TALLINN UNIVERSITY OF TECHNOLOGY
School of Business and Governance
Department of Law

Aliaksei Hrytsevich

PRIVATE SECTOR LIABILITY IN CYBER-SECURING EUROPEAN ELECTIONS

Bachelor's thesis
Programme HAJB08/14 - Law, specialisation European Union and International Law

Supervisor: Agnes Kasper, PhD

Tallinn 2019

I hereby declare that I have compiled the paper independently
and all works, important standpoints and data by other authors
has been properly referenced and the same paper
has not been previously presented for grading.
The document length is 9985 words from the introduction to the end of conclusion.

Hrytsevich Aliaksei ……

(signature, date)

Student code: 166251HAJB

Student e-mail address: aliaksei.hrytsevich@gmail.com

Supervisor: Agnes Kasper, PhD:

The paper conforms to requirements in force

……

(signature, date)

Co-supervisor:

The paper conforms to requirements in force

……

(signature, date)

Chairman of the Defence Committee:

Permitted to the defence

……

(name, signature, date)

TABLE OF CONTENTS

ABSTRACT

With the development of technologies that have become embedded in the modern election process, more opportunities for their attack have appeared. Nowadays it is already a common phenomenon when private platforms are exploited to influence the electoral process. However, there is no clear liability regime for private actors involved. The problem lies not only in talented hackers, but also in the vulnerability of platforms that are directly or indirectly related to the election process. Any digital system, even the most complex, can be hacked. For the research the qualitative method was used, with emphasis on the analysis of the scientific articles, European Law and case study. The paper provides an overview of the legal framework governing the liability of private actors in relation to meddling with elections in the EU.

Key words: elections, cyber security, private actors, liability.

INTRODUCTION

The last few decades have been the beginning of a new information age. Information and communication technologies are at the forefront. Modern technologies and the Internet can be used in the election process in different ways. On the one hand, these tools make it possible to create more open, accessible and simple election process. On the other hand, usage of technologies simultaneously makes this process more vulnerable. Powerful economic and political groups, as well as individual states, were able to use them as a tool to achieve their goals. This makes the problem of ensuring the cybersecurity of elections one of the most pressing issues of our time. The world was shocked by a series of hacks that occurred in the United States during the presidential elections in 2016. These events have shown that cyber attacks on elections represent a real threat to the security and independence of any state. There is a huge variety of cyber threats themselves, as well as subjects to combat them. The example of the United States shows that such fears are not at all groundless, and many facts indicate that the war in cyberspace — and this is how you can generally characterise this new type of threat — will fundamentally change the character of modern cyber war, just as it periodically changed under the influence of scientific and technological progress in past decades. Today, cybersecurity threats to elections are developing much faster than the ability of supervisory and regulatory authorities to identify violators and bring them to justice.

What adds to the problem of dealing with cyber threats to elections is that the majority of information and communication networks belong to private sector entities. However, it is reasonable to ask a question — does private sector actors bear any responsibility when their products are used to meddle with elections? These two groups of subjects, that is, the state on the one hand and private players on the other, often pursue different interests. This reduces the effectiveness of efforts to protect the elections.

The aim of this paper is to establish the liability regime for private sector actors when their products are used to cyber-meddle elections. Todays legislation on liability position of private companies in relation to interference with election is unclear.

As to the subject of the research question, author will try during particular thesis to answer the following question: under what conditions private actors involved in process of election are responsible for interference? To better understand importance of the chosen topic, in the first chapter of this work, author analyses what is the danger of cyber-meddling in the elections and why it is crucial to protect election process from cyberthreats. In the second chapter is dedicated to define main actors who are responsible for interference with election and techniques they are using to do so. By examining sources and threats to elections, the role of private sector in it will be determined. The last part will assesses the extent of liability of private actors in terms of cyber threats to elections.

1. THE IMPORTANCE OF PROTECTION OF FROM CYBER INTERFERENCE

Today cyber hacking and attacks on computer networks is not a new phenomenon. The first cyber attacks began in 1988 and since then they have firmly taken their place in our daily life.[1] Therefore, the question may arise: why should the hacking of elections be given special attention and how do they differ from regular hacker attacks? The main distinguishing features of hacking cyber elections are the purpose, nature and targets of the attacks.

One of the main differences between cyber interference in elections from the regular hacker attacks is the political motivation of the former. As the Radware study shows, most cyber crimes are in the first place financially motivated.[2] However, the motivation for cyber-interference in elections is not financial gain, but the desire to change the political balance in the attacked country and influence the outcome of the political race.[3]

Moreover, another difference in cyber interference with elections is the complex methods of the attacks. Usually, cyber meddling with elections not only include hacking of computers to manipulate or steal of data, but also informational warfare. These can include propaganda, attacks on television networks and other media. Moreover, hacking of computer networks is often accompanied by disclosure of information, obtained as a result of unauthorised entry, which is also a part of the information war.[4] Methods of interference with elections will be studied in more detail in the next chapter. It should be noted, that because of its complex nature and goals, cyber interference with elections targets a very specific group —voters. By conducting informational warfare attackers are trying to manipulate voting citizens into their desirable outcome. That is an important difference between cyber interference with election and regular hacker attacks.

---

[1] Middleton, B. (2017). – *History of Cyber Security Attacks: 1980 to Present*. Vol. 74. 129-147. Katy: Secur Refuge LLC, p. 33.

[2] Radware Global Application & Network Security Report 2018, p. 4.

[3] Nazario, J. (2009). Politically motivated denial of service attacks. – C*ryptology and Information Security Series*, Vol. 3, 163-181.

[4] Van De Velde, J. (2017). *The Law of Cyber Interference in Elections*. Accessible: https://ssrn.com/abstract=3043828, 20 March 2019.

Another distinguishing feature of cyber meddling with elections is unique relations of private and state actors. Although, attacks are aimed at state and its citizens, they are usually conducted through the privately owned assets.[5] It can be, for example, informational campaign in privately owned social media or attack on privately owned data servers. However, private companies are not the end targets — they are just a way to affect states political balance. That is a glaring difference between regular hacker attacks and attacks on elections. Regular attacks often directly aimed at private sector companies. For example, 42% of companies in the world became the object of hacker attacks, making them most popular target among hackers.[6]

However, what makes cyber meddling with elections so important? It should be understood that the attack on the elections is an attack on the sovereignty, independence of the state and its citizens. This is a modern form of warfare.[7] Thus, hackers can cause real chaos, directing their attack on the destabilisation of the political situation in the country. At the same time, attackers do not have to directly send troops to attack military or government targets. Moreover, this issue raises question about appropriate countermeasures. Currently, international law does not consider hacker attacks on elections as clearly military operations. This means that the provisions of Article V of the North Atlantic Treaty, or, in other words, also known as rule of self-defense, would not automatically apply to a country that was attacked. Therefore, attacked states legally can't use force in response.[8] Therefore, because cyber-attacks on elections is a direct threat to democratic system and sovereignty of the state and due to the lack of proper countermeasures, protection of elections from cyber interference is one of the most pressing issues that European Union faces.

---

[5] *Ibid.*, pp. 8-9.

[6] Radware Global Application & Network Security Report 2018, *supra nota* 2, p. 4.

[7] Van De Velde (2017), *supra nota* 4, pp. 8-9.

[8] *Ibid.*, p. 10.

2. SOURCES AND MEANS OF CYBER INTERFERENCE INTO ELECTIONS

One of the main problems in the fight against cyber meddling with elections is that it is often extremely difficult to accurately identify the perpetrators of the attacks and their country of residence.[9] In the next two sub-chapters the main participants in cybercrime and the methods by which they influence the election process will be discussed.

2.1. Sources of threats of cyber election

Foreign intelligence agencies can use computer technology to gather information and spy. Such actions can be directed against other states (both friendly and hostile) or against non-state actors of cyber attacks. States can carry out cyber attacks against unfriendly states for the purpose of disinformation, destabilisation, intimidation, or even within the framework of full-scale cyber warfare.[10] Government agencies may also resort to such means as interception and use of personal data, and in some cases this happens without proper authorisation by the judicial authorities and without proper democratic control.[11] These hacker operations can be carried out by state intelligence services, special services or law enforcement agencies.[12] However, it is worth noting that states rarely act directly. Governments cannot conduct their attacks directly because it can be viewed as a violation of the sovereignty and independence of another country.[13] Such actions can be regarded as an act of aggression.[14] Most often, states work through the hacktivist groups which are sponsored by governments. For example, APT28 also known as

---

[9] Buckland, B., Schreier, F., Winkler, T. (2015). *Democratic Governance Challenges of Cyber Security.* Accessible: https://www.dcaf.ch/sites/default/files/publications/documents/CyberPaper_3.6.pdf, 12 March 2019.

[10] Schreier, F. (2015). *On Cyberwarfare.* Accessible: https://www.gao.gov/assets/130/122454.pdf, 12 March 2019.

[11] Wilshusen, G. (2009). *Cyber Threats and Vulnerabilities Place Federal Systems at Risk.* Accessible: https://www.files.ethz.ch/isn/144868/OnCyberwarfare-Schreier.pdf, 15 March 2019.

[12] Buckland, Schreier, Winkler (2015), *supra nota* 9.

[13] Ohlin, D. (2017). Did Russian Cyber-Interference in the 2016 Election Violate International Law? – *Cornell Legal Studies Research Paper,* No.17-15.

[14] *Ibid.*

Fancy Bear, Pawn Storm and Sednit[15] where found involved in cyber attack on president candidate Emmanuel Macron before the 2017 French elections.[16] Estonian Foreign Intelligence Service believes that APT28 is associated with Russian intelligence service Main Directorate of the General Staff of the Armed Forces of the Russian Federation (GRU).[17] The term "hacktivism" originated from the combination of the two words "hack" and "activism." It denotes a new phenomenon of social protest, which is a kind of synthesis of social activity aimed at protesting against something and hacking certain government websites or services. Hacktivists seek to damage, distort content, or disable some websites to achieve their political goals. What differs hacktivists groups from regular hackers is that hackers most often engaged in hacking networks simply because of hooliganism or in order to gain authority in the hacker community, but hacktivists are pushed to this by other reasons, which are much more political in their nature. They are interested in promoting their political or social agendas.[18] The most prominent hacktivist groups are, formerly mentioned, APT28 and APT29.

Also, one should not confuse hacktivism and cyberterrorism: despite the apparent similarity of methods and goals, they differ in a number of parameters. Both phenomena are positioned as a way to protest in the Internet space. However, political or social hacktivism does not aim to spread the feeling of fear in a large group of people (as a result of a terrorist act in reality). The hacktivist methods are aimed at impeding the work of organizations in cyberspace, not at disabling systems and disrupting the access of ordinary citizens to information. Their goal is to express opinions, protest, political ideas. The use of hacking tools and technologies without specific motivation, goals do not fit into the framework of the concept. Hacktivism is an electronic form of civil disobedience.[19]

---

[15] Gogolinkski, J., Hacquebord F., Huq N., Kharouni L., Mercês F., Otis D., Remorin A. (2014). *Operation Pawn Storm: Using Decoys to Evade Detection.* Accessible: https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/white-papers/wp-operation-pawn-storm.pdf, 16 March 2019.

[16] Mansfield-Devine, S. (2017). Editorial. – *Computer Fraud and Security Series*, Vol. 2017, No. 5, 2.

[17] Valisluureamet (2019). *International Security and Estonia.* Accessible: https://www.valisluureamet.ee/pdf/raport-2018-ENG-web.pdf, 16 March 2019.

[18] Travaglino, G. A. (2019). Support for Anonymous as vicarious dissent: Testing the social banditry framework. – *Group Processes & Intergroup Relations*, Vol. 22, No. 2, 163–181.

[19] Delmas, C. (2018). Is Hacktivism the New Civil Disobedience? – *Raisons politiques*, Vol. 69, No. 1, 63-81.

APT28, may also be known as Fancy Bear, Sednit, Pawn Storm, STRONTIUM and Sofacy, is an hacktivist group that has been extremely active in recent years.[20] This organisation were involved in numerous cyber attacks concerning both European and US elections.[21] The Slovak company ESET, which develops antivirus and information security, has published their APT28 report according to which, APT28 has been active since 2004.[22] FireEye is a cybersecurity company, which specialises in cyber attack investigations. They released a report, in which they describe APT28's operations as promotion of Russian strategic interests.[23] Allegedly, APT 28 took direct orders from GRU.[24] Since the 2014 group was not only involved in above mentioned attack on Emmanuel Macron's presidential campaign, but also they attacked the German political party Christian Democratic Union and Ukrainian Central Election Commission.[25] The head of the service, Hans-Georg Maasen, stated that it was Fancy Bear that was behind the attacks on the Christian Democratic Union of Germany, whose leader is German Chancellor Angela Merkel.[26]

APT29 also known as Cozy Bear, The Dukes, Office Monkeys and CozyCar is a hacktivist group which has been active since at least 2008 and operates from the territory of the Russian Federation.[27] Their most recent operation wan an attempt attack on Dutch ministries right before 2017 Dutch general election. The head of the Dutch General Intelligence and Security Service

---

[20] Jensen, B., Maness, R., Valeriano, B. (2019). Fancy bears and digital trolls: Cyber strategy with a Russian twist, Journal of Strategic Studies. – *Journal of Strategic Studies*, Vol. 42, No. 2, 212-234.

[21] TrendMicro Two Years of Pawn Storm Report 2017, pp. 4-7.

[22] ESET (2016). En Route with Sednit, Part 1: Approaching the Target. Accessible: https://www.welivesecurity.com/wp-content/uploads/2016/10/eset-sednit-part1.pdf, 20 March 2019.

[23] FireEye APT28: A Window Into Russia's Cyber Espionage Operations, 2016 Report, p. 23.

[24] Blinderman, E. (2017). Hidden by Sovereign Shadows: Improving the Domestic Framework for Deterring State-Sponsored Cybercrime. – *Vanderbilt Journal of Transnational Law*, Vol. 50, 889-931.

[25] FireEye APT28: At the center of the storm Report 2017.

[26] BBC (2016). Russia 'was behind German parliament hack'. – *BBC,* 13 May 2016, Accessible https://www.bbc.co.uk/news/technology-36284447, 10 March 2019.

[27] Alperovitch, D. (2016). *Bears in the Midst: Intrusion into the Democratic National Committee.* Accessible: www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/, 18 March 2019

claims that APT 29 is associated with Russian intelligence services.[28] Security company FireEye supports that opinion saying that Cozy Bear has ties to Russian Federal Security Service (FSB).[29]

2.2.Means of interference with elections

One of the most popular ways of cyber interference in elections is by conducting massive information campaigns. It is important to understand that those campings can have several forms. One of the most prominent forms is so-called “fake news”. Fake news is an information hoax or the deliberate dissemination of misinformation in social media and traditional media in order to promote certain political agenda.[30] Authors of fake news can use fully fabricated news, or they can use catchy headlines for the news that the headline has little to do with. Recent french study shows that 59% percent of people that share the news links on social medias do not actually click or open them to read, suggesting that they only share the article based on it headline.[31] The fake news phenomenon has a number of common features with the concept of political propaganda - the same techniques are often used as in the tabloid press of the beginning of the 20th century.[32]

There are sever examples of information campaigns which were conducted in attempt to influence the outcome of elections among the members of the European Union. First of all, in the run-up to German Federal election of 2017 mass media which where sponsored by Russia, RT News for example, change the focus of their news on politically divisive topics such as issues of immigration. Moreover, completely fabricated news went viral. There were a fake story about

---

[28] Modderkolk, H. (2018). Dutch agencies provide crucial intel about Russia's interference in US-elections. – *De Volkskrant, 25* March 2018, Accessible https://www.volkskrant.nl/wetenschap/dutch-agencies-provide-crucial-intel-about-russia-s-interference-in-us-elections~b4f8111b/, 18 March 2019.

[29] Carr, N., Dunwoody, M., Leathery, J., Matonis, M., Thompson, A., Withnell, B. (2018). *Not So Cozy: An Uncomfortable Examination of a Suspected APT29 Phishing Campaign.* Accessible: https://www.ttu.ee/public/m/majandusteaduskond/uusJuhend_2018_08_18_EN_veebilehele.pdf, 20 March 2019.

[30] Acerbi, A. (2019). Cognitive attraction and online misinformation. – *Palgrave Communications,* Vol. 5, No. 1.

[31] Chaintreau, A., Gabielkov, M., Ramachandran, A., Legout, A. (2016). *Social Clicks: What and Who Gets Read on Twitter?* Accessible: https://hal.inria.fr/hal-01281190/document, 23 March 2019.

[32] Boyd-Barrett, O. (2019). Fake news and ‘RussiaGate’ discourses: Propaganda in the post-truth era. – *Journalism,* Vol. 20, No. 1, 87–91.

refugee who raped a 13-year-old Russian-German girl. This story was used in a campaign of right-wing party called Alternative for Germany (AfD).[33] This story became extremely popular. That situation forced Frank-Walter Steinmeier, Germany's foreign minister, to explain that the story was completely untrue.[34]

Secondly, right before 2016 Brexit referendum, a massive campaign was conducted where approximately 150,000 Russian-language Twitter bots started to post massages in support of Britain to leave the European Union.[35] It was also believed that Facebook was used as a platform for pro-Brexit propaganda, although later Facebook in the letter to the British Electoral Commission revealed that the scope of was very small — 3 promotional posts that reached 200 people. [36]

Third example is 2016 Italian local elections. During that period a massive propaganda campaign was conducted in which a number of social media accounts and websites spread false news that targeted Prime Minister Renzi. Half of the most popular stories related to the election that were shared on social media were completely untrue.[37]

What can be seen in common among those three incidents is a dominant role of social medias. In recent years, the role of bloggers and influencers of public opinion in social networks is growing, gradually pulling away the audience from traditional media and Internet information resources. Such modern means of communication, having, of course, a lot of advantages, however, are increasingly becoming sources of disseminating false information or simply rumours. Today, the

---

[33] Björnstjern, B. (2018). Fake News and International Law. – *European Journal of International Law*, Vol. 29, No. 4, 1357–1376.

[34] Lucian, K. (2016). *Russia having success in hybrid war against Germany.* Accessible: http://blogs.reuters.com/great-debate/2016/02/07/russia-having-success-in-hybrid-war-against-germany/, 24 March 2019.

[35] Ee, S., Galante, L. (2018). *Defining Russian Election Interference: An Analysis of Select 2014 to 2018 Cyber Enabled Incidents*. Accessible: https://www.atlanticcouncil.org/images/publications/Defining_Russian_Election_Interference_web.pdf, 24 March 2019.

[36] Scott, M. (2017). *Facebook says Russian groups spent less than £1 on Brexit advertising.* Accessible: https://www.politico.eu/article/facebook-brexit-russia-advertising-referendum-internet-research-agency/, 24 March 2019.

[37] Van De Velde (2017), *supra nota* 4, p. 13.

line between traditional media and social media is blurred, information easily travels between them, which means fake news is becoming more and more prominent in the modern information space. This, as can be seen from the examples, can easily be used as a part of informational warfare. False information can spread faster than you can debunk it. The mechanics of disseminating information in social networks create a fairly wide window for manipulation.

Moreover, besides information campaigns cyber meddling with elections can be done via hacking. There are number of ways to conduct hacking, however they can be divided into two groups: hacking by exploiting software or hardware vulnerabilities. Hardware vulnerabilities is weakness or a design flaw in the equipment itself that potentially can be exploited.[38] It can be an implementation error in voting equipment or in computers that, for example, can be used for internet voting. The fact is that EU Member States does not use a uniform way of voting, some already use electronic voting and some do not. For instance, Estonia and Belgium already use electronic voting in their elections and Lithuania is planning to implement it in their 2019 local elections.[39] [40] However, in Germany electronic voting was found unconstitutional.[41] Nonetheless, in modern process of elections technologies play significant role. And if technologies are involved there is always a possibility of hardware flaws. Software vulnerabilities is a weakness in application that allows hackers to exploit it to commit attack.[42] Hackers can use all above mentioned vulnerabilities to implement their cyber attacks. For instance in preparation to German Federal Elections in 2017 APT28, which are known to use software vulnerabilities in their cyber attacks, stole 16 gigabytes of private emails form a number of German politicians. Moreover, in 2015 Estonian parliamentary elections hackivist Märt Põder was able to find a vulnerability in the operating system and replace the number of one of the candidates for a non-existent number casting the vote to be invalid.[43] Moreover, hackers can conduct their attack using viruses. For example, according to Report on the Investigation into Russian Interference in

---

[38] ENISA. *Risk Management Glossary*. Accesible: https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/glossary#G52, 27 Match 2019.

[39] Riigikogu Election Act. RT I 2002, 57, 355.

[40] The Baltic Times (2017). *Lithuania: President says online voting wouldn't ensure secrecy and security.* Accessible: https://thevotingnews.com/international/europe/lithuania/ , 27 March 2019.

[41] Judgment of the Second Senate of 03 March 2009, BVerfG, 2 BvC 3/07 - paras. (1-166).

[42] Norman, T. (2018). – *Electronic Access Control*. 2nd ed. Oxford: Butterworth Heinemann.

[43] Heiberg, S., Parsovs, A., Willemson, J. (2015). *Log Analysis of Estonian Internet Voting 2013 – 2015.* Accessible: https://eprint.iacr.org/2015/1211, 27 March 2019.

the 2016 US Presidential Election it was established, that hackers got into Democratic Parties server systems using different types of malware.[44]

Furthermore, informational warfare and hacking can be performed in combination. The dominant way to do so is by doxing. Doxing is a concept from the cybercrime environment, meaning the public disclosure of confidential information about a person or organization. Doxers can get information about their person or organisation of interest from hacking closed databases, such as e-mails, social network accounts or cloud storages where important data can be stored.[45] One of the most prominent examples of doxing done in recent years is doxing done during 2016 US presidential elections and prior to 2017 French elections. In the former one, according to forensic analysis by American cybersecurity company which eliminated the effects of hacking CrowdStrike, APT28 and APT29, which worked separately and were unaware of each other actions, attacked an internal network and emails servers associated with the Democratic National Committee (DNC).[46] Hackers used known GRU malware called "X-agent" and "X-tunnel" to hack the e-mails of people associated with Democratic National Committee Hillary Clinton presidential campaign and then to steal and transfer the stolen data from DNC servers to their desired destination via special encrypted channels.[47] Later, in 2018 District Court of Columbia charged twelve GRU officers with large-scale cyber operations to meddle with the 2016 US presidential election concerns their attack on DNC.[48] Stolen material was doxed under the alias "Guccifer 2.0" using such platforms as WikiLeaks potentially damaging the candidacy of Hilary Clinton.[49]

---

[44] Muller, R. (2019). *Report On The Investigation Into Russian Interference In The 2016 Presidential Election*. Accessible: https://www.justsecurity.org/wp-content/uploads/2019/04/Muellller-Report-Redacted-Vol-II-Released-04.18.2019-Word-Searchable.-Reduced-Size.pdf, 2 May 2019.

[45] Hansen, I., Lim, D. (2019). Doxing democracy: influencing elections via cyber voter interference. – *Contemporary Politics*, Vol. 25, No. 2, 150-171.

[46] Alperovitch (2016), *supra nota* 27.

[47] Columbia District Court, 1:18-cr-00215-ABJ, *U.S. v. Viktor Borisovich Netyksho, et al.*

[48] *Ibid.*

[49] Ee, Galante (2017), *supra nota* 35, p. 10.

Similar case happened two days prior to French president elections. An unknown hacktivist group first stole more than nine gigabytes of private mails and documents from Emmanuel Macron's campaign and then leaked it via popular imageboard website 4chan.[50]

[50] Ee, Galante (2017), *supra nota* 35, pp. 11-12.

3. PRIVATE SECTOR ROLE AND LIABILITY

As it can be seen from previous chapter today it is impossible to host elections completely without any technology. Technology plays an important role in everything, from electronic voting machines to social networks, where voters share their opinions. Majority of these technologies are either owned or produced by private sector. Therefore it is a normal question to ask — do they bear any legal responsibilities when their platforms were used to interfere with elections?

3.1.Vulnerability report liability

Often private cybersecurity companies such as FireEye, ESET, CrowdStrike and SecureWorks conduct their own research and investigations on cyber meddling with elections. Sometimes cybersecurity companies share information about cybersecurity errors out of good will. However, a question might be asked — if cybersecurity company have information about vulnerabilities are they legally obliged to disclose this information to authorities or public? To tackle this issue ENISA introduced a procedure called Coordinated Vulnerability Disclosure (CVD).[51] Vulnerability disclosure is a process in which actors who find venerability share information about it to a party which was unaware of it via intermediate actor between them. After the flaw has been patched or the term for patching has expired, the information about it must be shared with public.[52] There are several actors involved in this process: vendor, finder and coordinator. Vendors include manufacturers, developers and distributors of software, hardware and services. Finder is an actor who finds and reports flaws. Finders can sometime be divided into finders, the one who actually find error, and reporters, the one who reports about it.[53] Coordinator is an organisation that ensures security and confidentiality of the disclosure process between finder and vendor. Government can play a different roles in CVD. Basically

---

[51] ENISA (2018). *Good Practice Guide on Vulnerability Disclosure: from challenges to recommendations*. Accessible: https://www.enisa.europa.eu/publications/vulnerability-disclosure, 29 March 2019.

[52] Kranenbarg, M.W., Holt, T.J., van der Ham, J. (2018). Don't shoot the messenger! A criminological and computer science perspective on coordinated vulnerability disclosure. – *Crime Science*, Vol. 7, No. 16.

[53] Software Vulnerability Disclosure in Europe: Technology, Policies and Legal Challenges, Report of a CEPS Task Force 2018.

anyone can be a finder: white hat hackers, users or cybersecurity companies. Usually, trustworthy organisations, such as Computer Emergency Response Teams (CERT), act as cooperator.[54] Therefore, potentially there can be an established process when cybersecurity companies will properly disclose information about flaws to the government officials via Task Force teams. In recently adopted EU Cybersecurity Act the steps were taken towards making CVD process to play more prominent role in EU cybersecurity. However, according to EU Cybersecurity Act, adoption of such policies is not mandatory for EU member states, Union institutions, bodies and agencies. Despite that, a number of large private companies, such as Microsoft, and Member States already implemented Coordinated Vulnerability Disclosure procedure.[55]

However, CVD procedure has number of problems. First of all, strict guidelines can force company to disclose information about the flaw before it was fixed.[56] Moreover, this procedure is hard to apply to the supply chains. It is a common practise today that products are developed by more than one company. This also applies to software that may be licensed for inclusion in other products. For example, the voting machine is assembled in Spain, but uses processors developed in China. This processor detects a vulnerability that can affect the voting process. Who should be vendor in this situation? Spanish company or Chinese company? And who actually should fix this flaw? Something similar happened in 2018, when a number of vulnerabilities were discovered in Intel x86 processors that allowed third-party actors to gain access to the registers and all the data contained in them.[57] This vulnerability has affected any machine that has used an Intel processor since 1990's.[58]

More prominent incident occur in 2017 in Estonia. An international team of information security researchers from the UK, Slovakia, the Czech Republic and Italy discovered a critical

---

[54] ENISA (2018). *Economics of vulnerability disclosure* (2018). Accessible: https://www.enisa.europa.eu/publications/economics-of-vulnerability-disclosure, 28 March 2019.

[55] Microsoft Security Response Center. *Coordinated Vulnerability Disclosure*. Accessible: https://www.microsoft.com/en-us/msrc/cvd, 29 March 2019.

[56] Kranenbarg, Holt, van der Ham (2018), *supra nota* 52.

[57] Hill, M. D., Hennessy, J. L., Masters, J., Ranganathan, P., Turner, P. (2019). On the Spectre and Meltdown Processor Security Vulnerabilities. *IEEE Micro*, Vol. 39, No. 2, 9-19.

[58] Abu-Ghazaleh, N., Evtyushkin, D., Ponomarev, D. (2019). How the spectre and meltdown hacks really worked. *IEEE Spectrum*, Vol. 56, No. 3, 42-49.

vulnerability in chips used in Estonian ID-cards.[59] Those chips are produced by company Infineon. Infineon, however, is a supplier for the Estonian ID-card vendor Gemalto. This bug affected ID-cards that were issued since October 2014. In theory, if someone's private keys are stolen, it will give criminals the opportunity to manipulate votes in elections. Due to the ROCA problem, the Estonian authorities withdrew certificates for 760,000 ID-cards.[60] As a result, the Estonian Police and Border Guard Board filed a lawsuit against Gemalto, demanding a penalty of € 152 million from the company for breach of contract. Under the terms of the agreement concluded with Gemalto, the keys could not be generated outside of the chip installed on the ID-card. In 2019, the court satisfied the police demands. [61]

It should noted, that a lot of cybersecurity companies are officially contracted by governments to provide cybersecurity. And under contractual obligations they must report about their findings directly. Moreover, sometimes governments create money rewards for finding cybersecurity flaws (bug bounties).[62]

3.2.Responsibility of Internet Service Providers

Another conclusion that can be made form previous chapter is that the Internet is playing an extremely important role in today process of electronic elections. The current development of technology makes it possible to widely use the Internet in election campaigns. This may include informing voters about the progress of the election or conducting online voting. By virtue of its accessibility, the Internet also contributes to increasing public participation in the democratic control of transparency of the electoral process.[63] Thanks to the Internet, it has become cheaper and more convenient for candidates or political parties to promote their ideas and agendsas.

---

[59] Klinec, D., Matyas, V., Nemec, M., Sys, M., Svenda, P. (2017). The Return of Coppersmith's Attack: Practical Factorization of Widely Used RSA Moduli. *24th ACM-SIGSAC Conference on Computer and Communications Security ,* Dallas, 30 October - 03 November 2017. New York: ACM, 1631-1648.

[60] RIA (2018). *ROCA Vulnerability and eID: Lessons Learned.* Accessible: https://www.ria.ee/sites/default/files/content-editors/kuberturve/roca-vulnerability-and-eid-lessons-learned.pdf, 28 April 2019.

[61] Riigikohtu halduskolleegium 3-17-1151

[62] Kranenbarg, Holt, van der Ham (2018), *supra nota* 52.

[63] Jaber, A. (2013). *Broadband Internet and Political Behavior: Evidence from the United States.* Accessible: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2353549, 29 March 2019.

Furthermore, due to the wide spread of the Internet, politicians can reach a larger audience.[64] Moreover, elections held over the Internet should not be neglected. The Internet Voting continues to gain popularity. For example, in the last parliamentary elections of 2019 in Estonia, a record 247,232 votes were cast via the Internet, which is 43.8% of the total.[65] Internet Service Providers (ISP) own equipment and infrastructure that allows customers to access the Web.[66] However, does Internet Service Providers have obligation to preventing risks and ensure security of their networks? To answer that question the Directive on Security of Network and Information Systems must be analysed to understand whether ISPs can be considered as operators of essential services (OES). NIS Directive states that OES is a private entity which "provides a service which is essential for the maintenance of critical societal and/or economic activities; the provision of that service depends on network and information systems; and an incident affecting those systems would have significant disruptive effects on the provision of that service ".[67] According to this criteria ISPs can be considered as OES. NIS Directive requires Member States to ensure that OES has technical and organisational measures to litigate risks and to prevent and minimise the effects of the occurrences that can compromise the security of the network. Moreover, they must report this kind of incidents.[68] To summarise, if it's presumed that ISPs are essential services, than under NIS Directive they will have have certain legal responsibilities to secure their networks. However, the problem is that a decision to count ISPs as essential services is up to each Member State individually.

Additional responsibilities ISPs have under the Directive on Privacy and Electronic Communications, also known as ePrivacy Directive. The ePrivacy directive establishes rules for how internet providers must handle their users' data. One of the main responsibilities of providers is to ensure the security of networks and services. The ISP must take appropriate

---

[64] Council of Europe (2017). *Study on the use of internet in electoral campaigns*. Accessible: https://rm.coe.int/study-use-of-internet-in-electoral-campaigns/1680776163, 29 March 2019.

[65] Valimised: Voting results in detail 2019.

[66] Avingo K. (2016). Intermediary Liability for User-Generated Content in Europe. (Master's thesis). Tallinn University of Technology, Department of Law. Tallinn.

[67] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, OJ L 194, 19.7.2016, p. 1–30.

[68] *Ibid.*

measures to ensure the security of the services it provides. Moreover, if the security of the Provider was violated, which led to the loss or theft of personal data of users, then he must inform the national authority, and in certain cases, the subscriber or individual.[69] In addition, traffic and location data must be erased or made anonymous if they are no longer needed for communication or for billing. Subscribers must give their prior consent before they are addressed to spam. [70] Protection of personal data is important because it potentially can be used to create users psychometric profile to influence political position and voting.[71] Spam can be used as part of a political advertising campaign.[72] The main purpose of this directive is to protect personal data and the right to privacy of users. This directive strikes a balance between security and the protection of human rights, including data protection and confidentiality, which can be exploited to interfere with elections.[73]

Furthermore, it is important to understand whether ISP are liable to actively monitor and delete illegal materials. Those materials can include doxed private data that infringe various rights of privacy or disinformative material that misleads users, for example fake news.[74] According to Article 12 of Directive on electronic commerce, also known as E-Commerce Directive, ISP are generally not liable for content that flows through their networks.[75] Internet provider plays a

---

[69] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector, OJ L 201, 31.7.2002, p. 37–47.

[70] *Ibid.*

[71] Tactical Tech's Data and Politics team (2019). *Psychometric Profiling: Persuasion by personality*. Accessible: https://tacticaltech.org/media/Personal-Data-Political-Persuasion-How-it-works_print-friendly.pdf, 21 April 2019.

[72] Enright, B., Kanich, C., Kreibich C., Levchenko, K., Paxson, V., Savage, S., Voelker, G. M. S*pamcraft: An Inside Look At Spam Campaign Orchestration*; Accessible: http://www.icir.org/vern/papers/spamcraft.leet09.pdf, 13 April 2019.

[73] De Vries, R. (2017). *The European Legal Context: EU Data Protection LII*. Accessible: https://www.law.cornell.edu/wex/inbox/european_legal_context_privacy_directives, 15 April 2019.

[74] Hansen, Lim (2019), *supra nota* 45.

[75] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce')OJ L 178, 17.7.2000, p. 1–16.

passive role, acting as a simple carrier of data provided by third parties through its network.[76] Provider only purpose is to carry out the transmission of the information between third parties. There are several exception to that rule. The provider will be liable for the data flow if he starts the transmission of data, selects the receiver of the transmission or interferes with the transmitted data.[77] In addition, according to Article 15 of the Directive, Member States are not allowed to impose obligation on providers to monitor data that flows through their networks.[78] On one hand this can be a problematic issue, because if providers would actively monitor their networks, they can potentially fight disinformation, doxing and fake news more efficiently. On the other hand, some experts say that this restriction is reasonable, since it would be impossible for ISPs to actually provide their services with such obligation implemented.[79] However, second paragraph of Article 13 imposes a duty on ISP to report to authorities an alleged illegal activities.[80]

3.3.Responsibility of software and hardware developers

Another issue that needs to be addressed is legal responsibility of software and hardware developers whose products play essential role in the elections. For example, manufacturers of voting equipment, developers of voting software or more general creators of operating systems (Windows, MacOS). Of course, if company is contracted to produce software or hardware for election they have certain contractual obligations to ensure the security of their products. For example, company Scytl, which provides electronic voting systems for number of EU member states, ensures the security and verifiability of their systems.[81] However, what is more important to understand is whether developers and manufactures have some sort of cybersecurity standards that they need to have in their products? In the 2019 EU Cybersecurity Act the Commission

---

[76] Baistrocchi P. (2003). *Liability of Intermediary Service Providers in the EU Directive on Electronic Commerce*. Accessible: https://digitalcommons.law.scu.edu/cgi/viewcontent.cgi?article=1315&context=chtlj, 15 April 2019.

[77] Kuczerawy, A. (2015). Intermediary liability & freedom of expression: Recent developments in the EU notice & action initiative. *Computer Law & Security Review*,Vol. 31, No. 1, 46-56.

[78] E-Commerce Directive.

[79] Baistrocchi (2003), *supra nota* 76.

[80] E-Commerce Directive.

[81] Scytl (2019). S*ecure and Fully Verifiability Online Voting.* Accessible*:* https://www.scytl.com/en/resource/secure-fully-verifiability-online-voting, 16 April 2019.

proposes the creation of EU cybersecurity certification framework for Information Communications Technology products. This certification would ensure the certified products or services comply with certain cybersecurity requirements.[82] However, that certification is currently voluntary, but Industry, Research and Energy committee indicated that potentially for specific areas this certification would be made mandatory.[83] Moreover, some experts propose risk-based test for Internet of Things to obtain security label.[84] The proposed assessment idea is an implementation of risk-based safety assessment and testing methods introduced by the European Telecommunications Standards Institute which are based on ISO 31000 and ISO 29119, and are adapted to the Internet of Things environment.[85]

Furthermore, another problem that arises is a discussion how the Product Liability Directive applies to software. The adoption of the Product Liability Directive took place in 1985 and since then the Directive has remained unchanged.[86] Only in 1999, it was amended so agricultural products would fall within the definition of a product.[87] Because of it's age Directive does not directly mentions software. Therefore, to understand whether the Directive applies to software, it needs to be determined whether software is a product or a service.[88] The difference is important because products and services have different liability regimes. There is no consensus on that

---

[82] European Parliament legislative resolution of 12 March 2019 on the proposal for a regulation of the European Parliament and of the Council on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification ("Cybersecurity Act''); http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P8-TA-2019-0151+0+DOC+XML+V0//EN&language=EN

[83] European Parliament (2019). *ENISA and new EU Cybersecurity Act Report.* Accessible: http://www.europarl.europa.eu/RegData/etudes/ATAG/2019/625160/EPRS_ATA(2019)625160_EN.pdf, 20 April 2019.

[84] Baldini, G., Hernández-Ramos, J.L., Matheu-García, S.N., Skarmeta A. F. (2019). Risk-based automated assessment and testing for the cybersecurity certification and labelling of IoT devices. *Computer Standards & Interfaces*, Vol. 62, 64-83.

[85] *Ibid.*

[86] Council Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products, Official Journal (OJ) L 210, 7.8.1985, 29–33.

[87] Directive 1999/34/EC of the European Parliament and of the Council of 10 May 1999 amending Council Directive 85/374/EEC on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products, OJ L 141, 4.6.1999, 20–21.

[88] Alheit, K. (2001). The Applicability of the EU Product Liability Directive to Software. *The Comparative and International Law Journal of Southern Africa*, Vol. 34, No. 2, 188–209.

issue among legal experts and this is an ongoing debate on this topic.[89] Some experts claim that because software is intangible it cannot be considered as a product.[90] However, most experts agree that the application can be considered as a product if it is sold on some sort of physical medium (Compact discs, for example) and it is evenly available for purchase to all customers.[91] However, cloud software and software which custom-designed for a specific client and meeting unique requirements are usually considered to be service.[92] When application qualifies as a service, responsibility for professional malpractice can be applied to the developer. Furthermore, programmer will only be responsible if he acted carelessly when compared to reasonable behaviour from specialist on similar field.[93] Therefore, to address this gap in mid-2019, the Commission will publish a guide to the Product Liability Directive and a report on broader implications.[94]

3.4.Responsibility of social medias

More indirect but nonetheless essential role in modern election play social networks. A great example of can social media be used to manipulate voters is recent Cambridge Analytica scandal. Company developed and used a special psychological test to collect data on users of social networks. For the completion of that test users were paid money. At the same time, the program requested information about the profiles of users and their friends (at that time, Facebook allowed third-party applications to collect such data). Cambridge Analytica argued that his test collects data exclusively for academic purposes to improve "microtargeting".[95] In fact, they sold data without the knowledge of users and used it to create psychologically targeted

---

[89] Vihul L. (2014). *The Liability of Software Manufacturers for Defective Products*. Accessible: https://ccdcoe.org/uploads/2018/10/TP_02.pdf, 25 April 2019.

[90] Alheit (2001), *supra nota* 88.

[91] Vihul (2014), supra nota 89.

[92] *Ibid.*

[93] *Ibid.*

[94] European Commission (2018). *Liability of defective products*. Accessible: https://ec.europa.eu/growth/single-market/goods/free-movement-sectors/liability-defective-products_en, 25 April 2019.

[95] Andrews, L. E. (2018). *The Science Behind Cambridge Analytica: Does Psychological Profiling Work?* Accessible: https://www.gsb.stanford.edu/insights/science-behind-cambridge-analytica-does-psychological-profiling-work, 26 April 2019.

political advertisements. When the research was done, company had psychological profiles on 87 million users of Facebook, although the test itself passed only 350 thousand people.[96] Those profiles where later used to support Donald Trumps presidential campaign via microtargeting in Facebook.[97]

This scandal happened just few weeks prior to implementation of the EU General Data Protection Regulation (GDPR). According to GDPR now social networks should make the policy of collecting and storing personal data more transparent. Any information about the purposes, methods and amounts of personal data processing should be as accessible and simple as possible.[98] Moreover, data should be collected and used exclusively for the purposes stated by the company. It is also impossible to collect personal data in a larger volume than is necessary for processing purposes.[99] Personal data that is inaccurate must be deleted or corrected at the request of the user. Furthermore, personal data should be stored in a form that allows you to identify data subjects for a period not exceeding that necessary for processing purposes. In addition, when processing user data, companies are required to ensure the protection of personal data from unauthorised or unlawful processing, destruction and damage.[100] GDPR significantly expanded user rights. Users now have the right to get information from organizations about their data and how they are used (for example, whether they are passed on to third parties) in a simple and accessible manner. Also, the regulation gives the right to prohibit the use of personal data, correct incorrect information and delete them completely from the Internet.[101] GDPR is essential in securing certain level of users privacy in social medias.

---

[96] Isaak, J., Hanna, M. J. (2018). User Data Privacy: Facebook, Cambridge Analytica, and Privacy Protection. *Computer*, Vol. 51, No. 8, 56-59.

[97] Ward, K. (2018). Social networks, the 2016 US presidential election, and Kantian ethics: applying the categorical imperative to Cambridge Analytica's behavioral microtargeting. *Journal of Media Ethics*, Vol. 33, No. 3, 133-148.

[98] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 4.5.2016, p. 1–88.

[99] *Ibid.*

[100] *Ibid.*

[101] *Ibid.*

Furthermore, the Commission in their Action Plan against Disinformation takes some steps to fight the spread of fake news on social medias. One of their ideas is that Member States should support the development of groups that will check truthfulness of news campaigns on social medias and expose it if they were fake.[102] In addition in September 2018 Code of Practice on Disinformation was adopted so social media industry can self regulate standards to fight disinformation. Signatures of this Code commit to clearly distinguish and disclose political advertisements, to support independent groups that fight fake news, to give priority to relevant and trustworthy news in search and feeds, to invest in tools that will allow users to have multiple-point perspective on topics of public interest and to invest in tools that will automatically warn users when they encounter news that is probably fake.[103] In addition, companies must put transparent policies concerning identity theft and rules on use of automated bots on their platforms.[104]

Amendment to Audiovisual Media Services Directive were adopted. First of all, now the Directive includes video sharing platforms and audio-visual data shared on social medias.[105] Secondly, such services now must ensure that their platforms don't have hatred materials that promotes violence based on race, sex, religion or nationality.[106] Thirdly, the video sharing platform provider will now comply with the AVMS Directive, even if it is located outside the

---

[102] European Commission (2018). *Action Plan against Disinformation*. Accessible: https://ec.europa.eu/commission/sites/beta-political/files/eu-communication-disinformation-euco-05122018_en.pdf, 28 April 2019.

[103] European Commission (2018). *EU Code of Practice on Disinformation.* Accessible: https://www.hadopi.fr/sites/default/files/sites/default/files/ckeditor_files/1CodeofPracticeonDisinformation.pdf, 28 April 2019.

[104] *ibid*

[105] Directive (EU) 2018/1808 of the European Parliament and of the Council of 14 November 2018 amending Directive 2010/13/EU on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (Audiovisual Media Services Directive) in view of changing market realities, OJ L 303, 28.11.2018, p. 69–92.

[106] *Ibid.*

EU, if another organisation from the corporate group is located within the EU.[107] [108] Moreover, in 2019 EU legislators want to implement rule that will oblige Social Medias to take active measures to find and delete extremist content within the 1 hour frame on their platforms. However, this legislation has a number of opponents.[109] For example, The Center for Democracy and Technology has published an open letter to the European Parliament, which states that the initiative will force Internet platforms to introduce untested technologies to limit online expression.[110]

Another problem is the debatable nature of social medias under eCommerce Directive. Initially, the concept of hosting providers was interpreted as a party who rented a web server space so that its customers could create their own websites. However, now the host concept includes a company that controls the website, which allows third parties to download or publish materials. Because of this, social networks are commonly referred as hosts.[111] Hosts can be active or passive. Passive hosts sole role is to provide access to data to their users.[112] Therefore, according to E-Commerce directive, hosts fall under the liability exemptions only in case when service they provide are of passive nature and purely automatic. Thus, it's being argued that if host looses it's neutrality by actively indexing, organising, linking adverts to user posted materials, blocking or deleting undesired data, even if host does that automatically, he will be considered as a active host and, therefore, will not have host protection under E-Commerce Directive.[113]

---

[107] *Ibid.*

[108] Laskowski, K. (2019). *Changes To The Audiovisual Media Services Directive – What Does It Mean For The Media Market?* Accessible: http://www.mondaq.com/x/795192/broadcasting+film+television+radio/Changes+To+The+Audiovisual+Media+Services+Directive+What+Does+It+Mean+For+The+Media+Market, 30 April 2019.

[109] EU Commission (2018). *Draft for a Proposal for a Regulation of the European Parliament and of the Council on Preventing the Dissemination of Terrorist Content Online*. Accessible: https://ec.europa.eu/commission/sites/beta-political/files/soteu2018-preventing-terrorist-content-online-regulation-640_en.pdf, 30 April 2019.

[110] Civil Society open letter, e-mail, 4 February 2019.

[111] Avingo (2016), *supra nota* 66.

[112] Van der Sloot, B. (2015) Welcome to the Jungle: the Liability of Internet Intermediaries for Privacy Violations in Europe. *Journal of Intellectual Property, Information Technology and Electronic Commerce Law,* Vol. 3, No. 3, 211-228.

[113] *Ibid.*

However, Advocate General Jääskinen in his opinion on the Case C-324/09 L'Oreal v eBay argued, that host providers will always have some sort of interference with their users.[114] His opinion was confirmed by CJEU as they interpreted neutrality as a lack of knowledge, which makes hosts fall under protection from liability, even if they play active role.[115] Therefore, with accordance with E-commerce directive host provider will be liable for the materials stored on their platforms only in cases when they know about illegal nature of materials or they become aware of materials illegal nature and they don't to remove it or disable access to it.

However, the problem may arise in relation to hosts liability about fake news or other defamatory materials generated by its users. The question is is whether those platforms should be considered as a host or a publisher. Different opinions on this issue were given by different national courts of EU member states: French court assessed that MySpace website is publisher and is liable for it's users content.[116] In opposite UK High Court in Kaschke v Hilton case ruled that political website-blog is not liable for it's users defamatory article, even though host was active and edited parts of a website.[117] However, nowadays the common approach to that issue is if platforms with user posted materials will be protected from liability for slander materials if they in no way involved in publishing such materials.[118] However, they can be liable if they fail to delete such content after complaint.[119]

It should be noted that social medias are also used to share and promote disinformation and propaganda via fake news. However, private companies took initiative in combating fake news on their platforms. For example, Facebook in cooperation with third-party experts in visual

---

[114] Judgment of 12 July 2011., L'Oréal SA and Others v eBay International AG and Others, C-324/09, ECLI:EU:C:2011:474.

[115] Van Eecke, P. (2011). Online service providers and liability: plea for balanced approach. *Common Market Law Review*, Vol. 48, No. 5, 1455-1502.

[116] Avingo (2016), *supra nota* 66.

[117] *Kaschke v Hilton* [2010] EWHC 690 (England & Wales High Court, Queen's Bench Division).

[118] *Ibid*

[119] Griffiths, R. (2013). *Normality restored: website hosts may again be liable for defamatory user generated content.* Accessible: https://www.fieldfisher.com/publications/2013/02/normality-restored-website-hosts-may-again-be-liable-for-defamatory-user-generated-content, 30 April 2019.

verification, will mark images that have been posted on Facebook in a misleading context.[120] Moreover, company started to use machine learning to identify copies of news that were already proven to be fake.[121] In addition, they also created a machine learning tool that uses various interaction signals, including feedback from users on Facebook, to identify potentially fake content.

[120] Shaban, H. (2018). *Facebook expands its fact-checking tools but says its work 'will never be finished'*. Accessible: https://www.washingtonpost.com/news/the-switch/wp/2018/06/21/facebook-expands-its-fact-checking-tools-but-says-its-work-will-never-be-finished/?utm_term=.c794ca57ebe6, 30 April 2019.

[121] Ikigai Law (2019) *How are social media platforms tackling the "fake news" problem?* Accessilbe: https://www.ikigailaw.com/how-are-social-media-platforms-tackling-the-fake-news-problem/#acceptLicense, 30 April 2019.

CONCLUSION

Modern technologies penetrate all spheres of society. The election process does not stand aside either. Electronic, Internet technologies work in many countries and have a high potential at various stages of the elections. However, at the same time, they jeopardise their integrity.

The aim of the thesis was to critically assess the legal responsibility of private sector actors to cooperate with sate authorities in order to do identify problematic areas to prevent future interventions. However, to properly understand context of cyber-interference with election it was necessary to determine main differences between regular cyber-attacks and cyber-meddling with elections. The cyber-attacks on elections differs in The main distinguishing features of hacking cyber elections are the motivation, nature and targets. In differ to regular cyber-assaults, cyber-cyber-meddling with elections purpose is not to monetary gain, but to change the political scene. Moreover, unique feature of cyber-attacks on elections is that it incorporates different methods of informational warfare. Furthermore, to achieve its goal cyber-cyber-interference with elections targets voters, oppose to regular cyber-crimes who usually targets private companies. Cyber-attacks on elections posses a direct threat to democracy and sovereignty. Moreover, attacked states legally has no option of using force to remedy the attacks.

Several actors can be a potential threats to election process. They can be states and their interagency offices. However, they rarely conduct their operations directly. Common practise is to use different hacktivist groups as a proxy. The most prominent examples of such groups are APT28 and APT29. They use different methods to conduct their attacks. One of the methods is informational campaigns. Promenent way of conducting informational campaigns is to create fake news and spread them through social medias. Examples of such campings occurred on 2017 German Federal Election, 2016 Brexit Referendum and 2016 Italian local elections. It is important to emphasis, that privately owned social medias played a huge role in above mentioned informational campaigns. Moreover, interference can be done via hacking. This can be done by exploiting software or hardware vulnerabilities. In addition, hackers can use malware to infect computers. Furthermore, above mentioned techniques can be used in combination — first steal data via hacking and then use stone data as a part of informational camping. This

method is called doxing. Incidents of doxing occurred during 2016 US President Elections and 2017 French President Elections. The conclusion can be drown, that private sector actors play prominent role in modern election process. They can develop software or hardware for voting, own social medias or simply provide access to the Internet.

To solve problem of disclosure of information about vulnerabilities ENISA introduced a procedure called CVD. In this procedure finder of the flaw will disclose information about it via intermediate actor. who ensures confidentiality and security of this information. However, this procedure might be to complicated for companies to implement. Moreover, this procedure is difficult to implement for supply chains, where multiple vendors are involved. Furthermore, a number of private companies use “bug bounty” process, where vendors work directly with finders without middle man in between them. Nevertheless, some companies implemented CVD procedure in their practise.

The ISPs play major role in modern elections. ISPs might have obligations under NIS Directive to take measures to litigate risks, prevent and minimise effects of attacks on their networks and to report if such attacks did happened. The problem is that ISP will fall under NIS obligations only if it would be considered an OES and this is a decision of each Member State. Moreover, ISPs have obligations under ePrivacy Directive. They must take appropriate measures to secure their networks, inform if security was compromised, delete or make unanimous unneeded users data and ask consent to sent spam. In addition, under eCommerce Directive ISPs don’t have to actually monitor their networks and they are not liable for content that is being transmitted. However, they have to report alleged illegal activities.

For software and hardware developers the Commission introduced cybersecurity certification framework for Information Communications Technology products. This certification would act as a stamp of cybersecurity quality. However, right now this certification is completely voluntary. Moreover, there is a debate on whether software would qualify asa product or as a service.Majority of legal experts believe that program can be viewed as a product if it is commonly available and has a physical medium.

Social medias played major role in the process of interference with recent elections. Most prominent example is Cambridge Analytica scandal, which created users profiles based on their Facebook data to later aid Donald Trumps presidential campaign. Soon after the scandal GDPR was implemented, which obliges social networks to make their rules on collecting and usage of users data clear. Moreover, users rights in regard to their personal data were drastically increased. Furthermore, the Commission introduced an Action plan to combat disinformation. Now Member States should support groups that can expose and check the validity of news articles. In addition self-regulatory Code of Practise for social networks was adopted. Social medias commit to disclose political advertisements, provide aid for groups that fight fake news, give priority to verified news articles in users feed, spend money to create tools that will give users different perspectives on topics of public interest and warn users when they encounter news that can be fake. AVMS Directive was made more modern, now it covers videosharing platforms. Problematic issue is whether social medias are active to passive hosts under eCommerce Directive. This differences drastically changes liability of social networks. CJEU said host provider can be potentially liable for materials on their websites only if they know about nature of data and they do not ban or delete it, no matter whether host passive or active. Another debate is role of social medias in relation to defamatory nature of user-posted content. Nowadays, the common approach is social medias are not liable for user-generated materials if they took no part in its creation and deleted it after notification. Moreover, a number of companies take steps on their own to battle fake news. For example, Facebook invested in machine learning tool that will automatically flag news that were proven to be disinformative.

To conclude, liability regime for private companies when their platforms were used for interference with elections is unclear and can be hard to understand. However, EU takes active steps to modernise it’s legislation and to cover gaps in exiting laws. For example to fix the gap in liability of software developers under t Product Liability Directive, the Commission is planning to publish a guide on that issue. Moreover, EU plans to strengthen responsibility for social medias — they will be obliged to delete extremist content within 1 hour.

LIST OF REFERENCES

Scientific books:

1.Middleton, B. (2017). – *History of Cyber Security Attacks: 1980 to Present*. Vol. 74. Katy: Secur Refuge LLC, p. 33.

2. Norman, T. (2018). – *Electronic Access Control*. 2nd ed. Oxford: Butterworth Heinemann.

Scientific articles:

1. Abu-Ghazaleh, N., Evtyushkin, D., Ponomarev, D. (2019). How the spectre and meltdown hacks really worked. *IEEE Spectrum*, Vol. 56, No. 3, 42-49.
2. Acerbi, A. (2019). Cognitive attraction and online misinformation. – P*algrave Communications,* Vol. 5, No. 1.
3. Alheit, K. (2001). The Applicability of the EU Product Liability Directive to Software. *The Comparative and International Law Journal of Southern Africa*, Vol. 34, No. 2, 188–209.
4. Baldini, G., Hernández-Ramos, J.L., Matheu-García, S.N., Skarmeta A. F. (2019). Risk-based automated assessment and testing for the cybersecurity certification and labelling of IoT devices. *Computer Standards & Interfaces*, Vol. 62, 64-83.
5. Björnstjern, B. (2018). Fake News and International Law. – *European Journal of International Law*, Vol. 29, No. 4, 1357–1376.
6. Blinderman, E. (2017). Hidden by Sovereign Shadows: Improving the Domestic Framework for Deterring State-Sponsored Cybercrime. – *Vanderbilt Journal of Transnational Law*, Vol. 50, 889-931.
7. Boyd-Barrett, O. (2019). Fake news and 'RussiaGate' discourses: Propaganda in the post-truth era. – *Journalism*, Vol. 20, No. 1, 87–91.
8. Delmas, C. (2018). Is Hacktivism the New Civil Disobedience? – *Raisons politiques*, Vol. 69, No. 1, 63-81.
9. Hansen, I., Lim, D. (2019). Doxing democracy: influencing elections via cyber voter interference. – *Contemporary Politics*, Vol. 25, No. 2, 150-171.
10. Hill, M. D., Hennessy, J. L., Masters, J., Ranganathan, P., Turner, P. (2019). On the Spectre and Meltdown Processor Security Vulnerabilities. *IEEE Micro*, Vol. 39, No. 2, 9-19.
11. Isaak, J., Hanna, M. J. (2018). User Data Privacy: Facebook, Cambridge Analytica, and Privacy Protection. *Computer*, Vol. 51, No. 8, 56-59.
12. Jensen, B., Maness R., Valeriano, B. (2019). Fancy bears and digital trolls: Cyber strategy with a Russian twist, Journal of Strategic Studies. – *Journal of Strategic Studies*, Vol. 42, No. 2, 212-234.
13. Klinec, D., Matyas, V., Nemec, M., Sys, M., Svenda, P. (2017). The Return of Coppersmith's Attack: Practical Factorization of Widely Used RSA Moduli. *24th ACM-SIGSAC Conference on Computer and Communications Security ,* Dallas, 30 October - 03 November 2017. New York: ACM, 1631-1648.

14.Kranenbarg, M.W., Holt, T.J., van der Ham, J. (2018). Don't shoot the messenger! A criminological and computer science perspective on coordinated vulnerability disclosure. – *Crime Science*, Vol. 7, No. 16.
15.Kuczerawy, A. (2015). Intermediary liability & freedom of expression: Recent developments in the EU notice & action initiative. *Computer Law & Security Review*,Vol. 31, No. 1, 46-56.
16.Mansfield-Devine, S. (2017). Editorial. – *Computer Fraud and Security Series*, Vol. 2017, No. 5, 2.
17.Nazario, J. (2009). Politically motivated denial of service attacks. – C*ryptology and Information Security Series*, Vol. 3, 163-181.
18.Ohlin, D. (2017). Did Russian Cyber-Interference in the 2016 Election Violate International Law? – *Cornell Legal Studies Research Paper,* No.17-15.
19.Travaglino, G. A. (2019). Support for Anonymous as vicarious dissent: Testing the social banditry framework. – *Group Processes & Intergroup Relations*, Vol. 22, No. 2, 163–181.
20.Van De Velde, J. (2017). *The Law of Cyber Interference in Elections*. Accessible: https://ssrn.com/abstract=3043828, 20 March 2019.
21.Van Eecke, P. (2011). Online service providers and liability: plea for balanced approach. *Common Market Law Review*, Vol. 48, No. 5, 1455-1502.
22.Ward, K. (2018). Social networks, the 2016 US presidential election, and Kantian ethics: applying the categorical imperative to Cambridge Analytica's behavioral microtargeting. *Journal of Media Ethics*, Vol. 33, No. 3, 133-148.

Estonian legislation:

1. Riigikogu Election Act. RT I 2002, 57, 355.

EU and international legislation:

1. Council Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products, Official Journal (OJ) L 210, 7.8.1985, 29–33.
2. Directive 1999/34/EC of the European Parliament and of the Council of 10 May 1999 amending Council Directive 85/374/EEC on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products, OJ L 141, 4.6.1999, 20–21.
3. Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce')OJ L 178, 17.7.2000, p. 1–16.
4. Directive (EU) 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector, OJ L 201, 31.7.2002, p. 37–47.

5. Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, OJ L 194, 19.7.2016, p. 1–30.
6. Directive (EU) 2018/1808 of the European Parliament and of the Council of 14 November 2018 amending Directive 2010/13/EU on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (Audiovisual Media Services Directive) in view of changing market realities, OJ L 303, 28.11.2018, p. 69–92.
7. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 4.5.2016, p. 1–88.

Estonian court decisions:

1. Riigikohtu halduskolleegium 3-17-1151

Other court decisions:

1. BVerfG, Judgment of the Second Senate of 03 March 2009 - 2 BvC 3/07 - paras. (1-166).
2. Columbia District Court, 1:18-cr-00215-ABJ, *U.S. v. Viktor Borisovich Netyksho, et al.*
3. Judgment of 12 July 2011., L'Oréal SA and Others v eBay International AG and Others, C-324/09, ECLI:EU:C:2011:474.
4. *Kaschke v Hilton* [2010] EWHC 690 (England & Wales High Court, Queen's Bench Division).

Other sources:

1. Alperovitch, D. (2016). *Bears in the Midst: Intrusion into the Democratic National Committee.* Accessible: www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/, 18 March 2019.
2. Andrews, L. E. (2018). *The Science Behind Cambridge Analytica: Does Psychological Profiling Work?* Accessible: https://www.gsb.stanford.edu/insights/science-behind-cambridge-analytica-does-psychological-profiling-work, 26 April 2019.
3. Avingo K. (2016). Intermediary Liability for User-Generated Content in Europe. (Master's thesis). Tallinn University of Technology, Department of Law. Tallinn.
4. BBC (2016). Russia 'was behind German parliament hack'. – *BBC,* 13 May 2016, Accessible https://www.bbc.co.uk/news/technology-36284447, 10 March 2019.
5. Baistrocchi P. (2003). *Liability of Intermediary Service Providers in the EU Directive on Electronic Commerce*. Accessible: https://digitalcommons.law.scu.edu/cgi/viewcontent.cgi?article=1315&context=chtlj, 15 April 2019.

6. Buckland, B., Schreier, F., Winkler, T. (2015). *Democratic Governance Challenges of Cyber Security.* Accessible: https://www.dcaf.ch/sites/default/files/publications/documents/CyberPaper_3.6.pdf, 12 March 2019.
7. Carr, N., Dunwoody, M., Leathery, J., Matonis, M., Thompson, A., Withnell, B. (2018). *Not So Cozy: An Uncomfortable Examination of a Suspected APT29 Phishing Campaign.* Accessible: https://www.ttu.ee/public/m/majandusteaduskond/uusJuhend_2018_08_18_EN_veebilehele.pdf, 20 March 2019.
8. Civil Society open letter, e-mail, 4 February 2019.
9. Chaintreau, A., Gabielkov, M., Ramachandran, A., Legout, A. (2016). *Social Clicks: What and Who Gets Read on Twitter?* Accessible: https://hal.inria.fr/hal-01281190/document, 23 March 2019.
10. Council of Europe (2017). *Study on the use of internet in electoral campaigns.* Accessible: https://rm.coe.int/study-use-of-internet-in-electoral-campaigns/1680776163, 29 March 2019.
11. De Vries, R. (2017). *The European Legal Context: EU Data Protection LII*. Accessible: https://www.law.cornell.edu/wex/inbox/european_legal_context_privacy_directives, 15 April 2019.
12. Ee, S., Galante, L. (2018). *Defining Russian Election Interference: An Analysis of Select 2014 to 2018 Cyber Enabled Incidents.* Accessible: https://www.atlanticcouncil.org/images/publications/Defining_Russian_Election_Interference_web.pdf, 24 March 2019.
13. ENISA (2018). *Economics of vulnerability disclosure* (2018). Accessible: https://www.enisa.europa.eu/publications/economics-of-vulnerability-disclosure, 28 March 2019.
14. ENISA (2018). *Good Practice Guide on Vulnerability Disclosure: from challenges to recommendations*. Accessible: https://www.enisa.europa.eu/publications/vulnerability-disclosure, 29 March 2019.
15. ENISA. *Risk Management Glossary*. Accesible: https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/glossary#G52, 27 Match 2019.
16. Enright, B., Kanich, C., Kreibich C., Levchenko, K., Paxson, V., Savage, S., Voelker, G. M. S*pamcraft: An Inside Look At Spam Campaign Orchestration*; Accessible: http://www.icir.org/vern/papers/spamcraft.leet09.pdf, 13 April 2019.
17. ESET (2016). En Route with Sednit, Part 1: Approaching the Target. Accessible: https://www.welivesecurity.com/wp-content/uploads/2016/10/eset-sednit-part1.pdf, 20 March 2019.
18. European Commission (2018). *Action Plan against Disinformation*. Accessible: https://ec.europa.eu/commission/sites/beta-political/files/eu-communication-disinformation-euco-05122018_en.pdf, 28 April 2019.
19. European Commission (2018). *EU Code of Practice on Disinformation.* Accessible: https://www.hadopi.fr/sites/default/files/sites/default/files/ckeditor_files/1CodeofPracticeonDisinformation.pdf, 28 April 2019.
20. European Commission (2018). *Liability of defective products*. Accessible: https://ec.europa.eu/growth/single-market/goods/free-movement-sectors/liability-defective-products_en, 25 April 2019.

21. European Parliament (2019). *ENISA and new EU Cybersecurity Act Report.* Accessible: http://www.europarl.europa.eu/RegData/etudes/ATAG/2019/625160/EPRS_ATA(2019)625160_EN.pdf, 20 April 2019.
22. FireEye APT28: At the center of the storm Report 2017.
23. FireEye APT28: A Window Into Russia's Cyber Espionage Operations, 2016 Report, p. 23.
24. Gogolinkski, J., Hacquebord F., Huq N., Kharouni L., Mercês F., Otis D., Remorin A. (2014). *Operation Pawn Storm: Using Decoys to Evade Detection.* Accessible: https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/white-papers/wp-operation-pawn-storm.pdf, 16 March 2019.
25. Griffiths, R. (2013). *Normality restored: website hosts may again be liable for defamatory user generated content.* Accessible: https://www.fieldfisher.com/publications/2013/02/normality-restored-website-hosts-may-again-be-liable-for-defamatory-user-generated-content, 30 April 2019.
26. Heiberg, S., Parsovs, A., Willemson, J. (2015). *Log Analysis of Estonian Internet Voting 2013 – 2015.* Accessible: https://eprint.iacr.org/2015/1211, 27 March 2019.
27. Ikigai Law (2019) *How are social media platforms tackling the "fake news" problem?* Accessilbe: https://www.ikigailaw.com/how-are-social-media-platforms-tackling-the-fake-news-problem/#acceptLicense, 30 April 2019.
28. Jaber, A. (2013). *Broadband Internet and Political Behavior: Evidence from the United States.* Accessible: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2353549, 29 March 2019.
29. Laskowski, K. (2019). *Changes To The Audiovisual Media Services Directive – What Does It Mean For The Media Market?* Accessible: http://www.mondaq.com/x/795192/broadcasting+film+television+radio/Changes+To+The+Audiovisual+Media+Services+Directive+What+Does+It+Mean+For+The+Media+Market, 30 April 2019.
30. Lucian, K. (2016). *Russia having success in hybrid war against Germany.* Accessible: http://blogs.reuters.com/great-debate/2016/02/07/russia-having-success-in-hybrid-war-against-germany/, 24 March 2019.
31. Microsoft Security Response Center. *Coordinated Vulnerability Disclosure*. Accessible: https://www.microsoft.com/en-us/msrc/cvd, 29 March 2019.
32. Modderkolk, H. (2018). Dutch agencies provide crucial intel about Russia's interference in US-elections. – *De Volkskrant, 25* March 2018, Accessible https://www.volkskrant.nl/wetenschap/dutch-agencies-provide-crucial-intel-about-russia-s-interference-in-us-elections~b4f8111b/, 18 March 2019.
33. Muller, R. (2019). *Report On The Investigation Into Russian Interference In The 2016 Presidential Election.* Accessible: https://www.justsecurity.org/wp-content/uploads/2019/04/Muellller-Report-Redacted-Vol-II-Released-04.18.2019-Word-Searchable.-Reduced-Size.pdf, 2 May 2019.
34. Radware Global Application & Network Security Report 2018, p. 4.
35. Schreier, F. (2015). *On Cyberwarfare.* Accessible: https://www.gao.gov/assets/130/122454.pdf, 12 March 2019.
36. Scott, M. (2017). *Facebook says Russian groups spent less than £1 on Brexit advertising.* Accessible: https://www.politico.eu/article/facebook-brexit-russia-advertising-referendum-internet-research-agency/, 24 March 2019.

37. Scytl (2019). S*ecure and Fully Verifiability Online Voting.* Accessible*:* https://www.scytl.com/en/resource/secure-fully-verifiability-online-voting, 16 April 2019.
38. Shaban, H. (2018). *Facebook expands its fact-checking tools but says its work 'will never be finished'*. Accessible: https://www.washingtonpost.com/news/the-switch/wp/2018/06/21/facebook-expands-its-fact-checking-tools-but-says-its-work-will-never-be-finished/?utm_term=.c794ca57ebe6, 30 April 2019.
39. Software Vulnerability Disclosure in Europe: Technology, Policies and Legal Challenges, Report of a CEPS Task Force 2018.
40. Tactical Tech's Data and Politics team (2019). *Psychometric Profiling: Persuasion by personality*. Accessible: https://tacticaltech.org/media/Personal-Data-Political-Persuasion-How-it-works_print-friendly.pdf, 21 April 2019.
41. The Baltic Times (2017). *Lithuania: President says online voting wouldn't ensure secrecy and security.* Accessible: https://thevotingnews.com/international/europe/lithuania/ , 27 March 2019.
42. TrendMicro Two Years of Pawn Storm Report 2017, pp. 4-7.
43. RIA (2018). *ROCA Vulnerability and eID: Lessons Learned.* Accessible: https://www.ria.ee/sites/default/files/content-editors/kuberturve/roca-vulnerability-and-eid-lessons-learned.pdf, 28 April 2019.
44. Valisluureamet (2019). *International Security and Estonia.* Accessible: https://www.valisluureamet.ee/pdf/raport-2018-ENG-web.pdf, 16 March 2019.
45. Vihul L. (2014). *The Liability of Software Manufacturers for Defective Products*. Accessible: https://ccdcoe.org/uploads/2018/10/TP_02.pdf, 25 April 2019.
46. Wilshusen, G. (2009). *Cyber Threats and Vulnerabilities Place Federal Systems at Risk.* Accessible: https://www.files.ethz.ch/isn/144868/OnCyberwarfare-Schreier.pdf, 15 March 2019.