Social Transformations in Contemporary Society, 2017 (5)
ISSN 2345-0126 (online)

CYBERCRIME MEANING AND IMPORTANCE IN THE LEGISLATION OF THE BALTIC STATES COUNTRIES

Elina Radionova-Girsa

Daugavpils University, Latvia
elinaradionova@gmail.com

Abstract

While using different new technologies, we are facing not only conveniences and bonuses but also problems and crimes. Every day we use world wide web pages, we leave there our track, our identity data, credit card's data, photos, and another important detail about ourselves and lives. With the growth of the internet usage people are facing a new problem and type of crime that has no limitations and no traditional understanding about location, that problem could reach them everywhere and in every time.

There is no secret that cybercrime has different types and ways of disclosure. There are such kind of cybercrimes as cyberbullying, stalking, bossing, children pornography, fraud, etc. Adults and children do not feel safe during their Internet sessions. And statistical data show us numbers that are only growing. From the time, Latvia is a part of the EU we have different possibilities and strategies to protect ourselves and our data in the internet environment. European Commission provide us with different recommendations and actions regarding to cybercrimes. The main idea and aim of those recommendations is to make people feel safe about them and their children and relatives while using internet.

Purpose –analyse the meaning and defending strategy of a cybercrime in the Baltic State legislation. Also, to find an importance of prevention of that cases and main methods of it.

Design/methodology/approach – the author of the paper comparing laws that connects to cybercrimes in the Baltic States and come across with differences and common points. As well as the main data of cybercrime in Latvia analysis. Case study of Latvian and Estonian case is shortly reviewed.

Finding – as all three Baltic States country are a part of the European Union they have very close to each other meaning and understanding of cybercrimes. Talking about Latvia it is should be pointed out that the number of cybercrimes has a growing tendency that means that this field is still unsafe for the citizens.

Research limitations/implications – the author uses legislation of the Republic of Latvia, Lithuania and Estonia to compare it and different European Union regulations regarding to cybercrimes.

Practical implications – the paper has mostly theoretical knowledge that can be used also in practice when dealing with cybercrime problems in the Baltic States.

Originality/Value – the problem of cybercrime is quite new for the Baltic States. That also causes a novelty of that paper – finding common and different sides in the three Baltic Countries in the view of cybercrime meaning and importance.

Keywords: Cybercrime, Internet, Legislation, Latvia, Baltic States
Research type: general review

Introduction

Nowadays there is a huge number of people using internet. There is no doubt that population growth, that means that there is crime growth. As well where there is internet growth, there is cybercrime growth.

The population of people, places (i.e. smart buildings, smart cities), and things (devices) comprise the cyber-attack surface, which is growing exponentially larger every year. Microsoft frames digital population growth with its estimate that by 2020 four billion people will be online — twice the number that are online now, and the world will store 50 times more data than it does today[1]. Just for understanding the 2017 Identity Fraud Study, released by Javelin Strategy & Research, found that $16 billion was stolen from 15.4 million U.S. consumers in 2016, compared with $15.3 billion and 13.1 million victims a year earlier. In the past six years' identity thieves have stolen over $107 billion[2]. This numbers are only for the United States and author underlines that this is a huge amount and of course in smaller countries there will be a smaller numbers but still it is a very significant threat.

As it can be found in the statistics database in 2016 there were 71% of individuals using internet daily. If we analyse the Baltic States statistical situation on internet usage (Latvia, Lithuania and Estonia) then the share amount is 77% for Estonia, 68% for Latvia and 60% for Lithuania[3]. And daily all those individuals are facing threats from the screen side. We never know who is in front of us when talking about world wide web. Talking about the data we share using the internet there is a point of Ginni Rometty, IBM Corp.'s Chairman, President and CEO that "data is the phenomenon of our time. It is the world's new natural resource. It is the new basis of competitive advantage, and it is transforming every profession and industry. If all of this is true – even inevitable – then cyber-crime, by definition, is the greatest threat to every profession, every industry, every company in the world."[4] The author of the paper completely agrees with such kind of explanation. Because all our data now can be find there, some of it is hidden and secured, some not and our task is to understand what kind of information do we leave by using internet, sending and receiving content, emails, etc.

[1] Cybersecurity and Cybercrime Statistics Report. (2016) http://cybersecurityventures.com/cybersecurity-and-cybercrime-statistics/ Retrieved: 19.04.2017.

[2] Identity Theft And Cybercrime (2016) http://www.iii.org/fact-statistic/identity-theft-and-cybercrime Retrieved: 19.04.2017.

[3] DIGITAL SINGLE MARKET (2016) http://digital-agenda-data.eu/charts/analyse-one-indicator-and-compare-countries#chart={"indicator-group":"internet-usage","indicator":"i_iuse","breakdown":"IND_TOTAL","unit-measure":"pc_ind","ref-area":["BE","BG","CZ","DK","DE","EE","IE","EL","ES","FR","IT","CY","LV","LT","LU","HU","HR","MT","NL","AT","PL","PT","RO","SI","SK","FI","SE","UK","EU27"]} Retrieved: 10.04.2017.

[4] IBM's CEO On Hackers: 'Cyber Crime Is The Greatest Threat To Every Company In The World' , Steve Morgan (2015) https://www.forbes.com/sites/stevemorgan/2015/11/24/ibms-ceo-on-hackers-cyber-crime-is-the-greatest-threat-to-every-company-in-the-world/#57c80dcf73f0 Retrieved: 11.04.2017.

Cybercrime meaning

As it can be found on the European Commission webpage[1] cybercrime consists of criminal acts that are committed online by using electronic communications networks and information systems. And here is a problem - all cybercrimes are taking place online and online network has no limits and borders.

At first there should be an understanding that there can be different cybercrime types. Parker[2] provide us with a categorization based on the role of a computer during the performance of a crime:

- computer as an object of a crime;
- computer as a subject of a crime;
- computer as the means for a crime;
- and computer as a symbol.

The author wants to point out that such categorization can be used also nowadays even it was drawn up more than 30 years ago. Kaspersen says that the term cybercrime is usually applied to any crime for the commission of which the use of Internet is essential[3]. The main legislative practice approach that shows to be less concerned with the role of a computer can be found in the Convention on Cybercrime proposed the following categorization:

- offences against confidentiality, integrity and availability of computer data and systems;
- computer-related offences;
- content-related offences;
- offences related to infringements of copyright and related rights.

This categorization may be therefore considered a de facto world standard due to the high acceptance of the Convention worldwide[4].

Cyber-dependent crimes can only be committed using computers, computer networks or other forms of information communication technology. They include the creation and spread of malware for financial gain, hacking to steal sensitive personal or industry data and denial of service attacks to cause reputational damage[5].

Cyber-enabled crimes, such as fraud, the purchasing of illegal drugs and child sexual exploitation, can be conducted on or offline, but online may take place at unprecedented scale and speed[6].

There can be a classification that will show the meaning of cybercrime in a little different way:

[1] Cybercrime (2016) https://ec.europa.eu/home-affairs/what-we-do/policies/organized-crime-and-human-trafficking/cybercrime_en Retrieved: 07.04.2017.

[2] Parker, D. B. (1983) Fighting Computer Crime. New York: Charles Scribner's Sons, 1983.

[3] Kaspersen, H. W. K. (2009) Cybercrime and Internet Jurisdiction, Discussion paper (draft), version 5 March 2009, prepared in the framework of the Project on Cybercrime of the Council of Europe

[4] Sauliūnas D. (2010) Legislation On Cybercrime In Lithuania: Development And Legal Gaps In Comparison With The Convention On Cybercrime. https://www.mruni.eu/upload/iblock/822/11_Sauliunas.pdf Retrieved: 11.04.2017.

[5] Cyber Crime Assessment 2016 . Need for a stronger law enforcement and business partnership to fight cyber crime (2016) http://www.nationalcrimeagency.gov.uk/publications/709-cyber-crime-assessment-2016/file Retrieved: 09.04.2017.

[6] Cyber Crime Assessment 2016 . Need for a stronger law enforcement and business partnership to fight cyber crime (2016) http://www.nationalcrimeagency.gov.uk/publications/709-cyber-crime-assessment-2016/file Retrieved: 09.04.2017.

- Crimes specific to the Internet, such as attacks against information systems or phishing (e.g. fake bank websites to solicit passwords enabling access to victims' bank accounts).
- Online fraud and forgery. Large-scale fraud can be committed online through instruments such as identity theft, phishing, spam and malicious code.
- Illegal online content, including child sexual abuse material, incitement to racial hatred, incitement to terrorist acts and glorification of violence, terrorism, racism and xenophobia. (European Commission website)[1]

In that classification, it is important to understand that all those crimes are happening not only involving computer, but also dealing with the world-wide web. Author shows that there can be different classifications and different points but the whole idea is one – cybercrime means illegal actions that causes performance of the crime in different ways like fraud, data stealing and more serious outcomes like terrorism. There are legislative actions in the world, in the European Union and in each country that deals with and protect us from that kind of a crime.

Legislative actions in the European Union and the Baltic State Region

Several EU legislative actions contribute to the fight against cybercrime. These include:

- 2013 – A Directive on attacks against information, which aims to tackle large-scale cyber-attacks by requiring Member States to strengthen national cyber-crime laws and introduce tougher criminal sanctions;
- 2011 – A Directive on combating the sexual exploitation of children online and child pornography, which better addresses new developments in the online environment, such as grooming (offenders posing as children to lure minors for the purpose of sexual abuse)
- 2002 – ePrivacy Directive, whereby providers of electronic communications services must ensure the security of their services and maintain the confidentiality of client information;
- 2001 – Framework Decision on combating fraud and counterfeiting of non-cash means of payment, which defines the fraudulent behaviours that EU States need to consider as punishable criminal offences.

Since 2006 in Latvia is active Convention on Cybercrime[2] and there is a point that in article 35 – 24/7 Network the party that shall designate a point of contact available on a twenty-four hour, seven-day-a-week basis, in order to ensure the provision of immediate assistance for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence. Such assistance shall include facilitating, or, if permitted by its domestic law and practice, etc. in Latvia is State Police General Crime police department. In that document, also can be found each cybercrime's meanings.

[1] Cybercrime (2016) https://ec.europa.eu/home-affairs/what-we-do/policies/organized-crime-and-human-trafficking/cybercrime_en Retrieved: 07.04.2017.

[2] Par Konvenciju par kibernoziegumiem un Konvencijas par kibernoziegumiem Papildu protokolu par rasisma un ksenofobijas noziedzīgajiem nodarījumiem, kas tiek izdarīti datorsistēmās https://likumi.lv/doc.php?id=146481#p35 Retrieved: 07.04.2017.

It should be pointed out that in the Republic of Latvia it is used the European Union legislation and only several points adopt them to the Latvian legislation[1]. The author of the paper thinks that there should be more points in the legislation in Latvia and exactly in the Criminal Law that specify points and their meanings. Otherwise it is just taking over legislation. Also, the author wants to stress out the last date of changings – 27/11/2008, which is almost 10 years ago. Considering that internet quality is growing up, people knowledge about internet usage and sometimes for not good reasons is also growing up, there should be some more amendments. But there were another changes in legislation. Personal Data Protection Law in Latvia was fulfilled in February 2014[2]. In May 2016 minor technical amendments were adopted through regulations of the Cabinet of Ministers on the application templates for the registration of personal data processing and personal data protection specialists[3].

National cyber security policy in Latvia is developed by the next institutions:

1) Ministry of Defence (MOD) – coordinates development and implementation of information technology security and protection policy, as well as cooperates in the provision of international cooperation. he National Cyber Security Policy Coordination Section of the MOD organises and provides support for the implementation of cyber security policy.
2) Ministry of Foreign Affairs (MFA) – coordinates international cooperation and Latvia's participation in various international initiatives related to the cyber security.
3) Financial and Capital Market Commission (FCMC) – regulates and supervises activities in cyber space of members of the financial and capital market cyber space; the Bank of Latvia (BoL) promotes secure and smooth operation of payment systems, while credit institutions are responsible for secure availability of electronic services in their sector.
4) Ministry of Economics (MoE) – develops economic policy and promotes the development of competitiveness and innovation.
5) Ministry of the Interior (MoI), State Police (SP) and Security Police (SeP) – implement the policies for combating crime, public order, security protection, and the protection of rights and legal interests of individuals, as well as coordinates the settlement of crisis situations.
6) Information Technology Security Incident Response Institution CERT.LV – monitors and analyses developments in cyber space, reacts to incidents and coordinates their prevention, carries out research, organises educational events and training, as well as supervises the implementation of obligations specified in the Law on the Security of Information Technology. CERT.LV provides support for Latvian and foreign state and municipal institutions, entrepreneurs, and individuals.
7) Ministry of Education and Science (MoES) – promotes knowledge and understanding of cyber space and its secure use.

[1] Par Konvenciju par kibernoziegumiem un Konvencijas par kibernoziegumiem Papildu protokolu par rasisma un ksenofobijas noziedzīgajiem nodarījumiem, kas tiek izdarīti datorsistēmās https://likumi.lv/doc.php?id=146481#p35 Retrieved: 07.04.2017.

[2] Data Security and Cybercrime in Latvia. Valts Nerets and Agita Sprude (2017) http://www.lexology.com/library/detail.aspx?g=f619dc4c-cf2b-4b48-9909-00e37dc75859 Retrieved: 07.04.2017.

[3] Fizisko personu datu aizsardzības likums https://likumi.lv/doc.php?id=4042 Retrieved: 07.04.2017.

8) Ministry of Welfare (MoW) – implements the social policy and the policy for the protection of children's rights.
9) Operation of the Safer Internet Centre of Latvia NetSafe Latvia is ensured by the Latvian Internet Association, educates society about possible risks and threats online, and promotes the use of secure internet content.
10) National Armed Forces (NAF) and Cyber Defence Unit (CDU) – provide support in crisis situations.
11) Non-governmental organisations in the IT sector – provide support, consult and cooperate with the Council in developing and implementing the cyber security policy1.
12) Ministry of Transport (MoT) – organises the implementation of communication policy.
13) Constitution Protection Bureau (CPB) – oversees the critical infrastructure.
14) Ministry of Justice (MoJ) and Data State Inspectorate (DSI) – develop, organise and coordinate the policy on rights in the field of personal data protection, freedom of information and supervision of electronic documents.
15) State Joint Stock Company "Latvian State Radio and Television Centre" (LSRTC) – the only provider of reliable certification services, which ensures the infrastructure of electronic identity cards and electronic signatures.

16) Ministry of Environmental Protection and Regional Development (MEPRD) – organises the governance of state ICT and coordinates the electrisation of public services, whereas State Regional Development Agency (SRDA) ensures the operation and development of solutions for shared use of state ICT[1].

After that list, the author of the paper wants to show that a lot of different institutions need to work together in order to support, consult, prevent and protect citizens from the cybercrime threats. The next two countries that will be shortly analysed will be Lithuania and Estonia and their legislation and regulation for the cybercrime.

Lithuania is also included in the states, where the provisions of the Convention have become binding on its legislator, obliging it to take all necessary measures to harmonize national legal acts with the framework set out therein[2]. The Criminal Code of the Republic of Lithuania in force is the legal act establishing liability for criminal offences known as computer crimes and Internet crimes. Although the legislator of Lithuania had been combating cybercrimes since as early as 1994 by means of the amendments to the Soviet Era Criminal Code of 1961, a significant effort was required to transpose the requirements of the Convention into the Lithuanian law, starting from the year 2007.[3]

The author points out that the situation in Lithuania is very close to the Latvian – both countries are using Convention as the main document and uses different organisation to cooperate together against cybercrime.

[1] CYBER SECURITY STRATEGY OF LATVIA 2014–2018 https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/lv-ncss Retrieved: 09.04.2017.

[2] Global Cyber Law Database http://www.cyberlawdb.com/gcld/lithuania/ Retrieved: 09.04.2017.

[3] Legislation on cybercrime in Lithuania: development and legal gaps in comparison with the convention on cybercrime. Darius Sauliūnas (2010) https://repository.mruni.eu/handle/007/11611 Retrieved: 11.04.2017

Estonia was one of the first countries in the world to adopt a national cyber security strategy in 2008.11 The strategy was drafted by the Ministry of Defence for the period 2008-2013 and was accompanied by Implementation Plans. The 2008 strategy offered a comprehensive view of cyber security and outlined the following core areas: application of a graduated system of security measures in Estonia; development of Estonia's expertise in and awareness of information security; development of an appropriate regulatory and legal framework to support the secure and seamless operability of information systems; and promoting international cooperation aimed at strengthening global cyber security.12 In September 2014, the renewed Cyber Security Strategy for 2014-201713 was adopted, the renewal process being led by the Ministry of Economic Affairs and Communication, with more than 30 public and private sector parties as well as academia involved in the development process. 14 [1]Talking about Estonia the primary cyber laws of that country are: Digital Signatures Act, Databases Act, Electronic Communications Act, Information Society Services Act, Penal Code, Code of Criminal Procedure and the Personal Data Protection Act[2].

Yet Steve Wilson, the head of the European Cybercrime Centre, noted that there were reasons to be positive about progress in tackling cybercriminals. "2016 has seen the further evolution of established cybercrime trends…. However there are many positives to be taken from this year's report. Partnerships between industry and law enforcement have improved significantly, leading to the disruption or arrest of many major cybercriminal syndicates and high-profile individuals associated with child abuse, cyber intrusions and payment card fraud, and to innovative new prevention programs such as the no more ransom campaign."[3]

Case Study

In Baltic State countries cyberattacks are quite rare actions. But there are some big cases that should be named. On April 26, 2007, the small Baltic state of Estonia experienced the first wave of denial-of-service (DoS) attacks. Accompanied by riots in the streets, these cyberattacks were launched as a protest against the Estonian government's removal of the Bronze Soldier monument in Tallinn, a Soviet war monument erected in 1947[4]. The cyberattack took place at 10 p.m. on April 26, 2007, as unknown attackers launched a full-scale cyberattack against the Estonian government. The cyberattack remained relatively unnoticed for the first twenty-four hours, but was discovered soon thereafter when Estonian Minister of Defense Jaak Aaviksoo found himself unable to log onto the prime minister's Reform Party website. The hackers had targeted this site first, subsequently spreading to other political party and government web-sites, including the official site for the Estonian parliament. By the end of the first week, the distributed denial-of-service attacks

[1] Osula A-M. National Cyber Security Organisation: Estonia (2015) https://ccdcoe.org/sites/default/files/multimedia/pdf/CS_organisation_ESTONIA_032015_1.pdf Retrieved: 12.04.2017

[2]Global Cyber Law Database http://www.cyberlawdb.com/gcld/category/europe/estonia/ Retrieved: 09.04.2017.

[3] The 2016 trends in cybercrime that you need to know about. Holly Ellyatt (2016) http://www.cnbc.com/2016/09/28/the-2016-trends-in-cybercrime-that-you-need-to-know-about.html Retrieved: 09.04.2017.

[4] International Affair Review http://www.iar-gwu.org/node/65 Retrieved: 19.05.2017

levied against these sites had knocked them completely offline. The cyberattacks continued in waves for two weeks until May 9, the anniversary of the end of the European theatre of World War II. At the stroke of midnight, Moscow time, Estonia witnessed its heaviest attack yet—up to 4 million packets of information sent per second. This time the hackers focused their efforts on the Estonian banking system. By May 10, the cyberattacks had forced Hansabank, the nation's largest bank and a pioneer of many of Estonia's IT developments in the 1990s, to shut down its Internet-based operations. This was disastrous on three counts. First, it ceased online banking capabilities for Estonians in a country where an estimated 97 percent of all banking transactions occurred online; second, it severed the connection between Hansabank and its ATMs throughout Estonia; and third, it broke the connection between Hansabank and the rest of the world, thus preventing Estonian debit cards from working outside of the country. It is now known that the attackers who waged cyberwarfare on Estonia acted on their own initiative, primarily as a form of political protest. These "hacktivists" turned out to be a combination of experienced hackers who would contract out their own botnets or write their own malicious programs, and "script kids" who were, by and large, individual novice hackers who attacked Estonian target sites by following "how-to" guides found on various hacker websites. The disparate nature of the attackers made them, in turn, difficult to track. In January of 2008, the Estonian government successfully traced and indicted one of the attackers, Dmitri Galushkevich, an ethnic Russian student residing in Estonia. Galushkevich had used his laptop to take part in the denial-of-service attacks targeting the Reform Party website, successfully taking it offline for ten days. Galushkevich pled guilty, claiming that he took part in the attacks to protest the removal of the Bronze Soldier, and was fined 17,500 kroons, an amount roughly equivalent to U.S. $1,635. To date, the Estonian government has made no subsequent arrests.

The second famous case of cybercrime that took place in the Baltic States was case of Deniss Calovskis – Latvian citizen that was involved in Gozi Virus production. Gozi was stealthily infecting and infiltrating computers for over five years. "Well over a million computers around the world" were infected by Gozi according to US prosecutors, including more than 160 PCs at NASA. Computers in Finland, France, Germany, Italy, Turkey and the United Kingdom were also affected. One way your computer could become infected by the Gozi malware was by opening a PDF file sent to you in an unsolicited email. Unfortunately for you, the PDF file was boobytrapped, and secretly installed Gozi onto your Windows PC. One in place, the malware could steal data from your computer – including your bank account login details – and send it to online criminals. Once banking information was stolen it would be shared with so-called money mules who would help the criminals launder stolen funds. New York US Attorney Preet Bharara described the malware as "one of the most financially destructive computer viruses in history."

It is possible to see that cybercrimes can cover not only one person or institution, there problem comes when it covers a country or the whole world internet users. In the next researches it would be good to analyse the system of regulation for cybercrimes that covers the whole world.

Conclusions

To conclude analysis of the meaning and importance of the cybercrime legislation the author come forward with the following points:

1) Cybercrime consists of criminal acts that are committed online by using electronic communications networks and information systems. And here is a problem - all cybercrimes are taking place online and online network has no limits and borders. It means that it is impossible to use only one kind of regulation in every country, but by using some common legislation and adopt and integrate it to each country will work good for preventing and protecting citizens.
2) All three Baltic countries having similar cybercrime legislation but there are some differences however the main idea remain the same. It should be pointed out that a lot of different institutions are working together to protect country from the cybercrime threats.
3) Every year the tendency of cybercrime is growing up that causes a real threat for the citizens using computer and internet, leaving their information and data inside in the web and sharing it with unknown people.
4) The main problem in legislation and regulation for cybercrime acts are huge countries coverage. The problem is hiding in the territory that covers and affects by actions from cybercrime.

It is a new and actual theme to continue analysis and make more new researches because of its growing tendency and popularity.

References

Cyber Crime Assessment 2016 . Need for a stronger law enforcement and business partnership to fight cyber crime (2016) http://www.nationalcrimeagency.gov.uk/publications/709-cyber-crime-assessment-2016/file Retrieved: 09.04.2017.

CYBER SECURITY STRATEGY OF LATVIA 2014–2018 https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/lv-ncss Retrieved: 09.04.2017.

Cybercrime (2016) https://ec.europa.eu/home-affairs/what-we-do/policies/organized-crime-and-human-trafficking/cybercrime_en Retrieved: 07.04.2017.

Cybercrime (2016) https://ec.europa.eu/home-affairs/what-we-do/policies/organized-crime-and-human-trafficking/cybercrime_en Retrieved: 07.04.2017.

Cybersecurity and Cybercrime Statistics Report. (2016) http://cybersecurityventures.com/cybersecurity-and-cybercrime-statistics/ Retrieved: 19.04.2017.

Data Security and Cybercrime in Latvia. Valts Nerets and Agita Sprude (2017) http://www.lexology.com/library/detail.aspx?g=f619dc4c-cf2b-4b48-9909-00e37dc75859

DIGITAL SINGLE MARKET (2016) http://digital-agenda-data.eu/charts/analyse-one-indicator-and-compare-countries#chart={"indicator-group":"internet-usage","indicator":"i_iuse","breakdown":"IND_TOTAL","unit-measure":"pc_ind","ref-area":["BE","BG","CZ","DK","DE","EE","IE","EL","ES","FR","IT","CY","LV","LT","LU","HU","HR","MT","NL","AT","PL","PT","RO","SI","SK","FI","SE","UK","EU27"]} Retrieved: 10.04.2017.

Fizisko personu datu aizsardzības likums https://likumi.lv/doc.php?id=4042 Retrieved: 07.04.2017.

Global Cyber Law Database http://www.cyberlawdb.com/gcld/category/europe/estonia/ Retrieved: 09.04.2017.

Global Cyber Law Database http://www.cyberlawdb.com/gcld/lithuania/ Retrieved: 09.04.2017.

IBM's CEO On Hackers: 'Cyber Crime Is The Greatest Threat To Every Company In The World' , Steve Morgan (2015) https://www.forbes.com/sites/stevemorgan/2015/11/24/ibms-ceo-on-hackers-cyber-crime-is-the-greatest-threat-to-every-company-in-the-world/#57c80dcf73f0 Retrieved: 11.04.2017.

Identity Theft And Cybercrime (2016) http://www.iii.org/fact-statistic/identity-theft-and-cybercrime Retrieved: 19.04.2017.

International Affair Review http://www.iar-gwu.org/node/65 Retrieved: 19.05.2017.

Kaspersen, H. W. K. (2009) Cybercrime and Internet Jurisdiction, Discussion paper (draft), version 5 March 2009, prepared in the framework of the Project on Cybercrime of the Council of Europe

Legislation on cybercrime in Lithuania: development and legal gaps in comparison with the convention on cybercrime. Darius Sauliūnas (2010) https://repository.mruni.eu/handle/007/11611 Retrieved: 11.04.2017

Osula A-M. National Cyber Security Organisation: Estonia (2015) https://ccdcoe.org/sites/default/files/multimedia/pdf/CS_organisation_ESTONIA_032015_1.pdf Retrieved: 12.04.2017

Par Konvenciju par kibernoziegumiem un Konvencijas par kibernoziegumiem Papildu protokolu par rasisma un ksenofobijas noziedzīgajiem nodarījumiem, kas tiek izdarīti datorsistēmās https://likumi.lv/doc.php?id=146481#p35 Retrieved: 07.04.2017.

Parker, D. B. (1983) Fighting Computer Crime. New York: Charles Scribner's Sons, 1983.

Sauliūnas D. (2010) Legislation On Cybercrime In Lithuania: Development And Legal Gaps In Comparison With The Convention On Cybercrime. https://www.mruni.eu/upload/iblock/822/11_Sauliunas.pdf Retrieved: 11.04.2017.

The 2016 trends in cybercrime that you need to know about. Holly Ellyatt (2016) http://www.cnbc.com/2016/09/28/the-2016-trends-in-cybercrime-that-you-need-to-know-about.html Retrieved: 09.04.2017.