INTERNET OF THE THINGS. SECURITY 4.0

Prof. Radulov N., PhD, New Bulgarian University, Sofia, Bulgaria
nradulov@nbu.bg

***Abstract**: The Fourth Industrial Revolution implies a total change in our way of life. To be adequate to the new security threats stemming from high technology, we need to analyze and evaluate them from the point of view of people's security.*

KEYWORDS: SECURITY, IOT, SMART SENSORS, INTELLIGENCE AND COUNTERINTELLIGENCE

1. Introducion

1.1. Security and industrial revolutions

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 organizations and those of security and later they appear as products for civilian use. The crime is directed at the illegal acquisition of goods by organized and disorganized criminal groups. With the development of industry, the wealth - capital, movable and immovable property, storage in banks, also increase and all of these are the object of 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 uses the benefits of the technical progress. Criminals are becoming more and more creative, educated, pretentious and greedy. Well-educated and well-equipped criminals are developing ever more innovative ways of criminal enrichment. This causes normal people to demand from the governing people adequate protection due to the fact of citizenship and paying taxes. Much of the criminal interests are focused on big capital. This makes the interests of poor and rich здзве to higher security synchronous. Therefore, resources are allocated, specialists are trained, and research and development is being carried out to tackle crime and, of course, espionage. There is no way for innovative industrial development without resource-intensive development. From the point of view of opposing countries, intelligence should be a productive force that, for example, spending a total of EUR 100 million, gives its producers an advantage worth billions.

There is no technical breakthrough without impact on the need of security – rail transport, in addition to its economic importance, allows for easy transport of people over long distances, whether military formations, criminals or police forces; construction of aircraft, photography, beyond their exceptional economic significance, have great value since their emergence for intelligence, counterintelligence, military and special operations. Cybercrime, cyber-intelligence, cyber-security are interconnected industrial and social phenomena demonstrating the possibility of modern crimes and the creation of modern products for civil and national security.

A stage of development of the security system corresponds to each stage of industrial development. So when we consider the security in the mean of Industry 4.0, we take into account innovative security paradigms, technologies and techniques that match high technology. We can unite them under the common name Security 4.0.

1.2. Forth industrial revolution

In practice, this is predictable with a high probability near future, which is already at the start. Massive cyber-physical systems in manufacturing, serving human needs will develop. The changes will affect the most widely all aspects of life. There are, of course, risks - increased instability and the possibility of collapse of the global system due to a change in basic paradigms of coexistence. The technologies that are already being developed and will cover everything are: Big Data; the Internet of Things (IoT); virtual, complementary and mixed reality; 3D printing; printed electronics; quantum computing; blockchain technology; artificial intelligence; neurotechnologies; new materials; space and geotechnology.

Security 4.0 is unthinkable without huge masses of data accumulated using millions of sensors and devices connected to each other, end devices in a modern internet environment that we call the Internet of Things.

2.0. Results and discussion

2.1. Internet of Things (IoT)

The Internet of Things (IoT), also known as the Internet of Objects (from Russian: Интернет вещей), is a concept of a computer network of physical objects (devices, vehicles, buildings and other objects) having built-in electronic devices to interact with each other or with the external environment. This concept considers the organization of such networks as a phenomenon capable of rebuilding economic and social processes so as to exclude the need of human participation in some of the actions and operations. IoT consists of networked intellectual sensors collecting information and transmitting it over the Internet to other devices or people for further use. IoT will increase people's interaction with machines, and economic relationships between machines will grow faster than between people. In the next 10 years, over 10 billion devices will be added to IoT, and their industrial use could bring the world economy up to $ 14 trillion until 2030. Security systems use a wide range of sensors – volume sensors, motion sensors, infrared, noise, fire, etc., resulting in increased security, rapid response to alerts, and overall improved security for citizens. The presence of security alarm systems (SAS) based on sensor systems, which is usually disclosed, has an additional prophylactic effect against criminal offenses. So far, much of the SAS's networks are connected to private security companies, but there are innovated internet-based systems, hidden video recordings, cloud-protected information cameras, use of reaction scenarios based on modern software. In recent years, security systems have been built with hundreds of thousands of sensors and video cameras to ensure the security of important events, communicating between each other and with the network management, reacting immediately through artificial intellect-aided computer systems – the Sochi Olympics, the football championship in Moscow.

The exponential distribution of sensors and devices and the traffic generated by them will lead to complications in interstate transmission of data, including confidentiality issues, property ownership, copyright, accessibility, etc. One of the important tasks of Industry 4.0 will be the creation of regulatory measures with regard to global information flows in the Internet of Things.

IoT is much more than intellectual devices connected to the Internet and services on their basis. The real value lies in the fact that it allows data collection, analyzes and manages them, finds unexpected correlations and opportunities for action, anticipating destructive changes or crises. For years in the security sector, there has been talk about insufficient information, the lack of information sensors allowing for truly interactive crime maps and for immediate counter-scenarios.

The use of real-time data-processing sensors will likely help to create a developing economy with positive results thanks to the optimization and stimulation of consumer and citizen behavior. This means that IoT can serve as a tool for solving systemic problems such as energy efficiency, traffic management, and environmental pollution. In fact, it is a tool to reach security either in the broad or in the narrow sense of the term.

Serious concern, however, is the impact of IoT at the level of labor and working habits, joining IoT with AI and robots, reducing the demand for routine and manual work for low-skilled workers. But the main risks of IoT systems are most often considered cybersecurity threats, related to low security of devices, lack of standards and legal frameworks for interstate data transfers. This poses new challenges for both the society as a whole and the individual qualification of the individual – the devices will displace the person from the low-skilled, routine work but will unleash the potential for hundreds of activities related to creativity, imagination, erudition, analytical and mental activity. However, this may be a positive trend if the system of life and education provides opportunities and stimulates conscious and uninterrupted training and retraining of people, in line with the exponential development of technology. In the field of security, this will be even more visible and necessary. Actually, the confrontation between crime and the systems of human rights protection will be an opposition between the high technology and the experts using them as a tool in the criminal and security services. Security and public order services are required to be proactive, and this means highly specialized training, a continuous cycle of training, practice and retraining, a special innovative and uncompromising system for selection, recruitment and employee development.

2.2. Special services and IoT. Security and IoT

There is a clear contradiction between the ability of the special services to use innovations and the preservation of individual information, personal data, the confidentiality of every person's life. What is certain is that special services need access to information, but it must be secured against abuse, legally framed and technologically secure. The danger of using the information collected by millions of sensors for the needs of criminal organizations and criminal activities is enormous, so safety must be ensured by the delegated bodies.

The revolution in data collection, which is already happening online, is ready to be repeated in the physical world thanks to the Internet of Things. The idea for IoT is that everyday objects (things) secured with sensitive sensors can now collect and transfer data over a wireless network. The variety of items that can be connected through internet is almost endless: from pavement slabs and concrete to walls to our shoes and clothes, and even toothbrushes. All of them get connected and in the near future they will start adding information to the cloud.

The potential use of IoT for surveillance is recognized by the intelligence services. Former US intelligence chief James Clapper said last year to the Guardian that the agencies would probably use the Internet of Things to "[identify, monitor, track, locate, and access the network or identification data of user]". This approach shows that the intelligence community takes into account this technology and the new extraordinary capabilities to collect and analyze data. All of this must undoubtedly change the current paradigm of intelligence and create a new one.

2.3. The emergence of a new security paradigm

In most special services, there are several paradigms that define the meaning and content of intelligence: radio-electronic intelligence; visual intelligence; intelligence by measuring signature and parameter of goals and objects; agency intelligence; intelligence analysis based on public sources and geospatial intelligence.

The emergence of the Internet of Things shows that intelligence services take into consideration, this new technology, new data collection and analysis potential. The introduction of the Internet of Things generates a new paradigm: temporal intelligence (TII). It is not a narrow methodology for collecting intelligence data that focuses on certain sources but a comprehensive approach to collecting and analyzing data. It implies that most people and infrastructures will be monitored and that some of the data can be collected, analyzed and stored, generated for intelligence and new ones will be created.

Such an approach allows us to explore new hypotheses on old data that have been collected and stored without any real purpose. In the past, intelligence services have collected data selectively due to the difficulties of the process and the high cost of storing a large amount of information. But now, when based on the connected sensors, the presence of devices that transmit data almost non-stop, the intelligence agencies only need to take care of data collection and storage. As a result, they have a powerful tool at their disposal, because if there are any changes, analysts can actually apply the "backward time" to the saved data to see what's behind these events. The final time intelligence platform, consisting of what's happening everywhere, allows the event to be expanded, stopped, rewind (like a video) – with a full comment on the physical and mental health of each person, details for which are obtained using portable devices.

There are two major technological issues related to temporal intelligence.

The first problem is the accumulation of data. Applying TII means that we need to store large amounts of data for later consideration. By 2019, the Internet of Things is expected to collect more than 500 zettabytes data – that's 500 trillion gigabytes. Irrespective of the huge volume, the resulting data can be divided into the following main groups: sound recordings, location and activity monitoring, and images taken from connected surveillance cameras. In addition, the mass storage capabilities over the last few decades have expended and there are no limits to improving and increasing the volume.

The second technological issue is to filter a huge amount of data to find the necessary information. This problem is resolved by the rapid improvement of artificial intelligence, which, with the help of a neural network, acquires the ability to recognize faces, subjects, and even abstract concepts in pictures and videos.

Should security agencies have all the capabilities of TII? In fact, secret services already have such powers today and collect the most available information. The Internet of Things will only increase the amount of collected and processed information. Citizens are, of course, seriously concerned about the growing ability of governments to control mass people in general. Special services should not ignore these fears; they should try to reduce them. For example, authorities can use artificial intellect to identify potential terrorists without the need for a particular employee to personally view the data of millions of citizens. These institutions could provide some of the algorithms for public control. Such transparency will help to prevent misuse of information as well as to detect errors.

Special services are often accused of not being prepared to solve future problems. Once the trends of Internet of things have been identified and a new intelligence paradigm has been created, these institutions now have the opportunity to act proactively. This, of course, is the most important advantage they can have against their opponents. And this is one of the compromises citizens of the democratic states will have to accept.

2.4. Crime and Internet of Things

Internet of Things has some particularities according to Marc Goodman[1], namely:

By plugging in new and new devices, people forget that everything accessible through the network sooner or later can be penetrated. No existing security technologies and agencies are enough to counteract the growing threat. The Internet evolves at times faster than the means to protect it.

[1] *The book "Crimes of the Future" is one of the popular science bestselling books in the US in 2015. In it, a former Los Angeles police officer with experience in Interpol, the CIA and Secret Service, advising the police services of dozens of nations, reflects on the subject of unprecedented crimes that await us in the 21st century.*

The crimes become so high-tech that they astound law enforcement experts. Particularly serious threats result from the realization of the "Internet of Things" concept, within which more and more devices get access to the network. Medical equipment and power stations, implanted devices and security systems – the easier and more convenient to use, the easier it is for criminals to access.

4.0. Conclusion

It is necessary to initiate a new project to bring together the best scientists and researchers, universities, governmental and non-governmental organizations, corporations, civil society. Security experts, entrepreneurs, politicians, lawyers, and military have to be involved – in order to create comprehensive, overall protection, including safer equipment, operating systems and software as a minimum on nationwide, and even better on a global level.

In this connection, some neuralgic points can be defined, allowing the study, analysis and influence of the values embodied in the technologies that guarantee security.

Educational programs – specialists using and developing new security technologies are particular specialists, they work on the edge of modern theoretical knowledge of security, binding it with high technology. However, they can only occur and develop with consciously created and followed specialized training programs and practical training.

Funding and investing in security resources – security money is never enough, but new technologies and the necessary preparation for their operation require a certain resource – financial, human, moral, ethical, and so on.

Organizational culture in security – knowledge of ways, methods, forms of use of new technologies, their use in a complex way to achieve a synergic effect.

Decision-making and ranking of priorities – priorities are tailored to the needs of security, resources, technological capabilities.

Creation and use of operational methodologies – possible, desirable, secured by resources.

Economic incentives – resources are directed to structures and specialists operating with modern technologies in the interest of the society and civil security.

Design of high-tech security products – technologies in intelligence, counterintelligence, special intelligence means. Historically, the latest technology has been deployed and developed in defense and security.

Effective technical architecture – networks, information systems, expert systems, modern security communications covered by a unified architecture, resulting in a synergic technological effect.

Overcoming the resistance of society. Disputes over the use and misuse of services by new technologies, incited by ongoing scandals, lead to doubts as to the appropriateness of the use, the legality and the illegality, the competence and the incompetence. Here again, the well-known contradiction – "Freedom or Security" – is emerging. However, the facts gathered over the past 30 years have shown that even denial of certain civil liberties clearly does not lead to more security, but to abuses, anti-constitutional laws, activities and actions, and ultimately the result is defective security. Obviously Benjamin Franklin appears to be right, saying, "[Those who would give up essential Liberty, to purchase a little temporary Safety, deserve neither Liberty nor Safety.]" Proven necessary use of new technologies to counter crime and assure civil security can lead to overcoming this natural resistance.

5.0. References:

Attali, J. A Brief History of the Future: A Brave and Controversial Look at the Twenty-First Century, Arcade Publishing, 2009, 291 p.

Burrows, M., The Future, Declassified Megatrends That Will Undo the World Unless We Take Action. St. Martin's Press, 2014, 288 p.

Goodman, M. Future Crimes. Inside the Digital Underground and the Battle for Our Connected World. Penguin Random House, 2016, 608 p.

Labaree, L. W. (ed.). The Papers of Benjamin Franklin, vol. 6, 1963, p. 242