CYBER SECURITY IN PUBLIC ADMINISTRATION OF THE CZECH REPUBLIC

Eva ARDIELLI, Jiří ARDIELLI

Abstract

The paper is focused on the cyber security in Czech public administration. It deals with the theoretical question of cybercrime, development of emerging trends in the use of the Intranet / Internet and online technologies, the usage of new technologies and systems that are the driving force behind the ever-increasing threats in IT. Health systems, intelligent energy, but also the whole concepts of Czech e-Government currently pose a cyber-security risk. In the introduction of the paper are described the legal standards in the CR and the basic document ensuring the cyber security in the CR. Cyber security law, national cyber security strategy, the establishment of a National center of cyber security and others are concrete steps to ensure or mitigate threats in the form of cybercrime. Despite all these activities there are repeatedly documented the security incidents in IT. There are many different types of attacks, the list of specific cases are documented in the paper. Current statistics show continuing trend of threats. The paper then tries to analyze the trend of increasing efforts to ensure cyber security on the one hand and on the other hand the growing trend in the number of incidents and the growing threat of cybercrime.

Key words

Cybercrime, Public Administration, Cyber security

JEL Classification: H00, H11, H10

Introduction

As is clear from the reports on the state of cyber security in the Czech Republic from 2014 (NBÚ, 2016) issued by the National Cyber Security Center (NCKB), the opening of NCKB as a part of the National Security Agency (NSA) and the adoption of the Act no. 181/2014 Coll., On cybersecurity (Parlament ČR, 2014), these events were the two most significant events of the year 2014 in securing the cyber security in the Czech Republic (CR). The Czech Republic will be faced in the coming years by many cyber security risks and threats and the national networks and systems must by always stable and secure, as stated in the preamble of the key document of the Czech Republic called the National Strategy for Cyber Security of the Czech Republic for the period 2015 - 2020 (NCKB, 2014). According to this Strategy the significant risks are cyber espionage (whether industrial, military, political or otherwise) which is increasingly supported directly by governments, or the security structure of a particular state, than the organized crime in cyberspace, hacktivismus (hacking for political purposes), intentional disinformation in order to achieve the political and military objectives, or in the future the cyber terrorism.

NSA, as the main guarantor of cybersecurity of Czech Republic clearly recognizes the growth dynamics of threats coming from the gray zone. Government and security structures of foreign countries, organized crime, hacker organization - they all make the Internet in the middle of the second decade of the 21st century the equivalent of the war no man's land. It is a land where everything is allowed and where the term of ultimate success justifies any actions (Fair, 2015; Henson, Reyns and Fisher, 2011)

The aim of the presented paper is to evaluate the current security trends in information crime in the Czech Republic and to evaluate the time series of security incidents and to determine the future estimate of incidents.

1. Cyber Security in the Czech Republic

Cyber security becomes steadily in importance and nowadays it is one of the defining aspects of the security environment of the CR. Specifically, the term “cyber security” represents in the CR the summary of organizational, political, legal, technical and educational measures and instruments designed to ensure the secure, protected and durable cyberspace in the CR, both for public and private sector and the general Czech public (Borovička, 2015). Cyber security helps to identify, evaluate and address threats in cyberspace, to reduce cyber risks and to eliminate the impact of cyber-attacks, cyber-crime, cyber terrorism and cyber espionage in the sense of strengthening the confidentiality, integrity and availability of data, systems and other elements of information and communication infrastructure.

1.1 Organizational and conceptual ensuring of cyber security in the CR

The coordinator and the national authority in the area of Czech cyber security is the NSA established in 2011. The part of its activities was the opening of the National Cyber Security Center CERT (Computer Emergency Response Team) in 2011 in Brno. This organization has a crucial role in addressing cyber security in the CR. NCKB represents an organizational component of the NSA and consists of government CERT (GovCERT.CZ) and the Department of theoretical support for education and research (OTPVV). The mission of GovCERT.CZ is to monitor current trends in cyber security. It addresses technical issues of cyber security including solving of security incidents of subjects that manage important communications and information systems for the government, then the malware analysis, collection and evaluation of information on cyber-attacks and threats and so on. GovCERT.CZ performs tasks such as ensuring the prevention of cyber threats and attacks against crucial information infrastructure operators and public authorities and ensuring and coordination of solutions of cyber security incidents of crucial information infrastructure operators and public authorities (CSIRT, 2015).

NSA took over after his predecessor in this post (Ministry of Interior) the cyber security strategy of the Czech Republic. The National Cyber Security Strategy of the Czech Republic is a document that declares the core values, interests, attitudes, ambitions and tools of the CR to safeguard the security and formulates the principles on which the security policy of the CR was founded. In this strategy are defined vital, strategic and other important interests of CR, the security environment of the CR as well as described the security system of the CR. Security Strategy is the basic document of the Security Policy of the CR. In the text is on the general level stressed also the cyber security. This strategy then builds sub-strategies and concepts. As part of ensuring cyber security are the most important two major follow-up strategies/concepts (Bagge and Pačka, 2014). It's "White Paper on Defense" (Parlament ČR, 2011), which defines in the area of cyber defense the main tasks of the Ministry of Defense and the national "Strategy for Cyber Security in the Czech Republic for 2012 - 2015", which was from 1. 1. 2015 replaced by the "National Strategy for Cyber Security for the period 2015 - 2020". The new strategy compared to the previous version (which operated more in the broader contours and tried to build mainly the basic tools, capabilities and legislative/strategy framework to ensure cyber security) addresses the issue of cyber security more comprehensively and systematically. It currently serves as the default document for the creation of related legislation, policies and standards, guidelines and other recommendations in the area of protection and cyber security of the country.

1.2 Cybercrime in criminal law

The massive emergence of the Internet and ICT in general is strongly reflected in criminal law. The information crime is understood as crime that is committed in an environment of information technologies, including computer networks. The object of attacks is the area of information technologies or this crime is committed with significant use of information technologies as a means for its commission. It is therefore the definition of the offenses, which include a common factor describing the method of committing. At present it is mainly about the abuse of the global computer network Internet (Kuchařík, 2014; Choi and Lee, 2017), and the person-based forms as phishing, hacking and malware (Reyns, 2015).

The basic international document which is dealing with criminal liability for acts committed in the context of cyberspace is the Convention on Cybercrime, the Act no. 104/2013 Coll. (Parlament ČR, 2013), at the European level it is than the Directive no. 2013/40 /EC on attacks against information systems (European Parliament and Council, 2013), which is directly based on the Convention. In the Convention are recognized three types of offenses related to cybercrime. The first types are offenses against the confidentiality, integrity and availability of computer data and systems. These are reflected in the Czech law in § 230 and 231 of the Criminal Code (Parlament ČR, 2009). These include unauthorized access to computer systems (hacking), interception (monitoring of communication at a time when runs) and data interference and system interference (changes, damage). Crimes are also production, provision or disclosure of viruses and other devices (whether hardware or software), created to gain unauthorized access to a computer system or electronic communications network. The second area of crimes described in Convention is the forgery and fraud. The third area is focused directly on the contents of communications. Specifically states the production and distribution of child pornography and impairment of intellectual property right (piracy). Piracy is an only offense related to the content, which is namely given in the Convention beyond child pornography, which negative effects and the needs to combat are indubitable (Hladká and Fousek, 2014).

Cybercrime is often investigates through traffic and location data that are compulsory by law stored by telecommunications operators - § 97 of the Electronic Communications Act (Parlament ČR, 2005) and are provided to investigators that can determine which web sites were accessed by the suspected person, with whom he communicated and where was his physical location. In order to ensure successfully detection of cybercrime and to be pursued it is required the intensive international cooperation. The bodies of criminal justice of different countries help each other in both situations of collecting of evidence and the detention and subsequent extradition of persons.

Since 1. 1. 2015 has been in the CR applied Act no. 181 Coll., On cybersecurity (ZOKB). ZOKB is a major step in the Czech legislation, leading to greater safety in the digital environment of state institutions and companies. The Act significantly increases the safety standard and availability of services that are provided to citizens in cyberspace (Krátký, 2014). ZOKB establishes rules especially for those subjects whose systems, networks and services are crucial for the functioning of the state or the information society. These are so called crucial information infrastructures, as well as significant information systems that are managed by public authorities. The disruption of information security of these infrastructures could endanger or severely limit the activity of public administration. These bodies are obligated by the law to provide systems for detecting cyber security events and incidents. Information security breaches in the operating systems must be reported to governmental centre CERT (Kniewald, 2014).

A crucial step in the implementation of technical measures of ZOKB was to build and launch of the Control Center of eGovernment (DCeGOV) to ensure cyber safety oversight - Security Operation Center for Continuous Reliability (SOCCR), enabling monitoring of communication and information systems within the critical information infrastructure and the significant Information Systems. To the Control Center on eGovernment as from 1 January 2016 are gradually linked information systems in accordance with the timetable set by law.

1.3 National Strategy for Cyber Security of the Czech Republic for the period 2015 - 2020

The director of the NSA submitted to the government of the CR for approval the new National Strategy on Cyber Security of the Czech Republic for the period 2015 to 2020 on the 16. 2. 2015. The approved strategy is based on the original strategy for cyber security for the period 2012 to 2015. The content of this strategy is a comprehensive package of measures aimed at achieving the highest level of cyber security in the CR and for this purpose the strategy defines the vision of the CR in this area. At the same time, the strategy identifies the basic principles that the CR is going to follow and abide in ensuring of cyber security. The strategy also defines the specific challenges and problems in the field of cyber security both for the CR and for the international environment in which the CR is located and to that it has to face.

The main part of the Strategy is presented by the major goals which are to be achieved in the coming five years and which are divided into 8 priority areas:

- Ensuring of the effectiveness and strengthening of structures, processes and cooperation with the ensuring of cyber security
- Active international cooperation
- Protection of National KII and VIS
- Cooperation with the private sector
- Research and Development / Consumer Confidence
- Support for education, awareness and information society development
- Promoting of the development of skills of the Czech police to investigate and prosecute the cyber-crime
- Legislation on cyber security (establishing of the legal framework). Participation on the formulation and implementation of European and international rules.

The Strategy is followed by the Action Plan of the National Cyber Security Strategy of the Czech Republic for the period 2015 - 2020, where are defined specific steps, responsibilities, deadlines for implementation and control.

Regarding the structure and the organization of the text in Strategy there are first introduced the visions of CR in the area of cyber security over the timeframe of the Strategy (2015 - 2020) and subsequently there are defined the basic principles which are followed to ensure the cyber security in the Czech Republic:

- Protection of human rights and fundamental freedoms and democratic principles of the state
- Comprehensive approach to cyber security based on the principle of subsidiarity and cooperation
- Building of the trust and cooperation between the public and private sector and civil society
- Development of capacities for ensuring cyber security.

This first general part is followed by a chapter on specific challenges in the field of cyber security both for the CR and for the international environment where the CR is located. Finally are presented the strategic objectives that are facing these challenges and these are the basis for the Action Plan for Cyber Security of the Czech Republic for the period 2015 to 2020. In the strategy, there are defined 19 challenges that were identified as crucial in the CR. These are the issues and trends that are for the CR and its citizens actual, and must by responded (by determining the main objectives and actions in the Action Plan).

2. Materials and Methods

The analysis of actual security incidents and the number of incidents is based on the annual reports from the years 2011 - 2015 published by the Ministry of Interior of the CR (MVČR, 2015), that describe the information criminality. Other sources of analysis are monthly reports of security incidents that are published by NCKB, for 2014 - 2015. The research results are determined by the usage of time series analysis and trend analysis.

Absolute growth was determined based on the formula 1:

$$\Delta_t = y_t - y_{t-1}$$

where $t = 2,3,...,n$.

Relative growth was determined based on the formula 2:

$$\delta_t = \frac{y_t - y_{t-1}}{y_{t-1}}$$

where $t = 2,3,...,n$.

Growth coefficients were determined based on the formula 3:

$$k_t = \frac{y_t}{y_{t-1}}$$

where $t = 2,3,...,n$.

Average absolute growth was determined based on the formula 4:

$$\Delta = \frac{y_n - y_1}{n - 1}$$

Average growth coefficient of time series was determined from the formula 5:

$$k = \sqrt[n-1]{\frac{y_n}{y_1}}$$

Then was performed the trend analysis. Using graphical analysis was verified the linear character of the trend curve and were estimated the parameters of the curve by the method of the least squares, see formula 6 and 7:

$$b_1 = \frac{n\sum ty_t - \sum t \sum y_t}{n\sum t^2 - (\sum t)^2}$$

$$b_0 = \frac{\sum y_t}{n} - b_1 \frac{\sum t}{n}$$

After that was determined the trend function T_t and the estimate t of the year 2016.

To evaluate the current security trends were observed and mapped current and emerging trends in online networking technologies that have an impact on the public administration. The analysis was based on sources of reputable companies such as Gartner (Gartner, 2015), or IEEE Computer Society (IEEE, 2015). There was performed the systematization of individual trends, their understanding in the broader context and subsequent the categorization and selection of key trends with respect to public administration.

3. Outputs of the research

The outputs of research are twofold. In section 3.1 are presented results of the analysis of current security trends in public administration, section 3.2 contains the outputs of trend analysis and time series analysis of security incidents in 2011 - 2015.

3.1 Assessment of current security trends in public administration

Based on the content analysis of data of reputable companies (Gartner, 2015; IEEE, 2015) were systematized current security trends and identified the key trends with regard to public administration and was done their categorization in tab. 1.

Table 1 Categorization of key security trends in public administration

1. Increasing volumes of data (Big Data) and the issue of governance and security of such amount of data
Big Data, thus generating datasets, which both complexity and volumes are growing exponentially, analysis, archiving and sharing is one of the great challenges of the 21st century. Protection and data security is very important for the CR, especially those that are a matter of public interest. In public and private sector is growing amount of data with which is worked and that it is necessary to continue to store. Therefore they began to use new forms of data storage, for example cloud storage. Increased use of these online services and cloud, however, often leads to non-transparent security solution whose credibility is at least questionable.
2. Diversity of mobile devices ("bring your own device" (BYOD))
Significant internal threat is a worrying trend of growing acceptance of model "bring your own device" (BYOD). Cybercriminals Increasingly, this trend will use to penetrate into target companies (initially infect personal employees devices who did not implement strict security measures, and then through them puts Trojan horse that infects the network). Policies on the use of hardware owned by employees must be thoroughly examined and, where necessary, updated and expanded.
3. Security and privacy of cloud
Attacks on cloud services are gaining strength, it is expected a great breach of security in the cloud in the near future. At present, according to IBM three-quarters of a security breach last for days, weeks or even months before they were discovered, and thus greatly increase the damage attackers.
4. Need for tracking the movement of data within the organization
Behavioral analysis technologies enable enterprises (companies, institutions) to monitor users within companies and end users. That may bring to them the warning about suspicious behavior that could be data theft or attacks by malicious software.
5. Attacks to destroy
Some ideologically profiled hacktivist group upheld, that they will continue to try to destructive attacks against the interests of certain companies or public institutions.
6. Safety risks associated with computerization of public administration (eGovernment)
E.g. electronic procurement process will entail new risks that may threaten the credibility of the procurement procedure and safety risks associated with the fact that electronic tools for procurement are connected to the public network.

Source: Own elaboration based on data from reputable companies (Gartner, 2015; IEEE, 2015).

3.2 Trends in cyber-crime

Cyber-crime trends were drawn from the annual reports published between 2011 and 2016, which are published annually by the Ministry of the Interior, Department of Security Policy. Each report on the situation in the field of internal security and public order in the Czech Republic in 2011 (till 2016) describes, among others information crime and cyber security for the previous year, i.e. for the period 2010 to 2015. Except to 2010 year there are in all reports the quantified data about information crime. In the years 2010 and 2011 were the most common manifestations of this crime identical, and ranked among them in particular, copyright violations, the spread of extremist and terrorist propaganda, disseminating of prohibited pornography, fraudulent conduct, threats, blackmail, scaremongering, slander and attacks on information systems and data. In 2012 was added stalking. In 2013 and 2014 were both about copyright violations, threats, extortion and swindling, where is monitored steady growth. Also noticeable was the increase of detection of crimes involving the unauthorized data manipulation. In 2015 the major trend was swindling - it was investigated 2,915 cases of fraud in the information technology and especially the Internet, which is an increase of 19% compared to 2014.

Regarding the number of cases for 2010 have not been published. In 2011, the Czech Police registered a total of 1,502 crimes committed by the Internet or other computer networks. In 2012 it was 2,195 (+693, +46.1%) crimes and in 2013 was registered 3108 (+913, +41.6%) crimes. In 2014, information crime was still rising and was dealt with 4,348 cases (+1240, + 40%). In 2015 it was 5023 cases (+675, +16 %). For the year 2016 the data are not published, so they will be estimated. In the tab. 2 are summarized the characteristics of time series. The number of cases per year increased by an average of 35.2% (average growth coefficient of time series), which in absolute terms represents an average annual increase of 880 cases (average absolute growth).

Table 2. Characteristics of time series

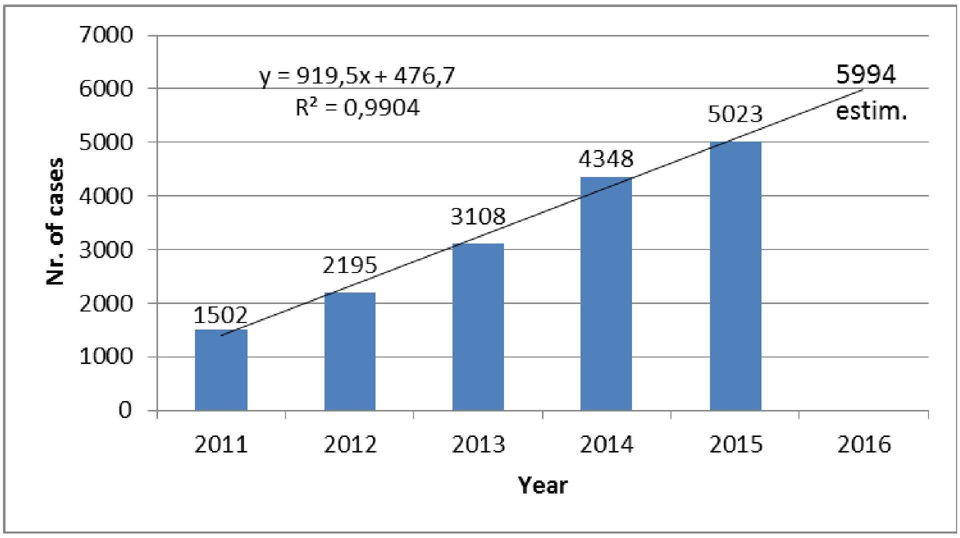
year	number of incidents	absolute growth	relative growth	growth coefficient
2011	1502	-	-	-
2012	2195	693	0.461385	1.461385
2013	3108	913	0.415945	1.415945
2014	4348	1240	0.39897	1.39897
2015	5023	675	0.155244	1.155244

Source: Own elaboration based on data from the annual reports of the MVČR (2011-2015)

Although relatively few observations are available, it is obvious from the graphical record that the trend line will be a regression line.

Linear trend line with a coefficient of determination of 0.99 estimated 5,994 cases in 2016 see graph 1. The parameter b_1 is 919.5, parameter b_0 is 476.7. The trend function is $T_t=476.7+919.5t$, the estimate t is 5993.7.

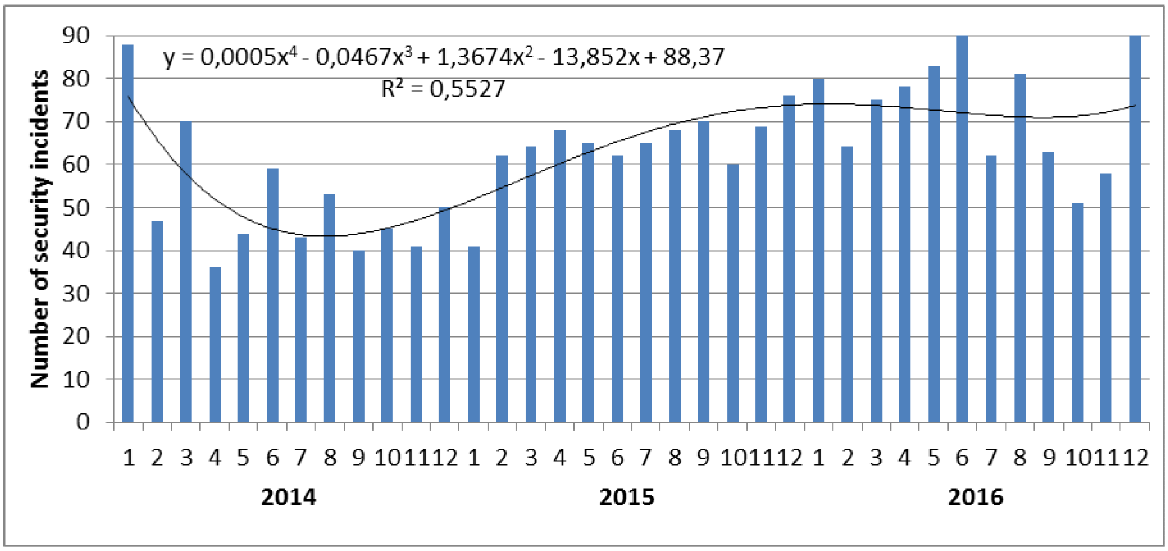
Fig. 2 Trend in cyber-crime in the years 2011-2015



Source: Own elaboration based on data from the annual reports of the Ministry of the Interior (2011-2015).

In addition to the data monitored by the Ministry of Interior has been also compiled data of cyber incident from NCKB, for the years 2013 to 2016. It was based partly on annual reports - Report on the state of cyber security in the Czech Republic, available for 2013, 2014 and 2015 (NBÚ, 2016), and partly on monthly statements published in the bulletin - Security incidents, available for the years 2014, 2015 and 2016 (NCKB, 2016). In annual reports is monitored number of requests and in report from 2014 and 2015 also the numbers of incident reports. In the monthly published bulletin Security incidents there are described individual incidents in a given month, see Fig. 2. The amount of incidents for 2014 is 616, for 2015 it is 770 incidents and for 2016 it's 881. Up to polynomial functions of 4th order with satisfactorily coefficient of determination of 0.55 reveals a slightly increasing trend for the future.

Fig. 2 Trend of security incidents in the years 2014-2016



Source: Own elaboration based on data from security incidents NCKB (2014-2016).

4. Discussion of the achieved results

As shown by the analysis of trends in cybercrime and security risks in the future it is expected that with the increase in the number of devices using computer technology and their network interconnection it will increase the possibility of abuse. It is documented by works of other authors on international level, that identified computer crime as a primary threat to computer systems, users, and organizations (Lu et al., 2010 or Leukfeldt et al., 2017). At the same time we can expect an increase in the sophistication of attacks. To sum up, in the future, are to be feared of significant attacks and because of dissemination of advanced technologies it will be able to cause much more damage. This corresponds to researches of experts in this field who predict the risk of "cyber wars", the conflict led through a computer network; see Singer and Friedman (2014), Kaiser (2015), Arquilla and Ronfeldt (1993). This may be conducted by individual states or by their security agencies (in this context, e.g. attack in Estonia was attributed to the test of potency of "cyber weapons" of NATO). From this perspective, there is a real possibility of a similar attack as well as in the Czech Republic, as highlighted Herzog (2011). NSA itself in the National Strategy 2015 - 2020 notes a lack of public confidence in the state and its security apparatuses. Not very positive NSA view the e-government, whose services and applications to citizens and to private enterprises indicates as considerable cyber security risks.

Czech Republic for its security use technology used by other countries. Therefore, CR can be served to attackers as a test object before the attack on allies or other countries with greater strategic importance, using the same technology and security mechanisms and processes, as shown NCKB (2014). This is suggested by the fact that the number of cyber-attacks is increasing steadily. From own analysis of cases of Internet crime revealed that the most prominent manifestations of cybercrimes include swindling and embezzlement, forgery, defamation and electronic vengeance, hoaxes, warez, system penetrations, a computer bank robbery (Phishing, Pharming, IP spoofing). This is confirmed by studies of other authors; see Bagge and Pačka (2014), Shamsi et al. (2016). At this point it should be noted that the obligation to report cyber-attacks by law (ZOKB) is mandatory and for non-compliance are applied fines (Parlament ČR, 2014).

Protection and security of data for the Czech Republic is very important, especially those that are a matter of public interest. In public and private sector growing amount of data with which to work that is needed to continue stored. Therefore they began to use new forms of data storage, for example cloud storage. Increased use of the online cloud services often leads to non-transparent security solution whose credibility is at least questionable, as stated NCKB (2014). But it is also essential for every citizen to use online crime prevention behaviors (Reyns, Randa and Henson, 2017).

Conclusion

Ensuring cyber security of the state is one of the key challenges of our time. Dependence of public and private sector on information and communications technologies is becoming apparent. Sharing and protection of information is nowadays essential to protect the interests of the state and its citizens in the area of security and the economy. While the general public is most concerned about financial losses or loss of their data and misuse of personal data, the reality of the whole issue of cyber security is much larger. Risk currently represent not only a very frequent cyber-attacks carried out in order e.g. economic benefits, but also security breaches and network integrity caused unintentionally, e.g. by human error, natural disasters and the like. The State must therefore be able to provide an effective response to all current and future challenges in an ever-changing cyber threats, which may come from dynamically evolving cyberspace and thus guarantee secure and reliable cyberspace.

The strategy of the national cyber security of CR is a fundamental change in the approach to the fight to preserve the Czech cyber security information environments. Czech Republic as a modern Central European country and active member of the European Union, NATO, the United Nations and other international organizations, will be to aspire in the coming years to leading positions in the field of cyber security, and both within their region and throughout Europe.

Acknowledgements

The article was created within the financial support of the student grant project SGS No. SP2017/129 "Economic Factors Affecting the Ensuring of Public Services with Collective Consumption" on Faculty of Economics, Technical University of Ostrava.

Refernces

Arquilla, J., Ronfeldt, D. (1993). Cyberwar is coming! *Comparative Strategy*, 12 (2), 141-165. ISSN 1521-0448

Bagge, D., Pačka, R. (2014). Kybernetický prostor viděn ze zahraničí: Národní strategie kybernetické bezpečnosti České republiky. In: *Sborník Evropského měsíce kybernetické bezpečnosti 2014*. Praha: Národní centrum bezpečnějšího internetu, s. 1-8.

Borovička, V. (2015). *Legislativa ČR v oblasti kybernetické bezpečnosti.* Brno: AFCEA, s 31.

Choi, K.-S., Lee, J.R. (2017). Theoretical analysis of cyber-interpersonal violence victimization and offending using cyber-routine activities theory. *Computers in Human Behavior*, 73 (1), 394-402. ISSN 0747-5632

CSIRT (2015). *Zákon o kybernetické bezpečnosti.* [on-line] [cit.: 2016-12-03]. Available at: https://www.csirt.cz/page/2630/zakon-o-kyberneticke-bezpecnosti/.

Evropský parlament a Rada (2013). *Směrnice o útocích na informační systémy*. [cit.: 2015-05-09]. Available at: http://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX%3A32013L0040.

Fér, O. (2015). *Česko chce hrát prim v boji o kybernetickou bezpečnost, zatím ale zaostává*. [on-line] [cit.: 2016-07-09]. Available at: http://www.ceska-justice.cz/.

Gartner (2015): *Gartner Identifies the Top 10 Strategic Technology Trends for 2015.* [cit.: 2016-02-02]. Available at: http://www.gartner.com/newsroom/archive/.

Henson, B., Reyns, B.W. and B.S. Fisher, (2011). Security in the 21st century: Examining the link between online social network activity, privacy, and interpersonal victimization. *Criminal Justice Review*, 36 (3), 253-268. ISSN 1057-5677

Herzog, S. (2011). Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses. *Journal of Strategic Security*, 4 (2), 49-60. ISSN: 1944-0

Hladká, E., Fousek, J. (2014). *Základy IT gramotnosti*. [on-line] [cit.: 2016-01-03]. Available at: https://is.muni.cz/do/1492/el/sitmu/phil/html/kyberkriminalita.html.

IEEE (2015): *Top Technology Trends for 2015*. [on-line] [cit.: 2016-02-02]. Available at: http://www.comsoc.org/blog/top-10-communications-technology-trends-2015.

Kaiser, R. (2015). The birth of cyberwar. *Political Geography*. 46. Elsevier. 11-20. ISSN: 0962-6298

Kniewald, K. (2014). Zákon o kybernetické bezpečnosti přinese nové nároky na vzdělávání odborníků. *Národní pojištění.* Praha: Ministerstvo práce a sociálních věcí ČR. 8-9/2014. ISSN 0323-2395.

Kozlowski, A. (2014). Comparative analysis of cyberattacks on Estonia, Georgia and Kyrgyzstan. *European Scientific Journal*, 10 (7), 237-245. ISSN 1857-7881

Krátký, P. (2014). Zákon o kybernetické bezpečnosti v praxi. *IT Systems*. Brno: CCB, s. r. o., s. 28-30. ISSN 1802-615X.

Kuchařík, K. (2014). Aktuální trendy informační kriminality v rámci šetřených případů PČR. In: *Sborník Evropského měsíce kybernetické bezpečnosti 2014*. Praha: Národní centrum bezpečnějšího internetu, pp 4.

Leukfeldt, E. et al., (2017). Origin, growth and criminal capabilities of cybercriminal networks. An international empirical analysis. *Crime Law and Social Change*, 67 (1), 39-53. ISSN 1573-0751

Lu, Y. et al. (2010). Social network analysis of a criminal hacker community. *Journal of Computer Information Systems*, 51 (2), 31-41. ISSN 0887-4417

MVČR (2015). *Bílá kniha o obraně.* Tiskárny Havlíčkův Brod. ISBN 978-80-7278-564.

NBÚ (2016). *Zpráva o stavu kybernetické bezpečnosti České republiky 2015*. [cit.: 2017-03-20]. Available at: <

https://www.govcert.cz/download/bulletiny/bezbecnost-2015/nbu-zprava-stav-kb-2015.pdf>.

NCKB (2016). *Bezpečnostní incidenty*. [cit.: 2017-03-20]. Available at: https://www.govcert.cz/cs/informacni-servis/publikace/.

NCKB (2014). *Národní strategie kybernetické bezpečnosti České republiky na období let 2015 až 2020.* [cit.: 2016-02-02]. Available at: http://www.govcert.cz/download/nodeid-1004.

Parlament ČR (2005). *Zákon o elektronických komunikacích*. [on-line] [cit.: 2016-08-02]. Available at: http://www.psp.cz/sqw/sbirka.sqw?cz=127&r=2005.

Parlament ČR (2009). *Zákon trestní zákoník*. [on-line] [cit.: 2016-07-07]. Available at: http://www.psp.cz/sqw/sbirka.sqw?cz=40&r=2009.

Parlament ČR (2013). *Úmluva o počítačové kriminalitě.* [on-line] [cit.: 2016-12-12]. Available at: http://aplikace.mvcr.cz/sbirka-zakonu/ViewFile.aspx?type=c&id=6571.

Parlament ČR (2014). *Zákon č. 181/2014 Sb. o kybernetické bezpečnosti*. [on-line] [cit.: 2016-12-12]. Available at: http://www.psp.cz/sqw/sbirka.sqw?cz=181&r=2014/.

Reyns, B.W., (2015). A routine activity perspective on online victimisation: Results from the Canadian general social survey. *Journal of Financial Crime*, 22 (4), 396-411. ISSN 1359-0790

Reyns, B.W., Randa, R. and B. Henson, (2016). Preventing crime online: Identifying determinants of online preventive behaviors using structural equation modeling and canonical correlation analysis. *Crime Prevention and Community Safety*, 18 (1), 38-59. ISSN 1460-3780

Shamsi, J.A. et al., (2016). Attribution in cyberspace: techniques and legal implications. *Security and Communication Networks*, 9 (15), 2886-2900. ISSN 1939-0122

Singer, W. P., Friedman, A. (2014). *Cybersecurity and Cyberwar: What Everyone Needs to Know.* Oxford University Press. ISBN 978-0199918119

MVČR, (2015). Zpráva o situaci v oblasti vnitřní bezpečnosti a veřejného pořádku na území České republiky v roce 2015. [on-line] [cit.: 2017-3-23]. Available at: http://www.mvcr.cz/clanek/zprava-o-situaci-v-oblasti-vnitrni-bezpecnosti-a-verejneho-poradku-na-uzemi-ceske-republiky-v-roce-2015.aspx.

Kontakt

Eva, Ardielli, Ing., Ph.D..
Katedra veřejné ekonomiky,
Fakulta ekonomická,
Vysoká šlola Báňská – Technická Univerzita Ostrava - VŠB-TUO
Sokolská 33, Ostrava,
Czech Republic
e-mail: eva.ardielli@vsb.cz

Jiří, Ardielli, Ing.
Tieto Czech s.r.o.
Czech Republic
e-mail: jiri.ardielli@tieto.com