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

Minttu Tasanko

ACDC – HIGHWAY TO HELL OR A LEGITIMATE SELF-DEFENSE IN CYBERSPACE?

Bachelor's thesis
Programme: Law, Specialization: EU and International Law

Supervisor: Agnes Kasper, PhD

Tallinn 2018

I declare that I have compiled the paper independently
And all works, important standpoints and data by other authors
Have been properly referenced, and the same paper
Has not been previously presented for grading.
The documents length is 7588 words from the introduction to the end of conclusion.

Minttu Tasanko ……

(signature, date)

Student code: a156118
Student email address: minttu.tasanko@gmail.com

Supervisor: Agner Kasper, PhD:
The paper conforms to the requirements in force

……

(signature, date)

Chairman of the Defense Committee:
Permitted to defense

……

(name, signature, date)

TABLE OF CONTENTS

LIST OF ABBREVIATIONS

ACD	Active cyber defense
ACDC	Active Cyber Defense Certainty Act
GDPR	General Data Protection Regulation
NATO	North Atlantic Treaty Organization
IP address	Internet Protocol address
IBM	International Business Machines Corporation
CFAA	Computer Fraud and Abuse Act
DDoS	Distributed Denial-of-Service
ECHR	European Convention for the Protection of Human Rights and Fundamental Freedoms
NSA	National Security Agency
ECtHR	European Court of Human Rights
TFEU	Treaty on the Functioning of the European Union
CJEU	Court of Justice of the European Union

ABSTRACT

This thesis examines the legalities of one of the less regulated fields of cybersecurity, active cyber defense (ACD), focusing on its implications on privacy laws. It describes the methods and objectives of ACD, and takes the recently introduced US bill, Active Cyber Defense Certainty Act (ACDC), as a real-life example of how this field may be regulated. Public and expert views both in support of and against legalizing of ACD will be discussed. By analyzing the content of the ACDC and setting it against privacy and data protection rules in the European Union, the thesis presents some of the weak points of the bill as well as the apparent conflict between these two.

Keywords: Cybersecurity, active cyber defense, privacy and data protection

INTRODUCTION

In the digitalized world that we live in, computer technology provides great convenience and benefit in our everyday lives, all the way from maintaining our social networks to taking care of our finances. Convenience is not all it provides, however: it also functions as a tool for new kinds of crime, such as denial-of-service attacks and data breaches, as well as new forms of traditional crime, such as theft and child sexual exploitation committed online. In many legal systems throughout the world there are provisions of self-defense against traditional crimes where there is a threat to your life, health or property. But, despite of the rapid digitalization of crime, there is still a lack of such provisions against cybercrime. Cybersecurity itself is a huge business and one of the most important areas of national security schemes, but active cyber defense, that is, taking "proactive measures … to defend against malicious cyber activities", [1] is – albeit a much discussed – still very little regulated branch of cybersecurity.

In this paper, the author will look into what would be the implications of legalizing active cyber defense, especially in regard to privacy laws. Specifically, if enforced, how would a US law allowing active cyber defense clash with the EU privacy and data protection laws in cases where the attacked party is located in the US and the attacker (or the servers they use) in the EU? Also, what are the rights of innocent by-standers in the event of hacking back? The qualitative methodology used in this thesis is a mix of traditional legal dogmatic methods and comparative methods. The study is presented with the concrete examples of the Active Cyber Defense Certainty bill (ACDC) in the US and privacy laws, especially the General Data Protection Regulation (GDPR), in the EU. The author will describe the content of both the ACDC and the GDPR as well as other relevant acts, and analyze active cyber defense and the ACDC in the light of existing literature and other legislation, finally putting them against and comparing them to EU privacy and data protection laws. Concrete hypothetical examples are used to demonstrate the possible real-life implications of legalized active cyber defense.

The thesis will start with the defining and describing of active cyber defense and its most important objectives, that is, attributing the attacker and retrieving the stolen data. Especially the difficulties

[1] Heinl, C. H. (2014). Artificial (Intelligent) Agents and Active Cyber Defence: Policy Implications. – *6th International Conference On Cyber Conflict*, 3-6 June 2014, Tallinn. (Ed.) P. Brangetto, M. Maybaum, J. Stinissen. Tallinn: NATO CCD COE Publications, 53-66, p 58.

of attributing and the mistaken concept of "retrieving" digital information are discussed. The main cybercrime law of the US, the Computer Fraud and Abuse Act, is introduced in this chapter, and a brief look is taken into the opinions and knowledge of US companies on the issue, to show the prevailing attitudes.

In the second chapter, the content of the ACDC will be explained in more detail. Questions on who can appeal to it, from what liability it provides an exemption, which cyber defense measures it allows, and what is its geographical reach, will be addressed. Possible downfalls and risks entailed in the bill are also presented along the way, such as collateral damage and subsequent tort liabilities as well as violating of laws of other jurisdictions.

The third chapter takes a relatively brief look into international and EU privacy principles and provisions and EU rules on data protection and cybercrime, emphasizing the similarities and differences between the EU and the US. The EU's lack of active cyber defense regulation is also brought up, with a mention of some arising national proposals in the direction of more lenient approach towards invasive criminal investigation methods in cyberspace.

The fourth and final chapter will present an analysis on the previously-discussed legislations – the ACDC and the European privacy and data protection laws, with the emphasis on the GDPR – and what sort of legal collision they could end up in. Diplomatic and economic implications of this collision as well as the risk of collateral damage are discussed in more detail, with the help of an example of hypothetical escalation between two companies. The ACDC and the GDPR will be proved to include inconsistencies with each other, and finally, a proposal is made to cater to both the need for better cybersecurity and the need for effective data protection.

In the Conclusion part, the content of the paper is summarized and the answer to the question in the title of the paper is provided.

1. ACTIVE CYBER DEFENSE – ACD

The fact that the security of computer systems affects billions of people in the world, tells us something about how reliant we are on computers these days. However easy and convenient this makes the daily lives of individuals and the commerce of companies, it also makes us very vulnerable to malicious attacks, which are becoming more and more persistent, threatening and global. [2] Against these, many companies and organizations use traditional perimeter defense technologies, such as firewalls and other preventive measures. There is no dispute of the legality of taking measures confined within the boundaries of one's own network. However, many argue, that these measures are not sufficient. [3] The legal issues come to play when we talk about more proactive approach to defending oneself against the increasingly complex and sophisticated cyberattacks.

Robert S. Dewar has formulated a useful and accurate definition for active cyber defense (herein referred to as ACD), which can be found in the NATO report on the 6th International Conference on Cyber Conflict. The definition, which is formulated upon different academic and policy sources, is the following: "proactive detection, analysis and mitigation of network security breaches in real-time combined with the use of aggressive countermeasures deployed outside the victim network." [4] Another helpful definition has been made by Rosenzweig, Bucci and Inserra in their article "Next Steps for U.S. Cybersecurity in the Trump Administration: Active Cyber Defense", according to which ACD includes measures that "go beyond protective software, firewalls, and other passive screening methods and instead actively deceive, identify, or retaliate against hackers to raise their costs for conducting cyberattacks." [5] Essentially, ACD is a cyberattack committed as self-defense.

As one of the most controversial areas of cybersecurity, ACD is a much-debated topic among scholars and policymakers. Those in support of legalizing ACD argue that it is a necessary defense

[2] Heckman K. E., et al. *Cyber Denial, Deception and Counter Deception: A Framework for Supporting Active Cyber Defense*, Springer International Publishing, Cham, 2015, p 1.
[3] *Ibid.*, p. 2.
[4] Dewar, R. S. (2014). The "Triptych of Cyber Security": A Classification of Active Cyber Defence. – *6th International Conference On Cyber Conflict*, 3-6 June 2014, Tallinn. (Ed.) P. Brangetto, M. Maybaum, J. Stinissen. Tallinn: NATO CCD COE Publications, 7-21, p 7.
[5] Rosenzweig, P., Bucci, S., Inserra D. (2017). Next Steps for U.S. Cybersecurity in the Trump Administration: Active Cyber Defense. – *Backgrounder*, No. 3188, Washington, D.C.: The Heritage Foundation, 1-11, p 2.

to be regulated because governments are not doing enough to protect private companies and persons from cybercrime. [6] In fact, according to Hoffmann and Levite, sometimes governments do not even possess the same capacity to respond to attacks as private sector does, [7] and it is nevertheless debatable whether public resources should be used to protect private companies. [8] ACD would also work as a way to avoid heavy prosecution processes, technologically uneducated juries and complicated legal and forensic issues. [9] Shortly, it is argued, legalizing ACD would make protecting one's own network more time and cost efficient and overall more effective. It would also function as a deterrence for cybercriminals. In the United States, the right-wing has been more pro-ACD than the left, with the 2016 Republican Platform including a controversial provision in it: "We will explore the possibility of a free market for Cyber-Insurance and make clear that users have a self-defense right to deal with hackers as they see fit." [10] Indeed, many of the voices in support of legalizing ACD seem to be voices of policy makers, not cybersecurity experts.

The dominant expert opinion seems to be that ACD should not be permitted. [11] Jan Kallberg, for example, thinks that allowing the private sector to commit counter cyberattacks could lead to a situation, where the authority and legitimacy of the state would be jeopardized. [12] Indeed, legalizing ACD could very well end up turning our digital world into the "Wild West" of cyberspace. An expert panel at the 2016 RSA Conference – which is one of the world's biggest cybersecurity meetings – had a unanimous stance, as well, that ACD was a bad idea. [13] However, surveys made on the opinions of companies and of average people, whose personal data might someday become subject to cyber theft, have had mixed findings. [14]

---

[6] Harrington, S. L. (2014). Cyber Security Active Defense: Playing with Fire or Sound Risk Management? – *Richmond Journal of Law & Technology*, Vol. XX, No. 4, 1-41, p 33.

[7] Hoffman, W., Levite, A. (2017). Private Sector Cyber Defense: Can Active Measures Help Stabilize Cyberspace? Washington, D.C.: Carnegie Endowment for International Peace, p 13.

[8] *Ibid*., p. 14.

[9] Katyal, N. K. (2005). Community Self-Help. – *Journal of Law, Economics & Policy*, Vol. 1, No. 1, 33-67, p 60.

[10] 2016 Republican National Convention, "Republican Platform 2016", July 2016. Accessible: https://prod-static-ngop-pbl.s3.amazonaws.com/media/documents/DRAFT_12_FINAL%5b1%5d-ben_1468872234.pdf, 13 February 2018.

[11] Holzer, C. T., Lerums, J. E. (2016). The ethics of hacking back. – CERIAS Tech Report 2016-01, p 7.

[12] Kallberg, J. (2015). A Right to Cybercounter Strikes: The Risks of Legalizing Hack Backs. – *IT Professional*, Vol. 17, No. 1, 30-35, p 30.

[13] Armerding, T. (2016). *Hacking back will only get you in more trouble*. CSO. Accessible: https://www.csoonline.com/article/3040408/security/hacking-back-will-only-get-you-in-more-trouble.html, 6 November 2017.

[14] Fidelis Cybersecurity survey. (2017). Deception Technology: Playing Cybercriminals at Their Own Game. Accessible: https://www.fidelissecurity.com/sites/default/files/Fidelis-UK-Survey-Stats-1711.pdf, 13 February 2018.

Not all ACD is hacking back in to the intruder's network to retaliate and damage the attacker's network. Instead, there are various levels of the offensiveness of ACD, which is also demonstrated in the definitions presented earlier. They range from relatively innocuous measures, including setting up decoying targets or identifying the attacker to more assertive ones, such as retaliatory or even disruptive measures. [15] In the following sections, some the most common concepts of ACD measures, attribution and retrieving the stolen data, will be explained.

1.1 Attribution

Who is behind the attack is an obvious question to tackle first after learning that one's computer system has been broken into. The process of answering this question is called attribution: at least theoretically, the victim can trace the attack back to a particular system, and this way, attribute it to a perpetrator. [16] Attribution does not include doing damage to the attacker's network. Its purpose is solely to identify him to either find out his motives and resources to plan the possible next move according to that information, [17] or to forward the gathered intelligence to the law enforcement.

Attribution entails both technical and legal dilemmas. First, it is important to address, that it is technically very difficult to carry out. Anonymizers, proxies and generally hiding behind various IP addresses impede technical attribution. [18] Also, often times a hacker uses a computer, or computers, other than their own, by controlling them remotely to carry out the attack. [19] The more servers included in this chain of "hop points", the more difficult it is to trace back to the intruder. And if the attack is traced back to a person, the stolen information might not be stored in his own network – it might be hidden in the network of an unknowing third party. [20] This makes the final attribution extremely difficult. Guitton points out, however, that attribution, as difficult as it is, is not a *problem* per se. Problems generally have two stages: solved and unsolved. Attribution, on the other hand, should be looked as a process: the certainty of the attacker's identity can be

[15] Hoffman (2017), *supra nota* 7, p 7.
[16] Holzer (2016), *supra nota* 11, p 3.
[17] Guitton, C. *Inside the Enemy's Computer - Identifying Cyber Attackers*, Hurst Publishers, London, 2017, p 3.
[18] Iasiello, E. (2014). Hacking Back: Not the Right Solution. – *Parameters: U.S. Army War College*, Vol. 44, No. 3, 105-113, p 111.
[19] Brill, A., Smolanoff, J. (2017). Hacking Back Against Cyberterrorists: Could You? Should You? – *Defense Against Terrorism Review*, Vol. 9, No. 1307-9190, 35-46, p 37.
[20] *Ibid*., p. 38.

anywhere between 0 to 100%, [21] depending on the extent of the gathered information. [22] Then again, the question of how valuable can attribution with a certainty less than 100% be, remains.

The legal problem, according to Kallberg, is that it is hard to establish a threshold for what constitutes an acceptable attribution, which would give access to a legal right to hack back. [23] In the paper "Attributing Cyber Attacks", where they extensively analyze the process of attribution, Rid and Buchanan conclude that while attribution is getting easier in the sense that the technology to do it is advancing, it is also getting harder because the technology to hide more effectively, as a perpetrator, is also advancing. [24] This on-going race between the "bad guys" and the "good guys" in utilizing emerging technologies for their respective intentions is clearly not something that one can expect to find a definite solution in the foreseeable future.

1.2 Retrieving and deleting the data

The next step after attribution would be to either forward the attacker's identity information to the law enforcement, or to take matters into one's own hands by deleting and/or retrieving the stolen data. The problem is, digital property is not comparable with physical property. While physical property can usually only exist in one place at a time, digital property can be copied multiple times and stored in multiple different locations. The stolen data can be deleted from the attacker's servers, but there might very well be another set of copies of the data stored somewhere else. In fact, one could argue that it is naïve to assume that the data is not stored in at least two different servers at the same time.

In cases where the criminals demand a ransom for the stolen data, many businesses have resorted to paying it. The IBM Security study "Businesses more likely to pay ransomware than consumers" shows, that among the participants 70% of those US businesses, that had experienced such attacks, paid to get their data back. [25] The technical challenges of attribution and recovering stolen data are a likely and obvious reason for why so many companies pay the ransom to get their data back.

---

[21] Guitton (2017), *supra nota* 17, p 184.
[22] Bradbury, D. (2013). Offensive defence. – *Network Security*, Vol. 2013, No. 7, 9-12.
[23] Kallberg (2015), *supra nota* 12, p 2.
[24] Rid, T., Buchanan, B. (2015). Attributing Cyber Attacks. – *Journal of Strategic Studies*, Vol. 38, No. 1-2, 4-37, p 33.
[25] IBM Security survey. (2016). Businesses more likely to pay ransomware than consumers. Accessible: http://www-03.ibm.com/press/us/en/pressrelease/51230.wss#release, 5 March 2018.

However, due to its sensitive nature, it is unclear how big a part the unlawfulness of ACD plays in these statistics.

1.3 Unlawfulness of ACD in the US

What is currently making hacking back a troublesome subject in the US, is the Computer Fraud and Abuse Act (CFAA) of 1986, last amended in 2008, which makes it illegal to access computers without authorization. Under the Act, someone violating its felony provisions can face both criminal liability and civil liability for compensatory damages or equitable relief. [26] When contesting the unlawfulness of back-hacking by looking for loopholes in the Act, the word 'authorization' seems to be the key. [27] The CFAA provides no definition for it, and therefore, one could raise a question of whether the fact, that you suspect your own data being stored in the attacker's network, gives you an authorization to access this network and retrieve the data. But this is hardly an argument that could stand in a court. Courts have generally interpreted CFAA in a broad sense, including various prohibited acts under its scope. [28] However, there seems to be no case law regarding of what the word 'authorization' *de facto* means, which supports the common understanding that this sort of situations rarely end up in court due to the illegal nature of the actions of both sides. Instead of criminal law suits, civil suits are more likely to be started when the victim makes a misattribution and accesses and damages a system belonging to a third party. [29] In the next chapter, collateral damage and other risks that ACD poses will be discussed more, after first introducing a current controversial effort of the US Congress to legalize hack-back.

1.4 Views of businesses on ACD

According to a survey conducted by Fidelis Cybersecurity in the United Kingdom, more than half of the respondents not only did support the right to hack back, but also considered themselves to have the resources and technical abilities – either in-house or outsourced to a third party – to attribute the intruder. A bit over half of the respondent also considered collateral damage and mistaken identity of attackers to be the biggest risks in hacking back. Only 16% was worried about

[26] Computer Fraud Abuse Act 1986 (US), § 1030(g)
[27] Baker, S. (2012). "The Hackback Debate". Steptoe Cyberblog. Accessible: https://www.steptoecyberblog.com/2012/11/02/the-hackback-debate, 19 February 2018.
[28] Kesan, J. P., Hayes, C. M. (2012). Mitigative Counterstriking: Self-defense and Deterrence in Cyberspace. – *Harvard Journal of Law & Technology*, Vol. 25, No. 2, 415-529, p 479.
[29] Harrington (2014), *supra nota* 6, p 27.

violating foreign policy while carrying out offensive cybersecurity measures. [30] While it does seem realistic to assume, that collateral damage and misattribution might indeed be the biggest risks of ACD, there is a chance that the violation of foreign policies plays a bigger role in it than expected, especially when it comes to diplomatic relationships between states.

If the Fidelis survey is any indication of a broader on-going trend, more than half of US companies seem to be in support of ACD. And yet, another survey shows, that only 10% of companies are taking adequate steps to protect their network with traditional – and undisputedly legal, of course – passive cyber defense measures, [31] such as firewalls and anti-virus software. Several other surveys have also shown, that taking the necessary steps, identified by security experts, to protect oneself has reduced vulnerability-based risks by as much as 88%. [32] This suggests that simple precatory measures may in fact be enough to prevent a large number of the attacks, but because of the lack of awareness among companies, ACD seems like an attractive option to have.

[30] Fidelis Cybersecurity survey (2017) *supra nota* 14.
[31] Lewis, J. A. (2013). Center for Strategic and International Studies: Raising the Bar for Cybersecurity. – *Technology & Public Policy*, p 4.
[32] Iasiello (2014), *supra nota* 18, p 111.

2. ACTIVE CYBER DEFENSE CERTAINTY ACT – ACDC

The obvious problem with active cyber defense is the fact that it consists of measures which require that you go outside your own network and enter another person's system without authorization or exceeding authorization. As discussed earlier, this may constitute a criminal act, determining of which depends on whether damage has occurred and how the legal provisions concerning illegal access are implemented and applied. What is now proposed in a newly introduced bill on ACD, is a legitimate defense for the criminal liability set in the CFAA, [33] on the grounds that the "conduct constituting the offense was an active cyber defense measure." [34] It resembles the concept of self-defense as an affirmative criminal defense in traditional crimes.

A revised version of the discussion draft of Active Cyber Defense Certainty Act (ACDC) was introduced by the US Congress representatives Tom Graves and Kyrsten Sinema, and published in May 2017. The bill is calling out for the right for companies and individuals to hack back to identify and stop cyberattacks. If enforced, the ACDC would create an applicable defense to liability under the CFAA.

2.1 The scope of the ACDC

Here, the scope of the bill is explained, with answers to questions on who can use ACD, what measures can be used, for what liabilities the bill provides exemptions, and where the bill applies. With these explanations, certain weaknesses and ambiguities of the ACDC are brought up.

2.1.1 Who can use it and in what situations?

The protection provided by the ACDC is targeted to victims of cyberattack. The bill defines victim as a "victim of persistent unauthorized intrusion of the individual entity's computer". It also states, that the ACD measures included in the ACDC can only be used by "qualified defenders with a high degree of confidence of attribution". However, it is not defined what makes a "qualified defender", which essentially seems to render the provision useless – unless the intention is to have

[33] Computer Fraud Abuse Act 1986 (US), § 1030(a)(2)(C) and § 1030(c)
[34] Active Cyber Defense Certainty Act Bill 2017 (US), Sec. 4 § 1

victims outsource the defending for cybersecurity professionals, but even this is not clear from the text. Also, having a "high degree of confidence" is very subjective, and not necessarily related to the *de facto* attribution skills.

What sort of cyberattacks can ACD measures be used against? Let us go back to the provision of "victim of persistent unauthorized intrusion". According to Robert Chesney, the important words here are 'persistent' and 'intrusion'.[35] As a requirement, persistency seems to prevent victims of only fleeting intrusion from using active defense. This might be intentional: the point might be to raise the threshold to intrude others' networks without authorization as a means of ACD. The word 'intrusion', on the other hand, seems to exclude a category of one of the most common cyberattacks: DDoS attacks. Distributed denial-of-service attacks flood the system by overwhelming it with data and requests, preventing internet users from accessing the website, but they do not penetrate the system per se. [36] One reason to exclude it from the scope of attacks covered by ACDC might be the fact that DDoS attacks are often carried out via botnet (network of hijacked computers), [37] which creates a high chance of so-called collateral damage in case of back hacking. Then again, there is the possibility that the nature of DDoS attacks was not entirely clear to the drafters of the bill, and they were not meant to be excluded, or that the word 'intrusion' does not only mean penetrating of another's network.

2.1.2 For what liabilities does it provide exemption?

The bill does not offer protection from possible civil liabilities, only from the criminal liability under the CFAA. It states, that third parties can seek a "civil remedy, including compensatory damages or injunctive relief" in cases of collateral damage. [38] Apart from the CFAA, the bill does not mention any other possible acts which might be violated in the process of ACD, and from which it might offer protection. For example, the Electronic Communications Privacy Act of 1986 and the Wiretap Act of 1968, which prohibit electronic surveillance, might be applicable in the attribution process in cases where the attribution techniques fall under the category of electronic

[35] Chesney, R. (2017). "Legislative Hackback: Notes on the Active Cyber Defense Certainty Act discussion draft", Lawfare Blog. Accessible: https://www.lawfareblog.com/legislative-hackback-notes-active-cyber-defense-certainty-act-discussion-draft, 28 October 2017.
[36] Kesan, Hayes (2012), *supra nota* 27, p 430.
[37] *Ibid*., p. 429.
[38] Active Cyber Defense Certainty Act Bill 2017 (US), Sec. 4 § 1(2)

surveillance. [39] The ACDC also fails to mention, whether state laws on hacking and illegal access still apply. This fact makes its utility questionable.

2.1.3 What kind of measures are allowed?

The ACD measures, which the bill allows to be used, are explained in the following way. They are measures "(I) undertaken by ... a victim; and (II) consisting of accessing without authorization the computer of the attacker ... to gather information in order to establish attribution of criminal activity to share with law enforcement or to disrupt continued unauthorized activity against the victim's own network…" [40] It is also clarified that the defender should not intentionally destroy any information that does not belong to them. [41] Therefore, the permitted measures seem to be limited to gathering information of the identity of the attacker, stopping the attack and retrieving and deleting of the stolen data, not allowing retaliation.

2.1.4 Where does it apply?

The geographical scope of the ACDC is clear: if enforced, it would become a national, federal US law, and therefore its scope would only cover the US jurisdiction. However, in practice the measures allowed by the bill might often reach beyond the US borders. Seeing as many cyberattacks come from abroad, [42] the ACD measures would very likely be targeted to a country, where the ACDC does not apply. The bill itself reads, that the defender should "exercise extreme caution to avoid violating the law of any other nation where an attacker's computer may reside." [43] This is not a very helpful provision. First of all, it is very vague and general, and there is no clarification as to what kind of steps should be taken for the actions to be considered done with "extreme caution". The second problem is, how will the defender know whether the attacker's computer resides outside the US without first conducting attribution by unlawfully accessing the intruder's (or a third party's) servers? By the time when the attribution is traced to a foreign country, the crime might have already been committed.

---

[39] Cook, C. (2017). "Hacking Back in Black: Legal and Policy Concerns with the Updated Active Cyber Defense Certainty Act". Just Security. Accessible: https://www.justsecurity.org/47141/hacking-black-legal-policy-concerns-updated-active-cyber-defense-certainty-act, 28 October 217.

[40] Active Cyber Defense Certainty Act Bill, Sec. 4 § 3(B)(i)(II)(aa)

[41] Active Cyber Defense Certainty Act Bill, Sec. 4 § 3(B)(ii)(I)

[42] Clinch, M. (2014). *China originates 35% of 'nuclear bomb' cyber attacks*. CNBC. Accessible: https://www.cnbc.com/2014/01/29/china-originates-35-of-nuclear-bomb-cyber-attacks.html, 21 March 2018.

[43] Active Cyber Defense Certainty Act Bill, Sec. 2 § 9

2.2 Risks of ACDC

Several possible risks, which approving of the ACDC would bring about, have been identified. Here, two main problems will be discussed.

The first concern of legalizing ACD is misattribution and the possible subsequent collateral damage and civil liabilities. The difficulty of attribution has been discussed in the first chapter. The voices against legalizing ACD are indeed often concerned about the difficulty of identifying the actual attacker, and the collateral damage that might occur in the process. The former White House cybersecurity director Chris Finan has said the following: "Attribution is nearly impossible to do perfectly, so the most likely implications would be retribution targeted against innocent third parties, whose machines were simply used as launch points without the knowledge of the owners". [44] Indeed, one of the biggest risks seems to be the negative implications to innocent third parties – mainly those, whose servers have been used, without their knowledge, for the attack. This might result in breaches of the principle of proportionality, [45] used in traditional self-defense, meaning that the results of the response are more damaging than the original attack.

Brill and Smolanoff, authors of the paper "Hacking Back Against Cyberterrorists: Could You? Should You?", presented a useful depiction of the escalation and damage that could possibly occur during the process of attribution. In the example, Company A fell victim to a cyberattack and decided to find the source of the attack by hacking back into the network which it came from. However, it turned out to be the network of another company, Company B, whose servers had only been used by the actual perpetrator. Company B ended up incurring dozens of thousands of dollars' worth of expenses to fight against the intrusion coming from the Company A, and eventually bringing these financial damages to court. [46] Taking matters into one's own hands creates risks regarding both tortious liabilities and the company's reputation and goodwill. In a situation described above, two victims of cyberattacks could end up fighting each other instead of the actual attacker being brought to the justice. This might even be the intention of the attacker.

---

[44] Bukszpan, D. (2016). *2016 GOP platform endorsing strike-back against hackers*. CNBC. Accessible: https://www.cnbc.com/2016/07/27/2016-republican-party-platform-on-cybersecurity-is-absurd-say-experts.html, 28 October 2017.

[45] Sexton, M. (2016). U.K. cybersecurity strategy and active cyber defence – issues and risks. – *Journal of Cyber Policy*, Vol. 1, 222-242, p 10.

[46] Brill, Smolanoff (2017), *supra nota* 19, p 41.

Secondly, there is the question of transnational back-hacking and violating of foreign laws. As mentioned earlier, the ACDC mentions this risk and requires the defender to practice caution in order to not violate other states' rules. However, when often the attacker's servers are located in a foreign country – possibly even around the world – it would be practically impossible to ensure, that the back-hacking is staying within the borders of the US jurisdictions. Therefore, there is a high risk of the defender hacking into servers outside the US, and ending up violating a foreign state's cybercrime or data protection laws. This will be discussed more in the section "Conflict between ACDC and EU laws".

3. EU LEGISLATION

Next we will take a look into European legislation. Various laws of privacy as well as laws of technology, mainly the ones concerning data processing and active cyber defense, will be discussed.

3.1 EU laws on privacy and data protection

3.1.1 Privacy

In its broadest sense, the right to privacy is included in the Article 7 of the Charter of Fundamental Rights of the European Union. The Charter states, that "everyone has the right to respect for his or her private and family life, home and communications". The Charter also includes a provision concerning protection of personal data. According to Article 8, "everyone has the right to protection of personal data concerning him or her." The Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR) similarly grants EU citizens the right to respect for private life and family life. It is also interpreted to extend to data protection by the ECtHR. [47] Right to privacy is something that most states in the world enforce and value as a fundamental human right, and it is not exceptional to the EU.

3.1.2 Data protection

However, compared to many other jurisdictions, EU has exceptionally robust data privacy laws. This is partly as a response to Edward Snowden's revelations on NSA's mass surveillance activities, after which the EU declared that the US legal framework is not sufficient to protect European citizens. [48] The legal basis of the EU data protection is laid down by the Treaty on the Functioning of the European Union (TFEU) in its Article 16, which states: "Everyone has the right to the protection of personal data concerning them". The CJEU case law on privacy and data protection is also extensive, "establishing itself as the leading jurisdiction in the field", according to Cole and Fabbrini. [49] What differentiates the EU data protection legislation from the one in the

[47] Cole, D., Fabbrini, F. (2016). Bridging the transatlantic divide? The United States, the European Union, and the protection of privacy across borders. – *International Journal of Constitutional Law*, Vol. 14, No. 1, 220-237, p 226.
[48] *Ibid.*, p 221.
[49] *Ibid*., p. 224.

US, are mainly the omnibus approach, [50] established in the 1995 Data Privacy Directive, limits of data transfer to third countries, [51] and the attention it gives to sensitive information. [52] An interesting practical and recent example of the EU's emphasizing of data privacy rights is the on-going landmark privacy battle between Microsoft and the US Justice Department, where Microsoft – working in Ireland under EU laws – has denied giving the US authorities data stored by its customer in Microsoft servers for drug trafficking investigation. The US had acquired a domestic warrant for gathering evidence, and Microsoft disputed whether the warrant covers data stored outside the US. [53] The case is a perfect picture of EU privacy rights versus rights of US authorities to go around those privacy rights.

Another good example of how seriously the EU takes its citizens' data privacy, is the new data protection reformation, that is, the General Data Protection Regulation (GDPR), the Directive on security of network and information systems (NIS Directive) and the Directive on processing of personal data for authorities responsible for preventing, investigating, detecting and prosecuting crimes (Police Directive), all of which significantly enhance the protection of rights of data subjects. The GDPR is going to amend the Data Protection Directive, which has established the foundations of EU data protection. [54] By the time when the GDPR comes into force, which would be 25 May 2018, companies who process personal data of EU citizens' must meet the strict requirements set by the Regulation in protecting that data. In cases of severe data breaches, the sanctions can go up to 20 million euros (or 4% of annual global turnover, whichever is greater), [55] which is a very heavy incentive for businesses to meet the requirements of the Regulation. It is important to note, that the GDPR does not only apply to companies located in the EU: it applies to any company, anywhere in the world, which stores information on EU citizens. Big changes in businesses' data governance and cybersecurity measures are taking place right now.

---

[50] Schwartz, P. M. (2013). The EU-U.S. Privacy Collision: A Turn to Institutions and Procedures. – *Harward Law Review*, Vol. 126, No. 7, 1966-2009, p 1974.

[51] *Ibid.,* p. 1977.

[52] *Ibid*., p. 1978.

[53] Hurley, L., Volz, D. (2018). *U.S. Supreme Court wrestles with Microsoft data privacy fight*. Reuters. Accessible: https://www.reuters.com/article/us-usa-court-microsoft/u-s-supreme-court-wrestles-with-microsoft-data-privacy-fight-idUSKCN1GB0GY, 4 March 2018.

[54] Savin, A. *EU Internet Law*, Edward Elgar Publishing, Copenhagen, 2013, p 191.

[55] 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, p. 83

The NIS Directive, which applies to companies of certain professions listed in the Annex II of the Directive, also seeks to make sure that data subjects' rights are taken care of by companies processing their personal data. It includes a number of requirements concerning cybersecurity measures and incident response. [56] The Police Directive ensures these rights in the process of criminal investigations and proceedings. [57]

3.2 EU laws on cybercrime and ACD

3.2.1 Cybercrime

The 2001 Council of Europe Convention on Cybercrime is a multilateral treaty concerning crimes committed in cyberspace. It has been signed by 54 countries, and it seeks to harmonize definitions of computer-related offences, hacking being one of them (Article 2 – Illegal access), also containing procedural provisions. The Convention, which is signed by most EU countries and some non-EU countries such as the US, requires signatory states to criminalize "the access to … a computer system without right" when it is "committed intentionally". In addition to seeking to unify national laws on cybercrime, the Convention also includes provisions to give law enforcement bodies better tools for digital investigations, which has created controversy among entities such as civil right organizations. It has been criticized for lacking the needed protection for privacy rights, [58] in the process of trying to make prosecution or criminals more effective.

Ever since the Convention, Europe has been increasingly active in regulating computer-related crimes. [59] In addition to the Convention, the EU member states' national laws criminalizing hacking must also be in line with the EU Directive on attacks against information systems (so-called "Botnet Directive"). In its Article 3, the Directive prohibits "the access without right, to the whole or to any part of an information system" when it is "committed intentionally" and "at least

[56] 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, p. 1-30, 19.7.2016.
[57] Directive (EU) 2016/680 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 by competent authorities for the purpose of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, OJ L 119, p 89-131, 4.5.2016.
[58] Lloyd, I. J. (2017). *Information Technology Law*. 8th ed. Oxford: Oxford University Press, p 213.
[59] *Ibid*., p. 212.

for cases which are not minor". [60] The Directive can be considered as EU level implementation of the Convention. The definition in the Directive does not much differ from the one in the CFAA, which states, that someone who "intentionally accesses a computer without authorization or exceeds authorized access … shall be punished". [61] The Convention, the Directive and the CFAA all require both intent and lack of right / authorization to access the network for the action to constitute an offense. Therefore, the definitions of hacking seem to be more or less the same in both EU and US.

3.2.2 **ACD**

When it comes to ACD, there is currently no EU level regulation on it. However, while more and more robust data protection regulation is taking place in the EU, some member states are taking steps to make it easier for the law enforcement to resort to back-hacking in criminal investigation and gathering of digital evidence. For example, in 2015 the Dutch government proposed the Computer Crime Act III, which would grant the police a whole new set of investigative powers including hacking back, installing spywares and destroying or disabling access to certain files. [62] Even though this has already been a much-disputed proposal and subject to criticism especially from privacy activists, [63] it is still a long way from allowing private companies and individuals to hack back. Given the increasing privacy concerns of the EU lawmakers, it does not seem likely that proposals such as the ACDC would come about any time soon.

[60] Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA, OJ L 218, p. 12.
[61] Computer Fraud Abuse Act 1986 (US), § 1030(a)(2)
[62] Pool, R. L. D., Custers, B. H. M. (2017). The Police Hack Back: Legitimacy, Necessity and Privacy Implications of The Next Step in Fighting Cybercrime. – *European Journal of Crime, Criminal Law and Criminal Justice*, Vol. 25, 123-144, p 129.
[63] *Ibid*., p. 131.

4. CONFLICT BETWEEN THE ACDC AND EU LAWS

Actions in the digital world – the world wide web being, indeed, world wide – are notoriously difficult to confine in one jurisdiction. Whereas breaking into a house requires for the burglar to be physically present in the location of the house, breaking into a company's or an individual's computer system is entirely possible to carry out from the other side of the world, from the comfort of the attacker's own home, using servers in several different countries. This makes the legalities of the flow of digital information complicated.

4.1 Diplomatic implications

If the act of the original attack also constitutes a criminal offense in the offender's country, and the offender is correctly attributed by the authorities, under normal circumstances – that is, without legalized ACD – the US could contact the other country to either request an extradition or to alert them and trust that the offender will be prosecuted under national laws. [64] However, these are bureaucratically heavy and slow processes, and several major states flat out refuse to participate in them. [65] Resorting to ACD measures may seem tempting in comparison.

As mentioned earlier, the ACDC is a domestic law and its scope is strictly within the US borders. However, it is impossible to make sure that the ACD measures taken will stay within those borders. Giving the US citizens a free pass to intrude foreign networks without consent includes far-reaching diplomatic consequences. First of all, merely by allowing this type of activity, the US can be seen as signaling disregard to other countries' policies, [66] not to mention the Cybercrime Convention, to which it is a signatory. Secondly, depending on who ends up being the target of hacking back as collateral damage, the possible escalation might have damaging effect on international relations. In the example presented by cybersecurity lawyer Michael Vatis, an attack to a US company is traced to a Chinese research institute, which turns out to be a wing of the People's Liberation Army. And when the PLA traces the hack-back back to the US, there is a risk

[64] Kesan, Hayes (2012), *supra nota* 27, p 469.
[65] Sklerov, M. J. (2009). Solving the Dilemma of State Responses to Cyberattacks: A Justification for the use of Active Defenses Against States Who Neglect Their Duty to Prevent. – *Military Law Review*, Vol. 201, 1-85, p 7.
[66] Cook (2017), *supra nota* 36.

that the situation could escalate into an actual international cyberwar. [67] It might even turn out, that the original attacker is located in, say, Russia, and he has just been using the Chinese servers as proxies from which to launch the attacks. These scenarios are also possible between the US and the EU. Closely related to diplomatic relations, international trade is similarly at stake. Seeing how the EU and the US are the biggest trading partners in the world, [68] the economic implications of miscalculated ACD measures could be devastating as well. For these reasons, an international consensus regarding ACD should be established before any nation taking those steps alone.

4.2 Rights of third parties

In the sub-chapter "EU laws on privacy and data protection", we have looked into what kind of legal tools there are protecting the EU citizens. And in the sub-chapter "Risks of ACDC", it has been stated that collateral damage and violating of foreign laws might just be the biggest risks of the ACDC. In this chapter, it is specified what kind of rights provided by the GDPR might be at risk, would the ACDC be approved.

The GDPR regulates how companies should handle their customers' data in order to respect their privacy and data protection rights. It also provides data subjects with a set of rights in order to allow them to have control over what sort of data of theirs is processed and how. Therefore, in the scenario where the GDPR collides with the ACDC, a company storing data of EU citizens is mistakenly attributed as the culprit of a cyberattack. To demonstrate this, let us expand the example provided by Brill and Smolanoff and introduced earlier in the sub-chapter "Risks of ACDC". In their example, the point was a possible escalation and damages caused by mistaken attribution: the "third party" was a company (Company B) who ended up paying dozens of thousands of dollars to protect themselves from the attack coming from the defender of the original attack (Company A). In our expanded version of this example, the third party is not Company B, but the number of private persons whose personal data, stored by Company B, is compromised by Company A.

[67] Vatis, M. (2012). "Taking the Offense to Defend Networks – Another Perspective", Steptoe Cyberblog. Accessible: https://www.steptoecyberblog.com/2012/06/22/taking-the-offense-to-defend-networks-another-perspective, 29 March 2018.
[68] European Commission. (2018). United States Trade factsheet. Accessible: http://ec.europa.eu/trade/policy/countries-and-regions/countries/united-states, 22 April 2018.

Let us first take a look into the data subject rights provided by the GDPR Chapter 3 – Rights of the data subject, [69] that might be affected by the ACDC. First, the data subject has rights to rectify incorrect personal data (right to rectification) and to have their personal data erased (right to erasure). Secondly, they have a right to data portability, that is, to receive their personal data collected by the company, in a readable format. Thirdly, they have a right to object, on grounds of relating to their particular situation, to using of their personal data. Finally, Article 5 also states that personal data shall be protected against accidental loss, destruction and damage, and Article 6 requires that data is only processed if consent from the data subject has been received.

In our example, Company A has attributed a cyberattack to Company B. In reality, Company B is only used as a tool for the attack performed by a perpetrator unrelated to Company B. Company A does not know that. Instead, they have hacked back into Company B's systems, where the personal data of the customers, some of which are EU citizens, is available to them. Here, a privacy violation might already have happened: the data subjects most likely have not given consent to have their personal data viewed by Company A. Even if Company A does not intent to cause any damage to the system of Company B, this might very well happen, especially since the ACDC does not clearly specify what sort of qualifications the defender must have in order to legally hack back. The senior security researcher at Kaspersky Lab, Brian Bartholomew, has confirmed that it is impossible to control what data the defender touches when hacking back. [70] Therefore, mistakes are likely to happen, and the data in Company B's system might get lost or damaged, in which case Article 5 has been violated. Should the data be lost or destructed, the data subject cannot exercise their rights to rectification or erasure (in case of lost data), or data portability. In addition to this data becoming available to Company A and the possibility of it getting lost, damaged or destructed, there is a possibility that Company B's security is rendered vulnerable by the attack, enabling cybercriminals to access the data. In this case, there is no way of knowing where it may end up and how it may end up being used. The right to object, as well as any other data protection and privacy rights, can no more be ensured.

As we can see, the ACDC opens a door to the possibility of various mistakes being made by defenders, and these mistakes may end up in grave violations of EU privacy and data protection

[69] Regulation (EU) 2016/679, *supra nota* 47, p 39.
[70] Blue, V. (2017). If hacking back becomes law, what could possibly go wrong? Engadget. Accessible: https://www.engadget.com/2017/06/02/if-hacking-back-is-law-what-could-possibly-go-wrong, 22 April 2018.

rights. Indeed, as well as these GDPR provisions, various privacy-related fundamental human rights of these third parties are violated in the example presented above.

4.3 How to fit together the two colliding needs

Now that we have established, that there is a need for more offensive cybersecurity measures, and that the proposed solution, the ACDC, has several downfalls and inconsistencies with privacy laws, a compromise must be found. As a solution to cover both the need for better cybersecurity and the need for privacy and data protection, the author proposes looking into certain pro-active measures which do not include intruding the attacker's computer.

Let us first define, what is passive cyber defense, in order to distinguish the proposed measures from it. According to the authors of the paper "Booby Trapping Software", passive defense is "anything which makes an attack harder to accomplish but does not react automatically during an attack". [71] An anti-virus software is a common example of a passive cyber defense tool. As confirmed before, there is no debate on the legality of passive defense measures, since they are strictly confined within the defender's own network. A lot of the discussion on ACD is concerned with the opposite: intruding the attacker's network to attribute and/or retaliate, that is, back-hacking. However, there is a middle ground between these two categories of defense. This middle ground includes so-called active-passive defense measures, [72] such as honeypots and other deception tools. Taking honeypots as an example, the function of them is to act as "traps to lure attackers in". [73] It is a system that is built to look like any computer system, but is deliberately made vulnerable to attacks. [74] Inside this system, the trap could be hidden in, for example, a document with the kind of file name that could attract hackers. Their purpose is to alert the defender of attempted attacks and this way, prevent them pre-emptively.

[71] Crane, S., Larsen, P., Brunthaler, S., Franz, M. (2013). Booby Trapping Software. – *New Security Paradigms and Workshop*, 9-12 September 2013, Banff. New York: ACM Publications, 95-106, p 95.
[72] Kesan, Hayes (2012), *supra nota* 27, p 458.
[73] La, Q., Quek, T., Lee, J., Jin, S. Zhu, H. (2016). Deceptive Attack and Defense Game in Honeypot-Enabled Networks for the Internet of Things. – *IEEE Internet of Things Journal*, Vol. 3, No. 6, 1025-1035, p 1025.
[74] Shi, L., Jia, C., Lu, S. (2008). Full Service Hopping for Proactive Cyber-Defense. – *IEEE International Conference on Networking, Sensing and Control*, 6-8 April 2008, Sanya. New Jersey: IEEE, 1337-1342, p 1338.

Many deceptive active-passive defense measures have their own shortcomings, but they are relatively free from controversy. [75] They are also safe from the risks of collateral damage or violating of foreign laws, since there is no need to resort to illegal access. Same applies to the kind of booby traps that respond to files being opened outside the company's network by destroying them, or triggering a different response. [76] Therefore, it would make sense to look into regulating the use of active-passive measures, rather than drafting bills on legalizing hacking back into intruders' networks. The author proposes, that these active-passive measures be regulated and their legality be made clear, in order to make it possible for companies and individuals to have better and stronger tools for cybersecurity without compromising third parties' privacy rights.

[75] Harrington (2014), *supra nota* 6, p 18.

[76] Reinicke, B., Cummings, J., Kleinberg, H. (2017). The Right to Digital Self-Defense. – *IEEE Security & Privacy*, Vol. 15, No. 4, 68-71, p 69.

CONCLUSION

As the relevance of the discussion on active cyber defense and its legality shows, many agree that purely passive defense is only marginally effective when it comes to the most sophisticated attacks. The problem is, that as technology is developing in a rapid speed the legislation guiding it keeps lagging behind. Therefore, it seems as cybercriminals are taking advantage of this technology for their own objectives faster than private persons and companies can secure themselves. But the notion that passive cyber defense – such as firewalls and anti-virus software – has failed, or that it is just innately inadequate in protecting ourselves from cyber threats, is not the whole truth. If passive cyber defense tools would be utilized in their full capacity, the issue of legalizing ACD measures would be much less discussed. As we established in the first chapter, taking the necessary steps in the form of passive defense measures would most likely eliminate a large part of the problem, and make the issue of ACD much less pressing. It is not often that you see the insufficiency of the use of traditional defense tools brought up in cybersecurity law literature, but since passive defense still remains the main means to protect one's computer system, it needs to be given the attention it requires. Therefore, we should first make sure that these risk-free and legal measures are taken, and only then focus on the back-hacking debate. When it comes to companies securing their users' and customers' data, it is safe to assume that the GDPR and its global reach will result in better awareness of cybersecurity and data protection. Consequently, better awareness will lead to more enhanced passive cyber defense.

Also, we need to question whether legalizing ACD in the way proposed by the ACDC bill would really bring much difference to what is already going on. First, it is a known fact, that many companies and individuals are already hacking back without any repercussions. [77] Why? Because it is unlikely that the one, who made the first attack, would alarm the authorities about the victim retaliating to their crime, and it is equally unlikely that the defender will go to the authorities after committing illegal access themselves, in the process of hacking back. The damage caused to third parties is also often left uninvestigated, partly because the victim is often unaware of the attack. [78] And even if it were to be investigated, the one negatively impacted by the ACD measures would still have a right to sue for civil damages even with the ACDC enforced, according to the Sec. 4 §

[77] Kesan, Hayes (2012), *supra nota* 27, p 461.

[78] Hinduja, S. (2007). Computer Crime Investigations in the United States: Leveraging Knowledge from the Past to Address the Future. – *International Journal of Cyber Criminology*, Vol. 1, No. 1, 1-26, p 11.

2 (Inapplicability to civil action) of the bill. Secondly, a major portion of the harm done to companies is carried out in a way of DDoS attacks, [79] which, as discussed in the second chapter, do not seem to be included in the ACDC. Therefore, the ACDC as it is now would most likely bring about less harm than many expect, mainly because it does not provide protection from civil liabilities but also because many of those, who have the resources to hack back, are already doing it. However, this does not diminish its impact as a harmful precedence for the future.

Finally, the issue of passive and active defense is not as black and white as the newspaper headlines make you think. The means to protect one's network are not divided into passive protection and hacking back into the attacker's systems, as established in the fourth chapter. Instead, there is a middle-ground between criminalizing certain cyber defense measures under provisions of unauthorized access and deception, and legalizing hacking back as self-defense. This middle-ground is those cybersecurity tools that are not active in the sense that the defender would have to intrude the attacker's network, but also not passive in the sense that they would merely function as a wall to block attacks. These deceptive measures are currently in the legal grey area, but should they become regulated, they could provide better cybersecurity for companies and individuals without the risks that the ACDC entails: collateral damage and violating of – foreign or national – privacy and data protection laws. The idea is, that when we are taking steps to regulate more offensive network protection, we should not dive straight into the deep end, but instead, take smaller steps to make sure the needs are met but no rights are violated in the process.

[79] Apps, P. (2014). *DDoS cyber attacks get bigger, smarter, more damaging*. Reuters. Accessible: https://www.reuters.com/article/us-cyber-ddos/ddos-cyber-attacks-get-bigger-smarter-more-damaging-idUSBREA240XZ20140305, 22 April 2018.

LIST OF REFERENCES

Books

1. Guitton, C. (2017). *Inside the Enemy's Computer - Identifying Cyber Attackers*. London: Hurst Publishers.

2. Heckman, K. E., Stech, F. J., Thomas, R. K., Schmoker, B., Tsow, A. W. (2015). *Cyber Denial, Deception and Counter Deception*: *A Framework for Supporting Active Cyber Defense*. 64. Cham: Springer International Publishing.

3. Lloyd, I. J. (2017). *Information Technology Law*. 8th ed. Oxford: Oxford University Press.

4. Savin, A. (2013). *EU Internet Law*. 2nd ed. Copenhagen: Edward Elgar Publishing.

Articles and policy papers

5. Brill, A., Smolanoff, J. (2017). Hacking Back Against Cyberterrorists: Could You? Should You? – *Defense Against Terrorism Review*, Vol. 9, No. 1307-9190, 35-46.

6. Bradbury, D. (2013). Offensive defence. – *Network Security*, Vol. 2013, No. 7, 9-12.

7. Cole, D., Fabbrini, F. (2016). Bridging the transatlantic divide? The United States, the European Union, and the protection of privacy across borders. – *International Journal of Constitutional Law*, Vol. 14, No. 1, 220-237.

8. Harrington, S. L. (2014). Cyber Security Active Defense: Playing with Fire or Sound Risk Management? – *Richmond Journal of Law & Technology*, Vol. XX, No. 4, 1-41.

9. Hinduja, S. (2007). Computer Crime Investigations in the United States: Leveraging Knowledge from the Past to Address the Future. – *International Journal of Cyber Criminology*, Vol. 1, No. 1, 1-26.

10. Iasiello, E. (2014). Hacking Back: Not the Right Solution. – *Parameters: U.S. Army War College*, Vol. 44, No. 3, 105-113.

11. Kallberg, J. (2015). A Right to Cybercounter Strikes: The Risks of Legalizing Hack Backs. – *IT Professional*, Vol. 17, No. 1, 30-35.

12. Katyal, N. K. (2005). Community Self-Help. – *Journal of Law, Economics & Policy*, Vol. 1, No. 1, 33-67.

13. Kesan, J. P., Hayes, C. M. (2012). Mitigative Counterstriking: Self-defense and Deterrence in Cyberspace. – *Harvard Journal of Law & Technology*, Vol. 25, No. 2, 415-529.

14. La, Q., Quek, T., Lee, J., Jin, S. Zhu, H. (2016). Deceptive Attack and Defense Game in Honeypot-Enabled Networks for the Internet of Things. – *IEEE Internet of Things Journal*, Vol. 3, No. 6, 1025-1035.

15. Pool, R. L. D., Custers, B. H. M. (2017). The Police Hack Back: Legitimacy, Necessity and Privacy Implications of The Next Step in Fighting Cybercrime. – *European Journal of Crime, Criminal Law and Criminal Justice,* Vol. 25, 123-144.

16. Reinicke, B., Cummings, J., Kleinberg, H. (2017). The Right to Digital Self-Defense. – *IEEE Security & Privacy*, Vol. 15, No. 4, 68-71.

17. Rid, T., Buchanan, B. (2015). Attributing Cyber Attacks. – *Journal of Strategic Studies*, Vol. 38, No. 1-2, 4-37.

18. Schwartz, P. M. (2013). The EU-U.S. Privacy Collision: A Turn to Institutions and Procedures. – *Harward Law Review*, Vol. 126, No. 7, 1966-2009.

19. Sexton, M. (2016). U.K. cybersecurity strategy and active cyber defence – issues and risks. – *Journal of Cyber Policy*, Vol. 1, 222-242.

20. Sklerov, M. J. (2009). Solving the Dilemma of State Responses to Cyberattacks: A Justification for the use of Active Defenses Against States Who Neglect Their Duty to Prevent. – *Military Law Review*, Vol. 201, 1-85.

Legislation

21. Active Cyber Defense Certainty Act Bill 2017 (US). Accessed: https://www.congress.gov/bill/115th-congress/house-bill/4036/text

22. Computer Fraud Abuse Act 1986 (US). Accessed: http://uscode.house.gov/view.xhtml?req=(title:18%20section:1030%20edition:prelim)#referenceintext-note

23. Council of Europe, Convention on Cybercrime, 23 November 2001, ETS 185. Accessed: https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561

24. Directive (EU) 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA, OJ L 218, p. 8-14, 14.8.2013: Accessed: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:218:0008:0014:en:PDF

25. Directive (EU) 2016/680 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 by competent authorities for the purpose of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the

free movement of such data, and repealing Council Framework Decision 2008/977/JHA, OJ L 119, p 89-131, 4.5.2016, Accessed: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L0680&from=EN

26. 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, p. 1-30, 19.7.2016, Accessed: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&from=EN

27. 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, p. 1-88, 4.5.2016, Accessed: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN

News articles

28. Apps, P. (2014). *DDoS cyber attacks get bigger, smarter, more damaging*. Reuters. Accessible: https://www.reuters.com/article/us-cyber-ddos/ddos-cyber-attacks-get-bigger-smarter-more-damaging-idUSBREA240XZ20140305, 22 April 2018.

29. Armerding, T. (2016). *Hacking back will only get you in more trouble*. CSO. Accessible: https://www.csoonline.com/article/3040408/security/hacking-back-will-only-get-you-in-more-trouble.html, 6 November 2017.

30. Blue, V. (2017). *If hacking back becomes law, what could possibly go wrong?* Engadget. Accessible: https://www.engadget.com/2017/06/02/if-hacking-back-is-law-what-could-possibly-go-wrong, 22 April 2018.

31. Bukszpan, D. (2016). *2016 GOP platform endorsing strike-back against hackers*. CNBC. Accessible: https://www.cnbc.com/2016/07/27/2016-republican-party-platform-on-cybersecurity-is-absurd-say-experts.html, 28 October 2017.

32. Clinch, M. (2014). *China originates 35% of 'nuclear bomb' cyber attacks*. CNBC. Accessible: https://www.cnbc.com/2014/01/29/china-originates-35-of-nuclear-bomb-cyber-attacks.html, 21 March 2018.

33. Hurley, L., Volz, D. (2018). *U.S. Supreme Court wrestles with Microsoft data privacy fight*. Reuters. Accessible: https://www.reuters.com/article/us-usa-court-microsoft/u-s-supreme-court-wrestles-with-microsoft-data-privacy-fight-idUSKCN1GB0GY, 4 March 2018.

34. Pieters, J. (2016). *Dutch Parliament Approves Bill to Hack Criminal Suspects*. NL Times. Accessible: https://nltimes.nl/2016/12/21/dutch-parliament-approves-bill-hack-criminal-suspects, 4 March 2018.

Reports

35. Crane, S., Larsen, P., Brunthaler, S., Franz, M. (2013). Booby Trapping Software. – *New Security Paradigms and Workshop*, 9-12 September 2013, Banff. New York: ACM Publications, 95-106.

36. Dewar, R. S. (2014). The "Triptych of Cyber Security": A Classification of Active Cyber Defence. – *6th International Conference On Cyber Conflict,* 3-6 June 2014, Tallinn. (Ed.) P. Brangetto, M. Maybaum, J. Stinissen. Tallinn: NATO CCD COE Publications, 7-21.

37. Heinl, C. H. (2014). Artificial (Intelligent) Agents and Active Cyber Defence: Policy Implications. – *6th International Conference On Cyber Conflict*, 3-6 June 2014, Tallinn. (Ed.) P. Brangetto, M. Maybaum, J. Stinissen. Tallinn: NATO CCD COE Publications, 53-66.

38. Holler, C. T., Lerums, J. E. (2016). *The ethics of hacking back*. West Lafayette: CERIAS Tech Report 2016-01. Accessible: http://ethics.calpoly.edu/hackingback.pdf, 13 February 2018.

39. Lewis, J. A. (2013). *Raising the Bar for Cybersecurity.* – Center for Strategic and International Studies: Technology & Public Policy, Accessible: https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/130212_Lewis_RaisingBarCybersecurity.pdf, 22 April 2018.

40. Shi, L., Jia, C., Lu, S. (2008). Full Service Hopping for Proactive Cyber-Defense. – *IEEE International Conference on Networking, Sensing and Control*, 6-8 April 2008, Sanya. New Jersey: IEEE, 1337-1342.

Other sources

41. Active Cyber Defense Act (2017) – summary. Accessed: https://tomgraves.house.gov/uploadedfiles/acdc_expaliner.pdf, 19 February 2018.

42. Baker, S. (2012). "The Hackback Debate". Steptoe Cyberblog. Accessible: https://www.steptoecyberblog.com/2012/11/02/the-hackback-debate, 19 February 2018.

43. Chesney, R. (2017). "Legislative Hackback: Notes on the Active Cyber Defense Certainty Act discussion draft". Lawfare Blog. Accessible: https://www.lawfareblog.com/legislative-hackback-notes-active-cyber-defense-certainty-act-discussion-draft, 28 October 2017.

44. Cook, C. (2017). "Hacking Back in Black: Legal and Policy Concerns with the Updated Active Cyber Defense Certainty Act". Just Security. Accessible: https://www.justsecurity.org/47141/hacking-black-legal-policy-concerns-updated-active-cyber-defense-certainty-act, 21 March 2018.

45. European Commission. (2018). United States Trade factsheet. Accessible: http://ec.europa.eu/trade/policy/countries-and-regions/countries/united-states, 22 April 2018.

46. Fidel Cybersecurity. (2017). *Deception Technology: Playing Cybercriminals at Their Own Game*. Accessible: https://www.fidelissecurity.com/sites/default/files/Fidelis-UK-Survey-Stats-1711.pdf, 13 February 2018.

47. Hoffman, W., Levite, A. (2017). Private Sector Cyber Defense: Can Active Measures Help Stabilize Cyberspace? Washington, D.C.: Carnegie Endowment for International Peace. Accessible: http://carnegieendowment.org/files/Cyber_Defense_INT_final_full.pdf, 13 February 2018.

48. IBM Security. (2016). *Businesses more likely to pay ransomware than consumers*. Accessible: http://www-03.ibm.com/press/us/en/pressrelease/51230.wss#release, 5 March 2018.

49. Rosenzweig, P., Bucci, S., Inserra D. (2017). Next Steps for U.S. Cybersecurity in the Trump Administration: Active Cyber Defense. – *Backgrounder*, No. 3188, Washington, D.C.: The Heritage Foundation, 1-11.

50. Vatis, M. (2012). "Taking the Offense to Defend Networks – Another Perspective". Steptoe Cyberblog. Accessible: https://www.steptoecyberblog.com/2012/06/22/taking-the-offense-to-defend-networks-another-perspective, 29 March 2018.