KOŠICKÁ BEZPEČNOSTNÁ REVUE

KOSICE SECURITY REVUE

Vol. 10, No. 1 (2020), p. 10 – 23

ISSN 1338-4880 (print ver.), ISSN 1338-6956 (online ver.)

Cyber Threats as One of the Most Serious Asymmetric Security Threats in 21st Century

Kybernetické hrozby ako jedny z najvážnejších asymetrických bezpečnostných hrozieb v 21. storočí

Radoslav IVANČÍK[1]

[1] *Akadémia Policajného zboru v Bratislave, Sklabinská 1, 835 17 Bratislava*

The manuscript was received on 09. 04. 2020 and was accepted after revision for publication on 18. 05. 2020

Abstract:

Release of international tension after the end of the Cold War, the dynamic increase in the intensity of cooperation at the transnational level and the impact of globalization processes have brought about a rapid expansion of several sectors, including the sphere of information and communications technologies at the end of the second and the beginning of the third millenniums. However, intensive internationalization, cooperation and interconnection of participating actors, together with weakening of time and space barriers, brought along with lots of positives also many negatives. These were reflected mainly in the gradual deterioration of the security environment, the security situation and the growth of asymmetric security threats in the form of international terrorism, illegal migration, cross-border organized crime and recently still more often in the form of cyber attacks on public and private computer networks. Therefore, an author, with the use of relevant methods of scientific research, deals with cyber threats that are becoming one of the most serious asymmetric security threats in the 21st century.

Keywords: *Cyber threats, asymmetric security threats, 21st century, information and communication technologies.*

Abstrakt:

Uvoľnenie medzinárodného napätia po skončení tzv. studenej vojny, dynamický nárast intenzity vzájomnej spolupráce na nadnárodnej úrovni a vplyv globalizačných procesov priniesli koncom druhého a začiatkom tretieho milénia prudký rozvoj viacerých odvetví, vrátane sféry komunikačných a informačných technológií. Intenzívna internacionalizácia, kooperácia a prepojenosť participujúcich aktérov spolu s oslabovaním časových a priestorových bariér však so sebou priniesli okrem mnohých pozitív aj viaceré negatíva. Tie sa prejavili najmä v postupnom

zhoršovaní bezpečnostného prostredia, bezpečnostnej situácie a raste asymetrických bezpečnostných hrozieb v podobe medzinárodného terorizmu, nelegálnej migrácie, cezhraničného organizovaného zločinu, či stále častejšie sa vyskytujúcich kybernetických útokoch na verejné i súkromné počítačové siete. Z toho dôvodu sa autor, s využitím relevantných metód vedeckého skúmania, zaoberá v článku kybernetickými hrozbami, ktoré sa stávajú jednými z najvážnejších asymetrických bezpečnostných hrozieb v 21. storočí.

Kľúčové slová: *Kybernetické hrozby, asymetrické bezpečnostné hrozby, 21. storočie, informačné a komunikačné technológie.*

Introduction

The dynamic evolution of human society, the ongoing processes of deepening globalization, social and economic modernization and political, economic and social liberalization of human society, together with the rapid onset of scientific and technological development, especially in the field of information and communication technologies, generated many adverse accompanying phenomena, which today are making a significant contribution to the continuous deterioration of the global security environment. The ever-increasing economic and social disparities in the development of human society, the failure of state structures in third world countries and their lagging behind development, together with the inability to adapt quickly enough to the new situation, create suitable conditions for the growth of new security threats and negative effects of non-state actors. This is one of the reasons why we encounter information about asymmetric security threats, asymmetric operations or asymmetric adversaries who use unconventional means, including the latest technologies, to achieve their goals.

The unprecedented development of information and communication technologies, coupled with the massive deployment and use of information and communication systems and means, on the one hand, brings higher quality to almost all spheres of society, but on the other hand increases the vulnerability of society and the individuals. According to Patel, development in this area is so rapid that legislation, morality, written and unwritten principles of decency and correctness in private and public relations, and other social attributes are not respected in many cases and thus fail to respond adequately to the changed situation. By creating a new virtual space in the form of cyberspace, supporting virtual existence, there is a rise and gradual increase in criminal and illegal activities in this space.[1]

The emergence of cyberspace follows the emergence of a modern information society, which is generally defined as "*a society in which the quality of life and its social and economic development depend on information and the ability to exchange, process and use it; and information is a key factor for such a society*".[2] From a technological point of view, the term of information society refers to a company that makes extensive use of information and communication technologies based on computer technology and related digitization. As a result, a networking society is created that enables people to exchange huge amounts of information anywhere in the world. This fact is aptly reflected in the commercially sounding slogan "*Everything is on the web*". Since the rapid development of communication technologies makes the exchange of information practically possible at any given time, irrespective of the

place of residence of the interpersonal communication participants, the distance limiting factor thus far loses its importance.[3]

Cyberspace itself is defined as "*a world of virtual reality in which various, paradoxically real things happen, such as phone calls, e-mail communications, bank transfers, etc.*"[4] Another definition says that "*Cyberspace is a human-created environment transmission and use of information in several formats, consisting of hardware, networks, operating systems and portable standards*".[5] There are also considerably more complicated definitions of cyberspace in the literature, with a broader view of the activities taking place in this area. At the same time, very simple definitions can be encountered, such as: "*Cyberspace is the information space made up of the sum of all computer networks*".[6]

As information in the modern information society is a very valuable resource,[1] many illegal and criminal activities are taking place in cyberspace, as has been mentioned above, which are the source of very specific and highly dangerous new asymmetric security threats - cyber threats. From this perspective, the significance and importance of cyber security is increasing. Security and protection against cybercrime are an increasing challenge for the security forces of the state. Security, as we have been used to perceiving, has been changing, and therefore, it is necessary to adjust the established tools of protection and prevention to new situation, or to create and apply new ones.

Cyber security is a set of organizational, political, legal, technical and educational measures and tools aimed at ensuring protected and resilient cyberspace for public and private sector actors. It helps to identify, evaluate and face threats in cyberspace, reduce their risks and eliminate the effects of cyber attacks, which are conducted in the form of cyberterrorism, cyber espionage, or cybercrime.[9]

1. Cyber terrorism

The term cyber terrorism or its shortened form cyberterrorism has become a very frequent term in recent years, which is related both to the wider perception of terrorism, especially following the attacks of 11 September 2001 in New York and Washington,[2] and to the rapid development and use of modern information and communication technologies. Cyberterrorism is described as a new type of terrorism from which it differs precisely by the use of communication and information technologies, systems and means. It is basically a misuse of cyberspace for terrorist purposes.

According to Denning, cyberterrorism is a convergence of terrorism and cyberspace. In general, it can be understood as an unlawful, dangerous attack against computers, computer networks and information stored therein, when the attack is

[1] For more details see: [7], [8].

[2] Historically known are bloody attacks in many other places around the world - Moscow, London, St. Petersburg, Madrid, Istanbul, Paris, Nice, Berlin, Manchester, Brussels, etc.

carried out to intimidate or force the government or the population to support the attacker's political, religious or social goals.[6]

In view of the fact that there is no uniform universal definition of terrorism yet, there is currently no uniform universal definition of cyberterrorism. If, however, we start from the relatively frequently used definition that "terrorism is violence, resp. threats of violence and intimidation against the defender until he is physically destroyed", then "cyberterrorism is the same activity that is only performed in the world of information systems, in which there is no physical destruction of man, but its effects negatively affect man and society".[10]

In another sense, "*cyberterrorism is the use of Internet-based attacks in terrorist activities, including acts of wilful widespread disruption of computer networks, personal computers connected to the Internet, through tools such as computer viruses and the like. The aims of such action must be political or ideological*".[11] Cyberterrorism can also be considered as a "*thoughtful, politically motivated attack by organized groups, individuals or secret agents directed against information networks, computer programs and data*".[12]

The North Atlantic Alliance considers cyberterrorism as "*a cyber attack with the use or misuse a computer or information and communication networks in order to cause sufficient destruction or disruption and generate fear or intimidate society on behalf of an ideological objective*".[13]

Several other definitions dealing with this phenomenon of the modern information society, rather than a generally valid definition, deal with a possible scenario for the development of a certain situation that corresponds to a cyber-terrorist attack. Frequently occurring scenarios include one in which a cyber-terrorist controls an air traffic and aerodrome traffic control system consisting of a large network of computers and seeks to achieve the objectives or targets of a terrorist group (organization).[3]

Another variant of the cyberterrorist scenario is a sophisticated attack on hospital computer systems, in which a cyberterrorist makes changes to patient records and quietly withdraws into the background. At first glance, no consequence is noticeable until patients begin to have allergic reactions to the wrong medication, when healthy people are preparing for surgery, or even some are dying of seemingly trivial diagnoses. Other possible variants envisage cyber attacks on financial institutions (banks, insurance companies, stock exchanges, etc.) for the purpose of extortion and subsequent monetary gain.[4]

In addition to the above scenarios, there are also those that are linked to attacks against critical state infrastructure or to the breakdown of military and civilian security systems. Their disruption, damage or destruction would have far-reaching consequences and cause damage of strategic importance. Of course, there are scenarios that do not allow for very sophisticated attacks. For example, an attack aimed at

---

[3] For more details see: [14], [15]
[4] For more details see: [16], [17]

decommissioning an energy source may cause the inhabitants of a modern intelligent city[5] will not be able to buy the essential food needed for their livelihood due to malfunctioning of cash registers in shops, or decommissioning of payment terminals. Even in such a simple case, the damage caused by a power outage in a relatively small area can, in a short time, rise to enormous heights and cause hardly manageable chaos.

In many cases of cyberterrorism, politically oriented terrorism, separatism and other forms of terrorism, especially on the Internet, play an important role. The actors do not have to be direct members of a terrorist group (organization). These can be hacking groups hired for a particular cyber attack (eg H4H).[6] Most often, however, these are special cells of terrorist groups (organizations), or special military units, or. units of other armed forces in the case of state terrorism.[7] They are characterized by high quality attacks, specific strategies and specific targets.

Another characteristic, objectives and method have cyber attacks carried out either by ideological sympathizers or so-called excitement seekers. While the first seeks to show their affiliation to a opinion group using hacking tools, mostly available on the Internet, exhibits are the main motive for the latter. A significant number of cyber attacks are influenced by the political atmosphere and the effort to use some of the ongoing media conflict known for its own visibility and so on.[1]

In the direct connection with the above forms of cyberterrorism it is necessary to mention the so-called indirect cyberterrorism. Its existence has been neglected until recently, although latency is in some cases more dangerous than direct cyber attacks. This group includes terrorism closely linked to the use of information and communication technologies without a direct link to existing infrastructure but linked mainly to the development of information and telecommunications. It is generally based on a sense of freedom supported by the perception of freedom on the Internet. In this context we distinguish:

1. Media terrorism.
   It is also commonly referred to as psychological terrorism in which mass media (including the Internet) and psychological means are being abused in peacetime in order to influence the views of the entire population or targeted groups of the population. In this case, information and communication technologies, systems and means are misused to spread an ideological message or media manipulation that may be supplemented by some means of psychological warfare.
2. Process terrorism.
   It uses the power of computer technology to overload the established democratic systems and mechanisms, resulting in their gradual overload and malfunction (eg generating a large number of court filings leads to a malfunction of the justice system, an enormous number of calls to emergency services leads to a malfunction of the rescue system, etc.) .

---

5 For more details see: [18], [19]

6 H4H is an acronym for groups called Hackers for Hire.

7 For example, recently repeated cyber attacks on US servers have been associated with China's military activities.

3. IT governance.
   It consists in taking the executive decision-making of the entity (company, corporation, institution) by IT elements of that entity. Dependence on information technology is possible especially in those entities where IT is controlled only by a narrow group whose requirements are difficult to assess by top management.

2. Cyber espionage

Cyber espionage can be considered an act of espionage or spying in order to obtain information on plans and / or activities, of a foreign government or a competing company (organization, group). It serves primarily as a tool for economic, political or military gain.[20] It is therefore a form of cybercrime, in which hackers focus on computer networks in order to gain access to classified, resp. other sensitive information that may be profitable or advantageous to the hacker or customer.[21]

Cyber espionage is an act carried out for the purpose of gaining secrecy, resp. classified information without the consent of the owner or the original holder of such information. This information may come from individuals, various economic or political organizations, groups or governments, and may be personal, sensitive or officially classified. Interest in obtaining them can be motivated for a variety of reasons, but usually for personal, economic, political, military or security reasons. This information is obtained by the use of various methods on the Internet or through the use of individual computer systems using malicious software, including the use of trojans and / or spyware.

Cyber espionage can be done by online experts in remote countries or by direct infiltration of home appliances. It can also be the work of malicious amateur hackers or programmers. The common goal is to access secrets and classified information or to control individual computers, resp. entire networks for strategic advantage and psychological, political and physical subversive activities and sabotage.[22] Cyber espionage can also be a form of cyber attack aimed at acquiring intellectual property in order to gain advantages over a competing company (organization) or government entity.[20]

3. Cyber attacks

Cyber attacks, compared to physical terrorist attacks, represent relatively inexpensive and low-risk activity of various forms, such as:

a) *modification of data* - a typical example may be different types of viruses that randomly misrepresent the word order in documents after entering the computer (for example, the sixth word from the third paragraph on page five is replaced with the fifth word from the last paragraph on page ten); or reorder individual digits in numeric data;

b) *disseminating disinformation* - cyberspace provides equality and freedom for everyone to express and share information. This brings one great advantage, but also a huge disadvantage, risk. One example of disinformation is the case in the United States, when several media reported that the FBI had created special tracking software to be placed on computers. As a result, a huge wave of protests against such action has risen. Only later it turned out that it was a rumour;

c) *electronic bomb* - is a program that performs a predefined action under certain pre-programmed conditions (pressing a specified key combination, reaching a certain date, etc.). This program will cause more or less serious damage to individual documents, files or entire systems;

d) *theft of information* - by hacking into computers or information systems, public or private, personal, commercial or public non-classified as well as classified data and information may be stolen. For example, employees of a financial institution started to receive e-mail messages with the attached RESUME.TXT.VBS file. If this file was run, a serious-looking job application appeared. However, this was just a virus manoeuvre that tried to download and run a file containing the password information used;

e) *blackmail* - obtaining (stealing) personal or business data may serve to blackmail specific persons or institutions. In the United States, for example, a hacker has accessed a US bank information system and stole a protected database of client information. Soon he contacted the bank's director to offer a database exchange for a certain amount of money. The director of the bank reported this fact to the police and the whole case was subsequently publicized. And that was a direct liquidation for the bank. Almost immediately it began to lose her clients, and it took her a long time to regain their trust;

f) *burden on the communication infrastructure* - systematic congestion or congestion of a system may render the system inoperable. A typical example is the US-registered Firkin virus that dialed the emergency services emergency number from the infected computers. If he could achieve a massive enlargement, he could endanger the operation of the entire emergency service;

g) *computers in war* - cyberspace are highly likely to be identified as one of the decisive battlefields in future conflicts. For example, the Taiwanese government acknowledges that it possesses an arsenal of aggressive viruses that can attack Chinese targets if necessary. This was officially acknowledged by a senior official in the IT Department of the Taiwan Ministry of Defence. He stated that they would be used as regular weapons now if China attacked first.

4. Cybercrime

The amount of criminal activities in cyberspace, like the damage caused by these illegal activities, is increasing every year. The cause can be seen in the reduced possibility of detection and subsequent punishment of the perpetrators. The cyberspace population is represented by virtual personalities that are projections of real personalities in it. These populations create virtual communities that can be understood as a global grouping of virtual personalities linked by common ideas, beliefs, political opinions, experiences and interests without constraints across national borders. Cyberspace also includes virtual corporations made up of entities focused on the same market segment.[23]

Therefore, it can be stated that cybercrime is the transfer of criminal activities to cyberspace, many times with improvements made possible by the latest modern technologies, as well as new crimes. Nine types of crime can be defined under the

International Cybercrime Agreement of 2001[8], which are divided into four other categories:

1. Offenses against the confidentiality, integrity and availability of computer data and systems. These include:
   a) unauthorized access to the system;
   b) unauthorized interception of information;
   c) unauthorized interference with data;
   d) unauthorized interference with the system,
   e) misuse of equipment.
2. Computer-related offenses, including:
   a) falsifying computer-related data;
   b) computer fraud.
3. Content-related offenses, such as child pornography offenses.
4. Offenses related to copyright infringement and related rights.

Later, an additional protocol on the criminalization of acts of a racist and xenophobic nature committed through computerized systems was drawn up. Essentially, the extension of groups of offenses was as follows:

- dissemination of racist and xenophobic materials through computerized systems,
- racist and xenophobic motivated threats,
- racist and xenophobic motivated attacks,
- denying, reducing, approving or justifying genocide or crimes against humanity.

From this point of view, the document modified the groups of offenses in which it introduced the first classification of cyber crime under a piece of legislation. Investigating and sanctioning cybercrime is still a major problem, as new or modified ways to exploit cyberspace also require the creation of new or adaptation of existing institutions. These should detect the perpetrator while ensuring the evidence that leads to his conviction. The problem associated with this type of crime lies in the lack of knowledgeability of judges, prosecutors and investigators, and in the imperfections of legal institutions. Many provisions are not supported by the Criminal Procedure Code; electronic (digital) evidence. Given the rapid technological development and sophistication of offenders in adopting new ways of violating legally protected interests, it is possible, in the near future, to anticipate the emergence of other international documents regulating the area in question. However, even the legislative readiness of the company does not ensure the subsequent ability to implement the legislation by the repressive and judicial units and does not ensure cooperation with other states.[24]

[8] The Council of the European Union Convention on Cybercrime was adopted in Budapest on 23 November 2001 after four years of work by experts from the Council of Europe, the USA, Canada, Japan and other countries. It was signed by the Slovak Republic on 4 February 2005, ratified on 8 January 2008 and has been in force since 1 May 2008.

The problem of cybercrime investigations and sanctions is not only regional but global. A quality investigation and the functioning of the law enforcement authorities would bring about a fundamental turnaround. However, the submission of electronic (digital) evidence itself is often problematic and very complex, since in many cases it does not exist in a "readable" or "tangible" form. Without sufficient evidence and timely cooperation between law enforcement authorities and forensic experts and specialists, it is almost impossible to detect the perpetrator.

Introduction of so-called the "best evidence rule" in the US admits that the printout of an electronic document and its original electronic form are identical for the purposes of legal proceedings, there are still many problems, as the loss of information contained in an electronic document when printed can be very substantial (eg in the simplest case, hyperlinks may be lost) and all efforts to convict and punish the perpetrator may be frustrated. The European institutions are no better off, especially given the different perceptions of the law in the different Member States of the European Union. Cyberspace does not have borders and, for example, simply determining the place that is applicable to the application of the relevant law is a problem that has not yet been legally resolved, even though several framework decisions and directives of the European Parliament and the Council of Europe have been issued. The adoption of Directive 2016/1148 of the European Parliament and of the Council of 6 July 2016 on measures to ensure a high common level of security of network and information systems in the Union (NIS Directive) can be considered as the most significant step in European Union legislation in the field of cyber security.[9]

The Slovak Republic adopted the Act no. 69/2018 on Cyber Security, which entered into force on 1 April 2018. Although the law undoubtedly established the basis of a systemic approach at national level to address the issue of cyber security, it will still be necessary to take a number of other related steps in this respect. Some such steps have already been defined in the Cyber Security Concept for 2015-2020 and in the Action Plan for the Implementation of the Cyber Security Concept for 2015-2020.[10]

5. Cyber wars

In the calculation of cyber threats, the threat of cyberwars, which are defined as activities conducted or coordinated by the State with a view to gaining information superiority or eliminating the technological infrastructure of the adversary, cannot be omitted. As a support to cyber war and its effects can be used information warfare, which can also be understood as a war on information or as a struggle between people working with information, eventually clashes where the main weapon is information -

[9] This Directive establishes a uniform approach to cyber security at the highest level in the Member States and brings clear rights and obligations for actors in this area. For more details see: [25]

[10] For more details see: *The Concept of Cyber Security of the Slovak Republic for the years 2015-2020* and *Action Plan for the Implementation of the Cyber Security Concept of the Slovak Republic for the years 2015-2020*

especially their quality, accuracy, credibility and availability, their targeted detention from the enemy party or the targeted misinformation of the enemy party.[26]

At present, many states are working very intensively on the concept of information warfare. In the case of so-called criminal states, it is crucial to find that their forces can hardly succeed in the conventional military conflict with the most advanced states in the world. That is why they focus their strategic activities primarily on the possibilities of fighting in cyberspace. Information war is a struggle that is very specific and basically relatively demanding in terms of personnel and material.

Its asymmetric nature is often highlighted, since an undetected or surprising attack can undermine the defence of a much stronger and "richer" adversary and cause damage many times higher than its cost.[27] Cyber wars bring with them a new name of the war arsenal – the infoware. This term means the sum of all combat means aimed at destroying the opponent's communication, information or electronic infrastructure and the information means necessary to conduct a cyber fight.

Based on current developments in this area, it can be stated that cyberwar weapons are placed in arsenals of several states (and groups) and ready for use. The current cyberwar is waged through computers and can take many different forms - from tapping or disrupting information and communication networks, to jamming television and radio broadcasts, spreading disinformation campaigns through "stolen" radio and television frequencies, disrupting logistics networks, disrupting financial flows to sabotage of pipelines or electricity distribution networks.

Cyberwar is no longer just a science fiction, but an existing real threat, the gravity of which continues to grow with the gradual transition into the era of the knowledge society. Meanwhile, most of the population is not aware of this asymmetric threat to such an extent as physical terrorism or limited access to energy resources and is trying to downplay this serious problem. However, the vulnerability of a modern society, increasingly reliant on electronic communications and the use of information and technologies communication, systems and means, is very high.

Conclusion

Cyber threats have become one of the most discussed topics related to national security in recent years, under the influence of a continuously deteriorating global security environment and security situation in several regions of the world. Ensuring security is considered one of the fundamental functions of the State. The difference from the past, a few decades ago, is that, thanks to technical and technological advances in cyberspace, it no longer only applies to the most developed, economically strong states, but its boom can be observed in almost all countries around the world, regardless of average living standards in them. Thanks to global interdependence, all actors become part of a single global information system, with countless accesses without geographic constraints. Participating actors, whether in the form of states, multinational corporations, public institutions and organizations or private entities, are thus becoming not only more interdependent, but also more dependent and more vulnerable.

Cyber attacks on government and private information networks and servers in several countries (eg Estonia, USA or Georgia, etc.) have confirmed the existence of cyber threats, regardless of whether they are aware of it. These attacks prove that states, as fundamental entities of the post-Westphalia international system, are facing a new kind of asymmetric security threats in a changing global and regional security environment. Given the dynamic developments in the sector of information and communication technologies, systems and means, it is highly likely that these types of attacks will most likely only spread in the near future and cyber threats will be at the forefront of the imaginary asymmetric security threat ranking.

At the same time, the ever-expanding tools for web presentations lead to a greater number of weaknesses and shortcomings on this site. Attacking websites or information networks, private or public, whether by cyber-terrorists spreading fear and their ideology, or by hackers - individuals or hacking groups pursuing their own specific interests (fame, money or liquidation of competition); rented hackers in various services is likely to lead to further development of offensive activities in this area. It is anticipated that direct attacks on e-mails will gradually become less effective as users grow, and attackers will move to other more sophisticated procedures. On the other hand, cyber-piracy, industrial and economic espionage, increased attempts to obtain individuals' personal data[11] or even theft of an entire identity, as well as increased sophisticated attacks on servers and virtual systems of banks, insurance companies and large corporations, including government and their armed and security forces.

Finally, cyberspace has no limits. It is a new battlefield with several unique features. Computers and their keyboards have become weapons, communication and information technologies, systems and means are weapon systems, and cyber fighters use software and hardware instead of conventional weapons. Cyber attackers are largely hidden, anonymous to attackers in conventional combat, not to mention zero risk of life compared to the real battlefield, but the results of their relatively inexpensive and low-risk activities are surprisingly effective and destructive. Thus, even the possibility of future conflicts will lose their conventional dimension and become unconventional wars in which individual parties to the conflict will not have to use conventional military tactics or physical lethal weapons at all. On the contrary, it is possible that a highly specialized group will be enough to liquidate an adversary (state, coalition) that will perform several cyber attacks on the critical infrastructure of the adversary. The result will be destabilization, chaos and liquidation of the adversary (state, coalition) from inside and his inability to respond adequately. Therefore, the pressure to create the most secure information networks and the development of methods, procedures, means and equipment for defence, cyberspace security and safety will increase even more in the future and will be one of the forefront in the further development of communication and information technologies, systems and means. Equally, the information and cyber security of the state, society and the individual will become more important.

[11] For more details see: [28]

References

[1] JIROVSKÝ, V. 2008. *Kyberterorismus – bezpečnostná hrozba 21. storočia*. 2008. In *EAQ*, 2008, roč. 3, č. 4, s. 8-9. ISSN 1336-8761.

[2] WEBSTER, F. 2002. *Theories of the Information Society*. New York: Routledge, 2002. 304 s. ISBN 978-0-41528-201-7.

[3] BARIČIČOVÁ, Ľ. 2011. *Kompetencie policajných manažérov*. Bratislava: Akadémia Policajného zboru, 2011, 160 s. ISBN 978-80-8054-514-7.

[4] KREMMER, J. F. – MÜLLER, B. 2013. *Cyberspace and Inter-national Relations: Theory, Prospects and Challenges*. Berlin: Springer Science & Business Media, 2013. 284 s. ISBN 978-3-642-37481-4.

[5] RATRAY, G. J. 2001. *Strategic Warfare in Cyberspace*. Cambridge, Massachusetts: *Massachusetts Institute of Technology* Press, 2001. 517 s. ISBN 978-0-26218-209-6.

[6] DENNING, D. 2000. *Cyberterrorism*. [on line] [cit 20-03-2020] available from: <http://palmer.wellesley.edu/~ivolic/>

[7] ANDRASSY, V. – GREGA, M. Možnosti optimalizácie informačných systémov v bezpečnostnom systéme. In *Košická bezpečnostná revue*, 2015, roč. 5, č. 2, s. 11-18. ISSN 1338-4880.

[8] BARIČIČOVÁ, Ľ. 2018. Informačná kompetentnosť v kontexte aktuálnych potrieb informačnej spoločnosti. In *Aktuálne výzvy prevencie počítačovej kriminality – zborník príspevkov z vedeckej konferencie s medzinárodnou účasťou*. Bratislava : Akadémia policajného zboru v Bratislave, 2019, pp. 8-17. ISBN 978-80-8054-773-8.

[9] BREZULA, J. 2018. Vývoj kybernetickej bezpečnosti vzhľadom na nové hrozby v súčasnosti. In *Tradície a dynamika vývoja manažmentu a informatiky z pohľadu univerzít s bezpečnostným zameraním. Zborník príspevkov*. Bratislava: APZ, 2018, s. 143-151. ISBN 978-80-8054-767-7.

[10] PŘIBYL, T. 2008. *Kyberterorizmus.* [on line] [cit 20-03-2020] available from: <http://www.virusy.sk/clanok.ltc? ID=402.html>

[11] DENNING, D. E. 2006. *Activism, Hacktivism and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy*. [on line] [cit 20-03-2020] available from: <http: //www:nautilus.org/info-policy/workshop/papers/ denning.html>

[12] JANCZEWSKI, L. – COLARIK, A. M. 2005. *Managerial Guide for Handling Cyberterrorism and Information Warfare*. Idea Group Inc., 2005. 229 s. ISBN 978-1-59140-550-4.

[13] BOTTESINI, B. J. 2008. *Medzinárodná kooperácia v boji proti kyberterorizmu*. In *EAQ*, roč. 3, č. 4, s. 10-11. ISSN 1336-8761.

[14] CAROLL, A. 2017. *Preparing for Worst-Case Scenarios with Cyber Attacks*. [on line] [cit 21-03-2020] available from: <https://lifelinedatacenters.com/data-center/cyber-attack-scenarios/>

[15] SCHILLER, J. 2010. *Cyber Attacks & Protection: Civilization Depends on Internet & Email*. Baltimore: Create Space Inc., 2010. 204 s. ISBN 978-1-45360-913-2.

[16] KORAUŠ, A. – DOBROVIČ, J. – RAJNOHA, R. – BREZINA, I. The safety risks related to bank cards and cyber attacks. In *Journal of Security and Sustainability Issues*, 2017, 6 (4), s. 563-574. ISSN 2029-7017.

[17] KORAUŠ, A. – DOBROVIČ, J. – KLJUČNIKOV, A. – GOMBÁR, M. Customer Approach to Bank Payment Card Security and Fraud. In *Journal of Security and Sustainability Issues*, 2016, 6 (1), s. 85–102. ISSN 2029-7017.

[18] KUCHTOVÁ, J. 2018. Aktuálne trendy súvisiace s využívaním moderných technológií. In *Aktuálne výzvy prevencie počítačovej kriminality – zborník príspevkov z vedeckej konferencie s medzinárodnou účasťou*. Bratislava : Akadémia policajného zboru v Bratislave, 2019, pp. 90-98. ISBN 978-80-8054-773-8.

[19] RÉVESZOVÁ, L. 2019. Kyberpriestor, kybernetická kriminalita a komparácia jej nárastu vzhľadom na dynamiku vývoja. In *Aktuálne výzvy kybernetickej bezpečnosti (v podmienkach bezpečnostných zložiek)*. Bratislava : Akadémia Policajného zboru, 2019, s. 97-101. ISBN 978-80-8054-819-3.

[20] CARBON, B. 2018. *What is Cyber Espionage*? [on line] [cit 22-03-2020] available from: <https://www.carbonblack.com/resources/definitions/what-is-cyber-espionage/>

[21] TECHOPEDIA. 2019. *Cyberspying*. [on line] [cit 21-03-2020] available from: <https://www.techopedia.com/definition/ 27101/cyberspying>

[22] PALMER, D. 2019. *Cyber espionage warning: The most advanced hacking groups are getting more ambitious*. [on line] [cit 21-03-2020] available from: <https://www.zdnet.com/article/cyber-espionage-warning-the-most-advanced-hacking-groups-are-getting-more-ambitious/>

[23] FOLTZ, B. C. 2004. *Cyberterrorism, computer crime, and reality*. [on line] [cit 22-03-2020] available from: <https://www.emeraldinsight.com/doi/abs/10.1108/09685220410530799>

[24] KURILOVSKÝ, R. 2018. Vyšetrovanie počítačovej kriminality. In *Polícia ako garant bezpečnosti. Zborník z medzinárodnej vedeckej konferencie*. Bratislava: APZ, 2018, s. 162-171. ISBN 978-80-8054-751-6.

[25] ŠIŠULÁK, S. – ŠALMÍK, M. 2018. Smernica NIS a dopad jej transpozície v policajnom prostredí. In *Polícia ako garant bezpečnosti. Zborník z medzinárodnej vedeckej konferencie.* Bratislava: APZ, 2018, s. 392-402. ISBN 978-80-8054-751-6.

[26] OLAK, A. – KRAUZ, A. 2014. Cyberwojna internetowa narzędziem grożnej broni cyfrowej na rubieży bezpieczeństwa globalnej infrastruktury krytycznej. In *Vojenské reflexie* 2014, roč. 9, č. 1, s. 130-143. ISSN 1336-9202.

[27] TOMÁŠEK, R. 2019. Aktuálne bezpečnostné hrozby. In *Národná a medzinárodná bezpečnosť 2019 – zborník príspevkov z 10. medzinárodnej vedeckej konferencie*. Liptovský Mikuláš : Akadémia ozbrojených síl generála M. R. Štefánika, 2019, s. 483-492. ISBN 978-80-8040-582-3.

[28] KOSTREC, M. 2019. Ochrana osobných údajov – Výsledky výskumov vykonaných vo Francúzsku, na Slovensku a v Českej republike. In *Aktuálne výzvy kybernetickej bezpečnosti (v podmienkach bezpečnostných zložiek)*. Bratislava : Akadémia Policajného zboru, 2019, s. 78-96. ISBN 978-80-8054-819-3.

Author:

[1]**Radoslav Ivančík –** Akadémia Policajného zboru v Bratislave, Sklabinská 1, 835 17 Bratislava 35, Slovenská republika, email: radoslav.ivancik@akademiapz.sk