ECOSYSTEM OF SECURITY 4.0

Prof. Radulov N., PhD
Department of National and International Security – New Bulgarian University, Bulgaria
nradulov@nbu.bg

Abstract: *The complex of interconnected structures of the security services, the opposing organizations and the environment in which they are immersed is a single living organism, building its own ecosystem.*

Keywords: ECOSYSTEM SECURITY; CRIME; OPERATIONAL SITUATION; HIGH TECHNOLOGY; STRENGTHS AND RESOURCES; THE ENEMY; ORGANIZED CRIME

1. Introduction

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 it emerges as products for civilian use. The reason is, of course, the preferential financing of projects in the military and security spheres – something that has led to a broad understanding of security – it goes into a broad denominator of all activities that need expanded financing.

Crime is aimed at the illicit acquisition of goods by organized and unorganized criminal groups. With the development of industry goods – capital, movable and immovable property, their storage in banks – are increasing and all of them are subject to interest and desire for illicit acquisition by the criminal world. Since it is dissolved in the normal world, it is also subject to development and benefits from technical progress. Criminals are becoming more creative, educated, sophisticated and greedy. Educated and well-equipped criminals are inventing more and more innovative ways to enrich themselves criminally [1]. This causes normal people to demand from the rulers the adequate protection they owe to them due to the fact of citizenship and the payment of taxes. Much of the criminal interests and raids are directed at large capitals. This unites the interests of the poor and the rich towards greater security. Therefore, resources are allocated, specialists are trained and research and development activities are carried out aimed at combating crime and, of course, espionage. It cannot exist innovative industrial development without resource-intensive developments. From the perspective of opposing countries, intelligence should be a productive force, which, by spending a resource of EUR 100 million, for example, gives its manufacturers an advantage costing billions. There is no technical breakthrough that is not significant in light of its usefulness and application in terms of achieving greater security. Rail, in addition to its economic importance, makes it easy to transport long-distance people, whether they be military formations, criminals or police forces; aircraft, photography, besides their economic importance, have been of great value since their inception for intelligence, counterintelligence, military and special operations. Cybercrime, cyber-intelligence, cybersecurity are interconnected industrial-social phenomena demonstrating the possibility of modern-day crime and the creation of modern products for civil and national security.

Each stage of industrial development corresponds to a stage of development of the security system. Therefore, when we think about security in the flow of concepts of Industry 4.0, we mean innovative paradigms, technologies, and high-tech security techniques that we can combine under the common name Security 4.0. [2]

2. Analysis

Security 4.0 does not exist on its own in space, but is closely intertwined with the interconnections and relationships between individual systems, groups of people and individuals. This makes it imperative to designate it as a distinct system – the Ecosystem of Security 4.0.

By definition, the term ecosystem refers to a biosystem made up of coexisting living organisms or a biotic community (biocenosis) in a given area (biotype), which interacts with the physical environment in such a way those substances are circulating and a clearly defined biotic structure, is created through the flow of energy.

After years of research and analysis in the field of security, management experts have found that in order to succeed, the system’s activities must be flexible, adaptable, and communicative. The system should assume and build relationships with the potential for fast and secure communications, to possess threat sensors, and to be sensitive to all areas, activities and actions that it is called upon to defend. These qualities are usually attributed to living organisms or systems of organisms.

Essentially, security systems are built by humans, exist and operate in a society of individuals, biological beings, and without the presence of living organisms, they cannot be subject to security. These living beings and systems do not exist in any kind of abstract symbolic space; they are attached to real territories, part of individual countries with their own specifics, goals and plans. This leads to the logical conclusion that, in the end, the security services and everything related to them - object and subject, forces and resources, architecture, territory, country, represent a complex system that we can rightly define as a specific ecosystem.

The Security 4.0 ecosystem is a social bio system as far as the main actors are people and their organizational structures – biological objects, part of specific social relations. They co-exist and interact in it – juxtaposition (counteraction) with high-tech modern security services, an adversary, who takes full advantage of modern technology to engage in criminal activity, immersed in an environment predetermined by existing technologies, conceptually envisioned by Industry 4.0

The ecosystem of security, considered in the light of the theory of intelligence, counterintelligence and operational intelligence, is essentially defined as a kind of operational environment: a dynamic combination of three factors – the environment, our forces and our opponent. These three factors, considered in their dynamics and interconnectedness, analyzed in today's technological society, allow us to perceive them as a single ecosystem.

Therefore, we can define the following concept: **The ecosystem of Security 4.0 represents the unity of people, organizations, high-tech elements and environments that create, provide and protect national and civic security.**

For its existence and its effective functioning, it is particularly important to put the following issues on the agenda and resolve them, not necessarily in the proposed order:

- Creation of legislative foundations for the establishment and existence of a high-tech security system (intelligent security);
- Digital transformation in security;
- Creating conditions for resource satisfaction of high-tech dynamically developing systems;

- Designing "smart" sub-structures of the security system, using information and communication technologies and other high-tech tools to create an innovative environment at an increased level of civil and national security within the city, the region, and the country. Such an environment should be shared with the EU in order to gain integrity and synergy in security;
- Persistent and coherent deployment, use and development of modern information and communication technologies in the management and provision of security in the country, synchronous with EU;
- Compulsory integration with other ecosystems of the state in order to achieve integrity at equal levels. Such an approach is only possible after understanding the concept of security ecosystem and adopting the national ecosystem as part of a pan-European and accelerated introduction and development of eGovernment.

The need to build a specialized security ecosystem is dictated by the high requirements for the operability, sustainability and information security of its management systems compared to other areas of government.

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 implementation of adjoining pan-European, national, regional and municipal digital security platforms;
- Gradual reduction of the total amount of automated security systems based on the transfer of their functions to integrated systems and formation of a single national digital ecosystem of security, and to envisage subsequent integration with the European system at the planning stage;
- Consideration and launch of building national, regional and municipal security platforms (smart RPS projects, smart Directorate, smart service, etc.) that will facilitate the creation of a single security ecosystem. Typical scenarios, protocols, forecasting and counteracting models are required.

The key elements that characterize the Security Ecosystem 4.0 are:

Environment. Of course, it will not be feasible to analyze it thoroughly, as it has legal, political, social, demographic, psychological and other constituents, but it will be sufficient for the needs of this report to consider its technological constituent – especially characteristic of Industry 4.0.

High-tech modern law enforcement and security services, which I will briefly refer to as *smart special services*. We should consider them in the light of the management system, while at the same time their forces and means should be analyzed in the light of the ecosystem.

Opponent – undoubtedly striving to carry out his activity in the most effective way for him, and therefore with his own technological potential. By opponent here, we will understand the generalized image of high-tech criminals – organized and standard crime, terrorist organizations and modern foreign intelligence services, without dwelling on specific organizations, but only on the nature of the opportunities and technological threats arising from their modern activities.

Undoubtedly, the high-tech environment is of particular importance. When high technology is being disseminated, it is a matter of time before it is generally accepted and implemented by the opponent [3].

The reason for this is that when they are used, the rate of criminal profits increases sharply, economic espionage, and espionage in general, become more effective, and delays in the legal evaluation of such crimes make them safer for the perpetrator.

At the same time, investing resources by criminal organizations in new technologies is one way of laundering money. Modern criminal organizations are abandoning the old, traditional hierarchical structures, and are constructed in the form of flexible network. They actively use outsourcing, collective entrepreneurship, platform solutions and more. [4] In a word, if criminals were in the midst of the 20th century at the tail of technical and financial technologies, today they are undoubtedly at the forefront. For example, the profit of an average cybercriminal is seven times higher than that of the average criminal. In New York, the detection of ordinary crime in different years ranges between 40 and 60%, and that of cybercrime – 4%. In other words, cybercrime is highly profitable and low-risk criminal activity[1].

3. Conclusion

All three elements of the Security 4.0 ecosystem should be examined for the presence and implementation of Industry 4.0'specific technology concepts such as Big Data; Internet of Things; Blockchain technologies; Additive technologies; Virtual, mixed and augmented reality.

The classic requirement for successful counteraction to crime and espionage is for the structures that do it to act proactively - the loss of initiative equals the failure of counteraction. Therefore, the advanced modeling and reorganization of the special services according to the new technologies is indispensable for the successful provision of national and civil security. In doing so, this process must be constant and timely, given the exponential technological development.

If we do not, the enemy will.

References

[1] Goodman, Marc. Future Crimes. Inside the Digital Underground and the Battle for Our Connected World, Penguin Random House, 2016, pp 512

[2] Radulov, N., Security 4.0. Part One: Security and the Forth Industrial Revolution, Int. sciantific jurnal Industry 4.0, STUME, 2019, 265-267

[3] Radulov, N., Internet of the things. Security 4.0, Int. sciantific jurnal Security & Future, STUME, 2018, 99-101

[4] Radulov, N., Artificial Intelligence and Security, Int. sciantific jurnal Security & Future, STUME, 2019, p. 3-5

[1] The Crime of the Future book is one of the most popular bestsellers of 2015 in the US. In it, a former Los Angeles police officer with experience in Interpol, the CIA and the Secret Service, which advises police services in dozens of countries, discusses the unprecedented crimes that await us in the 21st century. (a. n.)