Cyber Deterrence and Limitations of Punishment and Denial: Cyber Norms as Part of the Solution

By

Matej Spišák

Submitted to

Central European University Department of International Relations

In partial fulfilment of the requirements for the degree of

Master of Arts in International Relations

Supervisor: Professor Paul Roe

Vienna, Austria 2021

Word Count: 10,741

Abstract

Cyberspace is an environment with particular characteristics. Nevertheless, in the case of deterrence, cyber deterrence is yet another departure with its own difficulties. In 2016, the U.S. experienced unprecedented cyber interference during the presidential election and cyberattacks also continued afterward. The aim of the thesis is to evaluate existing assumptions about the efficacy of the traditional means of deterrence in cyberspace – punishment, and denial – on the case of the United States after the 2016 presidential election. The paper argues that states should pay additional attention to non-traditional means of deterrence such as norms, inasmuch traditional means are not always sufficient to deter cyberattacks. In some cases, even these means combined are not sufficient as the case of the United States shows. For these particular reasons, states should also focus on the development of norms in cyberspace, including norms related to electoral cyber interference and cyber espionage. The paper uses process tracing as a method to evaluate the efficacy of the traditional means of deterrence on the case of the United States between 2016 and 2020. The paper suggests that except for punishment and denial, states should pay attention to the development of norms. A coalition of like-minded democratic states might develop certain norms and clearly state punishment for their violation. Additionally, states such as China and Russia might be also included in the process, but they need to see and understand the benefits of it.

Acknowledgements

I would like to thank my thesis supervisor Professor Paul Roe for giving me invaluable advice and feedback throughout the whole writing process. Without his class Strategy, Security, and Contemporary Warfare, I would not be so passionate about the topic of deterrence.

Also, I express my deepest gratitude to the Department of International Relations and the whole Central European University for having an opportunity to study there and meet dozens of inspiring and enthusiastic people.

Furthermore, I would like to thank my family and my girlfriend Barbora for all their help during my studies. Even though it was sometimes difficult, they were always here to support me.

Table of Contents

Introduction

Cybersecurity is a very contemporary branch of security studies, and we can assume it will remain in the focus of scholars in upcoming years. There are estimates there will be some 20 billion devices connected to the Internet in the foreseeable future.[1] This might attract possible perpetrators of cyberattacks represented by various actors – individuals, groups, and governments. Just in May 2021, we saw significant ransomware attacks, including on gas pipeline in the U.S.[2] While all of the attacks pose a certain degree of threat, in my work, I will focus mainly on state-backed cyber warfare, including cyberattacks and cyber espionage with the aim to influence elections. Several states use cyberspace as an environment for the conduct of their operations. Russia, China, Iran, or North Korea are fully using the world that is becoming more connected, and systems characterized by interconnectedness.[3] The governments are deliberating how to benefit from the possibilities that cyberspace is offering, but at the same time need to pay attention to their own protection. One of the states we need to take into account, and that is aware of all aspects of cyberspace is the United States.[4]

Even though the U.S. is a powerful country with considerable cyber capabilities, it has been a victim of a number of cyberattacks. In 2016, we witnessed Russian cyber operations conducted to collect information to interfere in the presidential election in the U.S.[5] In 2018, twelve Russian intelligence officers were charged with hacking the e-mail accounts of Hillary Clinton's staff. Officers from Russian military intelligence, The Main Directorate of the

[1] Joseph S. Nye Jr., "Deterrence and Dissuasion in Cyberspace," *International Security* 41, no. 3 (Winter 2016/2017), 44.
[2] Michael D. Shear, Nicole Perlroth and Clifford Krauss, "Colonial Pipeline Paid Roughly $5 Million in Ransom to Hackers," *The New York Times* (May 13, 2021).
[3] Quentin E. Hodgson, Logan Ma, Krystyna Marcinek and Karen Schwindt, "Fighting Shadows in the Dark: Understanding and Countering Coercion in Cyberspace," *RAND Corporation* (2019).
[4] Ibid., 1-2.
[5] CNN Editorial Research, "2016 Presidential Campaign Hacking Fast Facts," *CNN* (October 28, 2020).

General Staff of the Armed Forces of the Russian Federation (GRU), achieved stealing mail communication and data of voters. The Russian Federation is rejecting any allegations, nevertheless, according to Deputy Attorney General Rosenstein, "*the goal of the conspirators was to have an impact on the election.*"[6] The fact that Russia did not pay a heavy price as a response to these malicious actions, might have implications for the deterrence of cyberattacks in the future.[7] It is important to mention that even though the Trump Administration took actions against Russia, the President himself was sometimes at odds with the administration.[8]

Susan Hennessey describes the event and consequences in her review essay *Deterring Cyberattacks* published in *Foreign Affairs*.[9] The text is heavily based on two books: *The Cybersecurity Dilemma* by Ben Buchanan and Martin Libicki's *Cyberspace in Peace and War*. She acknowledges that even though a number of the U.S. authorities concluded that the Russians were behind the hacks with the aim to influence the electoral process, the response was very mild. To cut a long story short "*Washington has failed to devise a strategy to deter cyberattacks or to respond strongly enough when such attacks have occurred*".[10]

Indeed, this was not the last attack conducted against the United States by Russia. There is a record of cyberattacks happening since 2016. According to a list composed by the Center of Strategic and International Studies (CSIS), we can find some cyber incidents aimed at the U.S. In July 2017, DHS together with the FBI announced attempts to breach energy facilities, while the behavior of the perpetrators looked similar to the already known group from Russia. In

[6] BBC News, " Twelve Russians charged with US 2016 election hack," *BBC* (July 13, 2018).
[7] Eric Lipton, David E. Sanger and Scott Shane, " The Perfect Weapon: How Russian Cyberpower Invaded the U.S.," *The New York Times* (December 13, 2016).
[8] Noah Weiland, "5 Times the Trump Administration Has Been Tougher Than Trump on Russia," *The New York Times* (January 21, 2019).
[9] Susan Hennessey, "Deterring Cyberattacks," *Foreign Affairs* (November/December 2017).
[10] Ibid.

March 2018, the same U.S. organizations warned of cyberattacks originating in Russia. The target was the U.S. critical infrastructure. Again, in early 2019, the Democratic National Committee that was also the victim of 2016 cyberattacks, announced Russian hackers targeted it just a couple of weeks after the midterm election in 2018. And 2020 was no different. According to private companies and U.S. agencies, allegedly Russian hackers from Foreign Intelligence Service (SVR) succeeded in compromising a product of the U.S. company SolarWinds to get access into private[11] and the U.S. government's networks.[12]

I also need to mention a development that emerged with the publication of a declassified version of the Intelligence Community's report on March 10, 2021.[13] Based on the document, Russia did not attempt to "*gain access to election infrastructure*"[14] and "*to alter any technical process in the 2020 US elections, including voter registration, casting ballots, vote tabulation, or reporting results*".[15] But, even though the Intelligence Community does not think there were efforts to access the infrastructure, it says that cyber units of Russia (e.g. GRU) collected information with the purpose to use them in their influence operations. According to the document, there was a number of occasions when the Russian intelligence actors tried to gather information: in 2019 and 2020, the GRU tried to hack political actors; in 2019, they tried to gather information through phishing campaigns targeted to Burisma holdings that were related to the family of current President Biden.[16] The information was gathered to influence the election through Russian operations. Therefore, even though the U.S. probably succeeded in

[11] Center for Strategic and International Studies, "Significant Cyber Incidents," *Center for Strategic and International Studies* (2021).
[12] Isabella Jibilian and Katie Canales, "Here's a simple explanation of how the massive SolarWinds hack happened and why it's such a big deal," *Business Insider* (February 25, 2021).
[13] National Intelligence Council, "Intelligence Community Assessment. Foreign Threats to the 2020 US Elections," *Office of the Director of National Intelligence* (March 10, 2021).
[14] Ibid., i.
[15] Ibid.
[16] Ibid., 3.

deterring cyberattacks on election infrastructure, it failed to deter cyber activities aimed at gathering information for the purpose of influencing the election. The United States is clearly an interesting object of cyber activities of different state actors, including Russia.

To understand what my research will consist of it is necessary to explain deterrence theory. As Jervis puts it," one *actor deters another by convincing him that the expected value of a certain action is outweighed by the expected punishment*".[17] In other words, actor A needs to know that the benefits of his action against actor B will be smaller than a possible response as revenge of that act. Possibly, actor B could harm actor A for conducting such an action. In the fear of consequences, actor A might restrain from a certain form of behavior. Deterrence theory was examined in various forms under various circumstances, including the Cold War period,[18] together with nuclear deterrence,[19] and deterrence of terrorism.[20] There are, similarly to a majority of theories, contradictory voices deliberating about the effectiveness and usage of deterrence. I will examine them in the literature review part in general.

Similar to other areas of deterrence, cyber deterrence is a frequently discussed topic. Among other authors, Joseph S. Nye Jr. writes about deterrence in cyberspace. In his work *Deterrence and Dissuasion in Cyberspace*,[21] he discusses possible means of cyber deterrence that are out of the traditional or narrow understanding of deterrence. In this regard, an explanation of these means is needed, even though it will be thoroughly addressed as a part of the literature review. Nye in the text examines deterrence and dissuasion by punishment and denial that are

[17] Robert Jervis, "Deterrence and Perception," *International Security* 7, no. 3 (1982-1983), 4.
[18] Patrick M. Morgan, *Deterrence Now* (New York: Cambridge University Press, 2003), 1-42.
[19] Andrew Brown and Lorna Arnold, "The Quirks of Nuclear Deterrence," *International Relations* 24, no. 3 (2010).
[20] Robert F. Trager and Dessislava P. Zagorcheva, "Deterring Terrorism," *International Security* 30, no. 3 (2005-2006).
[21] Nye

considered as more traditional means of deterrence, and also entanglement, and norms that are rather alternative means.[22] Therefore, Nye suggests there are other means of deterrence that should be taken into consideration, except for traditional ones.

The aim of the thesis is to evaluate existing assumptions about the efficacy of traditional means of deterrence, using the case of the United States from 2016 until 2020. From the available data, we can see that even though the U.S. was a victim of unprecedented foreign interference in the presidential election, we have been witnessing a number of cyber incidents also afterward. The research question is "*why do we need to pay attention to alternative means of deterrence in order to increase the effectiveness of overall cyber deterrence?"*. I argue that norms are potentially effective means of deterring cyberattacks, inasmuch traditional means such as denial and punishment are not always sufficient on their own, while norms might work in certain cases, such as cyber espionage, or cyber electoral interference. In the thesis, I will use the method of process tracing. A thorough evaluation of assumptions about deterrence on the case of the U.S. after the presidential election in 2016 will give us a general overview of the difficulties regarding cyber deterrence by traditional means. My goal is to contribute to the cyber deterrence debate by explaining events between 2016 and 2020, from which further discussion, ideas, and thoughts on cyber deterrence might stem. By evaluating assumptions existing in the literature about cyber deterrence, I will be able to identify obstacles that emerge, and subsequently, bring literature focusing on non-traditional means of deterrence that should be a part of a possibly successful deterrence strategy – deterrence by norms.

The thesis will be structured in the following way. Firstly, I will explain the methodology that I use in my thesis and discuss the meaning of cyberattack for clarification of terms. Secondly,

[22] Ibid., 63-68.

a literature review will follow positioning myself into the broader discussion of deterrence and cyber deterrence and identifying existing trends and assumptions in the literature. Thirdly, I will use the 2016 presidential election in the U.S. as my starting point, from which I will identify important events and trace actions taken in regards to cyber deterrence until 2020 to evaluate existing assumptions about the efficacy of deterrence on the case of the U.S. Also, I will bring literature on cyber norms to contribute to the discussion. Lastly, I will conclude all my findings.

1 Methodology and Conceptual Definitions

The thesis will consist of qualitative methods. Namely, I will use process tracing to evaluate existing assumptions. Process tracing could serve as a good tool to conduct my research and successfully address the research question. As Collier writes, process tracing could contribute to the successful evaluation of existing hypotheses and coming up with new ones.[23]

As it is inevitable for process tracing to engage with events that happened over some particular time, I have also decided to research the period between 2016 and 2020. Bennet and Checkel write extensively about process tracing and the necessities of the method. As they argue, through process tracing we try to "*identify the intervening causal process…between an independent variable (or variables) and the outcome of the dependent variable*".[24] In the case of my thesis, I will do the process tracing for particular means of deterrence. For example, in the empirical part, I will discuss existing assumptions about deterrence by punishment and evaluate them in practice on the case of the United States. Therefore, the dependent variable will be the efficacy of deterrence by punishment, while under independent variables I understand actions that were conducted to punish the perpetrator of cyberattacks. Then, I will do the same for another means of deterrence – deterrence by denial. My dependent variable will be the efficacy of deterrence by denial, while I will consider independent variables to be the actions taken to increase the difficulty of conducting cyberattacks.

I am also aware of the limitations of my study. Cybersecurity is a sensitive issue for which military and intelligence agencies are partly responsible institutions. For this particular reason,

[23] David Collier, "Understanding Process Tracing," *PS: Political Science and Politics* 44, no. 4 (2011), 823.
[24] Andrew Bennett and Jeffrey T. Checkel, *Process Tracing: From Metaphor to Analytic Tool* (New York: Cambridge University Press, 2015), 6. cited after Alexander L. George and Andrew Bennett, *Case Studies and Theory Development in the Social Sciences* (Cambridge: MIT Press, 2005), 206.

it is impossible to access all the documents that could be classified. In addition, not all cyberattacks are documented, and not all states confess to attacking or being attacked, therefore, I can only work with publicly available information and documents. Firstly, I will engage with academic literature focusing on various forms and cases of deterrence (nuclear deterrence, cyber deterrence, etc.), and cyber norms. Secondly, I am going to work with official documents issued by state institutions, such as National Intelligence Council's assessment.[25] Lastly, I will use articles from trustworthy media that informed about the events related to cyberattacks coming from the Russian Federation and targeting the United States. Among these, I include sources such as The New York Times,[26] Foreign Affairs,[27] BBC,[28] and others. I will use all the publicly available information to research my hypothesis and answer my research question. With the information from the sources, I will be able to examine what happened in the area of cyber deterrence, including by punishment and denial. I have decided to use these types of written sources as they will give me a general overview of cyber deterrence, and at the same time, I will be able to engage with existing assumptions through information from trustworthy media. I have decided to use media as my main source for the case of the U.S. because the events have been happening in the last couple of years, therefore, we are missing any extensive academic literature focusing on the topic.

But before we can move to cyber deterrence itself, we need to define what we consider under the term cyberattacks. In the existing literature, there are different definitions of cyberattacks. Martin Libicki dedicates a part of his work *Cyberdeterrence and Cyberwar* to defining them.[29] He defines a cyberattack as a "*deliberate disruption or corruption by one state of a system of*

[25] National Intelligence Council
[26] Lipton, Sanger and Scott
[27] Hennessey
[28] BBC News
[29] Martin C. Libicki, "Cyberdeterrence and Cyberwar," *RAND Corporation* (2009).

interest to another state".[30] However, it is also important to mention what Libicki does *not* consider a cyberattack. According to him, computer network exploitation (CNE), or in other words spying, is not an attack. He claims we must differentiate spying from cyberattacks because spying itself does not limit the user's ability to use the machine.[31] Nevertheless, we also have authors that refer to cyber espionage in terms of cyberattack. For example, Thomas Rid in his work *Cyber War Will Not Take Place* writes about espionage, sabotage, and subversion as about "*politically motivated cyber attacks*".[32] Also, Joe Burton writes about cybersecurity and four main categories of the concept based on the attacker's motivations and the target – "*cyber crime, cyber espionage, cyber terrorism and cyber warfare*".[33] For our purposes, the definition of cyber espionage might be extracted from Burton's work as conducted by state actors with an effort to obtain information from a foreign government with the aim of political gain.[34] Even though his definition is broader, this is an important part of it for the thesis.

In the paper, I will stick more to definitions by Rid and Burton. I do not only consider cyberattacks to be only those acts that aim to somehow disrupt the system. What I will also work with are espionage and cyber activities that aim to access information that could be then used for political goals and in broader operations.

[30] Ibid., 23.
[31] Ibid.
[32] Thomas Rid, "Cyber War Will Not Take Place," *The Journal of Strategic Studies* 35, no. 1 (2012), 5.
[33] Joe Burton, "NATO's cyber defence: strategic challenges and institutional adaptation," *Defence Studies* 15, no. 4 (2015), 299.
[34] Ibid., 300.

2 Deterrence Theory

For the purpose of the research, I need to explain exactly what the concept of deterrence means. The concept gained popularity mainly during the Cold War in the context of nuclear deterrence, but later became applied on different occasions, including deterrence of terrorism.[35] Deterrence in cyberspace is also one of these areas. Based on the already published literature, I will describe how deterrence in cyberspace works, what its main problems are, and how we might partly solve these issues by non-traditional means of deterrence, such as norms. After describing the theoretical framework, I will use it and evaluate it with a very recent case of U.S. cyber deterrence.

2.1 Deterrence in General and its Traditional Means

A very good point where to start the literature review is Glenn Snyder´s famous work *Deterrence and Defense*.[36] In his work, he discusses how deterrence works, and what it is. First of all, we need to recognize the difference between the concept of deterrence and defense. In brief, when talking about deterrence, we are thinking of a situation when a state is trying to discourage an aggressor by making the perceived costs higher than possible gains. Defense, he points out, comes into play mainly once the deterrence fails. Another important difference is related to when these two activities occur. While deterrence is mainly related to times of peace, defense is more typical for wars.[37]

To put it simply, "*deterrence means discouraging the enemy from taking military action by posing for him a prospect of cost and risk outweighing his prospective gain*".[38] There exist two

[35] Trager and Zagorcheva
[36] Glenn H. Snyder, *Deterrence and Defense* (Princeton: Princeton University Press, 1961).
[37] Ibid., 3-4.
[38] Ibid., 3.

traditional means of deterrence around which most of the discussion about deterrence is oriented – deterrence by punishment and deterrence by denial. Deterrence by punishment, Snyder writes, is related to the estimate of the attacker. In this case, the estimates about the costs imposed on the attacker.[39] As Snyder argues, an actor deters another actor by a threat of a sanction if the actor behaves in a certain way. In this sense, as he points out, we do not have to think about deterrence only in terms of the military, but, for example, trade restrictions.[40] According to Snyder, deterrence by denial is affecting the calculus of the aggressor, namely the estimate of how probably he will gain his objective. Assuming that the defender has denial capabilities, the attacker will be thinking about his possibility of making some gains. In this regard, Snyder mentions "*capacity to deny territorial gains to the enemy*".[41] It is important to have these two means in mind, as they will occur throughout the rest of the thesis very frequently.

Deterrence is accompanied by four different concepts that Snyder argues should be taken into consideration. Firstly, we need to think about rationality, and I will dedicate a section to the concept later in this chapter. In different cases, different actors do not have to be sure about each other's rationality which makes it difficult to assess possible actions.[42] At the same time, this partly leads the actors into uncertainty. The actors cannot be sure how the other will act or react. The only thing an actor might do is to collect the evidence available and try to estimate a possible behavior of the other. Therefore, states interact in an environment of uncertainty and in terms of probability and likelihood of certain actions.[43] Jervis broadly explains in his work *Deterrence and Perception* how strongly related deterrence is to perception.[44] Secondly, some

[39] Ibid., 15.
[40] Ibid., 9.
[41] Ibid., 14-16.
[42] Ibid., 6.
[43] Ibid., 27-30.
[44] Jervis, 3-30.

shared preferences between the actors should exist. This means that both actors should accept non-violence as an option. Thirdly, a deterrer needs to clearly communicate he will punish the aggressor if he conducts a certain kind of behavior. And lastly, the aggressor needs to perceive the defender as having the capabilities to punish.[45]

Deterrence can be applied in various cases and under different circumstances, and I will introduce some of them in the next sections. Also, the two traditional means of deterrence – punishment, and denial – have different levels of applicability under these circumstances, which I will also highlight in the following parts.

2.2 Nuclear Deterrence During the Cold War

It is necessary to better understand the concept of deterrence on a real-life example, so I can then continue with its application to and the difference in the cyber realm. For this particular reason, I will briefly explain how deterrence worked in the case of nuclear weapons during the Cold War. The Cold War was characteristic of a bi-polar world, where two competing powers stood face to face in the international arena. Both of these great powers had nuclear weapon arsenals after the Soviets developed their own in 1949. And, as time progressed, so-called "nukes" became a central component of deterrence theory that gained prominence during the Cold War.

Because both the U.S. and USSR thought that the hostility among them will survive for a long time, a sustained deterrence was needed. Shortly after that, a suggestion that stable peace might be developed by the possession of nuclear weapons by both sides of the Cold War appeared.

[45] Alex S. Wilner, "US cyber deterrence: Practice guiding theory," *Journal of Strategic Studies* 43, no. 2 (2019), 5.

Importantly, it was not only crucial to possess these weapons. The existence of a capability to retaliate (second strike) mattered as well. There were two essential points that influenced how nuclear policy looked during the Cold War. Firstly, as was mentioned, the states had to have the capabilities of a second strike. This means their facilities had to survive a situation when the opponent decided to strike first. Secondly, a certain degree of stability was needed, without any sudden actions.[46]

Inevitably, this moves us back to deterrence by punishment. Also, when Snyder writes about capabilities to punish, he mentions nuclear power for retaliation.[47] When it comes to nuclear deterrence, the ability to deter relied on a second-strike capability.[48] As Robert Powell writes, even though deliberating about a problem of credibility, in such a situation the "*second-strike forces would render defense impossible as neither state could physically protect itself from an attack*".[49] Even though deterrence by punishment can work in some cases, it might be problematic in different ones. Before I get to deterrence in cyberspace as another departure from deterrence in general, I will dedicate a section to discuss the rationality and motivation of actors, and then problems of deterrence by punishment under various circumstances in another section.

2.3 Rationality and Motivation

Importantly, rationality is a crucial aspect of deterrence in all cases. However, it has been mostly discussed in relation to various actors, such as terrorists and rogue states. Similar to Snyder, Brown and Arnold recognize different aspects related to deterrence, including the rationality of

[46] Brown and Arnold., 299.
[47] Snyder, 15.
[48] Brown and Arnold, 299.
[49] Robert Powell, "Nuclear Deterrence Theory, Nuclear Proliferation, and Missile Defense," *International Security* 27, no. 4 (Spring 2003), 88.

actors. They argue that the states are not necessarily governed by leaders that are rational. In addition, there are also non-state actors that one would like to deter. They mention terrorists that could lack rationality, and therefore, it might be more difficult to deter them.[50]

Trager and Zagorcheva also write about rationality and motivation in the case of terrorist organizations. As it seems that rationality and irrationality in terms of terrorists differ with each individual, in general, it cannot be said they are irrational. What is problematic is their motivation, because deterrence also depends on how they "*value their political goals over nonpolitical ends*". Among these, the authors include for example social standing or even life.[51] Some of the actors have low motivation, but others are highly motivated and value political goals over their lives. The latter, unfortunately, cannot be deterred by any threat.[52] Amitai Etzioni claims something very similar when he writes that "*if non-rational actors hold that attacking others serves their other-worldly goals, the threat of retaliation will not dissuade them*".[53]

This shows us the difficulty of deterrence. According to Trager and Zagorcheva, there are actors that have low motivation, but there are also highly motivated actors. The variation in the motivation of actors requires different actions by deterrer, but as was mentioned in the previous paragraph, sometimes it is even impossible. At the same time, the likelihood of success of deterrence changes.[54] Implicitly, deterrence should be proportionate to be successful. But, in some cases, e.g., terrorism, deterrence gets more complicated as it was during the Cold War. The next section will examine some other difficulties that deterrence by punishment brings.

[50] Brown and Arnold., 302-306.
[51] Trager and Zagorcheva, 95.
[52] Ibid., 105.
[53] Amitai Etzioni, "Rational Actors: Neither Mad nor M.A.D.: The Meanings of Rationality, Rogue States and Terrorists", *Defense and Security Analysis* 26, no.4 (December 2010), 435.
[54] Trager and Zagorcheva, 94-108.

2.4 The Difficulty of Deterrence by Punishment

The evidence that nuclear deterrence worked during the Cold War is that there was no nuclear war between the two superpowers. However, today we have more states that own nuclear weapons, not only the U.S. and Russia (the USSR during the Cold War). And some of the possessors, or at least of those who are consistently trying to acquire them, can be labeled as rogue states. In their case, a transfer of nuclear weapons is one of the worrying situations. Obviously, states would like to deter rogue states from transferring weapons to terrorist groups, but it can fail sometimes. If a state's survival is in jeopardy, Jasen Castillo writes while mentioning examples of Iran and North Korea in his text, "*deterrent threats lose their punch, removing restraints on the transfer of nuclear weapons to terrorists*".[55] It seems that even a prospect of the punishment could not deter the actor from such behavior under some circumstances. Also, as Etzioni claims, a rogue state can turn into an unstable state, and then a deterrer would need to deter a number of actors within the state, not only the state as one actor.[56]

What can be also seen as problematic is a nuclear state deterring a non-nuclear state by possible punishment. For example, a nuclear state trying to deter an attacker from using chemical or biological weapons by the prospect of nuclear retaliation might also experience failure. Scott Sagan writes that in some cases, the attacker might believe the "*attack was below the threshold of chemical or biological use that would trigger a U.S. nuclear response*".[57] In this situation, we see that deterrence by punishment might fail because the attacker would not perceive a nuclear retaliation as a proportionate response for his action – a biological or chemical attack.

[55] Jasen J. Castillo, "Nuclear Terrorism: Why Deterrence Still Matters," *Current History* 102, no. 668 (2003), 430.
[56] Etzioni, 435.
[57] Scott D. Sagan, "The Commitment Trap: Why the United States Should Not Use Nuclear Threats to Deter Biological and Chemical Weapon Attacks," *International Security* 24, no. 4 (Spring 2000), 106.

Partly coming back to the first case when deterrence by punishment might be complicated is deterring terrorism or non-state actors. Brown and Arnold also touch upon this issue in their work, arguing it is more difficult to deter and punish terrorists. As they write, terrorists might not be rational, and they also do not form a coherent large target that could hit as a part of retaliation in the case of nuclear attacks on a certain state.[58] Given these facts, it is more difficult to deter them through punishment in comparison to the Cold War nuclear deterrence working between two superpowers. Trager and Zagorcheva, even though providing a possible way to deter some terrorist networks, admit there are significant difficulties and concepts that need to be taken into consideration, including the motivation of terrorists,[59] and "the return address problem" that complicates the punishment.[60] But, even though the punishment is problematic, deterrence by denial is still an option,[61] and that is similar to deterrence in cyberspace.

This section showed us that deterrence is difficult, and punishment might fail under various circumstances. While during the Cold War, we had two superpowers with nuclear weapons, deterrence (second-strike capability) worked, but when we have more actors, including rogue states and non-state actors, it gets more complicated. Deterrence by punishment is also difficult, sometimes even impossible, in cyberspace. I will talk about that in the next sections.

2.5 Deterrence in Cyberspace

As Will Goodman argues, cybersecurity rose in prominence in the first decade of the 2000s because it turned out to be a significant sector of conflict between states. States like Estonia,

[58] Brown and Arnold, 306.
[59] Trager and Zagorcheva, 95-108.
[60] Ibid., 108-111.
[61] Ibid., 96.

Georgia, South Korea, or the U.S. became victims of cyberattacks from different actors with different aims.[62] And even though that deterrence in practice might be outpacing theoretical knowledge,[63] cyber deterrence is today a topic of interest mainly for three reasons. Firstly, it seems that we will witness many cyber conflicts in the future. Secondly, deterrence worked in different domains, therefore, it might work also in cyberspace. And lastly, the costs are relatively low in comparison with a possible conflict.[64]

Goodman writes that deterrence in cyberspace is no different from deterrence in general. It is successful if a possible attacker decides not to attack. The decision is mainly based on predictions if the costs of the cyberattack will be higher than the benefits, and whether restraining from aggressive behavior in cyberspace will bring more benefits than costs. All the calculations are not necessarily completely rational and are often accompanied by inaccuracies.[65] Besides, there are many problems encompassing deterrence in cyberspace, including complexity, interconnectivity, and anonymity in cyberspace.[66]

What is considered by actors that deliberate about a possible attack is how difficult it will be (denial) and how severe the punishment might be. This is important because deterrence by denial is an option, but it does not work on its own. However, denial is also problematic in a sense. As Erik Gartzke and Jon Lindsay argue, denial is less effective when the target is of a lower value. And on the contrary, the likelihood of the attack is lower, if the effort needed to conduct the attack is high. Quoting the authors, "*most attackers will attempt to fly below the*

[62] Will Goodman, "Cyber Deterrence: Tougher in Theory than in Practice?," *Strategic Studies Quarterly* 4, no. 3 (Fall 2010), 102.
[63] Wilner, 3.
[64] Goodman, 103.
[65] Ibid., 107.
[66] Wilner, 8.

radar in order not to waste their resources, blow their cover, or invite retaliation".[67] But, coming back to the punishment, a potential perpetrator has to know that he will be punished for his malign actions. If there is no prospect of punishment, denial does not make any sense. It does not need to be severe, nor immediate. An aspect that matters in cyberspace more is a certainty. To put it simply, a victim has to know who to punish.[68] And here we encounter possibly the most difficult problem. Goodman himself admits that "*attribution surely poses difficulties, but the evidence suggests that it is possible in many cases*".[69] So, what is the attribution problem, and why it is a problem?

2.6 Problem of Attribution

We see that in the case of the Cold War nuclear deterrence, the situation was clearer than it is in cyberspace. If an attacker fires a missile at a defender, it was coming with "*a return address*".[70] In cyberspace, this might pose a problem as the attacker does not have to be so obvious. It is difficult to punish an unknown perpetrator. In other words, Tsagourias argues that if a cyberattack gives you a right to punish the perpetrator, the victim needs to find out who is responsible for it.[71]

As Alex Wilner sees it, the problem of attribution is given probably the greatest attention of all difficulties that are dominant in cyberspace.[72] Emilio Iaseillo sees the problem of attribution as

[67] Eric Gartzke and Jon R. Lindsay, "Weaving Tangled Webs: Offense, Defense, and Deception in Cyberspace," *Security Studies* 24, no. 2 (2015), 343-344.
[68] Goodman., 108.
[69] Ibid., 124.
[70] Nye, 50. citing after William J. Lynn III, "Defending a New Domain: The Pentagon's Cyberstrategy," *Foreign Affairs*, (September/October 2010), 99.
[71] Nicholas Tsagourias, "Cyber attacks, self-defence and the problem of attribution," *Journal of Conflict & Security Law* 17, no. 2 (2012), 233.
[72] Wilner, 8.

a challenge with a lot of questions that we need answers for.[73] Libicki also sees attribution as an important aspect of deterrence. Not in the sense we need to know whom to punish, but also whom not to punish. If the retaliator punishes the wrong actor, he is not only facing the original perpetrator but might possibly have a new enemy.[74] Rid and Buchanan in their work *Attributing Cyber Attacks*[75] argue that "*decisions of life and death depend on attribution*".[76] The fact that they think about attribution as a difficult obstacle is their idea that instead of a problem it is a complex process, and that identification of the perpetrator is needed for almost any kind of response.[77] They provide an overview of how to attribute cyberattacks and see attribution to be "*at the core of virtually all forms of coercion and deterrence*"[78] that authors like Nye would disagree with and I will get to his ideas later in this chapter.

Goodman admits it is difficult to attribute the attack, but it is still possible. He mentions situations when cyberattacks accompany physical attacks.[79] Amir Lupovici comes with a slightly different approach to the problem of attribution in his work *The "Attribution Problem" and the Social Construction of "Violence": Taking Cyber Deterrence Literature a Step Forward*.[80] However, he does not see attribution necessarily as a serious problem, even though there might be some difficulties. Similarly, to Goodman, he argues that cyber warfare might come with a regular kinetic attack, therefore, he believes that context could give us a clue about

[73] Emilio Iaseillo, "Is Cyber Deterrence an Illusory Course of Action?," *Journal of Strategic Security* 7, no. 1 (2013), 65.
[74] Libicki, 2009, 41.
[75] Thomas Rid and Ben Buchanan, "Attributing Cyber Attacks," *The Journal of Strategic Studies* 38, nos. 1-2 (2015).
[76] Ibid., 4.
[77] Ibid., 27-28.
[78] Ibid., 1.
[79] Goodman, 125.
[80] Amir Lupovici, "The "Attribution Problem" and the Social Construction of "Violence": Taking Cyber Deterrence Literature a Step Forward," *International Studies Perspective* 17, no. 3 (2014), 322-342.

the identity of the perpetrator.[81] But, cyberattacks do not have to come hand in hand with regular military attacks.

As it seems from existing literature, deterrence by punishment and denial are the most discussed. The first one is relatively dependent on the problem of attribution, while the latter is not. However, Aaron Brantly argues that these two are not enough to "*fully remediate the cyber deterrence problem*".[82] Deterrence might be expanded, as different tools and means exist, including norm development and entanglement.[83] These are also discussed by Joseph Nye in his work *Deterrence and Dissuasion in Cyberspace*.[84] Nye argues that "*the problem of attribution should not be belittled*",[85] but he does so while explaining four means of deterrence – punishment, denial, entanglement, and norms. Not all of them have to be fundamentally limited by the problem of attribution, even though punishment (and norms in a smaller degree) is problematic in that sense. Nye acknowledges the difficulty of deterrence in cyberspace but offers several means of deterrence that I will explain more broadly in the next section.

2.7 Four Means of Deterrence and Dissuasion

As already mentioned, Nye examines four means of deterrence and dissuasion in cyberspace. The first means mentioned by Nye is deterrence by punishment. As I have already discussed it earlier, I am not going to dedicate it a lot of attention in this section. Nye agrees that the problem of attribution has the greatest influence on the punishment's applicability. If a victim wants to punish a perpetrator, it should know his identity. For this particular reason, deterrence by punishment in cyberspace does not represent such an important tool, compared to deterrence

[81] Ibid., 330.
[82] Aaron F. Brantly, "The Cyber Deterrence Problem," *NATO CCD COE Publication* (2018), 49.
[83] Ibid.
[84] Nye, 44-71.
[85] Ibid., 52.

by punishment in conventional warfare. However, the punishment still remains applicable in cyberspace. But we need to know where the attack is coming from.[86]

The attribution is no longer a problem when we speak about deterrence by denial. It is easy to imagine how deterrence by denial works. States should work on increasing their resilience to make the cyberattacks look not worth conducting them. Once hostile actors believe that the benefits of such an attack are lower than its costs, the motivation to perpetrate decreases as well. Investments into stronger defense do not have to be necessarily high. A particular state could pay more attention to cyber deterrence and cyber hygiene that might ultimately lead to a situation when the state can focus especially on those major and advanced threats.[87]

The third means introduced in the text by Nye is deterrence by entanglement. In this case, the problem of attribution does not play any role. Deterrence by entanglement is sometimes also referred to as ”self-deterrence”. Entanglement is based on interdependence, and also perception comes into play. If a hostile actor believes that a possible cyberattack will not only harm the victim but due to high interdependence it will also harm the perpetrator himself, it might serve as a means of deterrence.[88] It is very questionable if entanglement could have played an important role in U.S. cyber deterrence in our case study, where cyberattacks were precisely targeted as a part of broader operations aiming to achieve certain political or strategic outcomes. In the thesis, I am not going to further discuss entanglement as a means of deterrence, but it is surely worth researching in the future.

[86] Nye, 55-56.
[87] Ibid., 56-58.
[88] Ibid., 58-60.

The last means of deterrence that Nye discusses is deterrence by norms, including taboos. Importantly, we have to admit that the creation of all these cyber norms is in their very early beginnings. According to Nye norms might work as a possible means of deterrence, as they "*can deter actions by imposing reputational costs that can damage an actor's soft power beyond the value gained from a given attack*", but similarly to deterrence by punishment, a certain degree of attribution is needed. Nye provides a notional example of a powerful state using nuclear weapons against a weaker state, in something we can label as a low-level conflict. This behavior would violate existing norms and harm the soft power of the state that used nuclear weapons. In addition, as Nye writes, "*norms impose costs on an attacker even if the attack is not denied by defense and there is no retaliation*". There is one important limitation of norms that Nye mentions. The attacker has to perceive the costs imposed by violating norms to be higher than the possible benefits of the action, and we cannot be absolutely sure about the perception in some cases.[89]

Nye compares deterrence by norms in cyberspace to norms that have been developed regarding nuclear, biological, and chemical weapons. And even though he admits they do not work perfectly, they might restrain hostile activities in cyberspace, including non-targeting of specific types of targets.[90] Saying that Nye mentions a difference between possible norms in cyberspace and norms related to the non-use of certain weapons. He argues "*it would be difficult to reliably prohibit possession of the whole category of cyber weapons*", but non-use against certain types of targets might work better.[91] Because norms in cyberspace are still not well-developed, I consider this fact a convincing reason to contribute to the discussion about cyber deterrence through engaging with literature on norms in cyberspace.

[89] Ibid., 60.
[90] Ibid., 62.
[91] Ibid., 61.

Based on the literature review, I have achieved several conclusions. According to many authors, deterrence by punishment is at least problematic, in many cases even impossible, because we do not know the perpetrator. When it comes to deterrence by denial, it seems it is still an option, even though it is not enough on its own.[92] And even both punishment and denial conducted at the same time are not always sufficient.[93] Therefore, we should be thinking about and using alternative means of deterrence. In the next chapter, I will evaluate assumptions about the traditional means of deterrence – punishment, and denial – to demonstrate they were not sufficient on their own in the case of the United States, except for deterring attacks on voting systems. At the same time, I will discuss more broadly deterrence by norms as an alternative means of cyber deterrence.

3 2016 U.S. Presidential Election and What Happened Afterwards

In 2016, it was the first time in U.S. history that a hostile state used cyberspace to try and influence the presidential election.[94] As Hennessey writes, the U.S. failed to deter Russia from this kind of behavior.[95] However, we would expect that Washington's concerns about cyberattacks would increase together with willingness and capabilities to deter them. A number of cyberattacks targeting the U.S. occurred,[96] and there were attempts to influence the election in 2020, but without "*persistent Russian cyber efforts to gain access to election infrastructure*".[97] These happened despite the fact that the U.S. reacted to the actions of the Russian Federation, and I will examine these actions in the next sections. So, what do these

[92] See Nye, 57. or Goodman, 108.
[93] Brantly, 49.
[94] Lipton, Sanger, Shane
[95] Hennessey
[96] Center for Strategic and International Studies
[97] National Intelligence Council, i.

facts tell us about existing assumptions about cyber deterrence – namely by punishment and denial? And how do they highlight the importance of alternative means of deterrence?

3.1 Punishment

The literature review gave us a clear idea of how complicated deterrence really is. A majority of the authors mentioned in the review agree that deterrence by punishment is very complicated, and to some degree impossible due to unsuccessful attribution. To evaluate this assumption on a real case, I will examine the actions of the U.S. after the 2016 election to assess the difficulties that deterrence by punishment brings into practice.

In 2017, the U.S. security agencies (NSA, CIA, and FBI) confirmed the suspicion that the Russians tried to interfere in the presidential election. Their aim was to influence the outcome of the election in favor of Donald Trump, who then won the election.[98] The conclusion of the intelligence community was that Russia used disinformation and cyberattacks to interfere in the 2016 election.[99] Russian hackers did it on several fronts. They targeted systems dedicated to voter registration, accessed some of them, and even managed to steal the personal information of voters.[100] Also, agents from the Russian military intelligence GRU hacked e-mails of people that worked for Hillary Clinton during the campaign for a presidential seat.[101]

And while the punishment has its difficulties (including the problem of attribution), "*it remains a crucial part of the dissuasion equation in cyberspace*".[102] It is, therefore, important to

[98] Sophie Marineau, "Fact check US: What is the impact of Russian interference in the US presidential election?," *The Conversation* (September 29, 2020).
[99] Olivia Beavers, "US intelligence says Russia seeking to "denigrate" Biden," *The Hill* (August 7, 2020).
[100] Abigail Abrams, "Here's What We Know So Far About Russia's 2016 Meddling," *Time* (April 18, 2019).
[101] Ibid.
[102] Nye, 55.

examine what kind of action, if any, the U.S. took to punish the Russian Federation. Even though there was a 1000-page report published focusing on the Russian interference,[103] the punishment for these activities can hardly be seen as sufficient for deterrence of further attempts of Russia. And it seems that the problem of attribution was not really a problem in this case, as the perpetrator was identified by the victim. Already in 2016, then-President Barrack Obama used executive orders to impose sanctions on the Kremlin for its role in the 2016 elections. Some intelligence operatives were expelled as a response to the interference, and sanctions also targeted intelligence agencies in Russia.[104] In June 2017, the sanctions on Russia were extended and approved by the U.S. Senate. Among the others, they were supposed to be imposed on Russians involved in cyber operations.[105] In 2018, 12 Russians were indicted by special counsel Robert Mueller for their involvement in the hacks of the election systems.[106]

Also, in the same year, the administration of President Trump imposed sanctions on 19 people that took part in the election interference in 2016. Russian nationals indicted by Mueller were among these 19. The sanctions, therefore, targeted GRU officers whose assets in the U.S. were frozen, and they prohibited U.S. entities to engage in business activities with them. In addition, the Internet Research Agency that was responsible for the disinformation campaign to influence the elections in favor of Donald Trump was also among the targeted entities.[107] The goal of the U.S. administration was clear: "*to address the ongoing nefarious attacks emanating from*

[103] Mark Mazzetti, "G.O.P.-Led Senate Panel Details Ties Between 2016 Trump Campaign and Russia," *The New York Times* (August 18, 2020).
[104] Lauren Gambino and Julian Borger, "Senate approves new Russia sanctions as punishment for meddling in election," *The Guardian* (June 14, 2017).
[105] Ibid.
[106] Abrams
[107] France 24, "US levies first sanctions on Russia over 2016 election meddling, cyberattacks," *France 24* (March 15, 2018).

Russia".[108] The U.S., therefore, punished Russia for its hostile actions. However, did the punishment deter the Russians from this behavior?

It seems that the response was not sufficient to deter Russia from its activities. In the 2020 election, Moscow again acted in favor of Donald Trump. In September 2020, Microsoft issued a statement accusing the Russian hackers involved in 2016 Clinton's hacking of an attempted breach of a communication and strategy company. The firm was working with then-presidential candidate Joe Biden.[109] William Evanina who served as a director of the National Counterintelligence and Security Center also warned about foreign threats, including Russia's attempts to denigrate Biden.[110] But in contrast to 2016, the type of cyber activities was different. According to Intelligence Community Assessment by the National Intelligence Council, Moscow's strategy for the 2020 presidential election consisted mainly of spreading misleading allegations and influence narratives to harm Biden, while in 2016 the Russians also tried to access election infrastructure.[111]

This section showed us that deterrence by punishment is problematic. While the security and intelligence agencies in the U.S. succeeded in identifying the perpetrators of cyberattacks and election interference, it does not seem that the punishment managed to deter them from this kind of behavior. And even though that the problem of attribution is the most discussed obstacle of punishment, we see that in the case of the U.S. this did not happen. As Brantly writes, there is another problem when it comes to deterrence by punishment, and I have already mentioned it in the literature review part – motivation of actors and, therefore, the proportionality of

[108] Ibid.
[109] Joel Schectman, Raphael Satter, Christopher Bing and Joseph Menn, "Exclusive: Microsoft believes Russians that hacked Clinton targeted Biden campaign firm – sources," *Reuters* (September 10, 2020).
[110] Beavers
[111] National Intelligence Council, i.

punishment. Paraphrasing Schmitt, Brantly mentions that if a deterrer wants to "*to prevent escalation or violations of international law*",[112] there must be an asset of comparable value identified for punishment.[113] It is difficult to assess whether Russia perceived sanctions and indictment of its citizens as a proportionate punishment, but they were clearly not afraid to try to influence the U.S. elections once again, using disinformation and cyber operations to collect information. Amy Popes writes that the chance this could deter them from this behavior in the future is low.[114]

3.2 Denial

The fact that deterrence by punishment is not an ideal option in cyberspace is also recognized by William Lynn. In 2010, he wrote that "*deterrence will necessarily be based more on denying any benefit to attackers than on imposing costs through retaliation*".[115] From the previous section we see that even though the U.S. did something to punish the Russians for their behavior, it did not deter them from trying to influence the elections once again. It is necessary to assess what happened in terms of deterrence by denial.

First of all, it is difficult to evaluate how deterrence by denial worked in some cases. We can hardly know what changes institutions that were hacked in the previous elections made, and whether these changes deterred the attackers from conducting cyberattacks. There are many ways how to improve deterrence by denial, ranging from allocation of finance, enhancing and updating infrastructure,[116] or effective cyber hygiene.[117] Unfortunately, I am unable to assess

[112] Brantly, 45.
[113] Ibid.
[114] Amy E. Pope, "Cyber-securing our elections," *Journal of Cyber Policy* 3, no. 1 (2018), 28.
[115] William J. Lynn III, "Defending a New Domain. The Pentagon's Cyberstrategy," *Foreign Affairs* (September/October 2010).
[116] Brantly, 47.
[117] Nye, 57.

which of these practices were employed by institutions that were attacked in 2016 and were not in 2020. For this particular reason, I will look at it differently – what does a case of successful deterrence by denial tell us about existing assumptions.

There are cases where deterrence by denial could have worked. As the Intelligence Community Assessment puts it, it seems that in contrast to the 2016 election, there were no "*persistent Russian cyber efforts to gain access to election infrastructure*".[118] This point is very important when it comes to assessing existing assumptions in the literature on cyber deterrence. Gartzke and Lindsay write about low-value and high-value targets. In the case of low-value targets, it is easier for an attacker to use deception to intrude. However, as the authors claim, with increasing efforts an attacker needs to put into the attack, the chances he will actually conduct the attack decrease.[119] That might be the case of the U.S. election infrastructure in 2020.

From the already mentioned Intelligence Community Assessment, we know that the Russians did not try to access the election infrastructure through cyber efforts. If Gartzke and Lindsay are correct, Russia might have been deterred because it had to invest a lot of effort to attack the election infrastructure. And according to the information available, the presidential election in 2020 "*was the most secure in American history*".[120] In a joint statement of the U.S. officials responsible for the security of the election infrastructure, several measures to protect the integrity of the election were named, including voting equipment certification and pre-election testing.[121] After the 2016 Russian interference, it was made a priority of the U.S. Cybersecurity

[118] National Intelligence Council, 2.
[119] Gartzke and Lindsay, 343.
[120] Jen Kirby, "Trump's own officials say 2020 was America's most secure election in history," *Vox* (November 13, 2020).
[121] Cybersecurity and Infrastructure Security Agency, "Joint Statement from Elections Infrastructure Government Coordinating Council and the Election Infrastructure Sector Coordinating Executive Committees," *CISA* (November 12, 2020).

and Infrastructure Security Agency (CISA) to secure the election, and it put a lot of effort into it.[122] Seemingly, the election infrastructure was of a high-value for the U.S., and Russia could have been deterred, as Gartzke and Lindsay assume when it comes to high-value targets.

But obviously, deterrence by denial is not a panacea. Nye writes there are cases when it probably will not work. He argues that "*at least some advanced persistent threats from the military or intelligence agencies of a major power are likely to get through most defenses*".[123] Implicitly, deterrence fails in these cases. There is no assurance that deterrence by denial will be sufficient even together with punishment. Brantly admits that deterrence by denial and punishment cannot solve the problem of deterrence. Except for traditional concepts of deterrence, he advises to also focus on various actions, including the development of norms.[124] Because we saw that deterrence by punishment and denial (besides high-value targets) are in some cases not enough for a successful deterrence, I will bring literature on cyber norms to contribute to the ongoing debate about cyber deterrence. Even though it goes beyond traditional concepts of deterrence, I argue it is an important complement and we should pay increased attention to it.

3.3 Norms as a Part of the Solution

Even though norms are not considered as a traditional means of deterrence in cyberspace, their role should not be belittled. The importance of norms is also highlighted in the *National Cyber Strategy of the United States of America*.[125] The strategy mentions the U.S. promotion of a framework dedicated to responsible behavior by states in cyberspace. The framework is based

[122] Kirby
[123] Nye, 57.
[124] Brantly, 49.
[125] The White House, "National Cyber Strategy of the United States of America," *The White House* (September 2018).

on behavior according to international law and non-binding norms that should lead the conduct of states during peacetime.[126] How could, therefore, norms in cyberspace contribute to the cyber deterrence of states?

Norms work in a simple way and could be defined as expectations of a certain form of behavior that are shared.[127] If a state breaks a norm, it could have an impact on its reputation. Nye gives several examples of already existing norms and taboos, including an expectation to not use nuclear weapons.[128] Substantial international cooperation focused on behavior in cyberspace started already in 2004, when Budapest Convention on Cybercrime became effective. However, it is not dedicated to issues like cyber espionage, and cyber military activities.[129] In cyberspace, there are some already existing norms that were developed, but it is questionable if states are behaving according to them. One of the most important institutions dedicated to the development of cyber norms is the United Nations Group of Governmental Experts (GGE) on Advancing responsible State behavior in cyberspace in the context of international security,[130] formerly known as the UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. The group endorsed new norms in 2014-2015 that expected states not to target critical infrastructure through cyberattacks during peacetime.[131] As I have already mentioned, it is questionable if the states behave according to these norms, given the fact that Russia targeted the U.S. critical infrastructure in March 2018.[132] And indeed, GGE talks more or less failed in 2017.[133] Two

[126] Ibid., 20.
[127] Alex Grigsby, "The End of Cyber Norms," *Survival: Global Politics and Strategy* 59, no. 6 (2017), 111.
[128] Nye, 60.
[129] Sven Herpig and Thomas Reinhold, "Spotting the bear: credible attribution and Russian operations in cyberspace," in *Hacks, leaks, and disruptions. Russian cyber strategies* (Paris: EU Institute for Security Studies, 2018), 34-35.
[130] United Nations Office for Disarmament Affairs, "Group of Governmental Experts," *United Nations*.
[131] Grigsby, 113.
[132] Center for Strategic and International Studies
[133] Grigsby, 113

years later, the discussion started again,[134] but when this paper was written, there were no significant developments. In addition, there were other attempts to develop norms regarding interference in states' internal affairs, but once again it failed because of different opinions on freedom of expression.[135]

While the process is accompanied by difficulties, there are actions that could be done and might work well when it comes to norms. The U.S. has been looking for opportunities to establish a group of states with similar interests in norms building. These like-minded states would then act against actors violating these norms through various means.[136] When such a group of states is formed, they can engage in the development of norms promoting democratic values. In addition, the states might come with a possible response that would be taken after violation of these norms, and work on the identification of measures with the potential to deter the violators.[137] It is important to have these norms because as we saw in the case of deterrence by punishment, it was difficult to assess whether the punishment was proportionate to the action of Russia. However, once norms are developed and established, and actors know what kind of behavior in cyberspace is not going to be tolerated, it will "*further solidify retaliatory threats*".[138] At the same time, there are cases that showed norms in cyberspace might work. Paul Baines and Nigel Jones write about commercial cyber espionage conducted by China. According to them, the U.S. succeeded in dissuading China from this kind of activity after actions taken against its military hackers.[139]

[134] United Nations Office for Disarmament Affairs, "Developments in the field of information and telecommunications in the context of international security," *United Nations*.
[135] Pope, 28.
[136] Grigsby, 115.
[137] Pope, 28-29.
[138] Wilner, 20.
[139] Paul Baines and Nigel Jones, "Influence and Interference in Foreign Elections," *The RUSI Journal* (2018), 1.

When it comes to certain norms more concretely, Martin Libicki writes about new norms that the U.S. advocates for related to political cyber espionage. While the practice itself seems to be acceptable at the moment, the use of information acquired through the process for political influence operations might be problematic.[140] As Libicki writes, the expectation stemming from such a norm would be that "*it is unacceptable for states to acquire materials by cyber espionage and release them to the public for doxing*".[141] He writes about it in the context of the DNC hack (2016 election in the U.S.) and the subsequent release of the information to influence the election. Even though Libicki sees difficulties regarding such a norm, he argues it might be useful if it is well-prepared.[142] In contrast to the suggestion in the previous paragraph about the coalition of like-minded states, Libicki argues for a broader list of signatories. Even China might be included in the agreement, mainly if it is invited to the norm-writing process. The case of economic cyber espionage mentioned earlier shows that Beijing also recognizes certain limits of cyber espionage. It is questionable if Russia would accept the norm. However, Libicki argues that Russia might understand that possible gains of practicing doxing are lower than costs if other states do it against Russia.[143] If some states are concerned with effective U.S. cyber espionage operations, they would possibly agree to such a norm to constrain operations of Washington D.C.[144] In this sense, the U.S. will also have to adhere to the norms if it expects others to do so.

Additionally, already in 2013, a report by GGE acknowledged that international law also applies to cyberspace,[145] which means there is some existing ground for further action. And

[140] Martin C. Libicki, "The Coming of Cyber Espionage Norms," *NATO CCD COE* (2017), 8
[141] Ibid., 7.
[142] Ibid.
[143] Ibid., 7-8.
[144] Ibid., 12.
[145] Adam Segal, "The UN's Group of Governmental Experts on Cybersecurity," *Council on Foreign Relations* (April 13, 2015).

except for other forms of malign behavior, this point is important for election interference, such as the one in 2016 in the U.S. Nicholas Tsagourias discusses the application of international law in cyberspace, particularly in relation to non-intervention and self-determination.[146] He writes that the Russian action in 2016 represented "*an unlawful intervention*",[147] as it used various methods including disinformation, the release of confidential information, and hacks.[148] With these actions, he argues that people's will and choices are controlled, and their self-determination right is violated.[149] Once there is international law, including non-intervention, applied in cyber activities, it will be able to fill now existing normative gaps.[150] Once again, if the U.S. expects other states to act according to international law and norms, it has to do the same. As Grigsby writes, the U.S. together with Israel allegedly used malware known as Stuxnet to damage facilities for nuclear enrichment in Iran. He adds that many legal scholars concluded this act "*was almost certainly a use of force prohibited under the UN Charter*".[151]

Therefore, despite the existing differences between various states, there is an opportunity to create an alliance of like-minded states that would develop norms based on democratic values and propose a response that would be taken once a violator acts against these norms. We see that even though it will be difficult to find a common ground with states that conduct hostile actions, including cyberattacks, there are existing pillars, including international law, upon which the norms could be developed, and unacceptable behavior punished. In addition, according to Libicki's claims, there might be a chance to develop common cyber espionage norms not only with like-minded allies but also with other states including China and Russia.

[146] Nicholas Tsagourias, "Electoral Cyber Interference, Self-Determination, and the Principle of Non-intervention in Cyberspace" in Governing Cyberspace: Behavior, Power and Diplomacy, *Rowman & Littlefield Publishers/Rowman & Littlefield International* (2020), 45-64.
[147] Tsagourias, 2020, 54.
[148] Ibid.
[149] Ibid., 53.
[150] Ibid., 56.
[151] Grigsby, 114.

As Grigsby writes, even though there are differences between Russia and the U.S., their interests are similar in some sense. Both countries "*seek to improve the stability of cyberspace and remove the incentives inherent to cyberspace that encourage risk taking*".[152] Norms about behavior in cyberspace are still in their early stage, but because traditional means of deterrence are not always sufficient, more attention should be dedicated to alternative means.

[152] Ibid., 111.

Conclusion

Deterrence is difficult when it comes to anonymous and interconnected environments such as cyberspace. Even the most powerful and developed states do not always have the ability to deter cyberattacks from various perpetrators, including nation-states, through traditional means such as punishment and denial. As the case study of the United States showed us, the Russian Federation tried to attack targets in the country multiple times, often with political aims. One of the most important events when the Russians interfered through cyber operations and the spread of disinformation was the U.S. presidential election in 2016. And even though it could have been assumed that the U.S. would pay significant attention to cyber deterrence, and it is difficult to assess whether it did or did not, it was obviously not sufficient.

Because, as I have mentioned in the methodology chapter, cybersecurity is a sensitive issue for which military and intelligence agencies are partly responsible, it was impossible for me to access classified documents. However, publicly available documents provided plentiful information. The aim of the thesis was to evaluate existing assumptions about the efficacy of traditional means of deterrence – punishment, and denial. Based on the case of the U.S. we saw that sometimes it is not sufficient to only focus on traditional means of deterrence such as punishment and denial, but that alternative means of deterrence should be taken into consideration. Firstly, from the literature, I have deduced that deterrence by punishment is often very difficult and sometimes even impossible, complicated by the problem of attribution. While in the case of the U.S., the perpetrators of the attack were identified as GRU officers and punished, it seems that the punishment was not sufficient, as the intelligence agency was accused of further cyber activities. Therefore, it was not deterred from behaving in a hostile way. Secondly, deterrence by denial is an option but does not always work. It was impossible to assess what was done in terms of increasing the difficulty to attack particular institutions,

however, deterrence by denial is not a panacea. There was one assumption about deterrence by denial, namely about low-value and high-value targets. While in the case of the former, it is difficult to deter the attacker, in the case of the latter, the chances are better. And indeed, according to available information from the U.S. intelligence community, the Russians did not try to target election infrastructure, compared to 2016 when they did. The U.S. officials highlighted the very high security of the election, implicitly labeling it a high-value target.

Nevertheless, the mere fact that Russians tried to influence the election, and attempted cyberattacks in the period 2016-2020, shows that traditional means of deterrence – punishment and denial – are not always enough to deter a possible attacker. I consider it to be an answer to my research question that was "*why do we need to pay attention to alternative means of deterrence in order to increase the effectiveness of overall cyber deterrence?"*. It is because traditional means seem to be insufficient. I conclude that one of the means of deterrence we should also focus on is the development of norms dedicated to behavior in cyberspace. Even though talks between states with different perspectives are progressing slowly, like-minded democratic states should establish these norms among themselves. At the same time, they should state a possible response that would be taken against a violator of these norms and come up with measures to deter possible attackers. Possibly, the coalition can be broader, and under some circumstances including states such as China and Russia. Deterrence can hardly be perfect, but at least it could be improved by alternative means, such as norms. And we can predict that in the future, they will be even more necessary than they are today.

References

Abrams, Abigail. "Here's What We Know So Far About Russia's 2016 Meddling." *Time*, April 18, 2019. Accessed May 19, 2021. https://time.com/5565991/russia-influence-2016-election/

Baines, Paul and Nigel Jones. "Influence and Interference in Foreign Elections", *The RUSI Journal* (2018): 1-8.

BBC News. "Twelve Russians charged with US 2016 election hack". *BBC*, July 13, 2018. Accessed May 19, 2021, https://www.bbc.com/news/world-us-canada-44825345

Beavers, Olivia. "US intelligence says Russia seeking to "denigrate" Biden", *The Hill*, August 7, 2020. Accessed May 19, 2021, https://thehill.com/policy/national-security/511078-top-intelligence-official-warns-of-foreign-influence-ahead-of-2020

Bennet, Andrew and Jeffrey T. Checkel. *Process Tracing: From Metaphor to Analytic Tool.* New York: Cambridge University Press, 2014.

Brantly, Aaron F. "The Cyber Deterrence Problem", *NATO CCD COE Publication* (2018).

Brown, Andrew and Lorna Arnold. "The Quirks of Nuclear Deterrence", *International Relations* 24, no. 3 (2010): 293-312.

Burton, Joe. "NATO's cyber defence: strategic challenges and institutional adaptation", *Defence Studies* 15, no. 4 (2015): 297-319.

Castillo, Jasen J. "Nuclear Terrorism: Why Deterrence Still Matters", *Current History* 102, no. 668 (2003): 426-431.

Center for Strategic and International Studies, "Significant Cyber Incidents", *Center for Strategic and International Studies* (2021). Accessed May 19, 2021. https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents

CNN Editorial Research. "2016 Presidential Campaign Hacking Fast Facts". *CNN*, October 28, 2020. Accessed May 19, 2021. https://edition.cnn.com/2016/12/26/us/2016-presidential-campaign-hacking-fast-facts/index.html

Collier, David. "Understanding Process Tracing", *PS: Political Science and Politics* 44, no. 4 (2011): 823-830.

Cybersecurity and Infrastructure Security Agency. "Joint Statement from Elections Infrastructure Government Coordinating Council and the Election Infrastructure Sector Coordinating Executive Committees". *CISA*, November 12, 2020. Accessed May 19, 2021. https://www.cisa.gov/news/2020/11/12/joint-statement-elections-infrastructure-government-coordinating-council-election

Etzioni, Amitai. "Rational Actors: Neither Mad nor M.A.D.: The Meanings of Rationality, Rogue States and Terrorists", *Defense and Security Analysis* 26, no.4 (December 2010): 431-438.

France 24. "US levies first sanctions on Russia over 2016 election meddling, cyberattacks". *France 24*, March 15, 2018. Accessed May 19, 2021. https://www.france24.com/en/20180315-us-levies-first-sanctions-russia-2016-election-meddling-hacking-cyberattacks

Gambino, Lauren and Borger, Julian. "Senate approves new Russia sanctions as punishment for meddling in election". *The Guardian*, June 14, 2017. Accessed May 19, 2021. https://www.theguardian.com/us-news/2017/jun/14/senate-proposes-new-russia-sanctions-meddling-election

Gartzke, Eric and Jon R. Lindsay. "Weaving Tangled Webs: Offense, Defense, and Deception in Cyberspace", *Security Studies* 24, no. 2 (2015): 316-348.

Goodman, Will. "Cyber Deterrence: Tougher in Theory than in Practice?", *Strategic Studies Quarterly* 4, no. 3 (Fall 2010): 102-134.

Grigsby, Alex. "The End of Cyber Norms", *Survival: Global Politics and Strategy* 59, no.6 (2017): 109-122.

Hennessey, Susan. "Deterring Cyberattacks". *Foreign Affairs*, November/December 2017. Accessed May 19, 2021. https://www.foreignaffairs.com/reviews/review-essay/2017-10-16/deterring-cyberattacks

Herpig, Sven and Thomas Reinhold, "Spotting the bear: credible attribution and Russian operations in cyberspace," in *Hacks, leaks, and disruptions. Russian cyber strategies*, 33-42. Paris: EU Institute for Security Studies, 2018.

Hodgson, Quentin E., Logan Ma, Krystyna Marcinek and Karen Schwindt. "Fighting Shadows in the Dark: Understanding and Countering Coercion in Cyberspace", *RAND Corporation* (2019). Accessed May 19, 2021. https://www.rand.org/pubs/research_reports/RR2961.html

Iaseillo, Emilio. "Is Cyber Deterrence an Illusory Course of Action?", *Journal of Strategic Security* 7, no. 1 (2013): 54-67.

Jervis, Robert. "Deterrence and Perception", *International Security* 7, no. 3 (Winter 1982-1983): 3-30.

Jibilian, Isabella and Katie Canales. "Here's a simple explanation of how the massive SolarWinds hack happened and why it's such a big deal". *Business Insider*, February 25, 2021. Accessed May 19, 2021. https://www.businessinsider.com/solarwinds-hack-explained-government-agencies-cyber-security-2020-12

Kirby, Jen. "Trump's own officials say 2020 was America's most secure election in history". *Vox*, November 13, 2020. Accessed May 19, 2021. https://www.vox.com/2020/11/13/21563825/2020-elections-most-secure-dhs-cisa-krebs

Libicki, Martin C. "Cyberdeterrence and Cyberwar", *RAND Corporation* (2009).

Libicki, Martin C. "The Coming of Cyber Espionage Norms", *NATO CCD COE* (2017).

Lipton, Eric, David E. Sanger and Scott Shane.“ The Perfect Weapon: How Russian Cyberpower Invaded the U.S.“. *The New York Times*, December 13, 2016. Accessed May 19, 2021. https://www.nytimes.com/2016/12/13/us/politics/russia-hack-election-dnc.html

Lupovici, Amir. “The “Attribution Problem” and the Social Construction of “Violence”: Taking Cyber Deterrence Literature a Step Forward”, *International Studies Perspective* 17, no. 3 (2014): 322-342.

Lynn, William J. III. “Defending a New Domain. The Pentagon’s Cyberstrategy“. *Foreign Affairs*, September/October 2010. Accessed May 19, 2021. https://www.foreignaffairs.com/articles/united-states/2010-09-01/defending-new-domain

Marineau, Sophie. “Fact check US: What is the impact of Russian interference in the US presidential election?“. *The Conversation*, September 29, 2020. Accessed May 19, 2021. https://theconversation.com/fact-check-us-what-is-the-impact-of-russian-interference-in-the-us-presidential-election-146711

Mazzetti, Mark. “G.O.P.-Led Senate Panel Details Ties Between 2016 Trump Campaign and Russia“. *The New York Times*, August 18, 2020. Accessed May 19, 2021. https://www.nytimes.com/2020/08/18/us/politics/senate-intelligence-russian-interference-report.html

Morgan, Patrick M. *Deterrence Now*. New York: Cambridge University Press, 2003.

National Intelligence Council. “Intelligence Community Assessment. Foreign Threats to the 2020 US Elections“. *Office of the Director of National Intelligence*, March 10, 2021. Accessed May 19, 2021. https://www.dni.gov/files/ODNI/documents/assessments/ICA-declass-16MAR21.pdf

Nye, Joseph S. Jr. “Deterrence and Dissuasion in Cyberspace.” *International Security* 41, no. 3 (Winter 2016/2017): 44-71.

Pope, Amy E. “Cyber-securing our elections“, *Journal of Cyber Policy* 3, no. 1 (2018): 24-38.

Powell, Robert. “Nuclear Deterrence Theory, Nuclear Proliferation, and Missile Defense“, *International Security* 27, no. 4 (Spring 2003): 86-118.

Rid, Thomas and Ben Buchanan. “Attributing Cyber Attacks“, *The Journal of Strategic Studies* 38, nos. 1-2 (2015): 4-37.

Rid, Thomas. “Cyber War Will Not Take Place“, *The Journal of Strategic Studies* 35, no. 1 (2012): 5-32.

Sagan, Scott D. “The Commitment Trap: Why the United States Should Not Use Nuclear Threats to Deter Biological and Chemical Weapon Attacks“, *International Security* 24, no. 4 (Spring 2000): 85-115.

Schectman, Joel, Raphael Satter, Christopher Bing and Joseph Menn. “Exclusive: Microsoft believes Russians that hacked Clinton targeted Biden campaign firm – sources“. *Reuters*, September 10, 2020. Accessed May 19, 2021. https://www.reuters.com/article/us-usa-election-

cyber-biden-exclusive/exclusive-russian-state-hackers-suspected-in-targeting-biden-campaign-firm-sources-idUSKBN2610I4

Segal, Adam. "The UN's Group of Governmental Experts on Cybersecurity". *Council on Foreign Relations*, April 13, 2015. Accessed May 19, 2021. https://www.cfr.org/blog/uns-group-governmental-experts-cybersecurity

Shear, D. Michael, Nicole Perlroth and Clifford Krauss. "Colonial Pipeline Paid Roughly $5 Million in Ransom to Hackers". *The New York Times*, May 13, 2021. Accessed May 19, 2021. https://www.nytimes.com/2021/05/13/us/politics/biden-colonial-pipeline-ransomware.html

Snyder, Glenn H. *Deterrence and Defense*. Princeton: Princeton University Press, 1961.

The White House. "National Cyber Strategy of the United States of America". *The White House*, September 2018. Accessed May 19, 2021. https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf

Trager, Robert F. and Dessislava P. Zagorcheva. "Deterring Terrorism: It Can Be Done", *International Security* 30, no. 3 (2005-2006): 87-123.

Tsagourias, Nicholas. "Cyber attacks, self-defence and the problem of attribution", *Journal of Conflict & Security Law* 17, no. 2 (2012): 229-244.

Tsagourias, Nicholas. "Electoral Cyber Interference, Self-Determination, and the Principle of Non-intervention in Cyberspace" in Governing Cyberspace: Behavior, Power and Diplomacy, *Rowman & Littlefield Publishers/Rowman & Littlefield International* (2020), p. 45-64.

United Nations Office for Disarmament Affairs. "Developments in the field of information and telecommunications in the context of international security". *United Nations*. Accessed May 19, 2021. https://www.un.org/disarmament/ict-security/

United Nations Office for Disarmament Affairs. "Group of Governmental Experts", *United Nations Office for Disarmament Affairs*. Accessed May 19, 2021. https://www.un.org/disarmament/group-of-governmental-experts/

Weiland, Noah. "5 Times the Trump Administration Has Been Tougher Than Trump on Russia". *The New York Times*, January 21, 2019. Accessed May 19, 2021. https://www.nytimes.com/2019/01/21/us/politics/trump-administration-russia-president.html

Wilner, Alex S. "US cyber deterrence: Practice guiding theory", *Journal of Strategic Studies* 43, no. 2 (2019): 1-36.