ISSN 1392–6195 (print)
ISSN 2029–2058 (online)
JURISPRUDENCIJA
JURISPRUDENCE
2013, 20(4), p. 1457–1472.

CYBER SECURITY IN YOUNG DEMOCRACIES

Jakub Harašta

Institute of Law and Technology, Faculty of Law
Masaryk University
Veveri 70
611 80 Brno, Czech Republic
Telephone: 00420 549 497 628
E-mail: harasta.jakub@gmail.com

Received on 30 October 2013; accepted on 28 December 2013.

doi:10.13165/JUR-13-20-4-10

Introduction

Totalitarian past is not the only tie bringing together Lithuania and the Czech Republic nowadays. Both countries are young democracies that underwent dynamic social, legal and political changes during the 90s to ensure transition toward being modern democratic states. Now, both are members of the European Union and NATO and they share common interest of the small European countries. However, the totalitarian past remains present and it has certain influence on recent issues arising even from the current information society. Totalitarian regimes in both countries left some of the political approaches twisted beyond recognition and adversely affected the very core of the society and ways it approaches itself and the others.

This paper is aiming to provide the comparison of Lithuania and the Czech Republic mainly within the field of the cybernetic security, but with certain overlaps to general theory of the information society and the continental legal tradition of distributive rights. In both countries, the cybernetic security presents a new and interesting challenge, because both countries can be perceived as rookies within this particular field. The author

tries to describe the current state-of-art of the cyber security, particularly approaching the United States, the United Kingdom and Germany, and apply findings to the current state of cybernetic security in Lithuania and the Czech Republic. Part of the paper is also reserved for the comparison between the approaches of the countries themselves, because despite being part of the EU/NATO political and securital background and target of the currently proposed cyber security Directive, there are still differences present due to the national character of the cyber security. Despite the importance of the threats emerging from the cyberspace[1], this topic has been scarcely approached by the law and as far as the author of this paper is aware, the topic of this article has no prior coverage as such, although the literature referred to covers various aspects of cyber security, including recommendations for nation states. This contribution is not intended to present the exhaustive and overwhelming solution, but merely to approach the future, while taking into consideration both the present and the past. The abovementioned aims are sought mainly through the legal pragmatism, including the policy analysis as a valuable foundation for possible future legal regulation of the given area. The main purpose is to highlight weak spots, but at the same time to point various good practices accepted by both countries.

1. Information society

Natural tendency of any society is to evolve towards the more efficient dissemination of information[2]. Every technological step leading to the faster exchange of information has been used in the past as a tool for evolution of the society and the same happened to the latest step (or maybe leap) forward. With the massive proliferation of the information and communication technologies into the society appeared what can be understood as substantial changes regarding ways of communication or commerce[3]. Every aspect of the society is affected and the information society arises as the new state of society. Dissemination of information as such is not a new concept. What is new and what constitutes the information society is the rate of the dissemination and exchange of information, and also the importance of it. Changes underwent in the economy, culture and labor market have also changed the perception of territoriality and geographical proximity (or rather distance)[4].

Means to produce information have not been accessible to everyone in the past. Everyone was able to talk, but more permanent production of information, such as writing, has been exclusively reserved to small parts of society. The same applied for reading the

1 Among the most serious threats can be listed the following: Estonia 2007, as an example of attack targeting the nation state as such; Georgia 2008, as an example of the cyberspace being used for war effort; Stuxnet, as an example of cyberspace being use for special operation and sabotage, etc., not to mention serious threats to data and even assets of individuals and companies.

2 For more, see Wiener, N. *Kybernetika a společnost.* Praha: Československá akademie věd, 1963.

3 Klimek, L. Combating Attacks against Information Systems: EU Legislation and Its Development. *Masaryk University Journal of Law and Technology*. 2012, 6(1): 87–100.

4 Webster, F. *Theories of the Information Society.* Third edition. London: Routledge, 2006, p. 8–9.

information and multiplying (copying) the information. The first step in the revolution that brought the information society, digitalisation, erased this problem. Information is universally duplicable and distributable. The second step allowing the information society to exist is the step-by-step increase of the computational power, while at the same time the cost keeps decreasing[5]. This paper does not aim to conclusively answer whether the abovementioned is for the good or bad. On the other hand, it definitely brings to light certain problems that the law is no longer able to solve exhaustively in a timely manner. Law in general needs time to evolve and to operate, which turns out to be almost impossible to achieve in this post-modern state of affairs.

2. Informational self-determination

Every society brings to life the specific set of rules and principles it values (or should value) the most. The informational self-determination arises as the key element of the information society. Legal theory recognises it as the distributive right – the right that can be distributed among individuals and not entitling solely the society as such. Every member is individually entitled if fulfilling certain conditions (for example, being a citizen).

Informational self-determination appeared during the 80s in Germany, when the abuse of information switched from occasional violations toward the systemical phenomenon. It was originally constituted as a right to affect the processing of one's own personal data. During time, the informational self-determination developed into a much wider catalogue of the distributive information rights. This catalogue is hard to be exhaustively listed or described, because it varies both in time and space and it swiftly adjusts itself according to technological development (unlike the other areas of law). Informational self-determination currently involves freedom of speech, protection of privacy, right to active private life, right to education, protection of personal data and the right to public sector information[6].

In the Continental legal theory and legal philosophy, the concept of distributive rights, such as the informational self-determination, is crucial when ensuring the existence of non-distributive rights, such as cyber security. Cyber security cannot exist without protecting relevant distributive rights and, therefore, cannot exist per se (just for the sake of existence). If the protection of the relevant distributive information rights were not necessary, the cyber security would be irrelevant to exist – it would exist only to limit the freedom of the individuals. Because this is exactly what happens when the state gets to implement non-distributive right, it limits the freedom. Existence of relevant distributive rights is worthy of protection; therefore, it justifies the sole existence of non-distributive rights and the cyber security. Non-distributive rights cannot be divided among the individuals, it belongs to state and is indivisible. These rights serve the primary purpose and the primary responsibility of any state – the reproduction of the society by protecting the distributive rights.

5 The so-called Moore's law.

6 Polčák, R. *Internet a proměny práva.* Praha: Auditorium, 2012, p. 326–327.

3. Reflection of the totalitarian past

Cybernetic security arises from the need to establish and protect the distributive information rights within the information society. Information society and the distributive information rights do not present the new concepts, but in the time of constitution of those values, Lithuania and the Czech Republic were not entirely open to the up-to-date Western development.

Information society presents the society that is, compared to the previous societal states, depending on the information and communication of information. This dependence can be described through changes in the various fields of human activity, such as economic changes, cultural changes, changes of the labor market and changes in the human perception of territoriality and geographical distance[7]. Derived from these changes, as already mentioned, arises the information society, and from the information society, the concept of the distributive information rights arises, too. This catalogue, inherently attached to the information society, is called informational self-determination. As such, it presents value that gives legitimacy to the cybernetic security, because without the distributive rights to protect, the non-distributive security could not stand alone in any of the democratic societies.

The totalitarian heritage of both Lithuania and the Czech Republic comes from the delayed development of the information society and also from the utilitarian approach toward the distributive rights of citizens. In Western democracies, non-distributive rights (such as cyber security) can be emphasized only proportionately, therefore, only when it serves the protection of distributive rights (although after 9/11 this principle seems to be deteriorating throughout the whole Western civilization) and only when it does not negate distributive rights as such. This, however, was not a common practice in the totalitarian societies. Non-distributive rights were being used as tools to control the society through limitations imposed on distributive rights, such as privacy. The past can cause particularly strong unwillingness towards the new set of rules that can be perceived as limiting the freedom of the society[8]. Regulation toward strengthening the cybernetic security is perceived that way, which causes low political interest in pushing it forward due to interests of the citizens. Pushing the incoming legislation too hard can cause loss of votes in the next elections, which is directly against the interest of any existing political party.

4. Cyber security developed

Given the already mentioned earlier development of the information technologies in the Western Europe and the USA, the information society as such emerged earlier as

---

7 Webster, F. *Theories of the Information Society.* Third edition. London: Routledge, 2006, p. 8–9.

8 For further description of the Czech attitude, see Bobek, M.; Molek, P.; Šimíček, V. (eds.). *Komunistické právo v Československu: Kapitoly z dějin bezpráví.* Brno: Masarykova univerzita, Mezinárodní politologický ústav, 2009, p. 330–363.

well and is now more developed. This includes its positive influence on society as well as related negative phenomena, such as cybercrime. Critical information infrastructure also appeared earlier, calling for protection appropriately reflecting its importance. Necessity to properly ensure the security of the critical infrastructure was often answered only within certain areas of the public sector (for example, in army). On the other hand, other activities entirely omitted the public sector and focused solely on the private infrastructure. Enormous lead in the field of wholesome cyber security (which focuses on all the aspects and all the levels of cyber security) is, therefore, only virtual. Even in the world behind the Iron Curtain, only the massive emergence of threats and growth of importance and complexity of the critical infrastructure triggered the appropriate activity. On the national level, this usually means articulating the comprehensive national cyber security strategy or involving the cyberspace related issues into the national security strategy. Leading countries when assessing the legislative Framework are Germany, the United Kingdom and the USA. For our purpose, these three countries also present a very convenient triad of countries – all of these are members of the NATO, but also subjected to different influences. Germany is subject to the influence coming from the NATO and the EU and is also representative of the continental legal culture, while the United Kingdom, being the member of the EU and the NATO, represents the common law system. The USA is subject to the influence of its NATO membership and also represents the common law system, but obviously is not a member of the EU.

In the UK, when the new UK national security strategy appeared on 18th October 2012, it specified, among other things, threats considered to be the most dangerous to the existence and the functionality of the country as such. The category of the highest priority contained not only the international military crises, terrorism and natural disaster and other catastrophes, but it also mentioned cyber attacks[9]. The strategy emphasized not only risks arising from the independent attacks, including the cyber espionage or the cybercrimes, but also a supportive role of the cyberspace within the armed conflict or the organisation of the terrorist activity[10]. The document also mentioned the necessary cooperation of the public and private sector as a possible way to prevent not only the large cyber attacks, but also the day-to-day security incidents. *UK Strategic Defense and Security Review*[11] further specified some other threats, its nature and possible counter-measures. This document is strongly tied to the aforementioned security strategy. It allocated the amount of 650 million GBP over 4 years to establish a new national cyber security programme. *The UK Cyber Security Strategy: Protecting and Promoting the UK in a Digital World*[12], initially planned for the spring of 2011, was published in the

9 Bobek, M.; Molek, P.; Šimíček, V. (eds.). *Komunistické právo v Československu: Kapitoly z dějin bezpráví*. Brno: Masarykova univerzita, Mezinárodní politologický ústav, 2009, p. 28–31.

10 *Ibid*., p. 30.

11 *Securing Britain in an Age of Uncertainty: The Strategic Defense and Security Review*. London: 2010 [interactive]. [accessed on 01-10-2013]. <http://www.direct.gov.uk/prod_consum_dg/groups/dg_digitalassets/@dg/@en/documents/digitalasset/dg_191634.pdf>.

12 *The UK Cyber Security Strategy: Protecting and Promoting the UK in a Digital World*. London: 2011 [interactive]. [accessed on 01-10-2013]. <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf>.

autumn of 2011 and follows to specify the necessary measures – it presents the plan aiming to reach four goals until 2015[13]:

1) The UK has to be able to effectively sanction cybercrime and present the world's safe haven for the e-commerce;
2) The UK has to possess ability to protect itself and its interests in the cyberspace;
3) The UK has to contribute to formation of the stable and open environment that citizens can use without fear;
4) The UK has to ensure skills, knowledge and capacities to actively enforce the cyber security, which are possessed and further developed.

The strategy enacts the multi-layered structure to ensure the security – the structure involved individuals, corporations and the state itself (being the shining example of what was mentioned above as the wholesome security). According to this plan, an individual citizen must be aware of the risks within the network, and corporations shall be also aware of the risks and at the same time they possess ability to analyse and assess realistically all the possible risks and vulnerabilities within their systems. The cornerstone of the cyber security in the UK is activity of the private sector – corporations seek to eliminate vulnerabilities through the enhanced cooperation with their business partners, chambers of commerce and other associations of interest. Majority of the critical infrastructure is within the private hands[14], so this aspect is very rational. The role of the state is mainly to achieve higher efficiency of the law enforcement. It also should, at the same time, support citizens and corporations while supressing their own vulnerabilities, strengthen international cooperation, efficiently communicate threats to the public and stimulate the private sector to enact various security standards. The strategy is subjected to periodical assessment[15] and is modified by various related documents when necessary[16]. With the purpose of the protection of the information networks, the new body emerged within the Ministry of Defense. Defence Cyber Operations Group should focus and specialise on the research and development of the new tactical and operational procedures in the military cybernetics. This should include even the notorious hack-back. Hack-back as such is still not clearly determined with regards to its legal nature. Beside the Defence Cyber Operations Group, there are various CERT teams established in the UK, including the governmental CERT – GovCertUK. The possible creation of the cyber security law in the UK is discussed[17]; however, it seems that the executive acts and the secondary supportive legislation[18] present a sufficient framework to impose the cyber security. The

13 *Ibid*., p. 8.

14 *Ibid*.

15 *Progress against the Objectives of the National Cyber Security Strategy – December 2012*. London: 2012 [interactive]. [accessed on 01-10-2013]. <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/83755/Cyber_Security_Strategy_one_year_on_achievements.pdf>.

16 *The UK Cyber Security Strategy Report on Progress December 2012 – Forward Plans*. Lodon: 2012 [interactive]. [accessed on 01-10-2013]. <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/83757/Cyber_Security_Strategy_Forward_Plans_3-Dec-12_1.pdf>.

17 Clemente, D. *Defence and Cyber-security: Written Evidence*. 2012 [interactive]. [accessed on 01-10-2013]. <http://www.publications.parliament.uk/pa/cm201012/cmselect/cmdfence/writev/1881/dcs02.htm>.

18 Such as Computer Misuse Act of 1990, Data Protection Act of 1998, Electronic Communications Act of 2000, Electronic Signatures Regulation of 2002 and Civil Contingencies Act of 2004.

discussed new cyber security law (similar to the one that is now being prepared in the Czech Republic) is, therefore, most probably not necessary.

The USA has been focusing on the cyber security for a long time as a world-wide leading hi-tech based economy with modern army. Given the modernity of its armed forces and its high activity in the international military operations, the security of its military systems is crucial. The national security strategy from May 2010 has given the cyber threats a similarly prominent position as the UK security strategy. Cyber threats are emphasized mainly in the context of the current world security development toward the asymmetrical conflicts[19]. A previous document, *Cyberspace Policy Review,* from 2009[20] has formulated 10 short-term goals containing also the abovementioned and necessary education – not only of the experts and law enforcement agencies, but also of the general public[21]. The document as such follows a couple of key elements:

1) Constructing the cyber security "from the top"[22], giving the proper attention to it from the highest levels of the administration, including the presidential office;
2) Building the capacity of the "digital nation" – this can be generally understood as the awareness of citizens regarding the threats, but also their ability to participate in the necessary counter measures within the nation-scale incidents[23];
3) Establishing the principle of the shared responsibility for the cyber security in the form of the cooperation with the private sector[24];
4) Creating the platform for the cyber incidents reporting and for sharing information regarding the possible security breaches[25];
5) Strengthening innovations within the cyber security[26].

Rather a unique way to enhance the cyber security is presented by the *National Strategy for Trusted Identities in Cyberspace*[27]. It aims towards the creation of the trusted cyber environment. The so-called identity ecosystem[28] presents mechanisms allowing users to present their identity only with the data relevant for the particular transaction (or access to the particular content, e.g. answering simply yes or no, whether

19 *National Security Strategy*. Washington: The White House, 2010 [interactive]. [accessed on 27-02-2013]. <http://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf>, p. 17.

20 *Cyberspace Policy Review*. 2009 [interactive]. [accessed on 27-02-2013]. <http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf>.

21 *Ibid*., p. 37.

22 *Ibid*., p. 7–11.

23 *Cyberspace Policy Review*. 2009 [interactive]. [accessed on 27-02-2013]. <http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf>, p. 13–15.
See also Klimburg, A. The Whole of Nation in Cyberpower. *Georgetown Journal of International Affairs* [online]. 2011, special issue: 171–179.

24 *Cyberspace Policy Review*. 2009 [interactive]. [accessed on 27-02-2013]. <http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf>, p. 17–21.

25 *Ibid*., p. 23–29.

26 *Ibid*., p. 31–35.

27 *National Strategy for Trusted Identities in Cyberspace*. Washington: The White House, 2011 [interactive]. [accessed on 28-02-2013] <http://www.whitehouse.gov/sites/default/files/rss_viewer/NSTICstrategy_041511.pdf>.

28 *Ibid*., p. 21–27.

the user trying to access the mature content is of the legal age). This should mitigate the possibility of the identity theft. This concept is not brand new, it has been already mentioned by Lawrence Lessig[29], but the trusted identities is the first strategy toward its actual implementation.

International Strategy for Cyberspace[30] from May 2011 has presented the wholesome strategy towards the cyberspace and integrates the cyberspace strategy within particular aspects of the administration. This document focuses mainly on the critical infrastructure security, more efficient international security and the improvement in the ability to react properly on cyber attacks. This should be achieved through a more mature legislation and through the cooperation with allies. Exclusive supervision over the civilian networks is granted to the *Department of Homeland Security*, which very closely cooperates with the supervisory body for the military networks – US Cyber Command. The US Cyber Command presents the unified cybernetic headquarters for all the military (being it navy, air force, etc.) and emphasizes the role of the cyberspace within the US military doctrine as the separate operational domain of warfare[31]. The document from June 2011 entitled *Department of Defense Strategy for Operating Cyberspace* is also important[32]. According to this manual, the key to prevent attacks (more precisely, to minimalize the chances of successful attack to occur) is based on five elements:

1) a stronger role of cyberspace as the fifth operational domain[33];
2) emphasized active defense, including the abovementioned hack-backs;
3) more secure critical infrastructure[34];
4) international protection within the structures of the NATO and independently on it[35];
5) research and development within the field of the cyber security[36].

On the other hand, this strategy did not answer the long discussed possibility to retaliate using the conventional forces. It is widely assumed that part of the strategy involving this issue is confidential. Another confidential document, Presidential Policy Directive 20[37], should contain the rules of engagement for the cyberspace, including the active cyber defense possibilities and maybe even further specification of the possible conventional retaliation.

---

29 Lessig, L. *Code: Version 2.0*. New York: Basic Books, 2006, p. 51.

30 *International Strategy for Cyberspace: Prosperity, Security and Openess in a Networked World*. Washington: The White House, 2011 [interactive]. [accessed on 03-03-2013] <http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf>.

31 Cyberspace was added to the land, sea, air and space. *Department of Defense Strategy for Operating in Cyberspace*. 2011 [interactive]. [accessed on 03-01-2013] <http://www.defense.gov/news/d20110714cyber.pdf>.

32 *Ibid*.

33 *Ibid*., p. 5–6.

34 *Ibid*., p. 8–9.

35 *Ibid*., p. 9–10.

36 *Ibid*., p. 10–12.

37 Nakashima, E. Obama signs secret directive to help thwart cyberattacks. *WashingtonPost.com*. 2012 [interactive]. [accessed on 09-03-2013]. <http://articles.washingtonpost.com/2012-11-14/world/35505871_1_networks-cyberattacks-defense>.

As the UK, the USA is also without the general legislative act regarding the cyber security. The latest document aiming toward this goal was the *Cybersecurity Act* in 2012, receiving strong support by the president Barack Obama. This, however, did not help and the document was refused[38]. The private sector was afraid of the related economical cost during the ongoing economic crisis and end-users were mainly afraid of the excessive tracking[39]. Strong opposition of those two groups, arising from the different interests, created very strong pressure that turned out to be unbearable. However, given the massive surveillance in the PRISM affair, the fear of users was legitimate – but the tracking can obviously occur even without being enacted by any piece of legislation. The US has also established a vast amount of CERT teams, while the US-CERT presents the governmental CERT (similar to the GovCertUK in the UK).

A great focus is targeted on cyber security issues in Germany as Germany is one of the countries participating on the NATO Center of Excellence in Tallinn. National strategy[40] from February 2011 has been standing on two bodies – National Cyber Response Center[41] and the National Cyber Security Council[42]. Team of the National Cyber Response Center consists of six members and also includes ad hoc deputies from the police, army, security agencies and the duty office. All those bodies and agencies should cooperate to maximise the outcome of the National Cyber Response Center; however, the German strategy remains very vague in the expected outcomes of its activities and the efficiency; therefore, it strongly depends on the activity of the individuals and bodies directly involved. The National Cyber Security Council is the highest body involving deputies from all the relevant federal ministries and, as such, it approaches the most serious threats to the national critical infrastructure. According to the German strategy, research and development is another key issue. Germany also involved the technological neutrality and technological plurality as key principles within its strategy[43]. The periodical revision is also explicitly stated due to the limited durability of any implemented measures, facing the ever changing technological reality of the cyberspace. As in the UK and in the USA, in Germany the necessity of proper education and information disseminated to the citizens is also strongly emphasized. CERT teams are also established in Germany, amounting to more than 50 with the CERT-BUND

38 Couts, A. Senate Kills Cybersecurity Act of 2012. *DigitalTrends.com.* 2012 [interactive]. [accessed on 09-03-2013]. <http://www.digitaltrends.com/web/senate-votes-against-cybersecurity-act-of-2012/>.

39 Reitman, R. *New Cybersecurity Proposal Patches Serious Privacy Vulnerabilities.* 2012 [interactive]. [accessed on 02-03-2013]. <https://www.eff.org/deeplinks/2012/07/new-cybersecurity-proposal-patches-serious-privacy-vulnerabilities>.

40 *Cyber Security Strategy for Germany*. Berlin: Federal Ministry of the Interior, 2011 [interactive]. [accessed on 10-07-2012]. <https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/CyberSecurity/Cyber_Security_Strategy_for_Germany.pdf?__blob=publicationFile>.

41 *Ibid*., p. 8.

42 *Ibid*., p. 9–10.

43 *Ibid*., p. 11–12. In this context, another aspect of the cyber security can be articulated to be the general obligation to prevent technological monocultures to be used. These are more prone to what can be called the "cascade failure".
For further reference, see Geer, D. Cybersecurity and National Policy. *Harvard National Security Journal.* 2010, 1(1): 203–215.

serving as the CERT team for the government. Also, Germany has so far decided not to implement the exhaustive cyber security legislation.

As evidenced by the abovementioned documents and approaches, the following can be articulated as an inherent part of the modern cyber security:

1) apprehensive national cyber security strategy and its comprehensive connection with the national security strategy;
2) clear division of labour have to be present regardless of the emphasized leading role of the civil or military sector;
3) CERT teams are to be approached as the condition sine qua non for the cyber security of large networks;
4) governmental CERT with executive powers can be controversial, but as the communication platform and as the executive body with powers during the national crises is irreplaceable;
5) cyber security law is not necessary if the same result can be achieved through the secondary legislation and/or executive documents;
6) environment encouraging corporate and public actors to exchange their observations needs to be supported. If the support is not sufficient, legal obligation should be imposed;
7) education of the citizens is the key aspect in the wholesome cyber security and, as such, it cannot be omitted;
8) every measure undertaken has to be consulted with the private sector because the critical infrastructure lies largely in its hands;
9) technological neutrality (which is, however, explicitly emphasized only in Germany) needs to be perceived as the inherent part of the cyber security. No technological solution, being at the current time or future, should be preferred.

5. Cyber security developing

The situation in Lithuania and the Czech Republic is rather complicated. Due to the later development of the information society and the belonging values, both countries are still trying to comprehend what is happening and how to react properly. Cyber security has remained omitted for a long time. For Lithuania, the main events warning about the cyber attacks and possible consequences occurred in Estonia in 2007 (due to its geographical and political proximity) and in Lithuania in 2008. Attacks on Estonia presented the wake-up call for the whole NATO and as such, including the Czech Republic. In the Czech Republic, the direct effect came much later in 2013. At this time, the activity aiming to enhance the cyber security was ongoing.

Lithuania is, unlike the Czech Republic, a member state of the NATO Center of Excellence in Tallinn. Supervisor over the agenda of cyber security is the Ministry of Interior, mainly through its Center of Information and Communication Technologies. In the Czech Republic, the national authority regarding the cyber security is the National Security Agency as the independent public body. Lithuania's *Programme for*

the Development of Electronic Information Security (Cyber-Security) for 2011-2019[44] follows general values and goals. Rather extraordinary about it is that some of the goals can be quantified as such – until the year 2019, Lithuania has been seeking to achieve the state, when 60% of the users have been feeling safe in the cyberspace. At the same time, the response time on the security incident within the critical infrastructure should be at most 30 minutes and 98% of the national critical infrastructure should be secured according to the national legislation. The mid-term review is planned for the year 2015. The national CERT is the CERT-LT, but Lithuania established multiple other CERT teams, including the IST-SVDPT, the LITNET CERT and four military CERT teams[45]. Despite the obvious advances within this field, the country struggles in cooperation between the public and the private sectors. Also, a typical end-user is only vaguely aware of any threats. This is subject to the ongoing criticism[46]. Education within the program is, therefore, virtually non-existent and has to be enhanced, because the Lithuanian society remains sort of a fear-culture when it comes to cyber security.

The Czech Republic, on the other hand, presents the culture of uncertainty and paranoia. In 2013, banks were targeted by the DDoS attack and the lack of education regarding the cyber threats became apparent – banks were literally flooded with questions from people asking whether the DDoS somehow did affect the savings. Shortly afterwards, when the National Security Agency finally finished the proposal for a new law regarding the cyber security, multiple sources came with sort of a conspiracy theory, accusing the National Security Agency of orchestrating the attack in order to ensure the law is to be accepted as such. Whether they were unaware of the lengthy preparatory discussions regarding the new law or simply ignoring the fact remains unknown. However, the lack of education is strong in the Czech Republic as well as in Lithuania; while the Czech citizens, probably due to their generally sceptical nature, added another element into the discussion by accusing the state (namely, the National Security Agency) of trying to regulate the Internet and shut down its highly valued freedom.

Despite the existence of CERT teams in the Czech Republic and the recent legislative activity, the Czech Republic does not possess exhaustive measures (being it legal or else) to face the current technological world. The same applies for Lithuania. As witnessed even by the abovementioned set of documents of the developed countries, Lithuanians and the Czechs seem only barely aware of the threats and ways to face it. Despite the Lithuanian strategy formulating quantitative goals, which is very extraordinary and definitely a huge leap forward even compared to the developed countries, criticism emerges and the idea of cybernetic insecurity is still present.

---

44 *The Programme for the Development of Electronic Information Security (Cyber-Security) for 2011-2019*. Vilnius: 2011 [interactive]. [accessed on 20-02-2013]. <http://www.ird.lt/doc/teises_aktai_en/EIS(KS)PP_796_2011-06-29_EN_PATAIS.pdf>.

45 *Lithuania Country Report*. ENISA, 2011 [interactive]. [accessed on 20-02-2013]. <http://www.enisa.europa.eu/activities/stakeholder-relations/files/country-reports/Lithuania.pdf>.

46 Sapetkaite, V. Kibernetinis (ne)saugumas: Baltijos šalių situacija. *Geopolitika.lt.* 2012 [interactive]. [accessed on 20-02-2013]. <http://www.geopolitika.lt/?artc=5504>.

The general problem is the general lack of legal background of the cyber security in both Lithuania and the Czech Republic. The Czech Republic rather uniquely presented its own legislation, covering particularly the cyber security, but the legislation is far from perfect for the practitioners and at the same time far from being politically important and visible to get enough attention within the Parliament. Lithuania, on the other hand, seems to be content without the regulatory framework, relying on legal acts of lower force and policy. This approach, however, has its flaws, mainly because the public sector is allowed to do only what law prescribes and, therefore, the policy cannot turn legitimate some of the measures that need to be undertaken. The Czech approach is, as mentioned, rather unique, but it does not get enough attention and if it gets any at all, it is largely criticised, partially because of the totalitarian past.

Conclusions

In countries, where the cyber security does not have tradition and the totalitarian past is still vivid in memories, any activity on this field might be perceived as undesirable by both the users (who fear for their data and their freedom) and the corporations (which fear additional costs of any legislation which may arise). An additional problem is presented by mistakes (precisely, omissions), corruption and political instability in the post-totalitarian countries. The Czech Republic currently remains in the shade of a recent affair, involving the military intelligence – one of the close colleagues of the prime minister was using the military intelligence to surveille the prime minister's family. This affair, however extraordinary, does not exactly add any reliability to the system – a legitimate question appears whether there are any possible (and intentional) information leaks present. Mistakes are currently represented by the National Security Agency, establishing a secure website, providing the possibility to submit information on various cases of corruption. However, the responsible officials forgot to pay for the domain for another period and at the same time the hyperlink remained active within the National Security Agency's website. Is the organisation capable of doing this the right one to supervise the cybernetic security? Mistakes happen all the time, but in the very fragile environment with weak support and strong resistance to the centralised cyber security, these mistakes are enhancing the hostility towards any measures. At the same time, people are usually not aware of the emerging threats. Justifying any piece of legislation under these circumstances when most of the citizens are not able to see the reason remains increasingly difficult. Legislation in both Lithuania and the Czech Republic is, therefore, not very mature, given the overall immaturity of the society and its lack of education regarding these new threats. Lithuania probably does approach the issue more seriously, given its participation within the NATO Center of Excellence, but it is only scarcely enough. Cyber security in both of the countries remains insufficient, but it does not mean that both countries are helpless and defenseless in the cyberspace. Legislators often fail to understand that the totalitarian past and the ongoing mistrust to the government in the Internet related issues could backfire while imposing the new

legal obligations. Therefore, the first step should primarily aim to education, leading to citizens understanding the nature of the threats. The second step, rather than on imposing new obligations, should encourage the cooperation and create trusted environment for sharing the necessary information. However, given the current proposal for a Directive on network and information security working with the authority supervising the day-to-day maintenance of the Internet, this model might be rather difficult to sustain, despite its validity and usefulness. Other steps to follow could (and probably should) focus on creating a unified regulatory framework, but this cannot be done by the general understanding of the role of cyber security in a modern society.

References

Bobek, M.; Molek, P.; Šimíček, V. (eds.). *Komunistické právo v Československu: Kapitoly z dějin bezpráví*. Brno: Masarykova univerzita, Mezinárodní politologický ústav, 2009.

Clemente, D. *Defence and Cyber-security: Written Evidence*. 2012 [interactive]. [accessed on 01-10-2013]. <http://www.publications.parliament.uk/pa/cm201012/cmselect/cmdfence/writev/1881/dcs02.htm>.

Couts, A. Senate Kills Cybersecurity Act of 2012. *DigitalTrends.com*. 2012 [interactive]. [accessed on 09-03-2013]. <http://www.digitaltrends.com/web/senate-votes-against-cybersecurity-act-of-2012/>.

Cyber Security Strategy for Germany. Berlin: Federal Ministry of the Interior, 2011 [interactive]. [accessed on 10-07-2012]. <https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/CyberSecurity/Cyber_Security_Strategy_for_Germany.pdf?__blob=publicationFile>.

Cyberspace Policy Review. 2009 [interactive]. [accessed on 27-02-2013]. <http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf>.

Department of Defense Strategy for Operating in Cyberspace. 2011 [interactive]. [accessed on 03-01-2013]. <http://www.defense.gov/news/d20110714cyber.pdf>.

Geer, D. Cybersecurity and National Policy. *Harvard National Security Journal*. 2010, 1(1): 203–215.

International Strategy for Cyberspace: Prosperity, Security and Openess in a Networked World. Washington: The White House, 2011 [interactive]. [accessed on 03-03-2013]. <http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf>.

Klimburg, A. The Whole of Nation in Cyberpower. *Georgetown Journal of International Affairs* [online]. 2011, special issue: 171–179.

Klimek, L. Combating Attacks against Information Systems: EU Legislation and Its Development. *Masaryk University Journal of Law and Technology*. 2012, 6(1): 87–100.

Lessig, L. *Code: Version 2.0*. New York: Basic Books, 2006.

Lithuania Country Report. ENISA, 2011 [interactive]. [accessed on 20-02-2013]. <http://www.enisa.europa.eu/activities/stakeholder-relations/files/country-reports/Lithuania.pdf>.

Nakashima, E. Obama signs secret directive to help thwart cyberattacks. *WashingtonPost.com*. 2012 [interactive]. [accessed on 09-03-2013]. <http://articles.washingtonpost.com/2012-11-14/world/35505871_1_networks-cyberattacks-defense>.

National Security Strategy. Washington: The White House, 2010 [interactive]. [accessed on 27-02-2013]. <http://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf>. *National Strategy*

for Trusted Identities in Cyberspace. Washington: The White House, 2011 [interactive]. [accessed on 28-02-2013]. <http://www.whitehouse.gov/sites/default/files/rss_viewer/NSTICstrategy_041511.pdf>.

Polčák, R. *Internet a proměny práva.* Praha: Auditorium, 2012.

Progress against the Objectives of the National Cyber Security Strategy – December 2012. London: 2012 [interactive]. [accessed on 01-10-2013]. <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/83755/Cyber_Security_Strategy_one_year_on_achievements.pdf>.

Reitman, R. *New Cybersecurity Proposal Patches Serious Privacy Vulnerabilities.* 2012 [interactive]. [accessed on 02-03-2013]. <https://www.eff.org/deeplinks/2012/07/new-cybersecurity-proposal-patches-serious-privacy-vulnerabilities>.

Sapetkaite, V. Kibernetinis (ne)saugumas: Baltijos šalių situacija*. Geopolitika.lt.* 2012 [interactive]. [accessed on 20-02-2013]. <http://www.geopolitika.lt/?artc=5504>.

Securing Britain in an Age of Uncertainty: The Strategic Defense and Security Review. London: 2010 [interactive]. [accessed on 01-10-2013]. <http://www.direct.gov.uk/prod_consum_dg/groups/dg_digitalassets/@dg/@en/documents/digitalasset/dg_191634.pdf>.

The Programme for the Development of Electronic Information Security (Cyber-Security) for 2011-2019. Vilnius: 2011 [interactive]. [accessed on 20-02-2013]. <http://www.ird.lt/doc/teises_aktai_en/EIS(KS)PP_796_2011-06-29_EN_PATAIS.pdf>.

The UK Cyber Security Strategy Report on Progress December 2012 – Forward Plans. London: 2012 [interactive]. [accessed on 01-10-2013]. <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/83757/Cyber_Security_Strategy_Forward_Plans_3-Dec-12_1.pdf>.

The UK Cyber Security Strategy: Protecting and Promoting the UK in a Digital World. London: 2011 [interactive]. [accessed on 01-10-2013]. <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf>.

Webster, F. *Theories of the Information Society*. Third edition. London: Routledge, 2006.

Wiener, N. *Kybernetika a společnost*. Praha: Československá akademie věd, 1963.

KIBERNETINIS SAUGUMAS JAUNOSIOSE DEMOKRATIJOSE

Jakub Harašta

Masaryko universitetas, Čekija

Anotacija. *Ir Čekijos Respublika, ir Lietuva yra jaunos demokratijos, patyrusios esminius socialinius, teisinius ir politinius pokyčius devintajame dešimtmetyje, kai vyko jų virsmas moderniomis demokratinėmis valstybėmis. Kibernetinio saugumo užtikrinimas išlieka vienu iš šių valstybių tikslų, nes totalitarinis valdymas praeityje ir vėluojanti politinė evoliucija persekioja jų dabarties ir ateityje numatomą vystymąsi.*

Reikšminiai žodžiai: *kibernetinis saugumas, Čekijos Respublika, Lietuva, išsivysčiusios valstybės, informacinė visuomenė, išsilavinimas, kibernetinės grėsmės, informacinis apsisprendimas.*

Summary. *Totalitarian past is not the only tie bringing together Lithuania and the Czech Republic nowadays. Both countries are young democracies that underwent dynamic social, legal and political changes during the 90s to ensure transition toward becoming modern democratic states. Now, both countries are members of the European Union and NATO and they share common interest of the small European countries. However, the totalitarian past remains present and it has certain influence on recent issues arising from the current information society. Totalitarian regimes in both countries left some of the political approaches twisted beyond recognition and adversely affected the very core of the society and ways it approaches itself and the others.*

The author of the paper is aiming to provide the comparison of Lithuania and the Czech Republic mainly within the field of the cybernetic security, but with certain overlaps to general theory of the information society and the continental legal tradition of distributive rights. In both countries, the cybernetic security presents a new and interesting challenge, because both countries can be perceived as rookies within this particular field.

In the first and the second parts, the author describes the very essence of the information society and the informational self-determination as the core principle arising from the information society. Then, in the third part, the author describes reminiscences of the totalitarian past, which could be understood mainly as a general opposition towards limitations of distributive rights, because the means of cyber security are vastly understood as the government trying to regulate the Internet. This is a rather sensitive topic, due to the totalitarian past of both countries. In the fourth part, the author describes the current state-of-art of the cyber security, mainly approaching the United States, the United Kingdom and Germany as countries well-established within the field of cyber security. Estonia, as another small state, is also taken into consideration, providing their very mature legislation and approach toward the cyber security that may act as a role model for Lithuania and the Czech Republic. Part of the paper is also reserved for the comparison between approaches of Lithuania and the Czech Republic, because despite being part of the EU/NATO political background and target of the currently proposed cyber security Directive, there are still differences present due to the national character of the cyber security.

This contribution is not intended to be exhaustive and overwhelming source of answers, but rather as the approach to the future while taking into consideration both the present and the past.

Main findings could be summarised in the following way: (1) the legislation in Lithuania and the Czech Republic is not as mature as it could be; (2) Lithuania approaches this issue rather more seriously compared to the Czech Republic, given the geographical proximity to Estonia and the 2008 cyber incident as evidenced, for example, by its participation within the NATO Cooperative Cyber Defence Centre of Excellence; (3) public in both Lithuania and the Czech Republic seems to slowly understand the danger of the cyber insecurity, but it also approaches it carefully due to the totalitarian past; (4) cyber security in both countries is insufficient, but given the totalitarian past, the legislators should probably focus more on ensuring the cooperation of public and corporate/private sectors rather than imposing new legal obligations.

Keywords: *cyber security, the Czech Republic, Lithuania, developed countries, information society, education, cyber threats, informational self-determination.*

Jakub Harašta, Masaryko universiteto Teisės ir technologijų instituto Teisės fakulteto Teisės mokslų magistras, doktorantas, mokslinis darbuotojas, asistentas. Mokslinių tyrimų kryptys: kibernetinis saugumas, kibernetinė gerovė, teisinė informatika.

Jakub Harašta, Masaryk University, Institute of Law and Technology, Faculty of Law, Master in Law and Ph.D. candidate, research fellow and assistant lecturer. Research interests: cyber security, cyber warfare, legal informatics.