

3. Attali, J., A Brief History of the Future: A Brave and Controversial Look at the Twenty-First Century, Arcade Publishing, 2009, ISBN 1-55970-879-4
4. Burrows, M., The Future, Declassified Megatrends That Will Undo the World Unless We Take Action, 2014
5. Goldston, D., Big data: Data wrangling, In: Nature, 455 (7209), 2008

6. Goodman, M., Future Crimes. Inside the Digital Underground and the Battle for Our Connected World, Penguin Random House, 2016, 608 p.
7. Greengard, S., The Internet of Things, May, 2015, MIT press, Part 4., 181
8. Grossman, N., Drones and Terrorism. Asymmetrical Warfare and the Threat to Global Security, I. B. Tauris & Co. Ltd., 2018
9. Howe, D., M. Costanzo, P. Fey, T. Gojobori, L. Hannick, W. Hide, D. P. Hill, R. Kania, M. Schaeffer, S. St Pierre, S. Twigger, O. White, S. Yon Rhee, Big data: The future of biocuration, In: Nature, 455 (7209), 2008
10. Lowenthal, M. Intelligence: From Secrets to Policy, Publ. April 28th 2006 by CQ Press, 334 p.
11. Lynch, C., Big data: How do your data grow? In: Nature, 455 (7209), 2008
12. Nelson, S., Big data: The Harvard computers, In: Nature, 455 (7209), 2008
13. Platt, W., Strategic intelligence production: Basic principles, New York: Frederick A. Praeger, 1957
14. Reilly, B. C., Doing More with More: The Efficacy of Big Data in the Intelligence Community, In: American Intelligence Journal 32:1 (2015): 18-24.
15. Russell, S., P. Norvig, Artificial Intelligence: A Modern Approach, Prentice Hall, 2010, 1132 p.
16. Waldrop, M., Big data: Wikiomics, In: Nature, 455 (7209), 2008
17. Weigend, A., Big Data, Levine Greenberg Rostan Literary Agency and Synopsis Literary Agency, 2017,