PATRIOTIC HACKERS OR RUSSIAN CYBERWARFARE?

ANALYZING RUSSIAN CYBERATTACKS IN ESTONIA AND GEORGIA

International Public Management and Policy

First Reader: Dr. A. Zhelyazkova

Second Reader: Dr. S. Grand

By

Dominick van Rens

515877

24,478 Words

18-7-2019

Abstract

Cyberattacks, and especially Russian cyberattacks, have started to play an increasingly larger role within international politics. However, at the same time, within the field of International Relations, a gap exists in the applicability of IR-theories on cyberconflicts. This thesis, through a congruence analysis, tests which theory works better in analyzing the perpetration of Russian cyberconflicts: realism or constructivism? Both theories are tested in two different case studies: The cyberattacks on Estonia after the removal of the Bronze Soldier in 2007 and the cyberattacks on Georgia in 2008 during the Russo-Georgian war. Ultimately, this research finds that although constructivism can best explain both conflicts, due to the characteristics of cyberspace, a single IR-theory is highly unlikely to be able to fully explain cyberconflicts. Realism is unable to explain the involvement of non-state actors within the conflicts, while constructivism is unable to explain state involvement, which is often hidden or indirect. As such, this thesis proposes a synthesis between constructivism and realism in order to capture the full context of Russian cyberconflicts.

Acknowledgements

I would like to thank my first reader, Dr. Zhelyazkova, and my second reader, Dr. Grand, for their extensive help and comments during the writing process of the thesis. Especially, the brainstorming sessions in the early stages of the thesis were a huge help in creating this finalized research. I want to thank Dr. Zhelyazkova for her patience, while I tried to give form to my abstract thoughts.

Contents

Abstract 1
Acknowledgements 2
1. Introduction 5
1.1 Research Question 6
1.2 Scientific Significance 6
1.3 Societal Significance 7
1.4 Thesis Structure 7
2. Literature Review 8
2.1 Cybersecurity: A Definition 8
2.2 Cyberspace 9
2.3 Cyber Power 10
2.4 Cyberattacks 11
2.4.1 Type of Cyberattacks 12
2.4.2 Russian Cyberattacks 12
2.4.2 Hacktivism 13
3. Theoretical Framework 15
3.1 Cybersecurity in International Relations 15
3.2 Realism 17
3.2.1 Offensive Realism and Defensive Realism 19
3.2.2 Offensive Realism and Cyberattacks 21
3.2.3 Offensive Realist Hypotheses 22
3.3 Constructivism 23
3.3.1 Cybersecurity and Constructivism 24
3.3.2 Constructivist Hypotheses 25
3.4 A Taxonomy of Actorness 25
4. Research Design 27
4.1 Method Selection 27
4.2 Congruence Analysis 28
4.3 Case Study Selection 29
4.4 Internal and External Validity 29

4.5 Reliability 30

4.6 Data Collection 31

5. Empirical Analysis 32

Case-Study 1: Estonia (2007) 32

Background of the Conflict 32

Realist Analysis of the Conflict 33

Constructivist Analysis of the Conflict 39

Case Study 2: Georgia (2008) 43

Background of the Conflict 43

Realist Analysis of the Conflict 45

Constructivist Analysis of the Conflict 50

6. Discussion 56

7. Conclusion 62

7.1 Limitations 63

7.2 Future Research 63

8. Bibliography 65

1. Introduction

"My promise to you today, in the short amount of time that I have to deliver on it, is that you will understand how little we, as a scholarly community, understand about this problem. And also how little international relations and political science scholars have attempted to deal with these problems" (Dr. L. Kello addressing the 4th Annual International Cybersecurity Conference 2014, 4:23).

Over the past decade, Russian cyberattacks have increasingly started to appear in international headlines, as these attacks target vital, digital infrastructures and international organizations. For example, in 2015, Russian cyberattacks on a Ukrainian power grid led to over 200.000 Ukrainian citizens being without electricity for several hours (Zetter 2016). In addition, the US found proof of Russian hackers meddling in the 2016 US election (Mueller 2019). Similarly, in 2017, Russian ransom software NotPetya caused billions of dollars in damage worldwide and temporarily disrupted international shipping. The attack wiped the IT-systems of A.P. Moller-Maersk, a shipping conglomerate responsible for one-fifth of the global shipping capacity (Greenberg 2019). Finally, in October last year, Russian hackers targeted the Organization for the Prevention of Chemical Weapons (BBC 2018). Research by the Centre for Strategic and International Studies placed Russia as the second-largest perpetrator of cyberattacks. In addition, the study estimated that between 2006 until 2019, almost one hundred cyberattacks, each causing at least one million dollars in damage, could be attributed to Russian hackers (CSIS 2019). Thus, Russian cyberattacks are among the most devastating and influential cyberattacks in the world, while the number as well as severity of cyberattacks have been increasing in the past decade.

However, when confronted with these attacks, Russian President Putin denied the involvement of the Kremlin and argued: "Hackers are free people, just like artists who wake up in the morning and start painting…[These hackers] would wake up, read about something going on in interstate relations and…they may try to add their contribution to the fight against those who speak badly about Russia" (Qtd. in Calamur 2017, 1). Putin argued that these "patriotic hackers" operated without guidance by the Russian government. Several reports point to the involvement of the Kremlin in these cyberattacks (See for example, Brattberg and Maurer 2018, Turovsky 2018, Mueller 2019). However, it is often difficult to establish direct links, due to the difficulty of attributing an attack. Regardless, Russian hackers belong to some of the major players in cyberspace. They effectively influence international relations by disrupting government websites, news agencies, and other aspects of a state's digital infrastructure.

Although cyberattacks have increasingly come to play a significant role within international relations (IR), scholars struggle to incorporate these attacks within the traditional IR-paradigms. Initially, these issues were seen as too technological and were analyzed only by those with the technical know-how. Nevertheless, those who study international relations increasingly need to understand cyberattacks to make sense of conflicts. Increasing hostilities by Russian hackers show that cyber is rapidly becoming an integrated part of international politics. Although scholars have analyzed individual conflicts through empirical analyses (See for example Deibert et al. 2012, White 2018), studies on the integration of these conflicts with traditional IR-theories, such as realism, liberalism, and constructivism, are severely lacking. It thus becomes necessary to see how cyberattacks are changing global politics and if, perhaps, IR-theories need to be adjusted in response.

1.1 Research Question

In order to contribute to solving the large gap in literature on the theoretical analysis of cyberattacks, this thesis shall ask the following research question: ***Which theory best explains the perpetration of cyberattacks attributed to Russian hackers, realism or constructivism?***

1.2 Scientific Significance

Through this research question, this thesis contributes to the scientific literature on cyberconflicts. The thesis analyses two important cyberconflicts. Also, by testing these through realism and constructivism, the thesis contributes to the integration of cyberconflicts within the traditional IR-paradigms. Furthermore, through the empirical results of the case studies, this thesis will also reflect on how IR theories effectively fall short or even need to be adjusted in order to make cyberconflict analyses possible. Currently there is a lack of integration of cyberconflicts with IR-theories. The thesis thus contributes to the scientific literature by testing two main IR theories: offensive realism and constructivism.

1.3 Societal Significance

In regards to its societal relevance, this thesis analyses a topic that is becoming increasingly relevant and that has been entering the forefront of global politics. At the same time, few frameworks or tools of analysis exist for this topic. The two case studies examined within this thesis, Estonia in 2007 and Georgia in 2008, are considered to be landmark events in the history of cyberconflicts. Nevertheless, the number of empirical studies on these events are surprisingly minimal. As Kello (2013) argues: “[I]ntegrating cyber realities into the international security studies agenda is necessary both for developing effective policies and for enhancing the field’s intellectual progress” (Kello 2013, 8). In placing these conflicts within IR, this thesis hopes to contribute to policy frameworks that help clarify Russia’s intensions with its cyberattacks. Ultimately, these policy frameworks can reduce the grey areas in cyberspace through which these untraceable and unattributable cyberattacks are possible.

1.4 Thesis Structure

This thesis shall first commence with a literature review and define critical elements of cyberconflicts. As often there is no consensus on definitions, it is crucial to establish clear definitions of the concepts that shall be utilized throughout the thesis. Second, the theoretical framework shall formulate three hypotheses for offensive realism and constructivism. Third, after the theoretical framework, the research design shall discuss the method selected, the case study selection, the internal and external validity, the reliability, and the data collection for this thesis. Fourth, the thesis shall analyze the two case studies: Estonia and Georgia. Each section shall commence with a historical background of the cyberattacks. After this historical background, the context behind the cyberattacks shall be analyzed through each respective theoretical lens. After the analysis of the context, each of the three hypotheses shall be tested. Fifth, in the discussion, the results of the hypotheses of each case study shall be analyzed, and these results will be compared and contrasted *within* each case study as well as *between* the two case studies. These findings will then reflect on the applicability of offensive realism and constructivism to cyberconflicts. Sixth, the conclusion shall quickly summarize the results of the study, discuss generalizability and shortcomings, and shall provide new avenues for further research.

2. Literature Review

Research on cyberconflicts falls within the broader literature of cybersecurity. This literature, in turn, is a subsection of security studies. Due to the lack of established definitions within the field, analyses of cyberconflicts often struggle to form a consensus on definitions, the focus of analyses, and many more issues. Consequently, before one can discuss the literature on cyberattacks, and especially Russian cyberattacks, it is first necessary to analyze what is meant with "cybersecurity," or how one "defends" from cyberattacks. As shall become evident, different definitions and viewpoints on what constitutes "cyber" and "security" arguably make it a difficult field of analysis. Additionally, this chapter shall analyze how to define cyberspace and which different forms of cyberconflict exist. Finally, it shall zoom in on the literature on Russian cyberattacks and hacktivism in order to place this literature within the larger frameworks and definitions of the preceding paragraphs.

2.1 Cybersecurity: A Definition

The difficulty in studying cyber security comes from the lack of an established definition of the concept, both in academia as well as in real life. As Hansen and Nissenbaum (2009) argue, despite the popularity of the term, "there has been surprisingly little explicit discussion within Security Studies on what hyphenating "security" with "cyber" might imply" (Hansen and Nissenbaum 2009, 1156). Examining the available literature on cyber in international relations in the past decade, Reardon and Choucri (2012) add that: "[w]ithin this issue area, the authors discuss a wide variety of phenomena – so wide, in fact, that it begs the question of exactly what is meant when the authors use terms, such as "cyber conflict," "cybersecurity," or "cyber warfare" (Reardon and Choucri 2012, 19). Cybersecurity currently concerns more of a spectrum of different definitions, rather than a specific all-encompassing term.

As a result, two actors discussing cyber security might engage in similar topics, but the extent of what they consider cybersecurity can be very different (Luiijf et al. 2016). How one defines cybersecurity is significant, as it determines what an actor will seek to defend (from), what it will expect, and how it will respond.

Galinec et al. (2017) define cybersecurity as "the governance, development, management, and the use of information security, OT security and techniques for achieving regulatory compliance, defending assets and compromising the assets of adversaries" (Galinec et al. 2017, 273). Galinec et al.'s definition focuses both on the defense of assets as well as the compromise of assets of adversaries. As a result, it forms a good definition through which cyberconflicts can be analyzed. After all, states often utilize cyberattacks in order to maximize their own cybersecurity. To this definition, another important distinction can be added: Cybersecurity is also “the safety and survivability of functions operating beyond cyberspace but still reliant on a computer host” (Kello 2013, 18). Cybersecurity relates not just to the security of the operating information systems, but also to the (often material) functions and components that rely on the network to perform their normal operations.

2.2 Cyberspace

To understand how cybersecurity functions within international relations, it is also necessary to understand how one defines “cyberspace.” As with cybersecurity, not one single definition of cyberspace exists. This lack of definition is primarily caused by the different schools of thought that engage with cyberspace. A technician will analyze cyberspace from a technological perspective and will be interested in different aspects of cyberspace than a political scientist. For the sake of this research, this section shall identify how political scientists define cyberspace.

To make sense of cyberspace, it is important to highlight the different elements of which it is composed. Kuehl (2009) defines cyberspace as “a global domain…framed by the use of electronics and the electromagnetic spectrum to create, store, modify, exchange and exploit information via interdependent and interconnected networks using information-communication technologies.” (Kuehl 2009, 27). This definition brings us two important qualities of cyberspace: *interconnectedness* and most importantly, *interconnectedness through infrastructures*. To this definition, Nye (2010) adds that cyberspace is “a unique hybrid regime of virtual and physical properties” (Nye 2010, 3). It is important to constantly realize that cyberspace is a virtual world with physical components. It is through the physical, technical aspects of cyberspace, such as the routers that provide internet, that cyberspace can be constructed. Finally, cyberspace is *accessible*. As the internet was designed to provide open-access to everybody, those who can link to the internet (in theory) can access all of the internet (Nye 2010). Cyberspace holds no territory and instead forms a unique, virtual domain, where everyone can be an actor. Also, cyberspace adds a degree of anonymity. as cyberspace allows users to mask their identity as well as their location. Thus, cyberspace is a virtual, interconnected space, with both physical and virtual properties, that shares information through interconnected infrastructures around the globe. Regardless of its physical properties, cyberspace is non-territorial and therefore accessible to all.

2.3 Cyber Power

Actors can abuse aspects of cyberspace to perform cyberattacks for a variety of motivations, that can range from gathering information to destruction. In that sense, actors can have *cyber power*, which is “the ability to use cyberspace to create advantages and influence events in other operational environments and across the instruments of power” (Starr 2009, 38). To this definition, Nye (2010) adds: Cyber power can be used to produce preferred outcomes *within* cyberspace or it can use cyber instruments to produce preferred outcomes in other domains *outside* cyberspace” (Nye 2010, 4). This distinction is important. Actors can influence cyberspace, but actors can also utilize cyberspace as an extension of (desired) actions in the physical domain. For example, through the Stuxnet worm virus of 2010, the US disabled 1,000 nuclear centrifuges in Iran, by making the centrifuges spin at excessive speeds followed by slower speeds. As a result, the tubes in the centrifuges eroded, which destroyed several Iranian nuclear plants (Langner 2017). In this case, the US used an attack in cyberspace to disrupt Iran’s nuclear energy network. Through cyber power, actors can thus not only control the cyber domain, but actions in the cyberdomain can manifest itself into physical consequences.

Actorness and cyber power hold a very peculiar relationship within the cyberdomain. Although in the physical world, states traditionally form (one of) the most powerful units of analysis, within cyberspace this distinction is not so clear cut. Due to the accessibility and openness of the internet, every individual with a computer could (in theory) attack a state’s digital infrastructure. Actors within cyberspace thus range from individuals, to groups, to companies and organizations, to states, with each having different goals and interests within cyberspace. Depending on the type of attack and the motivations of attackers, the resulting damage to companies or state digital infrastructures could be disastrous. In theory, a lone-wolf hacker could destabilize the infrastructure of an entire country. Thus, within cyberspace, a large variety of actors exists and due to the characteristics of cyberspace, states are no longer the single most powerful entities.

2.4 Cyberattacks

The distinctive feature of cyberspace creates three main problems, which provide attackers with an advantage over defenders. The first problem is that *attackers have an inherent advantage over defenders*. The internet was designed to provide open-access. This core aspect of the internet promotes exchanges of information but makes it difficult to defend from perpetrators attempting to invade (Dunn Cavelty 2014). Cyberattackers are continually searching for weaknesses within the network and cyberdefenders can only respond to attackers after these attackers breach the system. Defenders can only fill the proverbial holes *after* these holes have been breached by the attackers. As a result, defenders operate at a disadvantage to attackers. In addition, due to a large number of actors and the diffusion of power within cyberspace, defenders are susceptible to a wide variety of possible attackers.

The second problem is the *problem of attribution*. As the internet favors anonymity, it is often challenging to determine who perpetrated an attack and why. In addition, as Lin (2016) argues, it might be possible to identify the computer from which you were hacked, yet the owner of the computer could be unaffiliated with the hacker, being a victim of the hacker him/herself. To make matters more complicated, in attempting to retrace the original point of origin of the attack, investigators might have to first gain permission to search this computer, which the hacker used as a proxy to launch the attack (Lin 2016). Hackers can further conceal their IP addresses and deliberately place different languages within their code to throw attackers off their trail, so-called “false flags” (Van der Meer 2017, 88). Finally, the problem of attribution also problematizes state-orchestrated cyberattacks. Several states, such as China and Russia, have state-funded education programs to create cyberwarriors (Kramer 2016). However, these countries can always deny involvement, should their individual hackers be discovered. As there is no way to link an attack to a perpetrator fully, defenders instead have to utilize estimations on who is most likely to be behind attacks.

The third problem is that defenders also struggle with creating an appropriate response. First, it is difficult to provide an appropriate response to a cyberattack. For example, if your website is hacked by a group of malicious hackers (who can possibly be state-sponsored), you must ensure that your response does not exceed the scope of the damage created by the attacks (Libicki 2009). Second, it is also complicated to respond through other (military) means, for example, kinetic methods[1] as no rules and regulations

[1] Kinetic in this sense refers to military action, involving warfare and the use of lethal force, and will henceforth be utilized when discussing such military action.

exist that validate such a response. Third, establishing rules and regulations on what type of attack justifies a kinetic response might prove counterproductive. Potential attackers can use these regulations as guidelines in order to determine to what extent they can damage your digital infrastructure without reaching the threshold for repercussions (Van der Meer 2017). Thus, these three problems highlight why cyberconflict is becoming a more and more pressing issue and why it is difficult to defend from cyberattacks.

2.4.1 Type of Cyberattacks

The concept of cyberattacks similarly lacks a clear definition and includes a large variety of possible attacks. There are four main types of cyberattacks: Espionage, Denial-Of-Service Attacks, Logic Bombs and Trojan Horses (McGravan 2009). Cyber-espionage aims at attempts by A to capture crucial information from B. A Denial-Of-Service Attack (DoS) is "any event that diminishes or eliminates a network's capacity to perform its expected function" (Wood and Stankovic 2002, 55). The goal of a DoS-attack is disruption. The most commonly used DoS-attack includes "flooding," where one or multiple actors attempt to overload a digital infrastructure, for example, a website, through fake data requests. This flooding continues, until the network's maximum capacity is reached and it is no longer capable of processing "real" data requests. A Logic Bomb "sits dormant until certain conditions are met, at which point the program executes its malicious function" (McGravan 2009, 6). As the logic bomb waits to perform its function, it often spreads undetected, until its conditions are met. Finally, a Trojan Horse provides the illusion to the original owner of a computer that it is performing the desired function. However, instead, it gives unauthorized access to the computer by a third party. The third party can then remotely control this infected computer. Each of these four attacks can be utilized to gain a variety of results and there is no single attack that can be utilized to achieve one single result. Instead, the consequences of these attacks depend on the severity of the attacks, the intentions of the attackers, and the responses of the recipient.

2.4.2 Russian Cyberattacks

Russia often uses cyberattacks as an extension of its foreign policy goals. The *Gerasimov Doctrine* is central to Russia's strategic approach to cyberattacks. The doctrine outlines that non-military and non-political tools "applied in coordination with the protest potential of the population" (Qtd. In Vilmer et al. 2018, 55) are utilized to further strategic objectives, while military involvement is often concealed. This notion of hiding the involvement of the Russian government, while using the full spectrum of political and economic tools, is further utilized in cyberspace. Rather than operating in a single domain, Russia develops its cyber-capacity as an extension of its other operational domains. These capacities can then be utilized in conjunction with its other enforcement tools (Popescu and Secriercu 2018, 22). Russia utilizes cyberoperations to dominate the information landscape in order to "[shape] individual and collective perceptions, to alter how people make decisions and how societies see the world" (White 2018, 3). This has recently become evident through the discovery of Russian "troll-factories" that are created to sway Western public opinion (Meduza 2017), Russian attempts to influence the US 2016 Presidential election (Mueller 2019), and its overall attempts to destabilize Western democracies (Brattberg and Maurer 2018). In addition, the Russian government views the struggle within the information space as relatively constant and unending. Consequently, Russia has a lower threshold in deploying its cyber-capabilities in ways which others, such as the US, will perceive as threatening or escalatory behavior (Connell and Vogler 2017). Thus, Russia utilizes cyberattacks as an extension of its other operational domains to achieve its goals. Furthermore, the usage of these cyberattacks as an extension of state power has become normalized for Russia in a way that differs sharply from other states.

2.4.2 Hacktivism

Cyberattacks are also perpetrated by individuals or groups of individuals for political purposes against states, corporations, and other individuals. These actors often perform these attacks out of protest. These acts seek to disrupt the normal functioning of governing authority in power or are hold a symbolic function and message. As a result, these acts are often called *"digital activism"* or "*hacktivism*." Karatzogianni (2015) defines digital activism as "political participation, activities and protests organized in digital networks beyond representational networks. It refers to political conduct aiming for reform or revolution by non-state actors and new socio-political formations such as social movements, protest organizations, and individuals and groups from the civil society" (Karatzogianni 2015, 3). Hacktivists utilize the same tools as many cyberattackers, but their attacks have different goals. The attacks are acts of *political symbolism*, meant to humiliate the enemy or draw attention to a specific (social) issue. For example, in speaking about DDoS attacks,[2] Sauter (2014) explains these attacks as modern-day sit-ins, much like the sit-ins of the 1960s. Where sit-ins would disrupt the functioning of a governing body or corporation by physically obstructing space, DDoS attacks cause the same, temporary disruption, but through digital means. In doing so, DDoS attacks open up space for new actors in the public discourse by disrupting the dominant narrative of those in power (Sauter 2014, 29). Therefore, hacktivists utilize cyberspace as an extension or a replacement for traditional activism. As a result, similar to traditional activists, they utilize their cyberattacks to convey a message within the public discourse.

Karatzogianni (2015) devised a distinction between two different causes for hacktivism and cyberconflicts: Sociopolitical and ethnoreligious causes. Ethnoreligious cyberconflicts "include hacking enemy sites and creating sites for propaganda and mobilizational purposes…there is a greater reliance on traditional ideas, such as protecting the nation or fatherland and attacking for nationalist reasons" (Karatzogianni 2015, 19). As a result these conflicts often have a clear us-versus-them approach, where the enemy is juxtaposed to their own, often imagined, community. Largely due to the War on Terror, ethnoreligious cyberconflicts emerged between 2001-2007 and these cyberconflicts were often conjoined with the battle against terrorism. In contrast, sociopolitical cyberconflicts focus more on utilizing the internet as a tool for mobilization, as a way to frame the narrative of a political conflict, and as a political opportunity structure (Karatzogianni 2015). Rather than utilizing the internet as a medium of attack and division, socio-political cyberconflicts utilize the internet in order to organize protests or provide alternative information to evade national censorship. Thus, the root causes between both conflicts differ from their usage in *othering* (ethnoreligious) and *mobilizing* (socio-political).

Russian hackers focus on perpetrating cyberattacks that are oriented towards the governments of other states and are often rooted in ethnic or identity conflicts, involving Russian-speaking minorities in other countries. As a result, these types of attacks primarily fall within the context of ethnoreligious cyberconflicts. Due to its societal focus on IT, Russia has a large population of "patriotic" hacktivists that carry out cyberattacks. At the same time, however, these hacker-groups are outward-oriented and focus on punishing other states rather than protesting against infringements by the Russian government (Connell and Vogler 2017).

[2] DDoS-attacks are similar to Dos-attacks. The extra "D" refers to "distributed," meaning that in contrast to a DoS-attack, which is launched from a single computer, DDoS attacks distribute their attacks through a multitude of computers around the world.

These hackers are often deemed patriots, and it is unclear whether these hacker groups are part of the Russian government, supported by it, or merely act on their own accord. There has been evidence that at least some of these hackers belong to the first category. The Internet Research Agency in St. Petersburg, also known as the Russian troll factory, is an organization with links to Russian companies and politicians that seeks to disrupt the functioning of other democracies through campaigns of misinformation (ODNI 2017). The existence of such companies erases the boundary between patriotic civilian hackers and government-coordinated political hackers, and this consequently affects the "activism" done by said hackers. If the Kremlin orders these hackers to coordinate a cyberattack on another state under the guise of "protest," this might resemble citizen-led activism, but the Russian government ultimately controls these forms of protest (Popescu and Secriercu 2018).

3. Theoretical Framework

To examine the role of cyberattacks in international relations, this thesis shall test two different competing theories on the subject: offensive realism and constructivism. The following paragraphs shall discuss the approach of IR's three core theories of realism, liberalism, and constructivism towards cybersecurity and why offensive realism and constructivism will be chosen for the thesis. Then, these paragraphs will describe each theory and formulate hypotheses.

3.1 Cybersecurity in International Relations

Originally, cybersecurity was little studied, as traditionally, the field of security studies has had a primarily classical realist and thus state-centric focus. Such a traditional approach associates security with "*the alleviation of threats to cherished values*, especially those which, left unchecked, threaten the survival of a particular referent object in the near future" (Williams and McDonald 2018, 6). Nevertheless, this approach towards security only allowed for the analysis of military warfare between states and left no room for many emerging security issues of the past decade, such as terrorists and other non-state actors. As Erikkson and Giacomello (2006) note, a divide has emerged within security studies between state-centric "traditionalists" and "wideners." Wideners argue for the broadening of the concept as the rise of new challenges in the political, societal, economic, and environmental domains also pose threats to security and thus a focus on military (in)security is no longer sufficient (Erikkson and Giacomello 2006, 227). This concept of "widening" is promoted by the

Copenhagen School, invented by Buzan, Waever, and De Wilde, which argues that through securitization theory "[s]ecurity is a particular type of politics' that occurs not just in the traditional military sector, but also in four other sectors: the political, economic, environmental, and societal sectors" (Qtd. in Nyman 2018, 105). Therefore, the Copenhagen school can bypass traditional approaches to security as limited to the military and instead engage with a wider variety of acts of securitization.

Before 2010, wideners rarely addressed the emergence of the internet and other elements of the information revolution. Nevertheless, due to the increased prevalence of security threats via cybersecurity in recent years, it has emerged as a subset of security studies within international relations. Historical events such as the Stuxnet virus in 2010 as well as increased Russian propaganda warfare have allowed cybersecurity to emerge at the forefront of the research agenda. In order for IR-analyses of cybersecurity to be possible, it is necessary to utilize wider definitions of security. Thus, the definition of security provided by the Copenhagen School serves as the basis for many of the new international relations analyses of cyber security, whether the study is realist, liberalist, or constructivist.

Although each of the theories approaches cybersecurity through this wider lens, the three main theories of international relations, realism, liberalism, and constructivism, nonetheless deal with cybersecurity in unique ways that are rooted in the core of each theory. First, within the school of realism, cybersecurity is posited within the traditional security dilemma, and realism gives little room to non-state actors. (Eriksson and Giacomello 2006, 229). Instead, realism primarily engages with cybersecurity from a state-centric focus. The emphasis lies on cyber defense and cyber warfare, as an extension of traditional military methods between states (Mehmetcik 2014).

Second, within the school of liberalism, cyberspace is often approached in terms of international cooperation rather than conflict. Erikkson and Giacomello (2006) argue that a liberal analysis of cybersecurity brings about two important realizations: "(1) the expanding partnership between the public and private sectors to provide services and (2) the merging of the civil and military spheres" (Erikkson and Giacomello 2006, 231). In that sense, liberal complex interdependence theory provides a lens to analyze emerging trends in cyberspace. Nevertheless, due to its reluctance to tread into both realist territory and security studies, liberal theories have often steered away from security analyses, focusing on economic issues instead. Liberal analyses of cyberspace have solely focused on the possibilities for cooperation and the institutionalization of cyberspace (Erikson and Giacomello 2006; Reardon and Choucri 2012; Petallides 2012).

Third, constructivism, due to its emphasis on symbolism and language analyzes the large diversity of threats emerging within the cyberspace. As discussed above, the Copenhagen School embodies the constructivist approach towards security (and thus cybersecurity), as it focusses on how language can turn political issues into security issues. Constructivism then focuses on how issues are framed and "seems apt for analyzing the symbolic, rhetorical, and identity-based aspects of digital-age security" (Erikkson and Giacomello 2006, 235). A constructivist analysis of cybersecurity can provide new insights that other theories cannot. For example, as Petallides (2012) argues: With no infrastructure, hierarchy, or set membership, *Anonymous* is being defined as "the first internet-based superconsciousness" (Petallides 2012, 3). By focusing on the language, symbols, and the significance of the imagery that binds the members of this diverse group together, a constructivist approach can shed light on how this group is constructed and forms a security threat, even though its members have no material connection to each other.

Thus, after comparing the three main theories of international relations and their approach towards cybersecurity, this thesis shall utilize realism and constructivism for its analysis. As the thesis aims to analyze conflicts, liberalism is not useful precisely due to its idealist focus on cyber-*cooperation* rather than *conflict*. Although liberalism does analyze the interaction between the public and private sector, which is a vital aspect of cybersecurity, liberalism is ultimately ill-suited for security analyses (Erikkson and Giacamello 2014). In contrast, realism provides a good lens to analyze cyberattacks, through its inherent focus on inter-state conflict and the usage of cyberattacks as a power-tool. Constructivism juxtaposes the realist interpretation of cyberattacks, through its emphasis on narratives and ideas. It focuses more on how differences in identities can lead to conflicts. In addition, constructivism analyzes how cyberspace, and thus conflicts, work as an extension of (physical) social life. Therefore, realism and constructivism provide the most interesting lens in analyzing Russian cyberattacks and will consequently be tested in the case studies.

3.2 Realism

In order to understand how realism intersects with cybersecurity, it is first necessary to understand the core assumptions of realism. Two main paradigms exist within the realist school of thought: classical realism and structural realism. Both paradigms agree on five premises that form the basis of realist theory. First, the international system is *anarchic*. Second, as states possess (some form of) military capacity to hurt other states, *power* is the defining feature in the international environment and the relations between states. Third, states can never be certain about the intentions of other states and are thus inherently *insecure* about the constant possibility of the outbreak of war. Fourth, states are ultimately solely concerned with *survival*. Fifth, states are *rational actors* and take strategic decisions to protect their well-being, although they are capable of making miscalculations in their decision-making (Mearsheimer 1994). To this, Glaser (2016) outlines two more premises: Sixth, states *assess* each other in terms of their power and *capabilities*. Seventh, states are the dominant actors within the international system and are thus the unitary focus of analysis (Glaser 2016). Together these seven premises paint a picture of an anarchic international system, dominated by states and characterized by *power* and *insecurity*. In this system where each state attempts to secure its *survival* and is inherently distrustful of other states who attempt to secure the same. As each state *assesses* the military capabilities of its competitors and uses this information to *rationally* inform its decision-making, states respond to the actions of other states.

However, classical realism and structural realism also significantly differ in their focus of analysis. First, both theories have different explanations for *why* states want power. Classical realists argue that this search for power is inherent to an imperfect human nature, dictated by self-interest, egoism, and emotions. Structural realists argue that power-seeking is dictated solely by the structure of the international system. Due to a lack of a global overseeing authority, states are afraid that rival states will seek out opportunities and attack them. Thus, states seek power to ensure their survival. Classic realists instead view anarchy as a “permissive force not a causal one” (Jepson 2012). Other factors, classical realists claim, such as nationalism or ideologies, can also affect a state’s search for power (Jepson 2012). Structural realists contrast this, as they claim that each state, regardless of its regime type or culture, is subject to the same incentives provided by the international system (Mersheimer 72). Second, both theories also differ in how they *define* power. As classical realism takes an imperfect human nature, as its cause for a search of power, classical realists focus on military capabilities, but also include a nation’s character and morale. Structural realists, due to their emphasis on ‘scientific realism’, view power solely in material (often military) terms, as these tangible variables are easier to quantify (Pashakanlou 2009).

Thus, although significant overlap exists between both strands, classic and structural realism differ primarily in how they define power and in explaining why states seek to acquire power. This thesis shall utilize *structural realism* as its theory of focus. As classical realism does not consider the structural power relations embedded within the international system, it is vulnerable to missing the intricacies of international power relations between states and how these power relations consequently play out within the cyber-domain. Due to its emphasis on the anarchic nature of the international system (which holds true for cyberspace as well) and the resulting search by states for survival, structural realism seems to be more applicable for an analysis behind the perpetration of cyberattacks. Also, structural realism has a more systemic approach in contrast to the empirical approach by classical realists. Thus, structural realism shall be utilized within this thesis for the realist analysis.

3.2.1 Offensive Realism and Defensive Realism

Structural realism can further be divided into two strands: Defensive realism and offensive realism. Defensive realism forms the original structural realism, as argued by Kenneth Waltz, and it argues that the international structure does not create a necessity for state competition. At the heart of defensive realism is the *balance of power:* States will seek to avoid conflict and instead ensure that no state is powerful enough to dominate all others. As Glaser (2016) argues: “A state’s acquisition of excessive power convinces other states to align against it, thereby undermining this strategy” (Glaser 2016, 16). Defensive realists add to this the notion of *the offense-defense balance*. This focus argues that the relative ease or difficulty of conflict determines whether a conflict will break out. “When military technology, geography, the character of diplomacy, etc., combine to make conquest difficult, then security is plentiful and the danger of war declines” (Walt 2017, 7). Defensive realists challenge the realist belief that security is scarce and instead focus on how states can increase their security through, for example, adoption of defensive military postures.

Offensive realists agree on the premises of defensive realism but differ from defensive realists on one important point: Where defensive realists (Waltz) predict that states want to maintain the status quo as a result of their search for security, Mersheimer (1994) argues that states want to *maximize* their power. States seek to increase their power in the international system, aiming to become hegemonic states and seek to expand their material, military capabilities (Mersheimer 1994). After all, the stronger the state, the better it will be capable of protecting its interests. For offensive realists, “power maximization is a *means*, not an *end*” (Glaser 2016, 20). In order to maximize their security, states will seek to maximize their power. Consequently, due to the anarchic nature of international society, states are forever engaged in this power/security maximization. As a result, states are continually seeking to maximize their own power/security by diminishing the power/security of competing states.

Due to their different approaches, offensive realism ~~juxtaposes~~ is distinguished from defensive realism in four distinct ways: First, defensive realists claim that a balance of power or status quo will form in global politics. Offensive realists argue that through security maximization the international system is inherently unstable (Craig and Valeriano 2018). Second, defensive realists claim that if a state attempts to maximize its power, other states will cooperate against this state to diminish its power. Consequently, the search for power-maximization is irrational. Offensive realists counterargue that balancing is often ineffective, which entails that aggressive states are likely to succeed. As a result, states will engage in "rational power-maximizing behavior" (Glaser 2016, 20). If states see the opportunity to increase their power without a likely rebuttal, they will always take that opportunity (Walt 2017). Third, defensive realists believe that cooperation between states is possible, as long as uncertainty about states' intentions can be reduced. Offensive realists argue that states often lie about their motivations and that each state will always seek to maximize its power (Hamilton and Rathbun 2013). Fourth, the defensive realists ultimately argue that conquest is hard and that the costs often outweigh the potential benefits. In addition, increases in military technology will make military conflict harder, as countries become better at defending themselves. Offensive realists claim the opposite, as they argue that historical conquests have provided benefits to the attacking states and that increases in military technology will facilitate attempts at conquest (Mearsheimer 2014). Thus, while defensive realists focus on the global status quo, power balancing, state cooperation, and the costs of conquest, offensive realists claim the opposite and have a more pessimistic view of states that inherently seek to increase their own power at the cost of other states.

Although each of the realist strands can provide valuable insights into the analysis of cyberattacks, this thesis will utilize *offensive realism* as its theory of focus. As defensive realism focuses more on the preservation of the status quo, rather than the expansion of a state's power, it is considered less relevant for the focus of this thesis. Defense realism posits that ultimately the international system will start to balance and conflicts will decrease, as the costs for conflicts begin to outweigh the benefits. Within cyberspace, however, as there is significantly less risk for retribution, the benefits of cyberattacks increase rather than diminish. Furthermore, although defensive realists claim that increases in military technology will lead to a decrease in conflict, within cyberspace the opposite development has happened. As cyberspace favors attackers over defenders, many of the offensive realists claims, such as power/security maximization, are applicable to cyberconflicts. Therefore, offensive realism provides the best lens through which cyberconflicts can be analyzed.

3.2.2 Offensive Realism and Cyberattacks

In general, realism has paid little attention to cybersecurity. It considers security to be primarily military and considers states as the sole unitary actors within global politics. As Walt argues: “[R]ealist theories define “security” as the security of the state and place particular emphasis on the preservation of the state’s territorial integrity and the physical safety of its inhabitants” (Walt 2017, 2). As a result, the emergence of non-state actors that hack governmental structures is not viewed as warfare, as states are the solitary actors. More so, these non-state actors are not considered to be “actors” that are capable of harming the security of a state. Realists focus on territorial integrity and this can only be harmed by another state.

Nevertheless, as Erikkson (2006) argues: “Some realists would likely consider information warfare as relevant, if defined as a new technological component in otherwise traditional interstate conflict” (Erikkson 2006, 231). Within this view, cyberattacks can be analyzed through a realist lens if approached as being part of an interstate conflict. Mehmetik (2014) argues that one can only consider cyberattacks as cyberwarfare, if the attacks are performed by groups with a political motive, as instructed by states. This thesis shall utilize Mehmetik’s argument that cyberattacks are “inter-state conflict through extension” in order to analyze the case studies through a realist lens. After all, since cybersecurity attacks are often untraceable, it is difficult to determine who perpetrated cyberattacks. Even if one can identify the attackers, it is still impossible to link these actors to the state without a confession. To evade this attribution problem in a realist analysis, this thesis shall instead focus on whether the cyberattacks could thus be considered as a vehicle for interstate-conflict.

If one views cyberspace as an existing, albeit virtual, space in which states seek to assert their dominance, many of the realist assumptions can be readily translated. In fact, the reigning anarchy within the cyberspace domain would be welcomed by structural realists, as it mirrors the premise of systematic anarchy in global politics. However, the lack of territory as a focal element of strength means that states can simply no longer be the only unit of analysis. In principle, one lone wolf with strong hacking expertise could challenge a state and threaten its security. Although one might posit that such attacks often do not threaten the direct physical security of citizens, such security is threatened through extension. For example, as has become evident in Ukraine, a hacker group can disable the energy system of a region. In addition, states are no longer limited by geography and geographic distances. Thus, cyberspace also brings with it a new set of rules that diminishes the relative power of states over other non-state actors and reduces the importance of geographic proximity for launching attacks.

How can offensive realism nonetheless be utilized to analyze cyberattacks? Although this field is severely underdeveloped, offensive realism offers several tools that can help to analyze cyberattacks. As offensive realism argues: States are more likely to attack if there is little chance for repercussions, as states continually seek to maximize their power. Thus, the problem of attributing cyberattacks will provide favorable conditions for attacks, as the problem of identifying culprits decreases the chance for repercussions by cyber-victims. If states are viewed as inherently competitive and have security maximization as a means, the prevalence of cyberattacks is further reinforced. Cyberattacks provide an opportunity to attack and diminish competitors or expand one's own security. For example, a cyberattack can be launched to immobilize a country's defenses in conjunction with a kinetic attack. In addition, as Mearsheimer (2014) argues, great powers seek regional hegemony and constantly seek to influence circumstances in different regions in order to prevent other great powers from becoming too powerful (Mearsheimer 2014). As cyberattacks do not require geographical proximity, cyberspace thus facilitates diminishing the security of regional hegemons across the globe, as attacks can be launched from any place and reach their target within seconds.

3.2.3 Offensive Realist Hypotheses

Therefore, by utilizing a realist lens to look at the motivation for the perpetration of cyberattacks in international conflicts attributed to Russia, I come to the following hypotheses:

H1: In an anarchic international system, cyberattacks are perpetrated solely by states, either directly or indirectly, in order to maximize their own cyber power, which functions as an element of the protection of national security.

H2: States act as "cybersecurity-maximizers," where states attack other states in their neighborhood or other international competitors in order to maximize their own national security relative to their competitors.

H3: As great powers seek regional hegemony, cyberattacks will be utilized in cases where outright kinetic warfare is not possible, in order to increase a state's regional power position)

3.3 Constructivism

In contrast to realism, constructivism concerns itself with ideas and discourses. A central concept of constructivism is that objectivism and facts are rarely "true." Instead, what we perceive as facts and objective reality are the result of narratives and constructs, which have caused some ideas to become dominant over others. Similar to realism, constructivism holds several core assumptions. However, these core assumptions are less strict than those of realist theory, precisely due to the dynamic perceptions by constructivists of international politics. First, international politics are not solely dominated by states, but also entail other actors, such as NGOs and multinational corporations. Second, in contrast to realism, "[c]onstructivists argue that the identity and interests of states (and actors) change across contexts and over time" (Ackerman et al. 2010, 2). As a result, the interests and identities of actors are malleable and dynamic. Consequently, constructivists do not believe that anarchy is the primary state of international politics. Instead, such a system is the result of a long process of interstate relations, rather than a structural component embedded in global relations (Wendt 1992, 394). In other words, as Wendt aptly named his landmark article, anarchy is what states make of it. Thus, constructivism rejects many of the core realist assumptions which view anarchy, self-help, security, and the resulting power struggles as a given, and instead argues that these are but one of the many possibilities that could characterize international relations. In fact, some constructivist explain the realist security dilemma as "the preservation of an existing identity and a set of recurring relations with others…[These constructivists'] view sees states not as trapped in security dilemmas that they would prefer to escape, but rather as attached to conflictual relationships that help preserve the state's own identity" (Mitzen 2006, 353). This example shows how even the security dilemma can merely be posited as a social relationship originating out of the need for the preservation of a state's identity. Therefore, many of the core realist assumptions on the structure of international politics are but one version of political reality.

Third, as a result, the nature and interests of actors cannot be described without taking into context the particular historical period that facilitated this nature. Fourth, constructivists emphasize the role of the immaterial characteristics of international politics by emphasizing ideas, institutions, and meanings (Ackerman et al. 2010). Finally, actors are as a consequence shaped by their social context, which determines their behavior, just as actors change this social context through their actions. This two-way dynamic ensures that everything in international relations, from the nature of actors to their interests, is never static, but continually changing. This is not to say that dominant narratives or ideas do not exist. In fact, national identities form a good example of a dominant narrative that shapes an actor's interaction, while this narrative is very robust to change. That said, national identities are also under constant pressure from narratives by those who do not fit the dominant narrative. Should one of these narratives prevail, the social context, ideas, and interests of the actors embedded within this narrative will effectively change. An excellent example of this is the social movements of the 1960s in the US, which effectively changed the dominant narrative to include women, minorities, and the LGBTQ+ community. No matter how robust the narrative or ideas, it is always susceptible to (slight) change.

Therefore, constructivists view international relations as emerging out of the ideas and interests of a wide range of actors embedded within the system. Actors are influenced by the narratives, which are produced by the social context that surrounds them. At the same time, these actors change these narratives through their actions. This makes the system dynamic and constantly under change.

3.3.1 Cybersecurity and Constructivism

In general, scholars that have focused on cybersecurity and constructivism have focused more on *how* cyberattacks are turned into a security issue, rather than *why* these attacks are perpetrated. Nevertheless, constructivist assumptions lead to several conclusions about cybersecurity and cyberattacks. First, states are not the only actors that engage in cybersecurity and cyberattacks. Instead, a wide range of actors is involved. Consequently, a constructivist analysis of cyberattacks can analyze actorness through a wider lens. Second, as Ciolan (2014) argues: "sustaining the engagement of private, local, or individual actors in the network's security has the same importance as the national or international attempts in protecting the digital environment" (Ciolan 2014, 130). Cybersecurity is not merely conducted by the government, but also by private companies and actors. In addition, the carelessness of a single individual can cause hackers to infiltrate a government's network and do critical damage. Both the power and responsibility of protection thus do not lie solely with the state as a security provider, but also emerge at an individual, local, organizational or regional level. Third, a cyberattack can form a greater threat than the immediate damage that it might inflict with an attack. It is not about the damage, but about what the attack potentially signifies: the weaknesses and vulnerabilities of the security of the state. Cyberattacks further contain a form of political symbolism: They signify a humiliation by the hackers of the affected party (Hansen and Nissenbaum 2009). "For example, defacing websites is symbolically similar to flag burning, as it denigrates and destroys national symbols of pride, with more damage to the image and confidence than to the financial side of the victims" (Ciolan 2014, 131). As a result, to understand cyberattacks, one has to place the attacks within the socially constructed world of the hackers. Finally, the goals of cyberattacks and the damage done by cyberattacks can differ greatly. For example, cyberattacks can overburden governmental websites and slow them down or make them crash (nuisance), but cyberattacks can also attack vital energy structures and cause blackouts (emergency). Due to its focus on ideas and meanings, constructivism is well equipped to analyze the motivations behind cyberattacks, by focusing on the message or the symbolism that the attacker wants to portray.

3.3.2 Constructivist Hypotheses

By utilizing a constructivist lens to look at the motivation for the perpetration of cyberattacks in international conflicts attributed to Russia, I come to the following hypotheses:
H1: Cyberattacks are perpetrated by a wide range of actors that operate in a socially connected world
H2: Cyberconflicts find their origins in clashes of identities and social relations
H3: Cyberattacks are a form of political symbolism, meant to humiliate the enemy, rather than overpower them

3.4 A Taxonomy of Actorness

As both theories operate on significantly different paradigms, it is necessary to highlight how the two theories will be compared and contrasted. In order to perform a constructivist and realist analysis of the case study, this research shall continually consider how each theory identifies *actorness*. Actorness refers to the perpetrators behind the attack. For a realist analysis, this will always be a state, as states are considered the only perpetrators behind cyberattacks. For constructivists, this shall instead be individual hackers and groups, as constructivists consider cyberattacks as resulting from social dynamics rather than inter-state warfare. Nevertheless, as mentioned in the literature review, the attribution problem is one of the most significant problems in cyberconflicts. This problem thus poses a significant issue in analyzing who performed the attacks. As Lin argues, to the question “who is responsible” three answers are possible: The machine, the intruder pressing the buttons, and the adversary that ordered the intruder to perform the attack (Lin 2016). The emphasis of this thesis shall be on the latter, the one who is ultimately responsible for the attack. Although this “ultimate responsibility” does not pose a problem for a constructivist analysis, it is more difficult to attribute attacks through a realist lens, due to the fact that a state can easily deny its connections to individual hackers. In order to solve this issue, this thesis shall utilize Heasley’s (2011) taxonomy for state responsibility within cyberattacks and Lin’s (2016) taxonomy of responsibility. Based on both taxonomies, a state can be seen as responsible for the attacks if it:

1. *Prohibits hacking activities, without the ability to enforce prohibition*: Hacking activities are orchestrated from within the territory of the state, but the state is unable to prohibit its own citizens from engaging in said activities (Lin 2016).
2. *Tolerates hacking activities*: The state is aware that hacking activities are taking place within its territory and it is capable of prohibiting these activities, but it chooses not to interfere and thus tolerates said activities. (Lin 2016).
3. *Encourages hacking activities*: Third party-attackers continue to be responsible for the attack, but the national government provides them with means of support or encourages these hackers through its policies (Heasley 2011, 2).
4. *Directs hacking activities*: Third-party attackers continue to be responsible for the attack, but the operational details of the attacks are orchestrated by the national government. The national government directs these third-party attackers as proxies to attack on its behalf (Heasley 2011, 2).
5. *Conducts hacking activities*: Rather than being a third-party, the attackers are under the direct control of the national government and thus operate under direct orders from within the government (Heasley 2011, 2).

If a state can be assigned responsibility through the taxonomy’s of 3-5 within the case study, this research shall consider the state as the responsible actor within the realist analysis. As taxonomies 3-5 include active involvement of the government within the cyberattacks, these cyberattacks can be seen as perpetrated by a state and thus as an extension of a state’s foreign policy.

4. Research Design

As outlined in the previous chapters, this thesis shall employ a congruence analysis in order to test realism and constructivism on two cases of Russian cyberattacks. This chapter shall outline why this method was chosen, what the method entails, and finally, the selection of case studies through which the hypotheses of both theories will be tested.

4.1 Method Selection

As mentioned before, cybersecurity is still uncharted territory within the field of international relations. Research on the subject either focuses on analyzing specific case studies or how, in general, IR-theories can be utilized to analyze certain aspects of cybersecurity. This thesis combines both approaches by testing two of the main paradigms of IR-theory, realism and constructivism, in this new emerging field of cyberconflicts.

As the thesis thus aims to test these theories, the focus shall lie on a qualitative analysis rather than a quantitative analysis. As Mahoney and Goertz (2006) argue, a key difference between both frames of analysis is that a qualitative analysis focuses on "the causes-of-effect approach, in which the research goal is to explain particular outcomes" (Mahoney and Goertz 2006, 230). Meanwhile, the quantitative analyses have an "effects-of-causes approach, in which the research goal is to estimate average effects" (Mahoney and Goertz 2006, 231). Precisely because analyses of cyberattacks are still an emerging field, it becomes difficult to perform an effects-of-causes approach, as there is little data that can be measured. Instead, rather than research of large n-cases, research on cyberattacks works better if focused on small N-research or case study designs. This is the case for a variety of reasons. First, there is a lack of public information on many cases of cyberattacks. Second, it is difficult to compare and contrast a multitude of cyberconflicts. The method of attack, the extent of the damage created, as well as the amount of actors involved are highly variational and should thus be studied on a case-by-case basis. Third, the novelty of the subject means that there is still much room for theory-development and improvement. A general, large approach is thus not (yet) possible. Therefore, the best way to approach the topic of cyberattacks is through a case study design.

Out of the possible options for case study designs, a congruence analysis is the best possible option to study cyberconflicts as well as test theories. As Blatter and Haverland (2012) outline in their book *Designing Case Studies: Explanatory Approaches in Small-N Research*, there are three possible options for research with case study designs: Co-variational analysis, causal-process tracing, and congruence analysis. The first, co-variational analysis, focuses on the explanation of causality by analyzing two or more similar case studies and how variation in certain factors leads to different results. The independent variable X becomes the central element to analyze the (extent of the) outcomes of the dependent variable Y in each case study. A co-variational analysis would be a good approach to compare and contrast different cases of cyberattacks. However, the large variability in cases makes it hard to draw conclusions on causal relationships between X and Y. The second, causal process tracing focuses on how a process has led to a certain outcome. In that sense, in contrast to co-variational analysis, the emphasis lies on the process and how factors together create Y, rather than how independent factors achieved outcome Y. The third and final small-N research design, congruence analysis, places theory testing as its central focus. A congruence analysis either juxtaposes multiple theories on a case study or analyses how one theory complements another theory. Case studies within a congruence analysis then highlight which theory is best applicable in which situation (Blatter and Haverland 2012). A congruence analysis works particularly well for studying cyber conflicts. As cyberconflicts contain elements of international security, yet also introduce new elements, they form a good test whether and which IR-theories can explain cyberconflict case studies. For this reason, a congruence analysis will be adopted as the research design for this master thesis.

4.2 Congruence Analysis

Within a congruence analysis, multiple theories either contrast or complement each other. In this case, realism and constructivism will be juxtaposed against each other and tested on three case studies related to cyberattacks in Russian conflicts. Both theories provide a completely different interpretation of the mechanisms behind international relations. Realism provides a positivist explanation, which means that the world operates according to certain laws and elements, the elements of which can be distinguished and measured. Based on these measurements, objective conclusions can then be asserted. Constructivism, instead, at its core is post-positivist, which means that there are no objective assertions that can be made and that instead what matters is how we construct our perception of the world. Realism has been the most prominent paradigm in explaining conflict, precisely due to its emphasis on security and material power. At the same time, however, constructivism has been gaining ground within security studies through its expansion of how we define security. As cyberconflicts form an interesting, new phenomenon that introduces new elements to security, it forms a suitable topic on which to test both theories.

4.3 Case Study Selection

In order to test both theories, the thesis shall look at two examples of cyberattacks orchestrated by Russian hackers: The 2007 Estonian cyberattacks and the 2008 cyberattacks during the Russo-Georgian War. These two case studies have been chosen for several reasons. First, within both cases, Russian hackers are the main perpetrators of the attacks. Furthermore, Russia is often considered as one of the most aggressive cybersecurity actors on the world stage (Limnell 2016). Second, both case studies have a history as former Soviet states in common, while at the same time, the countries differ in their economic and political development. In addition, Estonia is also part of both NATO and the EU, while Georgia is part of neither. Thus, both countries have a shared history as well as shared borders with Russia, but are also considerably different. These differences are likely to bring significant results, especially in relation to realist analyses of power-relations and cyberattacks. Finally, and perhaps most important, both cases are considered to be highly significant landmarks of cyberattacks: Estonia is widely considered to be one of the first cases of a major cyberattack and brought cyberattacks into the forefront of international relations (Howell O'Neil 2016). In addition, the resulting investigations into the attacks lead to more source material than would be possible for other cyberconflicts, which are inherently secretive. Second, Georgia is considered to be a similar landmark case, as it was the first time that cyberattacks were utilized in simultaneity with a war between two states. Due to their significance as landmark case studies, as well as their differences in the context of the cyberattacks, each case study forms an opportunity to test which theory best explains the conflict: constructivism or realism.

4.4 Internal and External Validity

As this thesis plans to do a congruence analysis, it has high internal validity, but low external validity. For quantitative research, internal validity refers to "the identification of causal relationships whereby certain variables may influence other variables in the research study" (Christie et al. 2000, 17). Blatter and Haverland (2012) argue that the internal validity of a congruence analysis is high, due to the competition in explanations between the two established theories (horizontal control) and due to the testing of the hypotheses through empirical observations (vertical control) (Blatter and Haverland 2012). This also helps to prevent any bias in performing the research and provides the researcher with multiple lenses. As each theory approaches the subject through its own paradigm, the researcher can likely capture more aspects of the case study by looking at it from different angles. In this case, I can look at both case studies through a positivist and a post-positivist lens. At the same time, by using two case studies, I can increase the internal validity of the research, as the results of the first case study can be compared and contrasted to the results of the second.

External validity refers to the possibility of generalization of the results of the research. (Christie et al. 2000). As this thesis concerns two theories that are tested in two specific cases, the likelihood of generalization of the results of the thesis in order to apply it to other empirical research is low. Nevertheless, the emphasis of this thesis is on the specific applicability of two main international relations paradigms on cyberattacks. Consequently, this lack of external validity does not pose a problem, as the emphasis lies on the functioning (and perhaps shortcomings) of the theories, rather than the generalization of the empirical results. It is highly likely that the research will provide some generalizable results with regard to the motivations and causes behind Russian cyberattacks. Nevertheless, the specificity of the cases makes it unlikely to provide generalizable results outside of cyberattacks perpetrated by Russian hackers. This is further reinforced by the notion that different countries perform cyberattacks for different reasons. For example, Chinese hackers are notorious for cyberespionage, but not for disrupting digital systems (as Russian hackers are). Therefore, the external validity of this research is low.

4.5 Reliability

The reliability of a study refers to what extent it can be replicated. In other words, if a researcher decided to focus on the same topic or retrace my steps, s/he should be able to duplicate the same study (Drost 2011). Reliability thus concerns the consistency and objectivity of the study. Blatter (2017) adds to this, as he argues that in order for the reliability of a study to be increased, studies must show *transparency* in the collection of data and *trustworthiness* with regard to the position of the researcher (Blatter 2017). As a result, throughout this thesis, I have attempted to outline as specifically as possible how and where data was collected. Furthermore, as several aspects of the thesis depend on assumptions that are drawn from the data or even made within the data, the thesis has outlined when assumptions are being made. Bringing the process of creating these assumptions to the forefront increases the reliability of the study. Finally, according to Blatter and Haverland (2012), the reliability of a congruence analysis is greatly improved if the hypotheses of the thesis are created prior to the empirical research (Blatter and Haverland 2012). Therefore, by testing these hypotheses that have been developed prior the research, one can measure to what extent the data agrees with the hypotheses that follow from the theory.

4.6 Data Collection

Due to the secretive nature of cyberconflicts, finding data is often very difficult. It is often impossible to determine who performed the attacks and from where. To make matters worse, once an attack happens, governments or companies tend to be secretive about the details surrounding the attacks, as they fear to expose their weaknesses. In addition, the fact that the hacks were performed by Russia(n hackers) entails that I face a language barrier that might prove to be challenging. In order to overcome both obstacles, this thesis shall thus utilize a large combination of the following resources: First, it shall utilize news articles on the conflicts and statements by Estonian, Georgian, and Russian officials with regard to the cyberattacks. These articles will be used to paint a picture of the motivations as well as the discussion on the possible culprit behind the attacks. The time period of the data collected shall thus focus on 2007-2008 for Estonia and 2008-2009 for Georgia. Second, it shall utilize articles written on each of these cyberattacks to supplement the analysis of each conflict through each theory. Through this method, the lack of data on the case studies can be overcome. The thesis will also focus on reports of third parties and cyber-security businesses that have investigated the conflicts in order to make sense of the attacks. However, one should consciously be aware of whether the text contains biases against Russia, for example, due to the rivalry between Russia and the institution, such as NATO, that published the document. Therefore, it is primarily through the collection of a vast amount of primary and secondary sources that cyberconflicts can be thoroughly analyzed.

5. Empirical Analysis

The first case study shall focus on the cyberattacks on Estonia in 2007 after the removal of the Bronze Soldier monument. The second case study shall focus on the cyberattacks on Georgian in 2008. Each case study shall commence with an analysis of the background to the conflict and the cyberattacks. After this, it shall perform a realist analysis and a constructivist analysis in which the hypotheses of each respective theory shall be tested. Within each analysis, the hypotheses are preceded by a theoretical *context*, as each theory offers a different contextualization of the conflict.

Case-Study 1: Estonia (2007)

Background of the Conflict

The conflict within Estonia originated with the removal of a monument dedicated to Soviet troops from central Tallinn to a nearby military cemetery. The monument, called “The Bronze Soldier” or “Monument to the Fallen in the Second World War” depicted a nameless soldier in order to honor those that died during the Second World War (Torsti 2008). In 2006, the liberal party *Reformierakond* had made the removal of the statue a part of its campaign promises. After they became the leading party in the new governmental coalition with 28 percent of the seats in parliament, they had to fulfill this promise (Ehala 2009). As the Russian minority considered the statue part of its cultural heritage, the removal of the statue seemed to be a slight to this population. Therefore, a conflict emerged on the removal of the statue.

The conflict took several forms but became famous due to it being the first instance of coordinated cyberattacks against a nation’s infrastructure. First, protests emerged surrounding the statue. Initially, the protests were peaceful, but these turned violent in the evening when protestors looted various nearby stores and homes. As a result, the police violently broke apart the demonstrations (Adomatis 2007). Russian media covering this police brutality caused outrage in both Estonia and Russia. In addition, the Estonian embassy in Moscow was blocked by angry protests of Nashi activists and resulted in physical attacks on Estonian ambassadors at a press conference (Myers 2007b). Second, several parts of the Estonian government experienced DDoS attacks that were meant to disrupt the websites of these sections of the government.

According to Schmidt (2013), the attacks operated in two phases. During the first phase, starting on the morning of 27th of April 2007, Estonian news outlets and the Estonian parliament were targeted. The e-mail services of the Estonian Parliament had to be shut down, due to the overload of data. In addition, on the 28th of April, the Estonian government's website, valitsus.ee, was taken offline for eight hours (Schmidt 2013). The damage during this first phase was relatively minor. Evidence found on Russian (language) forums indicated that the attacks consisted of a coordinated approach between many different persons (Landler and Markov 2007). The forums indicated times, methods, and targets for the attacks. Tikk et al. (2010) create a distinction of this phase as the 'emotional response,' as "the attacks were relatively simple and any coordination mainly occurred on an *ad hoc* basis" (Tikk et al. 2010, 18). The second phase proved to be far more problematic, however. This phase occurred in four waves: Wave one (May 4), wave two (May 9-11), wave three (May 15), and wave four (May 18) (Tikk et al. 2010). Due to the precise timing, the intensification of the attack, and the precision of the attacks, these attacks were conducted through botnets (Evron 2008). The attacks increasingly targeted government websites and Estonian banks and on May 15 succeeded in taking down the web portal of SEB Eesti Ühispank, Estonia's second-largest commercial bank (Tikk et al. 2010). Therefore, in contrast to the first phase, the second attack was much more calculated and better strategically oriented. The botnets were able to overload Estonian websites much more effectively than the collective attacks conducted by individuals during the first phase (Evron 2008).

Realist Analysis of the Conflict

Context

Estonian and Russian relations have historically been tense, although relations had slowly been improving since the early 2000s. Estonia used to be part of the Russian empire between 1710 until 1917. After a brief period of independence, in 1940, the Soviet Baltic Fleet enacted a military blockade of Estonia and, on the 16th of June, the Soviet Union invaded Estonia. Nazi-Germany then occupied Estonia between 1941 until 1944, but as soon as they left, the Red Army conquered Estonia once again (Pfoser 2013). When Estonia regained independence in 1991, Estonia viewed Russia's presence as an illegal occupation. In response, Russia viewed Estonia's response as ungratefulness for their deliverance from the Nazi invaders (Ehala 2009). Until 1994, Russia and Estonia engaged in a diplomatic dispute on the speed of the withdrawal of Russian troops from Estonia. In addition, Estonia's membership of NATO in 2004 has posited it against Russia, which has considered NATO and its members to be its geopolitical rival. Finally, Russian disinformation campaigns within Estonia, targeted towards the Estonian Russian minority, have often led to fear of internal instability within Estonia. Consequently, this security threat sours the Estonian-Russian relationship. Therefore, through a long history of military occupation and geopolitical rivalry, Estonia and Russia have historically had very tense bilateral relations.

Regardless of the tense relations, at first glance, the removal of the statue did not constitute a security threat to Russia. As a result, this situation would not warrant a response through (cyber)attacks. The removal of the statue seemed to be a primarily domestic situation for Estonia, one in which Russia had no role to play. In this case, the issue of the statue was combined with the notion of the Ruski Mir, that the Russian state does not end with its borders, but instead also seeks to protect its citizens abroad (Kallas 2015). As a result, the removal of the statue constituted an attack on the security of the Russian minorities in Estonia and thus to Russia by extension. The removal of the statue was taken out of the domestic politics of Estonia and instead placed within the Russian-Estonian relations by Russia. As Haukkala (2015) argues: Russia clearly sought to put political pressure directly on the Estonian government. It is also possible that Russia used the occasion to aggravate further ethnic tensions within Estonian society (Haukkala 2015, 205). Therefore, the statue was taken as a pretext to start a crisis by Russia to destabilize both Estonian-Russian relations as well as aggravate ethnic distinctions within Estonia. These ethnic distinctions would then increase Russian control over Estonia's Russian minority.

Several events preceding and occurring alongside the cyberattacks reinforce the notion that the Russian government was involved in the conflict surrounding the cyberattacks. First, preceding the removal of the statue, the Russian House filed a resolution to protest the removal of the statue. In addition, some high officials strongly condemned the removal. For example, a member of Parliament stated that the removal of the statue constituted an act of war (Ottis 2008). On April 3, Russian First Vice Prime Minister Sergei Ivanov made a plea to boycott Estonian goods and services, though this bullying attitude was not shared by those in Russia's foreign policy circles (Schmidt 2013). Second, after the removal, the Russian government suspended passenger rail services between Tallinn and St. Petersburg. In addition, the government installed "a sudden ban on heavy commercial truck traffic at a border bridge in Narva" (Ottis 2008, 2), which caused many Estonian businesses to suffer. Third, directly after the announcement of the removal of the statue, Russian patriotic youth groups with links to the government started to protest in front of the Estonian embassy in Russia. Tensions rose to such a point that the ambassador was physically assaulted and had to leave through a diplomatic convoy (Myers 2007a). The Russian government turned a blind eye to these demonstrations and permitted them. Finally, after the cyber-incidents, Russia refused to cooperate in the investigation of the cyberattacks, even though the investigation was based upon a legal agreement between Estonia and Russia (Herzog 2011).

The response of the Russian government to the removal of the statue is ambiguous. The Russian government did not escalate the conflict, but also did little to prevent escalation by its citizens. For example, the refusal to participate in the cyber-investigation and the lack of response to the attacks on the Estonian embassy show a reluctance by Russia to stop Russian patriots from interfering in the situation. In this sense, it was in the interest of Russia for the conflict to escalate without Russian intervention. The resulting instability in Estonia would improve the security of Russia in two ways: First, it would guarantee a weaker, divided Estonia, which in turn would pose less of a threat to Russia. Second, the conflict caused ethnic divisions, which would result in more sympathy from Estonia's Russian minority to Russia. As has become evident in Ukraine, Russia has attempted to promote dissent in neighboring countries and eventually utilize this dissent to expand its borders (Helmus et al. 2018). Haukkala (2015), in analyzing the conflict argues, "Russia also sought to internationalize the events, clearly seeking to isolate Estonia from its Western partners in the European Union and NATO" (Haukkala 2015, 207). Fourth, Liik (2007) argues that Russia mobilized the issue of the statue in order to redirect attention from its occupation of Chechnya (Liik 2007). Therefore, there was a clear interest for Russia to capitalize on the conflict surrounding the statue.

Realist Hypotheses

H1: In an anarchic international system, cyberattacks are perpetrated solely by states, either directly or indirectly, in order to maximize their own cybersecurity, which functions as an element of the protection of national security.

H1 is partially rejected. When taking Heasley and Lin's taxonomy for actorness, Russia ranks between 2 *Tolerates hacking activities* and 3 *Encourages hacking activities.* Although the control over the cyberattacks lay in the hand of third parties, Russia permitted the cyberattacks and it might even have encouraged the cyberattacks in some shape or form, At the same time, when looking at the evidence of the case, assumptions can be made that the Kremlin was involved, but there is too little evidence to make a credible claim of involvement of the Russian government in the cyberattacks.

These results are unclear. On the one hand, the Kremlin clearly elevated the statue issue to an international dispute between Estonia and Russia. On the other hand, there is little credible evidence that suggests that the attacks were directed by the Kremlin. First, as has been argued in the context section above, the Kremlin enacted several measures as a result of the removal of the statue, such as the ban on Estonian goods. These measures shows that the Kremlin had a vested interest in the statue dispute and turned the issue into a bilateral issue between Estonia and Russia. However, this involvement in the dispute does not immediately entail involvement in the cyberattacks. Second, the second stage of the cyberattacks showed that rather than the uncoordinated, people's led cyber-protest, the second attacks involved a larger, more coordinated player (Evron 2008). At the same time, there is too little evidence to assume that this larger player was in fact the Russian government and not another organized group of professional hackers that took charge during the second wave of attacks. Third, the responsibility of the attack was claimed by the Nashi Youth Group, a Russian nationalist youth movement with close ties to the Kremlin (Heikero 2010). Due to their close connection, it can be assumed that the Kremlin might have had some involvement with the attacks. Fourth, in 2009, Sergei Markov, a Russian State Duma deputy, "announced that his assistant later identified as Konstantin Goloskokov, had carried out the cyberattacks against Estonia" (Applegate 2011, 19). At the same time, this direct link to the Russian government was complicated as Konstantin claimed to have acted on his own (Applegate 2011). Fifth, after the cyberattacks, the Estonian State procurate requested cooperation from the Russian Supreme procurate in its investigation into the DDoS-attacks and hacks, based on the Estonian-Russian Mutual Legal Assistance Treaty. Nevertheless, Russia refused this request and similarly refused to hand-over the culprits responsible for the attacks (Herzog 2011). Therefore, although there have been some minor pieces of evidence that point to the involvement of the Russian government, ultimately the evidence is inconclusive. The only credible conclusion that can be drawn is that the Russian government permitted angry Russian citizens to enact cyberattacks upon Estonia.

H2: States act as "cybersecurity-maximizers," where states attack other states in their neighborhood or other international competitors in order to maximize their own national security relative to their competitors.

H2 is similarly rejected for several reasons. First, it is difficult to create an argument in favor of security-maximization. Estonia in 2007 was already a highly networked society and disrupting its digital infrastructure would have devastating effects for civilians, businesses, and the government (Ottis 2008). Nevertheless, the DDoS attacks performed on Estonia and their ultimate effects were relatively minor. At best, the attacks resulted in a minor inconvenience for Estonian citizens. Some of the websites of the Estonian government were down for hours and one Estonian bank suffered from monetary damages as a result of the attack.

In addition, the conflict surrounding the statue resulted in an international dispute between Russia and Estonia and the cyberattacks worked as an extension of the measures and protests that happened in real life. However, throughout the whole crisis, there was no direct threat for Russia within this situation. The removal of the statue concerned a domestic situation for Estonia. Therefore, the attacks were unprovoked in the sense that they created a situation of insecurity rather than improved Russia's security. Russia might have intended to maximize its own security by both intimidating Estonia and increasing ethnic divisions within the country. Ultimately, however, it failed to achieve these interests.

Finally, if viewed within the aftermath of the conflict, cyber-maximization has effectively failed. First, as Estonia has accused Russia of being the primary culprit in the cyberattacks, the relationship between both countries has effectively deteriorated even further (Herzog 2011). Second, Estonia has significantly invested in cybersecurity after the attacks and has established itself as the second strongest cybersecurity actor in the world (NCSI 2019). In addition, NATO has also invested in cybersecurity as a result of the attacks and established the NATO Cybersecurity Command Centre in Tallinn, Estonia. Rather than diminishing Estonian security or intimidating it through the threat of cyberattacks, the cyberattack have instead turned Estonia into a key player in the realm of cybersecurity. These developments are the opposite of Russia's interests as they contain security maximization in the cyber-domain by Russia's adversaries.

H3: As great powers seek regional hegemony, cyberattacks will be utilized in cases where outright kinetic warfare is not possible, in order to increase a state's regional power position)

H3 is somewhat supported by the analysis. Kinetic warfare within this situation would have been impossible since Estonia is part of NATO. Kinetic war or intervention in the removal of the statue would have severely exceeded Russia's interest. A military intervention would have created an Article 5 situation, which would entail a war between Russia and all of the other NATO members. Furthermore, such an intervention would severely contradict international regulation and would diminish Russia's standing in the world. In addition, Estonia is an important transit country for Russian oil and gas and Russia exports 90 percent of its oil and gas to Europe, Estonia's allies (Herzog 2011). Thus, it is essential for Russia to keep beneficial relations with Estonia.

The cyberattacks allowed Russia to circumvent this threat of triggering article 5 through cyberattacks. The conflict surrounding the statue created an opportunity for Russia to "punish" Estonia (Ruus 2008). In that sense, the cyberattacks convey a display of power. It highlights that at any time, Russia could destabilize Estonian society without many consequences and without any fear of retribution by Estonia. As Conell and Vogler (2017) argue: "[C]yber is regarded as a mechanism for enabling [Russia] to dominate the information landscape, which is regarded as a warfare domain in its own right" (Connel & Vogler 2017, 3). Furthermore, these digital displays of force are then not hindered by international rules and regulations (Herzog 2011, 53). These cyberattacks thus allow Russia to diminish Estonia's security without direct consequences. Second, Estonia was already a well-developed, technological nation in 2007 that based much of its governmental workings online. As a result, cyberattacks actually could diminish the functioning of Estonia and destabilize the country. Therefore, since kinetic warfare was not possible, as the response by NATO would be devastating, cyberattacks provided a good alternative for Russia in response to the dispute surrounding the state. Nevertheless, as Russia´s true involvement in the usage of the cyberattacks are unknown, this can only be posited as an assumption, as other reasons could also play a part.

Constructivist Analysis of the Conflict

Context

According to a constructivist analysis, in order to understand the motivations behind the cyberattacks of 2007, it is first important to understand the two driving narratives behind the conflicts. These narratives are rooted in two issues: 1) The historical narratives of Soviet oppression versus Soviet liberation, and 2) the ethnic divisions within Estonian society and the resulting tensions between ethnic, nationalist Estonians and Russian Estonians and Russian citizens.

First, the root cause of the tension within the conflict results from the differing historical narratives regarding the independence of Estonia and the role of the Soviet Union, and its predecessor Russia, in hindering it. As mentioned before, there is a dispute between Estonia and Russia on the historical narrative of Estonia's independence. Where Estonia envisions its independence as consisting pre-World War II, and thus as something that was taken from them by the Soviet Union, Russia views Estonia as a newly independent state since the early 1990s (Ehala 2009).

Second, this rejection of the Soviet legacy consequently influenced Estonia's citizenship policies towards its non-native, Russian inhabitants. Due to processes of mass immigration, a large number of Russian citizens settled within former Soviet territory, including Estonia. However, Estonia rejected citizenship for these migrants and instead reinstated a law from 1938 which required Soviet settlers to undergo naturalization through language and residence requirements. As a result, this new legislation concerning citizenship showed Estonia's independence and sought to increase Estonia's political coherence (Schmidt 1998, 4). The resulting system of naturalization provided Moscow the opportunity to create claims of discrimination in Estonia against a Russian culturally homogeneous group (Aalto 2003). Therefore, since its independence, Estonia has been characterized by deep ethnic divisions between its native population and its Russian-speaking minority.

Third, this long history of narratives on Estonia's history and ethnic divisions within Estonia culminated in the symbolic meanings surrounding the state of the Bronze Soldier in Talinn. Ehala (2009) indicates the four layers of meaning connected to the statue: 1) Commemoration of the fallen in WWII; (2) the victory of Russia during the 'Great Patriotic War;' (3) the 'liberation' of Talinn by the Soviet army; and (4) the symbol of Soviet occupation (Ehala 2009, 144-145). Where the official meaning of the memorial focused on the commemoration of the fallen, the monument had very different meanings for different ethnic groups within Estonia. In that sense, the conflict surrounding the removal of the statue exceeded the direct meaning of the statue and instead focused on what it signified to each group. For nationalist Estonians this was a symbol of oppression, while for the Russian minorities it was a symbol of pride. In addition, it gave them a historical narrative in which they were *liberators* rather than *oppressors* (Haukkala 2015). Therefore, the removal of this memorial indicated a removal of this narrative for the Russian minority as liberators. As this group felt discriminated against by the Estonian government, the removal of the statue became a symbol for this oppression.

Extremists on both sides effectively utilized the statue crisis to emphasize ethnic differences and re-ignite ethnic tension within Estonia. Between 1990 – 2004, distinctions between ethnic Estonians and Russophones had been decreasing, but the 2006 riots effectively divided both groups. In this case, marginal groups on the fringes of Estonian society effectively changed the values and attitudes of the majority. As Ehala argues: The relocation of the Bronze Solider fulfilled the goals of the ethnic activists: reaffirmation of the old identity distinctions and meanings increased" (Ehala 2009, 153). In addition, although many of the Russian minority understood the problems associated with the statue, the attempt by the Estonian government to quietly remove this contentious statue in order not to produce conflict, reignited the conflict. The Russian minority viewed the removal as an attempt to silence them and as a rejection of their existence and narrative (Liik 2007). Therefore, the conflict surrounding the removal effectively caused an old divide to re-emerge and fueled the flames for the 2007 cyberattacks.

Fourth, Russia has aggressively attempted to influence this Russian minority towards Russia's side. In addition, as many of these Russian minorities watch Russian television and other media, they are susceptible to the rhetoric emanating from Moscow. As Herzog (2011) argues:

"In the global Russian diaspora community, email and inexpensive international telephone services "create a shared immediacy and 'virtual' togetherness." When combined with satellite television, the wide availability of Russian-language publications and a plethora of Internet forums, these elements of globalization have enable the Russian ethnic identity to transcend geopolitical borders. (Herzog 2011, 51).

As a result, the Russian minority in Estonia has always been linked to the notion of a looming security threat; insiders within the nation who could be utilized as pawns by Russia (Meritt

2000). At the same time, however, Russian citizens have also been very engaged with conflicts happening to their “brethren” living in different countries. During the Estonian crisis, this became evident, as Kremlin Youth groups organized protests against the Estonian Embassy (Lowe 2009). One-sided coverage by Russian media, focusing solely on police brutality against protestors in Estonia (Krüggeman and Kasekamp 2008), mobilized Russian citizens to start protesting both in Russia as well as online, in what originally had strictly been a domestic dispute within Estonia. Therefore, the conflict expanded from within Estonia to encapsulate not just the Estonian-Russian population, but also large segments of Russian citizens as well.

Constructivist Hypotheses

H1: Cyberattacks are perpetrated by a wide range of actors that operate in a socially connected world

The perpetrators behind the cyberattacks are citizens of the Russian-speaking minority in Estonia and Russian citizens. Several facts support this assumption. First, the widespread cooperation and coordination on how to perform the cyberattacks on Russian-speaking language forums showed that attackers are Russian-speakers, but also include, non-tech savvy hackers. Instead, DDoS-modules were made accessible to a larger audience and could thus be utilized as a protest. Second, the investigation has led to the arrest of one Estonian, Russian-speaking citizen, Dmitri Galushkevich, which shows that Russian-Estonian citizens were involved (BBC 2008). Third, Nashi, the Russian patriotic youth wing, has claimed responsibility for the cyberattacks (Lowe 2009). Fourth, by analyzing the time-periods of each wave of attacks, the cyberattacks could be linked to the geographical location of Estonia and Russia (Ruus 2008). Fifth, attacks intensified on May 9th, the day that Russia had expelled the Nazi-invaders and historically this day had annually been a day of contention surrounding the statue, as it became a symbolic day for protest for the rights of the Russian minority in Estonia (Toth 2007). Finally, and perhaps most convincing, the code via which the government websites were attacked, contained insults against high-level Estonian officials in Russian, calling, for example, the prime minister a fascist (Ottis 2008). Therefore, the attackers were likely to be Russian speakers from Estonia and Russia and H1 turns out to be true.

H2: Cyberconflicts find their origins in clashes of identities and social relations

H2 is also supported. As has become evident from the context surrounding the statue, the cyberattacks originated out several issues rooted within clashes of identities and social relations. First, the differing narrative on Estonia's independence ensured that Estonia accuses Russia of invading Estonia, while Russia claims it has liberated Estonia from its Nazi-invaders. This narrative is the root cause of the conflict between Estonian nationalists and its Russian minority. Second, the strict immigration rules of Estonia toward its Russian immigrants are then perceived as unjust punishment. At the same time, Estonians perceive the Russian minorities as a possible security threat due to their close relations to Russia, which Estonians still view as an "enemy." Third, the Russian belief that the Russian nation is more than its territorial borders reinforces the notion of Russian citizens that the Russian minority in Estonia is part of Russia. As a result, these citizens require protection. Finally, all these different factors emerge in the dispute surrounding the removal of the Soviet statue, which simultaneously becomes the physical manifestation of these ongoing narratives. Therefore, the resulting cyberattacks are a response to this removal and thus the symbolic rejection of Estonia's Russian minority by the Estonian government.

H3: Cyberattacks are a form of political symbolism, meant to humiliate the enemy, rather than overpower them

H3 is also proven. These cyberattacks can be boiled down to both protest and punishment towards the Estonian government. As Sauter (2014) argues, cyberactivism can often be utilized in conjunction with traditional activism (Sauter 2014). In this sense, the protests in front of the Estonian embassy coincided with the cyberattacks. The targeting of Estonian governmental websites clearly shows a targeted attempt to punish the government. Website defacements as well as insults to public figures in the codes utilized by the attackers, similarly show the attempts to humiliate the government (Ottis 2008). This becomes evident by juxtaposing the first phase of cyberattacks with the second phase: The first phase consisted of a large number of computers coordinating the DDoS-attacks, but was less effective. The second phase consisted of botnet-attacks, was more professional, but also required fewer participants. In that sense, the first phase can truly be marked as a people's led protest. The inexperience, unruliness, and sloppiness of the attack reinforce the notion that the first wave was carried out by a large number of angry citizens. In addition, the cyberattacks did little monetary damage other than mild inconveniences and the shutting down of websites for several hours. Thus, attacks were not utilized to hurt innocent civilians or to leave lasting damage to the Estonian state. Finally, DDoS-attacks can be perceived as a form of activism in which the disruption of the ongoing narrative is considered to be the primary message. Consequently, the cyberattacks both disrupted the narrative as well as credibly changed the narrative. Therefore, the cyberattacks can clearly be linked to the removal of the statue and show that dissidents utilized cyberspace as a method to target the Estonian government and protest the removal of the statue.

At the same time, a caveat must be made to the conceptualization of the attacks as solely being a protest by a large audience. Embedded within a political protest is often the unequal power relations between the target (usually a state government) and the protestors. Nevertheless, as Sauter argues: The initial, assumed power struggle between activists and state entities is complicated when those activists are not citizens of the targeted states…There is the added power relationship between the state(s) from which the organizers and the bulk of the DDoS action originates and the targeted state." (Sauter 2014, 51). In addition, the second phase shows signs of a more sophisticated attack on Estonia that was orchestrated by a smaller, technologically superior group and thus not by a large group of angry citizens. Therefore, it is difficult to argue that the cyberattacks were only a protest enacted by a minority against the (more powerful) Estonian government. However, not enough evidence exists to designate different culprits.

Case Study 2: Georgia (2008)

In conjunction with the Russia-Georgian War in August 2008 over the separatist region South-Ossetia, Georgia experienced a multitude of cyberattacks. This chapter shall analyze the cyberattacks perpetrated during this period.

Background of the Conflict

Starting in 2006, occasional skirmishes between Georgian troops and South-Ossetian separatists increasingly militarized the South-Ossetian border. On August 1st, 2008, the conflict erupted when separatists started to attack Georgian-controlled villages (Whitmore 2008, 1). In response, on August 7, 2008, Saakashvili called for a unilateral ceasefire. Although it is unclear who broke the ceasefire, Georgia launched a surprise attack during the night of the 8th of August and headed for the capital of South-Ossetia, Tskhinvali.

Meanwhile, Russia had started to sneak troops through the Roki tunnel inside South-Ossetia (Council 2009). Russia responded on the 8th of August by launching a large-scale military operation against Georgia through airstrikes and by expelling Georgian military from South-Ossetia. In response, Georgia declared war on Russia and Russia invaded several Georgian cities. The war lasted five days, ranging from August 8th until the 12th of August, when French President Sarkozy, on behalf of the European Union, brokered a peace agreement and ended, or rather froze, the conflict (Council 2009).

Preceding the Georgian-Russian War, however, was a conflict within cyberspace. Russians started to hack the Georgian government websites and media, as the tensions within the region rose. The first attack started weeks before the conflict, on the 20th of July, when the website of President Saakashvili (www.president.gov.ge) was taken down by a DDoS attack and included messages within the codes, such as “win+love+in+Rusia” (Danchev 2008). As Corbin (2009) argues, “a group of cyberwarriors…managed to enlist scores of mercenaries and volunteers to cripple Georgia’s Internet infrastructure through an array of botnets, [DDoS] attacks, logic bombs and other online offenses” (Corbin 2009, 2). Attackers posted lists of targets online and disrupted government websites for several days. In response, the Georgian government started to host many of its websites in Turkey.

Nevertheless, the majority of the attacks did not start until the 7th of August. These attacks coincided with the time period of the war with Russia until August 12. Much like the Estonian cyberattacks, the attacks can be divided into two phases: During the first phase, DDoS attacks, consisting of botnets, targeted Georgian government and news websites. The specific type of botnets utilized in this phase were distinctive of Russian criminal organizations, such as the Russian Business Network (Markov 2008). During the second phase, Russian cyberattacks continued to attack these websites, but also expanded its target list to include “financial institutions, businesses, educational institutions, Western media (BBC and CNN), and a Georgian hacker website” (Shakarian 2011, 64). In addition, Russian hackers started to deface these websites. Finally, in order to create a spam-email campaign, hackers made the email-addresses of several Georgian politicians available to the public. Through several online websites, the hackers recruited volunteers to participate in the attacks, the most infamous of which was StopGeorgia.ru. These websites provided easily accessible DDoS attacks, where, with merely the click of a button, a volunteer could help in flooding a website. The system would then pick and target these websites automatically. Ultimately, 54 media, government, and financial websites were attacked (Tikk et al. 2010), and Georgia’s internet networks suffered decreased functionality. By overloading financial systems through faulty payments, attackers ensured that during the conflict, for several days, no transaction could be processed within Georgia (Corbin 2009). Furthermore, the national bank of Georgia suspended all of its electronic activity between August 8th until August 19th (White 2018). Therefore, the cyberattacks on Georgia caused significant disruption to the country's governmental websites and damaged the country's digital infrastructure.

Realist Analysis of the Conflict

Context

The conflict between South-Ossetian separatists and Georgia provided an opportunity for Russia to increase its territory as well as its sphere of influence. Historically, relations had always been tense between Georgia and South-Ossetia. Following the October Revolution of 1917, South-Ossetia joined the Russian Bolsheviks against Menshevik Georgia. In 1921, the Red Army captured Georgia and brought it within the Soviet Union. During the 1991 Georgian-Ossetian conflict, South Ossetia became de facto independent (Council 2009). In order to preserve peace in the region, in 1992 a peacekeeping mission was developed under an OSCE mandate of Russian, Georgian, and South-Ossetian troops. Nevertheless, this peacekeeping mission proved to be a failure, causing tensions between the three players only to grow (Tikk et al. 2008). As a result, tensions within the region escalated, as Georgia entered a face-off with both Russia and South-Ossetian rebels for control of the region.

As a result of the Rose Revolution in 2003 and the resulting election of Saakashvili, nationalist sentiment rose in Georgia. This nationalism combined with the idea that all of Georgia's former territories should be reintegrated, including Abkhazia and South-Ossetia. In 2007, Georgia started to support an alternative civil government in South-Ossetia through a $12 million infrastructure plan, clearly indicating that it did not recognize the current sitting government (Deibert et al. 2012). In addition, Saakashvili, the new president of Georgia, fed nationalist sentiment regarding the reunification of Georgia with the autonomous oblasts of South-Ossetia and Abkhazia, especially through his creation of a Ministry of Unification. Furthermore, Saakashvili rapidly began building Georgian military capabilities (Liklidadze 2007). Similarly, "in 2004, Saakashvili forced Ajaria's autocratic ruler Aslan Abashidze to resign and reintegrated the autonomous republic into Georgia" (Karagiannis 2013, 78). Naturally, this alerted South-Ossetians due to their region's history of usurpation by Georgia through new nationalist, militant presidents. In order to destabilize the sitting South-Ossetian government, Georgia implemented several anti-corruption measures that consequently disrupted smuggling within South-Ossetia and thus affected important economic revenue within the region (AFCEA 2012). Although the Georgian government strictly attempted to target the South-Ossetian government and not its citizens, the plans resulted in the blockage of critical infrastructure. The Moscow-backed president of South-Ossetia, Kokoity, utilized this blockade to portray these acts as attacks on South Ossetia rather than on criminality, and thus further polarized the region (Toal 2009, 680). Saakaskvili, in 2005, presented a plan for unification with South-Ossetia before the Council of Europe with the support of the US and the OSCE. The following year, a referendum was held in South-Ossetia in which 95 percent voted against the plans for unification by Saakashvili (Indans 2007). Nevertheless, in 2007, Georgia established a "Provisional Regional Administrator" to create a competing governing authority in the region. Therefore, the nationalist movement of Georgia under Saakashvili, which focused on unification, only further alienated South-Ossetians. The South Ossetians viewed the aggressive attempts at unification and destabilization of the South-Ossetian government as being forced against the wishes of the South-Ossetian population and as attacks on South-Ossetia.

At the same time, relations were also degenerating between Russia and Georgia, albeit for different reasons. First, Georgia had accused Russia of secretly supporting the separatist movements in Abkhazia and South-Ossetia since 1994 (International Crisis Group 2007). Second, in 2005, the Russian Ministry of Agriculture restricted the import of Georgian agricultural products, followed by a ban on Georgian wine and restriction in land and air transportation between both countries (Livny et al. 2007). According to Human Rights Watch, this ban was likely enacted as punishment for Georgia's lack of support in Russia's bid to join the WTO (Human Rights Watch 2007). Similarly, tensions started to build between Russia and Georgia, which increasingly took the turn of military conflicts. In 2006, Georgia arrested four Russian intelligence officers and placed the four officers on trial. Russia responded by "temporarily halting the process of withdrawing military personnel from its military installations on Georgian territory" (Human Rights Watch 2007, 16). The remaining Russian troops were similarly put on high alert. Between 2006 and 2007 there were several conflicts over Russian warplanes flying over Georgian territory and in one such incidents, Georgia downed one of these surveillance planes (Council 2009). In 2008, Russia officially recognized the independence of South-Ossetia and began distributing Russian passports to the region (Deibert et al. 2012). As a result, tensions between Russia and Georgia on the recognition of the two separatist regions started to escalate. Therefore, in the preamble of the conflict between South-Ossetia and Georgia, Georgian-Russian relations had been deteriorating rapidly due to conflicts on trade, security, and the status of South-Ossetia and Abkhazia.

Finally, the conflict was reinforced by an underlying, geopolitical clash between Russia and the West over control within the region. Russia's suspicions regarding Western interference emerged during the Rose Revolution and the election of Saakashvili (Indans 2007). In 2008, after Georgia applied for NATO membership, Russia warned that this application would reinforce the split between Georgia and the South-Ossetian and Abkhazian regions (Lowe 2008). Russia considered Georgia's NATO membership to be a serious infringement of the agreement made in Berlin in 1989. In this agreement the US had promised not to expand NATO membership further eastward than the reunification of Germany (Kramer 2009). Consequently, Russia viewed Georgia's NATO membership as a significant increase of Western influence in its sphere of influence. This suspicion by Russia was not unjustified. According to Karagiannis (2013), the US had lost influence in the region, as relations between Turkey and Russia improved. To increase its footing in the region, the US offered NATO expansion to Georgia through which it could then act as an off-shore balancer (Karagiannis 2013). In addition, Russia viewed the establishment of a gas line via Turkey and the parallel Baki-Tbilisi-Erzurum gas pipeline as "an attempt to undermine the bargaining power of Russia in international energy markets" (Toal 2009, 683). Russia thus credibly saw its regional power diminishing through these actions. Finally, the recognition of the independence of Kosovo for Russia was in clear violation of international laws on the sovereignty of borders (Deibert et al. 2012). Kosovo's recognition then provided the legitimization for Russia to stop its economic sanctions towards Abkhazia and officially recognize the regions of Abkhazia, South-Ossetia, and Transnistria, much to the detriment of Georgia. Therefore, the conflict between Russia and Georgia was further exacerbated through geopolitical conflicts between Russia and the West.

Realist Hypotheses

H1: In an anarchic international system, cyberattacks are perpetrated solely by states, either directly or indirectly, in order to increase their own power in the cyberspace and their cybersecurity, which functions as an element of the protection of national security.

H1 has shown to be partially correct. It is difficult to answer whether the Russian government was involved or not. If placed within the taxonomy of state involvement, Russia scores either between *2: Tolerate hacking activities* and *4: Directs hacking activities.* Several factors argue for at least some level of agency by the Russian government in the 2008 cyberattacks. First, the cyberattacks started right before the Russian invasion and continued during wartime. Presumably, these cyberattacks sought to destabilize the governmental digital infrastructure to promote chaos and confusion, which would facilitate the ground-based invasion. Second, the hackers knew precisely which websites to target for maximum results. The cyberattacks required high expertise and knowledge. As this information was not available to ordinary citizens, it can be assumed that there was some form of coordination between the Russian military and the hackers. Similarly, attacks were traced back to Russia (Tikk et al. 2008). Third, several of the botnets utilized during the attacks belong to the Russian Business Network, a criminal organization involved in cybercrime with clear links to the Russian government (Warren 2007). Fourth, The IP-address for *StopGeorgia.ru*, one of the primary sites through which the hacks were orchestrated, was further located “in a Moscow district where almost all the buildings are affiliated with Russia’s Main Intelligence Directorate (GRU)” (Turovsky 2018, 10) In addition, the building across the street housed a research institute of the Ministry of Defence that focused on military-technical information and foreign states’ military potential. The proximity of this IP-address to Russian Intelligence-affiliated buildings creates further suspicions that the Russian intelligence services in some way were involved in the creation of the website.

Fifth, Project Grey Goose (2009), an International Open Source Intelligence Initiative, through its investigation on the involvement of the Russian government, concluded that direct attribution between the cyberattacks and the Russian government could not be established. However, this link to the attacks and the hackers *could* be established to several government officials. The report further argues: “We assess with high confidence that the Russian government will likely continue its practice of distancing itself from the Russian nationalistic hacker community thus gaining deniability while passively supporting and enjoying the strategic benefits of their actions” (Project Grey Goose 2009, 6). In that sense, several indicators thus point to the Russian government, although no direct attribution can be made on their involvement in the cyberattacks. Instead, the Kremlin most likely directed the attack from a distance, maximizing the opportunities for Russian hackers in their attack on Estonia.

H2: States act as "cybersecurity-maximizers," where states attack other states in their neighborhood or other international competitors in order to maximize their own national security relative to their competitors.

H2 has proven to be true. Russia orchestrated the cyberattacks on the Georgian governmental websites in order to maximize the effectiveness of its military campaign. The cyberattacks coincided with the military conflict and had confusion as their primary purpose. The 2008 cyberattacks also achieved their purpose, somewhat. First, as the motivation focused on disruption and confusion, the cyberattacks disrupted the targeted governmental websites for several days. In addition, a Georgian bank could not make payments until several weeks after the conflict. The downing of 54 governmental, media, and banking websites caused large damage to the Georgian infrastructure and hindered communications within the country, while it was engaged in military conflict. In contrast to Estonia, Georgia did not have a sophisticated cyber-defense. Websites were down for several days during the conflict. Therefore, the 2008 cyberattacks formed a good supplement to the Russian military invasion of 2008 and consequently achieved their aims of confusion and distortion.

However, the effects of the cyberattacks were rapidly minimalized. First, several Western countries, especially Estonia, quickly mobilized to help Georgia to improve its cyber-defense. The Georgian government moved its most crucial servers to different IP-addresses in Estonia to ensure the safety and stability of these servers. As a result, apart from initial disruption, the cyberattacks were unable to do much more damage. Therefore, ultimately, the achievement of interests through the cyberattacks were minimal.

H3: As great powers seek regional hegemony, cyberattacks will be utilized in cases where outright kinetic warfare is not possible, in order to increase a state's regional power position)

H3, in this case, has proven to be partially untrue. Outright, kinetic warfare was possible, but the the cyberattacks were utilized in conjunction with kinetic warfare to increase the effectivity of the invasion. The increased sophistication of the attacks showed a militarization of cyberspace as a new domain of warfare. Therefore, the attacks contributed to an overall disruption of information flows that destabilized the Georgian government. The attacks similarly showed how third parties, such as Russian citizens, can be motivated to participate alongside kinetic warfare.

Finally, it is unclear to what extent the cyberattacks helped in increasing Russia's regional power position. The attacks served another purpose: The complete domination of Georgia both in the physical domain through the military invasion as well as through the cyber domain. Essentially, the Georgian-Russian war over South-Ossetia can be viewed as Georgia challenging Russia's power position within the region. In that sense, through its successful attacks, Russia showed that it was able to completely overpower Georgia. Consequently, this reinforced Russia's power position within the region. In addition, the attacks served as a warning to NATO to halt the spread of its influence within the region (Karagiannis 2013). The Russian invasion also reflected this that Russia will no longer accept further encroachment within what it considers its own region of influence. Georgia has not joined NATO since the attacks and South-Ossetia has effectively become part of Russian territory. Thus, Russia was able to expand its influence within the region. That said, it is difficult to establish to what extent this was truly caused by the cyberattacks. Rather, one needs to view the cyberattacks as one of the tools utilized to create this result, rather than the determining factor.

Constructivist Analysis of the Conflict

Context

In order to understand the social ideas and narratives behind the conflict between Russia and Georgia, it is first necessary to understand the conflict between Georgia and South-Ossetia. This conflict forms the driving engine that fueled the war. The conflict between Georgia and South-Ossetia was rooted in clashes of ethnicity, identity, and ideologies, which primarily find their origins in the claim for the South-Ossetian territory. Ossetian separatist and Georgian nationalists have very different narratives as to whom the territory belongs.

To begin with, historically, the South Ossetian oblast has been very different from the rest of Georgia. First, the 1989 Soviet census showed that within South Ossetia, around 65 percent is South-Ossetian and 35 percent is Georgian. Only 14 percent of the Ossetian population in the Oblast speaks Georgian, and the Ossetian and Georgian language are from two different language families. Instead, many Ossetians utilize Russian as their primary language (Dammut and Cvetkovski 1996). As a result, historically, many Ossetian have favored integration with Russia and North-Ossetia over integration with Georgia. Second, in contrast to Kosovo or Abkhazia, South-Ossetia during the Soviet era was an autonomous *oblast*. This entailed that it was an autonomous region within USSR Georgia granted to a specific minority. This minority was thus allowed to keep its language and culture. As Toal and Loughlin (2013) argue: “South-Ossetia was the first ‘third-tier’ administrative entity to be recognized as a state. On its face, the South Ossetia Autonomous Oblast (SOAO) was a most unlikely candidate for independent statehood, and indeed remains so today” (Toal and Loughlin 2013, 136). In addition, Georgia and South-Ossetia have competing narratives on the legitimacy of the claim of South-Ossetians to the territory, as Georgians claim that Ossetians occupied the lands 200-300 years ago. From the view of Georgia, the South-Ossetians have been little more than a historical immigrant community, similar to its Armenian population. Georgia grants these communities the right to “cultural autonomy but not self-government” (Broers 2008, 285). Therefore, the Ossetians are different from Georgians, yet have conflicting narratives with Georgia on the legitimacy of their claim to the territory. Consequently, South-Ossetia has always been a contested space within Georgia.

As a result of nationalist movements within Georgia focused on unification, the ethnic divisions between Ossetians and Georgians increased and thus resulted in a clash of identities. As Markedonov (2015) argues, the conflict in South-Ossetia dates back to the 1980s when a national movement in Georgia attempted to create an independent Georgia. “[These nationalists] failed to engage the autonomies and national minorities in a common movement based on democratic civil values. Thus since the late 1980s, the movement for Georgian independence became pretty nationally exclusive” (Markedonov 2015, 111). This Georgian nationalism led to armed conflict in 1991 and 1992 between South-Ossetian separatists and Georgian nationalists. The election of Saakishvali in 2003 led to a resurgence of patriotic nationalism within Georgia and a return of the narrative of “humiliation” by South-Ossetia in 1991. “Increasingly radical ethnocratic policies in Tbilisi prompted counter-mobilization by Abkhazia and South-Ossetia” (Toal 2008, 676). Consequently, since 2006, the conflict in the South-Ossetia re-emerged. Georgia used the protection of the Georgian minority in South-Ossetia as a rallying-cry and argument for the legitimization of violence within South-Ossetia (Broers 2008). Thus, Georgia’s historical quest for unification has led to armed conflicts between South-Ossetia and Georgia.

Within this contested space of conflict Russia then intervened under the guise of the “peacekeeper” of the region. Russia’s role has essentially changed from protecting the status quo within the region to supporting South-Ossetian independence. Within Russia’s narrative, Russia is established as “protector” of the region, while Georgia views Russia’s protection as neo-imperialism, which Russia pursues through a puppet-government in South-Ossetia. However, Russia’s position is reinforced by separatists in the regions of South-Ossetia and

Abkhazia. This strengthens Russia in its assertion as well as in its resolve to protect these regions. What emerges then is a conflict between Russia and Georgia on Russia's role in the conflict. Georgia views South-Ossetia as part of its territory, while Russia views South-Ossetia as an independent state that requires protection.

In turn, the Russian-Georgian relationship is also constructed differently by both parties. As Tsygankov and Targer-Wahlquist (2009) argue: "Not only is Georgia's rejection of Russian a humiliation to a nation which has considered itself Georgia's historic protector, but Saakashvili's schizophrenic approach to Georgian-Russian relations…undermines Georgia's credibility" (Tsygankov and Targer-Wahlquist 2009, 309). As Georgia both condemns as well as seeks closer contact with Russia, the relationship has become strained throughout the past decade. As Tsygankov and Targer-Wahlquist (2009) argue: "Ultimately, each actor interprets the others' actions in the context of externally generated stereotypes, and its own actions in the context of personal (national) honor and self-esteem" (Tsygankov and Targer/Wahlquist 2009, 319). Therefore, the narratives that Georgia and Russia construct both about themselves as well as about the motives of the "other" ultimately led to an escalation of the situation, which culminated in the 2008 war.

Constructivist Hypothesis

H1: Cyberattacks are perpetrated by a wide range of actors that operate in a socially connected world

H1 is accepted, as the perpetrators behind the attack were Russian (and presumably some South-Ossetian) hackers who organized through the website *StopGeorgia.ru*. Russian citizens "took up arms" alongside the military conflict through the perpetration of cyberattacks. Patriotism combined with the narrative of Georgia acting unfairly both towards Russia as well as to the South-Ossetian people became the primary motivator for regular citizens to enact cyberattacks.

Several facts reinforce that the cyberattacks on Georgia were a people's led protest: First, the website *StopGeorgia.ru* functioned as the primary base for the attackers. In various other Russian-speaking online forums, users posted links to the website and urged other programmers to join the fight. In a manifesto on the website, the site's owners declared:

"We are representatives of the Russian hack-underground, we will not tolerate provocations from Georgian in any of its manifestations. We want to live in a free world, and to exist in a network space free from aggression and lies. We do not need instructions from the authorities or other persons, but we act according to our convictions based on patriotism, conscience and faith. You can call us criminals and cyber-terrorists, while unleashing war and killing people. But we will fight and prevent aggression against Russia in the network space"[3] (StopGeorgia.ru 2008, 1).

Protecting Russia in a provoked war against Georgia formed the primary narrative around which the hackers formed their activities. Consequently, this assertion justified their attacks.

Second, the website would provide clear, specific targets for its hacker-community as well as easy to use packages, which allowed even less tech-savvy members to contribute to the fight. Consequently, this lowered the entry-level of participating in the fight and allowed for more like-minded people to join the cyberattacks. Third, there were also several individuals, who proclaimed that they led attacks, furthering the assumption that the cyberattacks were a people-led initiative. For example, Leonid Stroiker, under his hacker-alias, *Roid*, individually targeted local news sources in Georgia, in order to "strike a blow for Russia in the information war" (Schachtman 2008, 2). Therefore, the prevailing narrative of Russia under attack, and especially under an unprovoked attack, caused a large number of Russian citizens to mobilize. These citizens then started to conduct cyberattacks in conjunction with the ongoing military conflict.

H2: Cyberconflicts find their origins in clashes of identities and social relations

H2 is partially supported. The roots of the conflict lie within the clash of narratives and identities between Georgia and South-Ossetia. In addition, South-Ossetians have historically

[3] This concerns a translation through Google. The original text reads as follows: "Мы - представители русского хак-андеграунда, не потерпим провокации со стороны Грузии в любых ее проявлениях. Мы хотим жить в свободном мире, а существовать в свободном от агрессии и лжи Сетевом пространстве. Мы не нуждаемся в указаниях со стороны властей или иных лиц, а действует согласно своим убеждениям, основанных на патриотизме, совести и вере. Вы можете называть нас преступниками и кибер-террористами, развязывая при этом войны и убивая людей. Но мы будем бороться и недопустим агрессии в отношении России в Сетевом пространстве."
Retrieved from: https://web.archive.org/web/20080812013618/http://www.stopgeorgia.ru/

distinguished themselves from Georgia, both through ethnicity as well as through their political affiliation. In that sense, as South-Ossetians feel more connected to North-Ossetians, which is a federal subject of Russia, their identities align more with Russia. Similarly, the involvement of Russia as a broker within the conflict culminated in the war between Georgia and Russia. The cyberconflict emerged to reinforce the military invasion. However, this clash of social relations that lies behind the military conflict is at the heart of the cyberconflict.

H3: Cyberattacks are a form of political symbolism, meant to humiliate the enemy, rather than overpower them

H3 has been rejected. The cyberattacks were perpetrated to destabilize Georgia's digital infrastructure and sow confusion alongside the ongoing kinetic warfare. As a result, the attacks were not merely political symbolism. With regard to the motivation for the cyberattacks, three primary motivations can be outlined that are all interconnected: 1) Defense of the mother country Russia, 2) punishment of the Georgian government and media, 3) control of the international narrative surrounding the conflict. First, the defense of the mother-country becomes evident as the mobilizing tool through which the hackers organized themselves. As the country entered a war, the hackers emerged to defend their home country. In addition, the timing of the attacks coincided with the military invasion, suggesting at least an attempt to increase governmental disruption to strengthen the ongoing attacks by the Russia troops. Second, punishing the Georgian government and media becomes more apparent through the type of attacks, as the cyberattacks only targeted government and media sources. Similarly, the statements by the hackers indicate that they viewed the Georgian government as operating unjustly. As Georgia "caused" the war, the hackers were justified in retaliating, in order to punish Georgia for this unjust provocation.

Finally, the attackers prevented Georgia from presenting its narrative of the conflict, which in turn affected the international perception of both invasions. As several Georgian media and governmental channels were disrupted during the war, Georgia had little opportunity to present its version of the five-day war online. Only an OP-ed by Saakashvili published in the Wall Street Journal, and several individual interviews with spokespersons from the Georgian Ministry of Foreign Affairs showed Georgia's version of the conflict (Deibert et al. 2012). This motivation also becomes evident as the manifesto on *StopGeorgia.RU* states: "[W]e appeal to all media and journalists to objectively cover current events. Until the situation changes, we will attack the Georgian government and information sources. We did not unleash the information war, we are not responsible for its consequences" (StopGeorgia.RU 2008, 1). This statement shows a conscious attempt to disrupt Georgian media in what the hackers viewed as presenting a biased version of events. In essence, this biased version boils down to the Georgian version of events, which was effectively silenced, in juxtaposition to the Russian version of events. As Stratfor argues: "[I]n a war where accusations of genocide have been levied, the degradation of Georgia's ability to communicate its perspective of the situation through the Ministry of Foreign Affairs and its own media coverage undermine[d] its ability to help shape international perception" (Stratfor 2008, 2). By doing this, Russia was able to control the international narrative of the conflict and was able to portray itself as the defender of the South-Ossetians, rather than the aggressor. This became especially important in a multi-layered conflict like the one between Georgia and South-Ossetia. In such a conflict it is difficult to establish who is the aggressor and who is merely defending the interests of (its) citizens. Such information-control is crucial, as it affects both the responses of the other countries in the international community as well as future policies towards the countries involved in the conflict. As Corbin (2009) argues: "One of the principal aims of cyberwarfare, which is seen increasingly as a prelude to overt military conflict, is to isolate and silence the enemy (Corbin 2009, 2). Therefore, by controlling the flow of information, Russia initially was able to define the conflict within its own interests. This prevented other countries from interfering, as it was unclear whether Russia was justified in its military intervention.

It should, however, also be noted that the Russian cyberattackers showed restraint in the damage done to the Georgian government. The attackers only perpetrated attacks that caused an inconvenience rather than lasting chaos or injury (White 2018). In addition, the damage did not exceed the intended causes of disruption, nor were innocent Georgian civilians hurt by the attacks, meaning that the attack maintained the intended proportionality (White 2018). As a result, the cyberattacks within cyberspace alongside the military attacks in the physical sphere were meant to show Georgian impotence and Russian superiority and its ability to completely dominate Georgian aggression, both in the military as well as the digital spheres. In addition, as images emerged that portrayed Saakashvili as Hitler, it could be noted that there was indeed an aspect of humiliation behind the attacks. However, "humiliation" was not the primary motivation behind the attacks. The primary motivation was to create a disadvantage for the Georgian government in fighting the war against Russia. The attacks commenced on the 8th, alongside the military invasion, and by August 10, the majority of the online presence of the Georgian government and media were effectively shut down. However, one can only measure the success of these attacks in conjunction with the military victory, which it sought to reinforce.

6. Discussion

This discussion will outline the results of the empirical analysis as well as the overall conclusion that can be drawn from these case studies on the application of realism and constructivism in the analysis of Russian cyberattacks. It shall start by examining the results of the Estonian case and the resulting realist and constructivist analysis. Then it shall do the same for the Georgian case. After contrasting realism and constructivism *within* both cases, the discussion shall continue by comparing and contrasting the results *between* both cases. Finally, the discussion shall conclude by highlighting the shortcomings of each theory in analyzing cyberattacks. In addition, it shall discuss how one can synthesize realist and constructivist analyses in order to provide a better tool of analysis for cyberconflicts.

The first case study clearly outlined that a constructivist analysis provided better insight in the perpetration of Russian cyberattacks. Concerning the realist hypotheses, both H1 and H2 were rejected and only H3 showed some merit. Since Estonia was part of NATO, outright kinetic warfare was indeed not possible and cyberattacks provided a good cost-benefit alternative. That said, the direct effects of the cyberattacks were rather limited and the aftermath led to a decrease of Russia's regional power rather than an increase. As a result, ultimately, a realist analysis of the Estonian cyberattacks of 2007 provided scant explanation for the attacks. The situation is different when looking at the constructivist hypotheses. All three constructivist hypotheses were confirmed. The attacks consisted of a large variety of actors; were embedded within issues of identity and social relations; and were ultimately performed as a form of protest and political symbolism, rather than as a means to overpower Estonia. As the conflict concerned an ethnoreligious conflict, Russian citizens and the Estonian Russian minority perpetrated the attacks and the conflict was rooted in the perceived mistreatment of this Russian minority by the Estonian government. It is impossible to credibly claim that the Kremlin was the main culprit behind the attacks. At the same time there are also several signs that at least some elements of the Russian government were involved. However, as ultimately constructivism provides a better explanation of the cyberattacks, a realist analysis focusing on state versus state relations thus proved to be less relevant. The motivations of the perpetrators were not rooted in power relations *between* states, but rather on the power relations *within* a state, where in this case, the minority suffers from (apparent) abuse by the dominant, hegemonic powers of Estonian society. The statue of the Bronze soldier then holds symbolic meaning and created a clash between an Estonian version of history versus a Russian version of history. Native Russians share the same version of history as the Estonian Russian minority. Consequently, the perceived abuse as a result of this clash of narratives becomes an important motivator to "protect one's own." Therefore, since the conflict surrounding the statue was rooted in narratives and clashes of identities, a constructivist analysis of the conflict gave the most thorough explanation of the cyberattacks.

The results are less clear cut in the second case study. Within the realist analysis, H1 and H2 were accepted. There was ample evidence that the Russian government was at least involved to some degree in the attacks, albeit no direct involvement. If the Kremlin was directly involved, they concealed their attacks considerably well. However, this is precisely embedded within the nature of the attacks: The lack of attribution towards the Kremlin is what makes the cyberattacks (through citizens) so attractive. Ultimately, the Kremlin presumably facilitated an environment for hacking without participating itself.

Similarly, the cyberattacks led to cybersecurity-maximization as Russia displayed its dominance over Georgia both in the physical and the digital sphere. Essential within this case study is that the attacks were utilized *in conjunction* with military warfare. H1 and H2 of the constructivist hypotheses are accepted. The profile of the attackers concerned a wide-variety of actors involved, albeit primarily Russian citizens. In addition, the conflict was rooted in both the Georgian-South Ossetian conflict, which had clear elements of clashes of identity, and in a clash between Georgia and Russia on Russia's role within the region, which in turn had similar clashes of elements of history and identity. As a result, a constructivist analysis provided insights in the narratives that drove the attackers. However, H3 was rejected, as the hackers did not conduct the attacks out of political symbolism. It is here that the most important distinction of the Georgian case becomes apparent: The ongoing military conflict completely changes the goals and objectives of the cyberattacks. The attacks can no longer be seen as forms of protest if 1) they are performed by citizens of a different, more powerful country, and 2) are performed alongside kinetic warfare with the clear goal of overpowering a rival state. Thus, the context in which the cyberattacks are performed proves to be crucial in the applicability of the theories. The Georgian case shows that both realism and constructivism can be applied to the case study.

` When juxtaposing the case studies, one can make several crucial distinctions. First, the origins and the nature of the conflicts differ considerably. The cyberattacks behind the Estonian conflict were primarily an ethnoreligious conflict. The Georgian conflict concerned an ethnoreligious conflict that had culminated into a kinetic war between two states. In addition, the Estonian conflict concerned a domestic matter *within* Estonia. The Georgian conflict concerned a conflict surrounding the claim to the South-Ossetian territory. This conflict was first within Georgia, between South-Ossetian rebels and the Georgian government. However, it quickly became a conflict between Russia and Georgia as soon as Russia expressed support for and recognition of South-Ossetian autonomy. In that sense, the ethnoreligious conflict within Georgia spilled over into an interstate conflict. Consequently, although constructivism was able to explain the early onset of the conflict, as soon as the conflict became between two states, realism was better capable of explaining its ramifications.

Second, the international positions of both countries differ considerably as well. Estonia is a member of NATO and the EU. Georgia is a member of neither but wanted to become a member of NATO. Where outright military actions against Estonia would lead to a war between Russia and the West, due to Article 5, the same cannot be said for Georgia. Similarly, the Georgian conflict also had an element of the struggle between Russian regional hegemony and expanding NATO influence. Consequently, in the Georgian case, a realist analysis gains more merit, as it draws attention to these power relations.

Third, the damage done by the attacks differs considerably. Wherein Estonia damages were relatively minor and less coordinated, within Georgia the damages were significant. Hackers took down the digital presence of the government for several days, even though Georgia suffered from the same type of attacks and the same type of targets (government websites and the media) as Estonia. This damage is further reinforced by the positions of both countries: Estonia was much more technologically developed than Georgia. This provided Estonia with more ammunition to defend itself against cyberattacks.

Fourth, the timing of the attack differs considerably. As several sources argue, Russia has learned from its earlier cyberconflicts and how it can utilize cyberattacks as a tool of its foreign policy (Connell and Vogler 2017). In that sense, Estonia forms an earlier conflict in which cyberattacks were used more circumstantially. In the Georgian case, there was a more conscious attempt by the Kremlin to incorporate cyberattacks to further its own agenda. After all, it could utilize the lessons-learned from Estonia and transfer these to its goals in the conflict with Georgia. The Georgian cyberattacks showed a similar attack pattern to that of Estonia. Within both cases, hackers utilized Russian language forums to recruit citizens and cause an attack by many computers. However, within the Georgian case, hackers showed better coordination in their selection of the targets of the cyberattacks. In addition, the threshold for joining the attacks as a non-tech savvy hacker was lowered due to clear instructions on the specific StopGeorgia.ru-website. The attacks were also more technologically sophisticated. Finally, hackers utilized botnets much more rapidly during the attacks. All of this created a more coordinated, devastating attack that brought far more destabilization to Georgia's critical infrastructure than the attacks on Estonia. Thus, the most important distinctions lie in the context of the attacks, the positions of each victim-state to defend itself, the damages done by the attack, and finally the quality of the coordination/preparation of the cyberattacks.

Both case studies also highlight several gaps that exist within both theoretical paradigms. First, when utilizing a realist lens, it becomes difficult to analyze conflicts in which state-involvement is not so clear-cut. As both Estonia and Georgia have shown, cyberattacks involve specific coordination between citizens hackers. Even if the state is involved, the perpetrators are often solitary actors. At the same time, however, these solitary actors are capable of challenging state authority within the digital domain. This is a critical caveat that hinders realist analyses of cyberattacks. In addition, the problem with attributing the attack ensures that it becomes even more difficult to enact realist analyses of cyberconflicts. It is often unclear what the specific purpose of a cyberattack is. As a result, realism runs the risk of perpetually falling short in analyses of cyberattacks due to its narrow focus on state interests. Second, constructivism, due to its focus on narratives and social relations runs the opposite risk: through its broad focus, constructivism spreads its attention too thin and focuses on everything, instead of providing detail. In addition, state involvement in cyberattacks is often hidden or unclear. A constructivist analysis will imminently point to the motivations of individual hackers and conclude the analysis, rather than analyze how states can pull the strings behind the scenes.

Therefore, in order to provide a comprehensive analysis of cyberconflicts, there is merit in providing a synthesis of both constructivism and realism. Both theories are capable of covering for the other theory's shortcomings. The idea of a synthesis of IR-theories has been hotly debated within the field of IR, with some opponents arguing that such an approach is impossible. Such an approach is compared to integrating different language systems with limited mutual translatability. (Jupille 2003). Nevertheless, as the previous chapters of this thesis have shown, the peculiarity of cyberspace completely shakes up original assumptions on established rules on IR-theories. Accordingly, synthesis is necessary if one wants to attempt to analyze the full picture. The synthesis of rationalist and constructivist theories should be viewed as the natural progression of IR-theoretical paradigms adapting to new developments within international politics.

Since the Cold War, several scholars have attempted to open this discourse on theoretical synthesis. Out of this, a framework emerged with three possible options for synthesis: 1) domains of application, 2) sequencing, and 3) subsumption (See Jupille et al. 2003; Andreatta and Koenig-Archibugi 2010; Craven 2013). Domains of application occur when both theories have a radically different focus of variables and "[a]dmittedly…works best when multiple theories explain similar phenomena, when explanatory variables have little overlap, and when variables do not interact in their influences of outcomes without overlap" (Jupille 2003, 22). Sequencing occurs when one theory is utilized to fill the gaps in explanation of a different theory (Craven 2013, 4). In addition, "[w]here domain-of-application approaches posit different empirical domains within one frame of time…sequencing approaches suggest that variables from both approaches work together over time to fully explain a given domain" (Jupille 2003, 22). Finally, subsumption occurs when the conclusion of one theory logically follows from the other. In this case, theory A is incorporated within the framework of theory B and only explains particular cases or outliers. These three options provide possible frameworks for synthesis.

It is difficult to estimate which form of theoretical synthesis works best for analyzing cyberconflicts and as such research will have to be judged on a case-by-case basis. The "domains of application"-approach provides the best starting position for theoretical synthesis, as it allows both theories to analyze the different elements and variables of the conflict. Nevertheless, within this thesis, through the second case study, one can also make an argument for integrating the "sequencing" approach in the analysis of cyberconflicts. First, one can only analyze the war between Georgia and Russia by taking into account the ethno-identity conflict that lies at the root of the South Ossetian-Georgian conflict. This second, underlying conflict requires a constructivist understanding to see how an ethnoreligious conflict leads to a different interstate conflict. Second, when discussing the estimated involvement of the state as the main attacker, there is also room for constructivist elements in a realist analysis. As the second case study has shown, it is clear why the Kremlin would hire and deploy hackers. However, a realist analysis is less clear in analyzing the motivations of individual citizens in joining the cyberattacks. Constructivism can provide substance to a realist analysis, as it analyzes the individual motivations of citizens. Russia has likely started to employ hackers (or cyberwarriors) within its subsequent cyberconflicts after 2008 (Connell and Vogler 2017). Nevertheless, individual citizens continue to form an important part of

Russia’s cyber-arsenal. These hacking citizens are not under Russia’s direct control. Due to the interconnectedness of cyberspace, regular citizens can decide to “take up arms” in international military conflicts. Realist analyses cannot explain why regular citizens would join the fight nor analyze the motivations for these regular citizens. Thus, empirical case studies that seek to integrate both approaches must always start from a “domains of application”-approach. One can only focus on sequencing and reinforce one specific theoretical strand if one discovers that one theory clearly dominates over the other, yet still requires theoretical input to cover emerging gaps.

To conclude, theoretical synthesis within cyberconflicts is necessary. As states start to enlist individual hackers as cyberwarriors, realist analyses will continue to fall short. Constructivism is better at explaining international cyberconflicts, because individual citizens form an important actor within these conflicts. At the same time, the majority of hackers will often not enter employment by the government, but rather act upon their own accord, triggered by patriotism or anger. These hackers are then guided by the operating government in conducting their cyberattacks. As shown in the Georgian case, when cyberattacks are conducted in situations that concern inter-state warfare, realism provides a better analysis of the context behind the conflict. However, both theories are necessary in order to make sense of both case studies. As the possible actors within cyberconflict range from lone hackers to states, a single IR-theory is unable to fully grasp the scope of a cyberconflict. By integrating a constructivist and realist analysis, this hybrid framework would serve as the perfect ground for the analysis of cyberconflicts due to the conflicts’ diverse nature.

7. Conclusion

This thesis has sought to contribute to the literature on cyberconflicts by analyzing how realism and constructivism can be utilized to analyze two instances of cyberattacks in Estonia in 2007 and in Georgia in 2008. Constructivism works best in both cases, as it analyzes how hackers use cyberattacks to send a political message. In addition, the focus of constructivism on non-state actors allows for a broader integration of actors within the analysis. As the digital space provides room to a large variety of actors, this approach can thus capture the intricacies of cyberspace better than realism.

Nevertheless, when cyberattacks are used in conflicts between states, one requires integration between realism and constructivism to capture the full spectrum of the cyberattacks. In addition, if one focuses primarily on constructivism, one misses state involvement. This state involvement is hidden within these cyberconflicts, as states use these hackers as vehicles for their interests. This also entails that it is difficult, if not impossible to attribute these attacks to the state. In this case, realism's focus on the state as a unit of analysis is both its weakness as well as its strong point.

This finding becomes important, if one considers that Russia has increasingly started to integrate hackers into its military arsenal. Russian cyberattacks have become more bold, more sophisticated, and more destructive. The case studies discussed within this thesis form early attempts by Russian hackers to influence other countries through cyberattacks. Russia has learned from this approach, as is becoming apparent in its cybercampaign against Ukraine. Realism is more and more likely to gain a prominent role within the analysis of cyberattacks, as cyberattacks will increasingly be conducted by states. The 2010 Stuxnet attack on the Iranian nuclear plants required both a high level of technological expertise and precision as well as intelligence officers to install the virus into the system of the nuclear plants (Domingo 2016). As technology develops, cyber power is likely to shift more towards states, as they can develop such technologically sophisticated attacks. As a result, realism needs to be integrated more and more into analyses of cyberconflicts.

Ultimately, this research shows that by integrating two different theoretical strands, one can overcome some of the inherent shortcomings of each theory. Such an approach is necessary for the analysis of cyberattacks where details are often unclear and an extensive approach to data collection is necessary. Cyberattacks are often purposefully designed to throw off pursuers and fool investigators. As a result, situational analyses can be helpful in placing cyberattacks within their larger contexts. Consequently, researcher can more readily identify all the perpetrators involved in the conflict. Therefore, the thesis has aimed to contribute to the growing literature on integrating cyberattacks within the literature on IR theory.

7.1 Limitations

Regardless, the thesis also suffered from several limitations. First, the lack of (credible) data meant that a wide variety of sources had to be consulted. However, at the same time, this has resulted in the usage of several sources that are difficult to verify and are often not peer-reviewed. Similarly, due to the language barriers of Georgian, Estonian, and Russian, it is difficult to gain primary documents on the conflicts. For example, I was able to find the Russian hackers fora, but was unable to search on these fora. I could not search in Russian within the sites and Google translate attempts were often unfruitful. Second, the focus on Estonia and Georgia might not capture the most recent picture of Russian cyberattacks. Although it was not the focus of this thesis, due to the contemporaneous nature of the case studies, less could be written on Russia’s changing approach towards cybersecurity. One can already see increasing involvement of the Kremlin in Georgia case and this involvement is only likely to have further improved. That said, future studies on, for example, the NotPetya-attack of 2017, are likely to face even more difficulty in finding credible source-material. This lack of data forms the third, and final limitation. Much of the documentation on the attacks is classified and only accessible for military personnel. Cybersecurity scholars will have to navigate through this maze of classified and unclassified information to make sense of cyberattacks. As states are reluctant to share the details on their cyber-weaknesses, this will continue to prove an obstacle inherent in the discipline.

7.2 Future Research

Therefore, future research will be required to outline the specific aspects of cyberconflicts that differ from regular conflicts and how researchers can nonetheless integrate these conflicts within the IR-domain. The cyberattacks within Ukraine since 2013 would provide a good example for further case study research on Russian cyberattacks. In addition, the results of this potential research is also likely to reflect on the results of this thesis. Together the results can paint a fuller picture of Russian cyber capability development. At the same time, the results of this thesis are not solely applicably to Russian instances of cyberwarfare. For example, both China and North-Korea have pointed towards dissident citizens as the culprits behind major cyberattacks. Both countries have also started to enlist talented North-Korean and Chinese citizens and train them as cyberwarriors. What has been distinctive within the Russian case, however, is the usage of frozen conflicts from the Soviet Union, as fuel for their cyberattacks. Therefore, although other countries might also similarly enlist their citizens for cyberattacks, more attention must be paid by researchers to the distinctiveness and similarities behind the motivations of cyberattackers across countries. By analyzing the Russian perspective, this thesis has sought to add to this difficult, but intriguing research problem.

To conclude, cyberattacks are difficult to analyze. IR-theories can make sense of cyberconflicts, but only if they can capture the full picture. In analyzing Russian cyberattacks, one is often reminded of the classic Reagan campaign ad: "There is a bear in the woods…Some people say the bear is tame. Others say its vicious and dangerous. Since no one can really be sure who is right, is it not smart to be as strong as the bear? If there is a bear?" (Qtd. In Morgado, 0:00 – 0:30) The question, whether there is a bear, has become much less symbolic than intended. Several notorious Russian cyberespionage groups have even adopted names to reflect this symbolism of the bear, such as Cozy Bear and Fancy Bear. If one takes the woods as an analogy for cyberspace, one can see that there is indeed a Russian bear in the woods, even if the Kremlin might want to make the world believe that there is not. It might deflect attribution for Russian cyberattacks towards patriotic Russian citizens, but such claims would ignore the evidence to the contrary. The Russian bear cub has grown-up, modernized, and joined the internet, and has far outsmarted the other creatures living in the woods. It is time that other countries learn from these cyberconflicts and become as strong as the bear. If there is a bear.

8. Bibliography

Aalto, P. (2003). Revisiting the Security/Identity Puzzle in Russo-Estonian Relations. *Journal of Peace Research* 40 (5): 573-591.

Ackerman, J., Carlson, B. and Han, Y. (2010). Constructivism and Security. *Air Command and Staff College (ACSC) Distance Learning Program.* Maxwell AFB, AL: ACSC.

Adomatis, N. (2007). Estonian Capital Suffers Second Night of Violence. *Reuters*. Retrieved from https://uk.reuters.com/article/uk-estonia-russia/estonian-capital-suffers-second-night-of-violence-idUKL2754678920070427.

AFCEA. (2012). The Russian-Georgian War: The Role of Cyberattacks in the Conflict. *AFCEA International*. Retrieved from https://www.afcea.org/committees/cyber/documents/therusso-georgianwar2008.pdf.

Albini, J. L., Rogers, R. E., Shabalin, V., Kutushev, V., Moiseev, V., & Anderson, J. (1995). Russian organized crime: its history, structure and function. *Journal of Contemporary Criminal Justice, 11*(4): 213–243.

Andreatta, F. and Koenig-Archibugi, M., 2010. Which Synthesis? Strategies of Theoretical Integration and the Neorealist-Neoliberal Debate. *International Political Science Review*, 31(2): 207–227.

Applegate, S. (2011). Cybermilitias and Political Hackers: Use of Irregular Forces in Cyberwarfare. IEEE Security & Privacy. 9. 16-22. 10.1109/MSP.2011.46.

BBC. (2008). Estonia Fines Man for Cyberwar. *BBC News*. Retrieved from http://news.bbc.co.uk/2/hi/technology/7208511.stm.

- . (2018). How the Dutch Foiled Russian 'Cyber Attack' on OPCW. *BBC Europe*. Retrieved from https://www.bbc.com/news/world-europe-45747472.

Bizeul, D. (2007). Russian business network study. *Bizeul. Org*, *20*(11), 2007.

Blatter, J. (2017). *Truth seeking and sense making: Towards configurational designs of qualitative methods*. https://doi.org/10.5281/zenodo.2563151.

- , & Haverland, M. (2012). *Designing Case Studies: Explanatory Approaches in Small-N Research*. Springer.

Brattberg, E. and Maurer, T. (2018). *Russian Election Interference: Europe's Counter to Fake News and Cyber Attacks.* Washington: Carnegie Endowment for International Peace.

Broers, L. (2008). Filling the Void: Ethnic Politics and Nationalities Policies in Post-Conflict Georgia. *Nationalities Papers* 36 (2): 276-304.

Calamur, K. (2017). Putin Says ‘Patriotic Hackers’ May Have Targeted U.S. Election. *The Atlantic*. Retrieved from https://www.theatlantic.com/news/archive/2017/06/putin-russia-us-election/528825/.

Christie, M., Rowe, P., Perry, C., and Chamard, J. (2000). *Implementation of Realism in Case Study Research Methodology.* Brisbane: International Council for Small Business.

Ciolan, I. (2014). Defining Cybersecurity as the Security Issue of the Twenty First Century: A Constructivist Approach. *The Public Administration and Social Policies Review* 12 (2014): 120-136.

Council. (2009). International Independent Fact-Finding Mission on the Conflict in Georgia. *Council of the European Union*. Retrieved from https://www.echr.coe.int/Documents/HUDOC_38263_08_Annexes_ENG.pdf.

Craig, A. and Valeriano, B. (2018). Realism and Cyber Conflict: Security in the Digital Age. In *Realism in Practice: An Appraisal*. Ed. By Orsi, D. et al. Bristol: E-International Relations Publishing.

CSIS. (2019). Significant Cyber Incidents Since 2019. *Centre for Strategic and International Studies*. Retrieved from https://www.csis.org/programs/cybersecurity-and-governance/technology-policy-program/other-projects-cybersecurity.

Connell, M. and Vogler, S. (2017). Russia’s Approach to Cyber Warfare. *CNA*. Retrieved from https://www.cna.org/cna_files/pdf/DOP-2016-U-014231-1Rev.pdf.

Corbin, K. (2009). Lessons from the Russia-Georgia Cyberwar. *Internetnews*. Retrieved from www.internetnews.com/government/article.php/3810011/Lessons+From+the+RussiaGeorgia+Cyberwar.htm.

Craven, K. (2013). Theoretical Synthesis in International Relations. *E-International Relations Students*. Retrieved from https://www.e-ir.info/2013/09/04/theoretical-synthesis-in-international-relations/.

Dammut, D. and Cvetkovski, N. (1996). Confidence-Building Matters: The Georgia-South Ossetia Conflict. *Vertic*. Retrieved from http://www.vertic.org/media/Archived_Publications/Matters/Confidence_Building_Matters_No6.pdf.

Danchev, D. (2008). Georgia’s President’s Web Site Under DDoS Attack From Russian Hackers. *Zero Day*. Retrieved from https://www.zdnet.com/article/georgia-presidents-web-site-under-ddos-attack-from-russian-hackers/.

Deibert, R. J., Rohozinski, R., & Crete-Nishihata, M. (2012). Cyclones in cyberspace: Information shaping and denial in the 2008 Russia–Georgia war. *Security Dialogue*, *43*(1), 3–24. https://doi.org/10.1177/0967010611431079.

Domingo, F. (2016). Conquering a new domain: Explaining great power competition in cyberspace. Comparative Strategy 35(2): 154-168, DOI: 10.1080/01495933.2016.1176467.

Dunn Cavelty, M. (2014). Breaking the Cyber-Security Dilemma: Aligning Security Needs and Removing Vulnerabilities. *Science and Engineering Ethics*, *20*(3), 701–715. https://doi.org/10.1007/s11948-014-9551-y.

Ehala, M. (2009). The bronze soldier: Identity threat and maintenance in Estonia. *Journal of Baltic Studies*, *40*(1), 139–158.

Evron, G. (2008). Battling Botnets and Online Mobs: Estonia's Defense Efforts during the Internet War Science & Technology. *Georgetown Journal of International Affairs*, *9*, 121–126.

Eriksson, J., & Giacomello, G. (2006). The Information Revolution, Security, and International Relations: (IR)relevant Theory? *International Political Science Review*, *27*(3), 221–244. https://doi.org/10.1177/0192512106064462.

- . (2014). International Relations, Cybersecurity, and Content Analysis: A Constructivist Approach. In *The Global Politics of Science and Technology*. Eds M. Mayer et al. Berlin: Springer-Verlag. DOI: 10.1007/978-3-642-55010-2_12.

Galinec, D., Moznik, D., and Guberina, B. (2017). Cybersecurity and Cyber Defence: National Level Strategic Approach. *Automatika* 58 (3): 273-286. DOI: 10.1080/00051144.2017.1407022.

Geers, K. (2007). Cyberspace and the Changing Nature of Cyber Warfare. *CCDCOE*. Retrieved from https://ccdcoe.org/uploads/2018/10/Geers2008_CyberspaceAndTheChanging NatureOfWarfare.pdf

Glaser, C. (2016). Realism. *Contemporary Security Studies*. Ed. by Collins, A. Oxford: Oxford University Press.

Greenberg, A. (2018). The Untold Story of NotPetya, the Most Devastating Cyberattack in History. *Wired*. Retrieved from https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.

Hamilton, E. and Rathbun, B. (2013). Scarce Differences: Toward a Material and Systemic Foundation for Offensive and Defensive Realism. *Security Studies* 22 (3): 436-465, DOI: 10.1080/09636412.2013.816125

Hansen, L., & Nissenbaum, H. (2009). Digital Disaster, Cyber Security, and the Copenhagen School. *International Studies Quarterly*, *53*(4), 1155–1175.

Haukkala (2010). A Close Encounter of the Worst Kind? The Logic of Situated Actors and the Statue Crisis Between Estonia and Russia. *Journal of Baltic Studies* 40 (2): 201-213. DOI: 10.1080/01629770902884250.

Heasley, J. (2011). *Beyond Attribution: Seeking National Responsibility for Cyber Attacks.* Washington: Atlantic Council.

Heikero, R. (2010). *Emerging Cyber Threats and Russian Views on Information Warfare and Information Operations.* Stockholm: FOI, Swedish Defence Research Agency.

Helmus, T. et al. (2018). *Russian Social Media Influence: Understanding Russian Propaganda in Eastern Europe*. Santa Monica: Rand Corporation.

Herzog, S. (2011). Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses. *Journal of Strategic Security* 4 (2): 49-60. DOI: http://dx.doi.org/10.5038/1944-0472.4.2.3.

Howell O'Neill, P. (2016). The Cyberattack That Changed the World. *The Daily Dot*. Retrieved from https://www.dailydot.com/layer8/web-war-cyberattack-russia-estonia/

Human Rights Watch. (2007). Singled Out: Russia's Detention and Expulsion of Georgians. *Human Rights Watch*. Retrieved from https://www.hrw.org/reports/2007/russia1007/russia1007web.pdf.

Indans, Ivars. (2019). Relations of Russia and Georgia: Developments and Future Prospects. *Baltic Security and Defence Review* 9 (2009): 131-149

International Crisis Group. (2007). Abhkazia Ways Forward. *Europe Report N179*. crisisgroup.org. Retrieved from https://www.crisisgroup.org/europe-central-asia/caucasus/abkhazia-georgia/abkhazia-ways-forward.

Jepson, V. (2012). The Differences Between Classical Realism and Neo Realism. *E-International Relations*. Retrieved from: https://www.e-ir.info/2012/01/24/the-differences-between-classical-realism-and-neo-realism/

Kallas, K. (2015). Claiming the Diaspora: Russia's Compatriot Policy and Its Reception By Estonian-Russian Population. *Journal on Ethnopolitics and Minority Issues in Europe* 15 (3): 1-25.

Karagiannis, E. (2013). The 2008 Russian–Georgian war via the lens of Offensive Realism, European Security, 22:1, 74-93, DOI: 10.1080/09662839.2012.698265

Karatzogianni, A. (2015). *Firebrand Waves of Digital Activism 1994-2014: The Rise and Spread of Hacktivism and Cyberconflict*. Retrieved from https://lra.le.ac.uk/handle/2381/32191.

Kello, L. (2013). The Meaning of the Cyber Revolution: Perils to Theory and Statecraft. *International Security* 38 (2): 7-40

- . (2014). Cyber Studies in International Relations: Problems and Priorities. *YouTube*. Retrieved from https://www.youtube.com/watch?v=HfYSIY_EEC4.

Kramer, A. E. (2016). How Russia Recruited Elite Hackers for Its Cyberwar. *The New York Times*. Retrieved from https://www.nytimes.com/2016/12/29/world/europe/how-russia-recruited-elite-hackers-for-its-cyberwar.html.

Kramer, M. (2009). The myth of a no-NATO-enlargement pledge to Russia. *The Washington Quarterly*, *32*(2), 39–61.

Kuehl, D. (2009). "From Cyberspace to Cyberpower: Defining the Problem," in Franklin D. Kramer, Stuart Starr, and Larry K. Wentz, eds., *Cyberpower and National Security* Washington, D.C.: National Defense UP.

Landler, M., & Markoff, J. (2007). Digital Fears Emerge After Data Siege in Estonia. *The New York Times*. Retrieved from https://www.nytimes.com/2007/05/29/technology/29estonia.html

Langner, R. (2017). Stuxnet und die Folgen (Stuxnet and the Consequences). *Langner.com*. Retrieved from https://www.langner.com/wp-content/uploads/2017/08/Stuxnet-und-die-Folgen.pdf

Martin Libicki, Cyberdeterrence and Cyberwarfare. Santa Monica: RAND Corporation. http:// www.rand.org/pubs/monographs/2009/RAND_MG877.pdf.

Merritt, M. (2000). A Geopolitics of Identity: Drawing the Line Between Russia and Estonia. *Nationalities Paper* 28 (2): 243-262.

Liik, K. (2007): The 'Bronze Year' of Estonia-Russia relations. In: Estonian Ministry of Foreign Affairs Yearbook, 2007, Tallin, pp. 71-76.

Limnell, J. (2016). The West Must Respond to Russia's Increasing Cyber Aggression. *Defenseone*.

Lin, H. (2016). Attribution of Malicious Cyber Incidents. *Hoover Working Group on National Security, Technology, and Law, Aegis Series Paper*.

Livny, E., Ott, M. and Torosyan, K. (2007). Impact of Russian sanctions on the Georgian Economy. *International School of Economics in Tbilisi (ISET), ISET Working Paper No 1*.

Lowe, C. (2008). Russia Warns Against Georgia NATO Membership. *Reuters*. Retrieved from https://www.reuters.com/article/us-russia-nato-georgia/russia-warns-against-georgia-nato-membership-idUSL1185178620080311.

Lowe, C. (2009). Kremlin loyalist says launched Estonia cyberattack. *Reuters*. Retrieved from https://www.reuters.com/article/us-russia-estonia-cyberspace-idUSTRE52B4D820090313.

Luiijf, E., Besseling, K., and De Graaf, P. (2013). Nineteen national cyber security strategies. *International Journal of Critical Infrastructures 6*, *9*(1–2), 3–31.

NCSI. (2019). National Cyber Security Index. *Ncsi.org*. Retrieved from https://ncsi.ega.ee/

Mahoney, J. and Goertz, G. (2006). A Tale of Two Cultures: Contrasting Quantitative and Qualitative Research. *Political Analysis* 14 (3): 227-249.

Markedonov, S. (2015). The South Ossetia Conflict. In "*Frozen Conflicts" in Europe*. Ed. Anton Bebler. Berlin: Barbara Budrich Publishers.

Markoff, J. (2008). Before the Gunfire, Cyberattacks. *The New York Times*. Retrieved from https://www.nytimes.com/2008/08/13/technology/13cyber.html.

McGavran, W. (2009). Intended Consequences: Regulating Cyber Attacks. *Tulane Journal of Technology and Intellectual Property* 12 (1): 259-277.

McKirdy, E. and Ilyushina, M. (2017). Putin: 'Patriotic' Russian Hackers May Have Targeted US Election. *CNN Politics*. June 2, 2017. Retrieved from https://edition.cnn.com/2017/06/01/politics/russia-putin-hackers-election/index.html.

Mehmetcik, H. (2014). A New Way of Conducting War: Cyberwar, Is That Real? In J.-F. Kremer and B. Müller (Eds.), *Cyberspace and International Relations: Theory, Prospects and Challenges* (pp. 125–139). Berlin, Heidelberg: Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-642-37481-4_8.

Mearsheimer, J. (1994). The False Promise of International Institutions. *International Security* 19 (3): 5-49. DOI 10.2307/2539078.

- . (2014). *The Tragedy of Great Power Politics* (Updated edition). New York: W. W. Norton & Company.

Meduza. (2018). An Ex St. Petersburg "Troll" Speaks Out. *Meduza.com*. Retrieved from https://meduza.io/en/feature/2017/10/15/an-ex-st-petersburg-troll-speaks-out

Mitzen, J. (2006). Ontological Security in World Politics: State Identity and the Security Dilemma. *European Journal of International Relations* 12 (3): 341-370. Doi: 10.1177/1354066106067346

Morgado, A. (2006). Ronald Reagan TV Ad: "The Bear." *YouTube*. Retrieved from https://www.youtube.com/watch?v=NpwdcmjBgNA

Mueller, R. (2019). *Report on the Investigation into Russian Interference in the 2016 Presidential Election Volume I of II.* Washington D.C.: US Department of Justice.

Myers, S. (2007a). 'E-stonia' Accuses Russia of Computer Attacks. *New York Times*. Retrieved from https://www.nytimes.com/2007/05/18/world/europe/18cnd-russia.html

- . (2007b). Friction Between Estonia and Russia Ignites Protests in Moscow. *New York Times*. Retrieved from https://www.nytimes.com/2007/05/03/world/europe/03estonia.html

Nyman, J. (2018). "Securitization," In *Security Studies: An Introduction*, Ed. Paul Williams and Matt McDonald, New York: Routledge. 100-113

Nye, J. (2010). *Cyber power.* Cambridge: Belfer Center for Science and International Affairs.

ODNI. (2017). *Assessing Russian Activities and Intentions in Recent US Elections*. US Office of the Director of National Intelligence. Retrieved from https://www.google.com/search?q=Assessing+Russian+Activities+and+Intentions+in+Recent+US+Elections&oq=Assessing+Russian+Activities+and+Intentions+in+Recent+US+Elections&aqs=chrome..69i57j69i60.236j0j7&sourceid=chrome&ie=UTF-8

Ottis, R. (2008). Analysis of the 2007 Cyberattacks Against Estonia from the Information Warfare Perspective. *Proceedings of the 7th European Conference on Information Warfare*.

Pashakhanlou, A. (2009). Comparing and Contrasting Classical Realism and Neorealism. *E-International Relations.* Retrieved from: https://www.e-ir.info/2009/07/23/comparing-and-contrasting-classical-realism-and-neo-realism/

Petallides, C. J. (2012). "Cyber Terrorism and IR Theory: Realism, Liberalism, and Constructivism in the New Security Threat." *Inquiries Journal/Student Pulse*, *4*(03). Retrieved from http://www.inquiriesjournal.com/a?id=627.

Pfoser, A. (2014). Between Russia and Estonia: Narratives of place in a new borderland. *Nationalities Papers*, 42 (2), 269–285. https://doi.org/10.1080/00905992.2013.774341.

Project Grey Goose. (2009). Russia/Georgia Cyber War – Findings and Analysis. *Scribd*. Retrieved from: https://www.scribd.com/doc/6967393/Project-Grey-Goose-Phase-I-Report.

Reardon, R., & Choucri, N. (2012). The role of cyberspace in International Relations: a view of the literature. In *ISA Annual Convention, San Diego, CA*.

Ruus, K. (2008). Cyber War I: Estonia Attacked from Russia. *European Affairs* 9 (1). https://www.europeaninstitute.org/index.php/42-european-affairs/winterspring-2008/67-cyber-war-i-estonia-attacked-from-russia

Sauter, M. (2014). *The Coming Swarm: DDOS Actions, Hacktivism, and Civil Disobedience on the Internet*. New York: Bloomsbury Academic

Schatz, D., Bashroush, R., and Wall, J. (2017). Towards a More Representative Definition of Cyber Security. *Journal of Digital Forensics, Security and Law* 12 (2): Article 8. DOI: https://doi.org/10.15394/jdfsl.2017.1476

Schmidt, A. (2013). The Estonian Cyberattacks. In *The fierce domain – conflicts in cyberspace 1986-2012*, edited by Jason Healey, Washington, D.C.: Atlantic Council, 2013.

Shakarian, P. (2011). The 2008 Russian Cyber-Campaign Against Georgia. *Military Review* (November): 63-68.

Starr (2009). Towards a Preliminary Theory of Cyberpower. in Franklin D. Kramer, Stuart Starr, and Larry K. Wentz, eds., *Cyberpower and National Security* (Washington, D.C.: National Defense UP.

StopGeorgia.ru. (2008). Наш ответ на агрессию со стороны Грузии, *StopGeorgia.RU*. Retrieved from https://web.archive.org/web/20080812013618/http://www.stopgeorgia.ru/.

Stratfor. (2008). Georgia, Russia: The Cyberwarfare Angle. *Stratfor Worldview*. Retrieved from https://worldview.stratfor.com/article/georgia-russia-cyberwarfare-angle

Tikk, E., Kaska, K. and Vihul, L. (2010). *International Cyber Incidents: Legal Considerations*. Tallinn: Cooperative Cyber Defense Centre of Excellence.

Toal, G. (2008). Russia's Kosovo: A Critical Geopolitics of the August 2008 War over South Ossetia. Eurasian Geography and Economics. 49. 670-705. 10.2747/1539-7216.49.6.670.

- and Loughlin, J. (2013). Inside South Ossetia: A Survey of Attitudes in a De Facto State. *Post Soviet Affairs* 29 (2): 136-172. DOI: 10.1080/1060586X.2013.780417.

Toth, B. (2007). Estonia Under Cyberattack. *HUN Cert*. Retrieved from https://www.google.com/search?q=estonia+cyberattack+2007&ei=gLb_XLjvBIjZwALmz5moCw&start=10&sa=N&ved=0ahUKEwi4r-_zzeHiAhWILFAKHeZnBrUQ8tMDCK8B&biw=1536&bih=722

Torsti, P. (2008). *Why do History Politics Matter?: The Case of the Estonian Bronze Soldier*. University of Helsinki Department of Social Science History.

Turovsky, D. (2018). ‘It’s Our Time to Serve the Motherland:’ How Russia’s War in Georgia Sparked Moscow’s Modern Day Recruitment of Criminal Hackers. *Meduza.* Retrieved from https://meduza.io/en/feature/2018/08/07/it-s-our-time-to-serve-the-motherland.

Van der Meer, S. (2017). *Deterrence of Cyberattacks in International Relations.* Den Haag: Clingendael Institute. Retrieved from https://www.clingendael.org/sites/default/files/2017-06/Cyber_Deterrence.pdf

Vilmer, J., Escorcia, A., Guillaume, M., and Herrera, J. (2018). Information Manipulation: A Challenge for Our Democracies. Paris: IRSEM.

Vishik, C., Matsubara, M., & Plonk, A. (2016). Key Concepts in Cyber Security: Towards a Common Policy and Technology Context for Cyber Security Norms. *NATO CCD COE Publications, Tallinn*, 221-242.

Walt, S. M. (2010). *Realism and Security* (Vol. 1). Oxford University Press. https://doi.org/10.1093/acrefore/9780190846626.013.286.

Waltz, K. (1979). *Theory of international politics* (1st ed.). New York: Random House.

Warren, P. (2007). The Hunt for Russia's Web Crims. *The Age.com.* https://www.theage.com.au/technology/the-hunt-for-russias-web-crims-20071213-gdrsp3.html.

Wendt, A. (1992). Anarchy is what states make of it: The social construction of power politics. *International Organization, 46*(2), 391-391. doi:10.1017/S0020818300027764

White, S. (2018). *Understanding Cyberwarfare: Lessons from the Russia-Georgia War*. Westpoint: Modern War Institute.

Whitmore, B. (2008). Is the Clock Ticking for Saakashvili? *Radio Free Europe*. Retrieved from https://www.rferl.org/a/Is_The_Clock_Ticking_For_Saakashvili/1199512.html.

Williams, P. and McDonald, M. (2018). "An Introduction to Security Studies." In *Security Studies: An Introduction*. Ed. Paul Williams and Matt McDonald. New York: Routledge. 1-13.

Wood, A. and Stankovic, J. (2002). *Denial of Service in Sensor Networks.* Charlottesville: University of Virginia

Zetter, K. (2016). Inside the Cunning and Unprecedented Hack On Ukraine's Power Grid. *Wired*. Retrieved from https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/

Zimet and Skoudis. (2009). A Graphical Introduction to the Structural Elements of Cyberspace. in Franklin D. Kramer, Stuart Starr, and Larry K. Wentz, eds., *Cyberpower and National Security* (Washington, D.C.: National Defense UP, 2009).