M. Szyłkowska, *PhD, research and teaching assistant professor*
(Military University of Technology in Warsaw)

IT THREATS TO NATIONAL SECURITY: DESCRIPTION, CLASSIFIFCATION AND PROBLEMS

This article deals with the main threats to national security in field of information and communications technologies, their classification and challenges they present. Some threats that set a wide range of potential IT problems have been analysed. Also, the definitions of main notions in field of national security, national vital infrastructures and cyber-threats were provided. Besides, the prior work directions that depend on challenges have been defined. Such methods as analysis, synthesis and conclusion were applied in the article.

Key words: Information and communications technologies, national security, cyber-threat and cyber-crime.

М. Шилковска

ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНІ ТЕХНОЛОГІЇ ЗАГРОЗИ НАЦІОНАЛЬНІЙ БЕЗПЕЦІ – ОГЛЯД, КЛАСИФІКАЦІЯ, ПРОБЛЕМИ

У даній статті розглядаються основні загрози національній безпеці в сфері інформаційно-комунікаційних технологій_, їх класифікація і виклики,які вони становлять. Було проаналізовано кілька таких загроз,які представляють широкий спектр потенційних проблем у сфері ІТ, а також було наведено визначення основних понять в сфері інформаційної безпеки, державних об'єктів життєзабезпечення, а також в сфері кіберзагроз. Крім того, було визначено пріоритетні напрями роботи в залежності від викликів. Наступні теоретичні методи були застосовані під час роботи над статтею: аналіз,синтез, висновок.

Ключові слова: Інформаційно-комунікаційні технології, інформаційна безпека, кіберзагроза, кіберзлочин.

In the sphere of the security, the technological revolution imposes the necessity of the faster, more versatile and more complex reaction to the current events. Among the vast variety of the threats to the national security more and more often there are real risks related to the area of the information and communications technology – including the risk of operations and activities aimed at: disorganization of the key information systems (of both the public institutions and private sector) directly affecting the national security system, *as well as operations associated with the database penetration and performing disinformation activities.*

The sphere of the information security of the country and – as follows – **risks** are primarily in the group of economic risks (destruction of disruption of the information network), however, taking into consideration the rapid growth of the technological development, in a broader sense, it would seem appropriate to separate said category. **Information security threats** may have a negative impact on all of the spheres of the activities performed by the country- civil and military- and, particularly, in the context of a critical infrastructure which serves as the base of each country's operations (interrelated systems of communication, transport, energy networks *et cetera*). It is assumed that the degree of this kind of threat is directly proportional to the degree of technical and technological advancement of the nation, and, respectively, the degree of the dependence of its operating to the information flow in the area of the country's information economy (i.e. business, social, political, economic areas.) **Information security threats are perceived as horizontal**- they apply to the data storage media, as well as to the systems of their preparation, aggregation, processing, storing and transmitting. Disruption of those systems- isolation from the information- may not only paralyze them, but also prevent the access to the devices which provide the control over conventional means of protection and defense of the state (including combat assets).

In accordance with the definition provided by the United Nations in 2000, computer crimes in the **narrow sense** are the illegal activities performed in a form of an electronic operation, targeted against the safety of computer systems, or processed by those data systems. In the **broader sense** (offences related to computers), however, they are defined as illegal activities committed on computer systems or networks, or with the use of them. The Council of Europe (2001) defines them as targeted against the confidentiality, integrity and availability of digital data (the crimes related to CIA – *Confidentiality, Integrity, Availability)*; *classic*, committed with the use of a computer; *of content*, related to the content of the network's elements; and linked to, *inter alias*, infringements of copyright and related rights.

The general classification of the ICT threats includes:

a) risks resulting from human activities:
   – purposeful (cybercriminals, cyberterrorists, as well as "non-virtual" offenders, for instance the stealth or damage of devices,),
   – inadvertent (untrained staff),
b) risks resulting from the natural environment (e.g. natural disasters causing power cuts,)
c) risks not directly related to human activity (failure of systems, software bugs, power failures,)
d) hybrid risks (a combination of human and software errors)

An example of the hybrid risk is- with the tragic result- the programming error in the Patriot Missiles, which took the life of 28 American soldiers. In February 1991, an Iraqi Scud hit the barracks in Dhahran, Saudi Arabia. The reason for the failure of its former interception was a software bug in the system clock of the computer. Patriot batteries' combat duty lasted more than 100 hours without a break, which caused the system clock to steadily increase the wrong timing, which, at the scheduled time of the shot, was already 1/3 second miscalculated which, in turn, led to the **faulty calculation** of the position of as much as **687 meters**. The Scud missiles were correctly detected by the radar installation, and computers managed to define their trajectory and speed, but due to the wrong time calculation they failed at predicting the targeted place of the destruction of the rocket. At the time defined by the system, the target was not on the position in which it should have been according to the faulty outcome, as a result of which the computer defined the wrong calculations- it deleted the data concerning the target from the system, which caused a failed attempt to intercept the missile that eventually hit the barracks. The undermentioned chart presents the effect of the mistake.

The effects of the error ***(chart 1):***

Hours	Seconds	Seconds calculated	Difference (error) in seconds	Errors in meters
0	0	0	0	0
1	3600	3599,9966	0,0034	7
8	28800	28799,9725	0,0275	55
20	72000	71999,9313	0,0687	137
48	172800	172799,8352	0,1648	330
72	259200	259199,7528	0,2472	494
100	360000	359999,6667	0,3333	687

Source: *GAO Reports, www.wikipedia.com*

An example of a purposeful human activity are, above all, digital tools, called also digital combat assets. The role and nature of cyber-attacks is the most accurately described by Jaap de Hoop Scheffer, the Secretary General of NATO: ***Cyber-attacks do not require the use of a single soldier or violation of boundaries****, but* ***can paralyze the country****. Interruption of energy supplies can disrupt social and economic functions of the state in a manner reminiscent of the effects of the war. Without firing a single shot.*

A cyberattack may also take a form of **the use of tools and information resources** (computers, systems and ICT networks, and **other means** of storing or transferring data and information.), an **aim** of which are **devices, systems and ICT networks**. Hacking into systems and computer networks through the software or hardware to their destruction, modification or manipulation of the data, information and the functionality of the system as such or the network as a whole or parts would be an abovementioned attack. The attack may also include physical destruction of components caused by manipulation or modification of the software. Among the specifically cyber threats are: cybersurveillance, cybercrime, cyberterrorism and cyberwarfare. Cybersurveillance is the tighter control through ICT tools, to which sufficient are the appropriately constructed interception tools that allow, e.g., to control the content of the conversation in the real time (for instance the US PRISM program). The common ground for all kinds of ICT crimes in the cyberspace is a mass scale and unlimited range. Currently, the cybercrimes are becoming the core activity of the growing number of organized criminal groups (i.e. Yakuza.) The growth of the amount of cybercrimes is a result of numerous components, *inter alias*, compatibility the increasing number of remote systems, the access to remotely cheap devices and software, the establishment of the common standards for devices and software, the availability of the tools that simplify the illegal activities. The ICT threats determined the new meaning of the term **information war**, defined by Ivan K. Goldberg as: *a defensive or offensive use of information and information systems, and computer networks to disrupt or destroy enemy information networks, its computer networks and databases.* As mentioned before, information threats understood in such way affect every sphere and area of country's activities.

In the world of a *new era* the information is not only a product, but also a strategic and fundamental element of functionality in every aspect- **the lack of consciousness or (what is worse) ignoring the threats** may lead to the worst scenario coming true, the scenario not predicted by any security strategy. Exploited by the government or authorities, the systems and ICT networks as well as, strategic from the point of view of national security, business entities serve as the **stock of critical ICT infrastructure of the country** (e.g. operators' telecommunications networks, communication and information systems processing classified information, banking systems, SCADA systems, administration systems performing services for citizens, information systems important for the functioning of government, etc.). Taking as a criterion the subject information in relation to the **critical infrastructure**, composed of such components: communications, healthcare, rescue systems, transport, information services, energy sector, raw materials, water supply and sewage systems, service organizations, and protection of the state and public policy, finance and banking sector, food distribution systems, etc., it is possible to determine **the general classification of the risk**, **including** particularly: interfering with air traffic control, operation of telephone communications, disturbances and changes in the level of pressure in the pipelines, manipulating recipes in pharmaceutical production lines, identity theft, manipulation or damage to equipment used in rescue and hospitals, access to critical data (damage or change), sabotage of the data financial markets, manipulation of information that may result in a reduction in the area of foreign investments.

It shall be not disputed that the **information safety of the country is the core of its correct operating**, and the threats to information will always result in a substantial effect. **Modern security threats in this area determine the specific challenges and objectives to be taken: the first strategic aim is to ensure the safe conditions to accomplish the national interest through the protecting them from each external critical threats and warfare threats. Those aims include, most importantly:** defense against armed aggression - in particular to ensure the inviolability of borders of land, airspace and sea. Participation in cooperative defense - in the case of participating in international alliances and the development of environmentally safe state by expanding the military partnership with other countries (especially neighboring countries). A support for international institutions and organizations in responding to the crisis and in stabilizing operations (both political and military).

The best example would be NATO which, *by starting a new type of the political-military activity in the 90's of the XX century and by expanding beyond the area of the contemporary activity, became the leading Euro-Atlantic structure which has an enormous impact on the preserving the global security. In relation to the upcoming threats and challenges that awaits the Alliance, it is aware that the tasks that it will have to accomplish cannot be accomplished independently, but only with the cooperation with other international organizations, both governmental and non-governmental* [Kulczycki, 2010, p.389]. [4]

The key challenges of the new security environment (that is **cyberspace**) are especially those associated with the legal regulation of the principles of protection and establishing areas of responsibility to protect cyberspace- in particular within the area of critical information infrastructure, ensuring coherent security policy. The development of mechanisms of cooperation in the field of cyber protection shall also apply to part of the critical IT infrastructures that are under the control of both the public administration and private sector, with which the country should establish the scope, methods of cooperation and area of responsibility. Another **challenge** in terms of ensuring security in cyberspace is to **implement prevention solutions**, "development of early warning systems against attacks and special protection of key IT systems combined with exercises that make it possible to assess the resistance of this infrastructure to cyber attacks ". It is also necessary to develop in this area a plan for the use of the system of open communication in a crisis situation and to create backup solutions that would allow to take over the tasks previously performed by critical infrastructure if the unavailability of basic systems occurs (for example – according to officially unconfirmed information - a parallel ICT infrastructure is being built in the United States.) Of a considerable importance is also a high level of awareness of as many users as possible, the training of professionals from the IT security branch and clerical staff.

The response of the state to the opportunities, challenges and threats in cyberspace shall be first and foremost the proper construction of the whole security system- starting from the legal system (including, for instance, regulation of the matter of response to a cyber-attack), through the activities related to the organization of institutions responsible and dedicated to securing national critical ICT infrastructure and to the infrastructure of other countries, but also neuralgic from the point of view of connectivity and communication at the national level, and to educational activities for the public. Furthermore, the *stricte technical* activities in the field of the possibilities to ensure the protection of the national information security shall concentrate on the national solutions in the field of cryptology, cryptography and on the ability to provide the relative technological sovereignty. It should be noted that it would also be of a significant importance to create the architecture of a system for the whole country on the basis of national solutions, which would be an integration platform for modular solutions to specific sectors.

It is worth mentioning that the current, most potential threat to the IT systems are digital attacks, which occur through the use of the adequate tools in order to attack and achieve the desired effect (e.g. espionage, theft, destruction of data or systems.) Among the basic tools are, primarily, programs designed to perform an attack: computer viruses (all the kinds and types), bugs *et cetera*. The aims and methods of cyberattacks may vary: from the propaganda, to an attempt to impose the ransom, to permanent damage or destruction of critical infrastructure; they may also serve as the source of acquiring information, to spread misinformation or perform as technological intelligence.

It should be noted that the possibility to ensure the absolute security to the nation practically does not exist (taking into consideration, for instance, the risk of the occurrence of prosaic defects or human errors), therefore it is assumed that the correct solution is its creating through the risk analysis which should ensure the proportional degree of safety. However, the base of all activities is the organization of possibly the most comprehensive system for national IT security, including the abovementioned crucial aspects.

References

1. Adamski A.(2000), *Prawo karne komputerowe*, Wydawnictwo C.H. Beck, Warszawa.
2. Ciborowski L.(1999), *Walka informacyjna*, Toruń.
3. Dworecki S.(1994), *Zagrożenia bezpieczeństwa państwa*, AON, Warszawa.
4. Kulczycki M. (2010), *NATO gwarantem bezpieczeństwa międzynarodowego, [w:] Współczesne problemy bezpieczeństwa*, A. Gałecki, (red.), Oficyna Wydawnicza Uniwersytetu Zielonogorskiego, Zielona Gora, ISBN 978-83-7481-355-6.

Author's translation. Original: Najlepszym przykładem może być Organizacja Traktatu Połnocnoatlantyckiego, ktora *rozpoczynając nowy rodzaj aktywności polityczno-wojskowej w latach dziewięćdziesiątych XX wieku oraz wykraczając poza obszar dotychczasowego działania, stała się wiodącą strukturą euroatlantycką, która ma ogromne znaczenie w zachowaniu bezpieczeństwa globalnego. W oparciu o przyszłe zagrożenia i wyzwania, które stoją przed Sojuszem, jest on świadomy, że zadania, które przyjdzie mu wypełniać nie może zrealizować samodzielnie, ale w oparciu o współpracę z innymi organizacjami międzynarodowymi, zarówno rządowymi jak i pozarządowymi*. From: Kulczycki M., 2010, p. 389.

5. Sienkiewicz P.(2005), *10 Wykładow*, Akademia Obrony Narodowej - Wydział Wydawniczy, Warszawa.

Other sources

1. Jemioło T., *Wyzwania i zagrożenia dla globalnego bezpieczeństwa informacyjnego w pierwszych dekadach XXI wieku*, retr.: http://www.dobrauczelnia.pl/upload/File/KONFERENCJE/Cyberrteroryzm/Jemiolo.pdf.

2. Grzelak M., Liedel K., *Bezpieczeństwo w cyberprzestrzeni. Zagrożenia i wyzwania dla Polski – zarys problemu*, s.137. retrieved: http://www.bbn.gov.pl. Last access: 17.10.2015

3. GAO Reports, retrieved: http://www.wikipedia.org

4. http://www.infor.pl/cyberprzestępstwo. Last access: 17.10.2015.

5. Czyżak M., *Wybrane aspekty zjawiska cyberterroryzmu*, Instytut Łączności, PIB, retrieved: http://www.wnp.pl/artykuly/,6548_0_0_1_0.html. Last access:: 17.10.2015.

❖❖❖