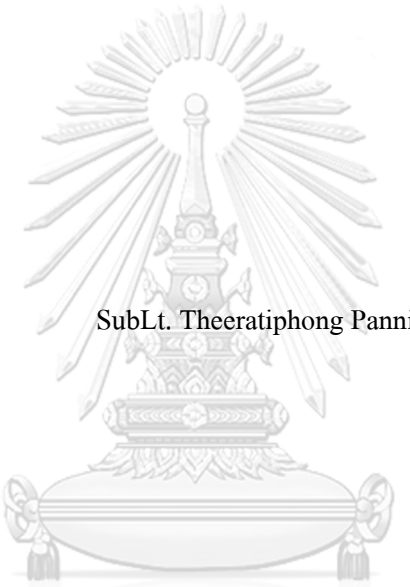
RUSSIAN MOTIVES IN CYBERATTACKS: CASE STUDIES OF ESTONIA AND UKRAINE

SubLt. Theeratiphong Pannil



An Independent Study Submitted in Partial Fulfillment of the Requirements

for the Degree of Master of Arts in International Relations

Department of International Relations

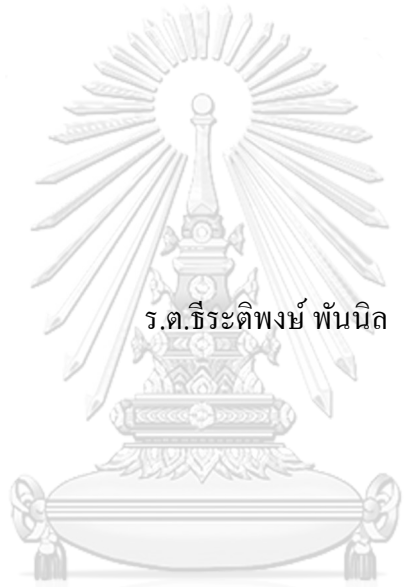
FACULTY OF POLITICAL SCIENCE

Chulalongkorn University

Academic Year 2022

แรงจูงใจของรัสเซียในการโจมตีทางไซเบอร์: กรณีศึกษาของเอสโตเนียและยูเครน

ร.ต.ธีระติพงษ์ พันนิล



สารนิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญารัฐศาสตรมหาบัณฑิต
สาขาวิชาความสัมพันธ์ระหว่างประเทศ ภาควิชาความสัมพันธ์ระหว่างประเทศ
คณะรัฐศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย
ปีการศึกษา 2565

Independent Study Title	RUSSIAN MOTIVES IN CYBERATTACKS: CASE STUDIES OF ESTONIA AND UKRAINE
By	SubLt. Theeratiphong Pannil
Field of Study	International Relations
Thesis Advisor	Captain Dr. HASSACHAI MANGKANG, RTN

Accepted by the FACULTY OF POLITICAL SCIENCE, Chulalongkorn University in Partial Fulfillment of the Requirement for the Master of Arts

INDEPENDENT STUDY COMMITTEE

---------- Chairman

(Associate Professor NATTHANAN KUNNAMAS, Ph.D.)

---------- Advisor

(Captain Dr. HASSACHAI MANGKANG, RTN)

---------- Examiner

(BHANUBHATRA JITTIANG, Ph.D.)

ธีระติพงษ์ พันนิล : แรงจูงใจของรัสเซียในการโจมตีทางไซเบอร์: กรณีศึกษาของเอสโตเนียและยูเครน . (RUSSIAN MOTIVES IN CYBERATTACKS: CASE STUDIES OF ESTONIA AND UKRAINE) อ.ที่ปรึกษาหลัก : น.อ. ดร.หัสไชยญ์ มั่งคั่ง

สารนิพนธ์ฉบับนี้ มีวัตถุประสงค์เพื่อศึกษาแรงจูงใจของรัสเซียสำหรับการโจมตีทางไซเบอร์ต่อโครงสร้างพื้นฐานข้อมูลที่สำคัญของเอสโตเนียในปี 2550 และการละเมิดโครงข่ายไฟฟ้าของยูเครนในปี 2558 นอกจากนี้ยังวิเคราะห์ผลกระทบ และผลลัพธ์ที่ตามมาของการโจมตี ตลอดจนความพยายามในการแก้ไขปัญหาดังกล่าว

จากการศึกษาพบว่า เป้าหมายหลักในการโจมตีทางไซเบอร์ของรัสเซีย คือ เพื่อดำรงความอยู่รอดจากระบบระหว่างประเทศที่เป็นอนาธิปไตย ซึ่งรัฐไม่สามารถไว้วางใจซึ่งกันและกันได้ และต้องพึ่งพาตนเอง การกระทำของเอสโตเนียและยูเครน ตลอดจนความทะเยอทะยานของนาโต้ ในการขยายตัว การแทรกแซง และการครอบงำเขตอิทธิพลของรัสเซีย เป็นภัยคุกคามอย่างยิ่งต่อความอยู่รอดของรัสเซีย ส่งผลให้รัสเซียใช้มาตรการตอบโต้ต่างๆ เพื่อสถาปนาการปกครองในภูมิภาคขึ้นมาใหม่ จำกัดการขยายตัวของนาโต้ และจำกัดอิทธิพลของชาติตะวันตกที่มีต่อประเทศเพื่อนบ้าน ทั้งนี้เพื่อรับประกันความอยู่รอด

ด้วยเหตุผลเหล่านี้ การโจมตีทางไซเบอร์จึงเป็นเครื่องมืออย่างหนึ่งที่ถูกนำมาใช้ เพราะมีความสะดวกและความคุ้มค่า โดยเฉพาะอย่างยิ่ง การใช้สงครามเครือข่ายและการจารกรรมทางไซเบอร์ต่อโครงสร้างพื้นฐานที่สำคัญในช่วงแรกของกลยุทธ์การสู้รบในสงครามสมัยใหม่ ซึ่งสร้างการรับรู้ถึงความตั้งใจ ความสามารถ และพฤติกรรมของอีกฝ่าย อีกทั้งยังสามารถขัดขวาง ระงับการใช้งาน หรือทำลายระบบคอมพิวเตอร์หรือเครือข่ายของฝ่ายตรงข้าม ตลอดจนสามารถขโมย จัดการข้อมูลที่ละเอียดอ่อน และหลีกเลี่ยงการละเมิดจริยธรรมและข้อผูกมัดทางกฎหมายที่จะถูกลงโทษภายใต้กฎการใช้กำลัง เนื่องจากการโจมตีทางไซเบอร์ไม่มีขอบเขตทางภูมิศาสตร์ มีต้นทุนต่ำ และมีขอบเขตเฉพาะที่อยู่นอกเหนือขอบเขตของปทัสถานดั้งเดิม เช่น อนุสัญญาเจนีวา ดังนั้น รัสเซียจึงได้เปิดการโจมตีทางไซเบอร์หลายครั้ง และโฆษณาชวนเชื่อที่สนับสนุนรัสเซียและต่อต้านชาติตะวันตก

สาขาวิชา	ความสัมพันธ์ระหว่างประเทศ	ลายมือชื่อนิสิต .....
ปีการศึกษา	2565	ลายมือชื่อ อ.ที่ปรึกษาหลัก .....

6480061824 : MAJOR INTERNATIONAL RELATIONS

KEYWORD: Cyberattack, Russia, Estonia, Ukraine

Theeratiphong Pannil : RUSSIAN MOTIVES IN CYBERATTACKS: CASE STUDIES OF ESTONIA AND UKRAINE. Advisor: CAPT Dr. HASSACHAI MANGKANG, RTN

The purpose of this independent study is to examine Russian motivations for the 2007 cyberattacks on Estonia's critical information infrastructure and the 2015 Ukraine power grid breach. It also analyzes the aftermath and consequences of the attacks, as well as efforts to address the issues.

The study found that Russia's primary purpose in cyberattacks is most likely to survive the anarchy of the international system, in which states can never trust each other and must rely on themselves. The acts of Estonia and Ukraine, as well as NATO's ambitions to expand, intervene, and achieve dominance in Russia's sphere of influence, would be the most dangerous to its survival. As a result, Russia retaliated in a number of ways to restrict NATO expansion, limit Western influence over neighbouring countries, and reestablish regional dominance in order to assure its survival.

For these reasons, cyberattacks have been utilized as one of the instruments since they allow for a more convenient and cost-effective course of action, particularly the use of network warfare and cyber espionage against critical infrastructure in the early stages of modern warfighting strategies, which provides awareness of a prospective enemy's intentions, capabilities, and behaviour. They can also disrupt, disable, or destroy an opponent's computer systems or networks and steal or manipulate sensitive data, shattering the traditional foundation of conflict by allowing states to avoid ethical violations and legal obligations that would be punished under conventional rules of engagement. Because cyberattacks have no geographical boundaries, low costs, and unique domains beyond the reach of conventional norms such as the Geneva Convention, Russia has therefore launched a series of cyberattacks as well as propagated pro-Russian and anti-Western misinformation.

Field of Study:	International Relations	Student's Signature .....
Academic Year:	2022	Advisor's Signature .....

ACKNOWLEDGEMENTS

With the assistance of three components, this individual study was effectively accomplished.

Firstly, the author would like to thank Captain Dr.Hassachai Mangkang, RTN for accepting the adviser role for this individual study. Your helpful guidance in every way, with the highest warmth and care, is comparable to that of a father who has good intentions and is always willing to assist his children.

Secondly, the author would like to thank the Chairman, Associate Professor Dr.Natthanan Kunnamas and the thesis examination committee, Associate Professor Dr. Bhanubhatra Jittang for their significant time in proposing relevant material that makes this thesis more comprehensive.

Thirdly, the author would like to thank parents, Faculty of Political Science Chulalongkorn University fellows, and HTMS Naresuan crews for their encouragement and support of education.

Finally, the author truly believes that this thesis will be beneficial in increasing awareness of the significance and impact of cyberattacks. If this thesis is valuable to others, the author would like to dedicate good deeds to everyone stated above as well as the author of the material that I have referred to. However, I apologise if there is an error and will only accept one.

Theeratiphong Pannil

TABLE OF CONTENTS

Page

CHAPTER 1

INTRODUCTION

1.1 Background and problem statement

Nowadays, cyberspace is used for more than simply peaceful purposes; it is also employed for military operations, criminal activity, and terrorism.[1] From the perspective of nations and international organizations, its growth in terms of users, capabilities, and technological sophistication, as well as the fact that it has become an essential part of culture and daily life, make it unquestionably vulnerable to threats affecting economic, social, and political dimensions.[2] It rapidly developed from a novelty to a weapon capable of impacting global economies and destroying regimes, known as a "cyberattack," which nation-states and religious ideologies utilized to remarkable effect.[3] The Tallinn Manual defines a "cyberattack" as "any cyber activity, offensive or defensive, that can be expected to cause individuals to suffer fatal or serious injuries and material to be damaged or destroyed."[4] Cyberattacks on the military's critical infrastructure might severely damage or disable military equipment and communications, threatening national security.[5] Since the September 11 attacks, various security sectors, including nuclear power plants, retail malls, sports stadiums, airports, and computer and telecommunications infrastructure, have received special attention.[6] Individuals, nonstate actors, intelligence services, and militaries will likely continue to penetrate information technology for intelligence gathering and its implications as states attempt novel methods and techniques to defend their interests in cyberspace and develop their own offensive capabilities.[7] It is believed

---

[1] Solange Ghernaouti, "Cyber power : Crime, conflict and security in cyberspace " (CRC Press, 2013), 149.

[2] S. C. McQuade, *Encyclopedia of Cybercrime*, Non-Series, (ABC-CLIO, 2008), 52-53.

[3] M. Lehto and P. Neittaanmäki, *Cyber Security: Power and Technology*, Intelligent Systems, Control and Automation: Science and Engineering, (Springer International Publishing, 2018), 25-26.

[4] M. N. Schmitt and Nato Cooperative Cyber Defence Centre of Excellence, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge University Press, 2017), 415.

[5] T. A. Johnson, *Cybersecurity: Protecting Critical Infrastructures from Cyber Attack and Cyber Warfare*, Zones of Religion, (Taylor & Francis, 2015), ix.

[6] N. R. Council, D. E. P. Sciences, and C. S. T. Board, *Cybersecurity Today and Tomorrow: Pay Now or Pay Later* (National Academies Press, 2002), 1.

[7] D. S. Reveron, *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World*, Cyberspace and National Security, (Georgetown University Press, 2012), 3.

that all future wars, whether armed, diplomatic, or simply the result of public relations efforts, will be accompanied by cyber conflicts.[8] Cyberattacks, particularly Russian cyberattacks, have begun to play a growing role in international politics, as harmful cyberattacks sponsored by Russia show that it will not be reluctant to use its cyber capabilities.

With the Estonian intrusions in 2007, which are regarded as the first real cyberwar with national consequences,[9] and the Ukrainian power grid in 2015, which is the first verified cyber operation capable of shutting down electricity systems,[10] the situation with Russian cyberattacks was dynamic and constantly changing in both 2007 and 2015. There are numerous types of cyberattacks, including denial-of-service (DoS) attacks that render an adversary's websites inaccessible, communication breakdowns on military networks, and malware that may impede manufacturing facilities, electric power plants, transportation lines, and the Nuclear Command and Control System (NCCS).[11] The frequency of cyberattacks is increasing and tied to nation-state actors or fanatical organizations aiming to achieve geopolitical and economic aims.[12] After land, sea, air, and space, the Pentagon declared in July 2010 that "war has reached the fifth domain: cyberspace" and that the internet is now a "strategic national asset."[13] Russia's hostile cyber actions are being thoroughly investigated because they aim to encourage huge cyber espionage, obtain proprietary information, and inflict damage on adversaries.[14]

The purpose of this independent study is to examine Russian motives for cyberattacks in Estonia and Ukraine in 2007 and 2015. It also looks at the aftermath and outcome of the attack, as well as efforts to address the issues.

---

[8] R. Stiennon, *Surviving Cyberwar* (Government Institutes, 2010), 59.

[9] Office United States. Government Accountability, K. T. Norwood, and S. P. Catwell, *Cybersecurity, Cyberanalysis and Warning* (Nova Science Publishers, 2009), 64.

[10] J. Scott, *Metadata: The Most Potent Weapon in This Cyberwar: The New Cyber-Kinetic-Meta War* (CreateSpace Independent Publishing Platform, 2017), 53-54.

[11] N. Dyer-Witheford and S. Matviyenko, *Cyberwar and Revolution: Digital Subterfuge in Global Capitalism* (University of Minnesota Press, 2019), 4-5.

[12] McQuade, *Encyclopedia of Cybercrime*, ix, 151.

[13] K. Zetter, *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon* (Crown, 2014), 138.

[14] "FACT SHEET: Imposing Costs for Harmful Foreign Activities by the Russian Government," The White House, accessed 15 November, 2022, https://www.whitehouse.gov/briefing-room/statements-releases/2021/04/15/fact-sheet-imposing-costs-for-harmful-foreign-activities-by-the-russian-government/?utm_source=link.

1.2 Research question

How motivated was Russia to launch cyberattacks in Estonia and Ukraine in 2007 and 2015? What are the outcomes and consequences of the attack?

1.3 Literature review

Before delving into Russia's motivations for launching cyberattacks in Estonia and Ukraine, it is necessary to examine how the cyberattacks have progressed thus far. This study focuses on how Russia's cyberattacks play a role in achieving military or political goals and divides the literature reviews into two main parts: 1) the development of cyberattacks; and 2) the significance of Russian cyberattacks.

1) Development of cyberattacks

Firstly, it is necessary to define the terms "cyberspace" and "cyberattacks," although most writers find this challenging due to their vast characteristics. Cyberspace can be described as "the worldwide realm inside a technical framework that comprises an interconnected network of information technology infrastructures such as the Internet, telecommunications networks, computer systems, processing units, and control."[15] Cyberattacks are also defined differently, with the most prevalent definition founded on the Tallinn Manual, which defines a "cyberattack" as "any cyber activity, offensive or defensive, that can be expected to cause individuals to suffer fatal or serious injuries and material to be damaged or destroyed."[16] The information revolution, along with governments' desire to prevent nuclear war, has shifted state warfare from military fighting or kinetic assaults to cyber assaults or non-kinetic strikes.[17] Since the internet grew increasingly accessible in the 1990s, the possibility of digital warfare and espionage rose, with multiple cases of state-level cyberwarfare.[18] This evolution has significance because it alters how to determine adversaries, respond to difficulties, and create regulations to keep up with the

[15] Reveron, *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World*, 5.

[16] Schmitt and Excellence, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, 415.

[17] S. D. Applegate, "The dawn of Kinetic Cyber" (paper presented at the 2013 5th International Conference on Cyber Conflict (CYCON 2013), 4-7 June 2013 2013), 1-15.

[18] "What Is a Cyber War – Explained," accessed April 31, 2023, https://www.neit.edu/blog/what-is-a-cyber-war-explained#:~:text=Cyber%20espionage%20can%20gather%20intelligence,and%20aid%20conventional%20warfare%20efforts.

expansion of the cyber domain in order to build appropriate strategies and courses of action.[19] Because the nature of cyberspace brings new and considerable uncertainty to warfare, the type and manner of an attack are inadequate to determine the perpetrator's intents or purposes with any confidence; hence, further information is always required.[20] Military forces additionally employ information and communications technology to gather intelligence and perform surveillance or spying, since they are now part of modern warfighting techniques.[21] In a nutshell, the earliest phases of assaulting and occupying a country include information gathering to determine who you are fighting against, their aims, and their capabilities.[22] The continual collection of information against important infrastructures serves the goal of creating and maintaining offensive and defensive military capabilities against the potential of conflict or efforts to compel or shape the circumstances of the opponents.[23] Therefore, the evolving cyber threat landscape is increasingly sophisticated and will be utilized as a tool to achieve foreign policy objectives.

Furthermore, whether the opponent is a state's elite military or a criminal organization, many upcoming disputes will include digital elements that will require a technological, political, and diplomatic reaction.[24] In the present *status quo*, the employment of cyberattacks is a two-edged sword: on one side, it is a necessary evil; on the other, there appears to be inadequate information and controls in place to prevent tensions from escalating. When whole communities or states rely heavily on information technology for fundamental requirements, small disruptions in essential operations such as financial services, communications, the production process, national security, and transportation can be disastrous.[25] Spreading malicious code to exploit software vulnerabilities can cause significant damage to critical infrastructure, including ruining internet pages, gaining authority over entire platforms, and thus gaining the ability to read,

---

[19] Marie O'Neill Sciarrone, "Cyber Warfare: The New Front," *The Catalyst*, no. 6 (2017), https://www.bushcenter.org/catalyst/modern-military/sciarrone-cyber-warfware.

[20] Ghernaouti, "Cyber power : Crime, conflict and security in cyberspace ", 171.

[21] Ibid., 166.

[22] "The Phases of War: Thoughts in and around geopolitics.," 2022, https://geopoliticalfutures.com//pdfs/the -phases-of-war-geopoliticalfutures-com.pdf.

[23] Johnson, *Cybersecurity: Protecting Critical Infrastructures from Cyber Attack and Cyber Warfare*, 127.

[24] "NATO's Role in Global Cyber Security," 2022, accessed October 2, 2022, https://www.gmfus.org/news/natos-role-global-cyber-security.

[25] McQuade, *Encyclopedia of Cybercrime*, 55.

modify, or delete confidential data, interfering with activities, initiating attacks against other institutions' structures, or eradicating systems.[26] Artificial intelligence and machine learning are increasingly being used in digital warfare, a key trend that has the potential to significantly improve capabilities while also increasing the potential for digital attacks and conflicts, as attackers could use AI to automate the identification and exploitation of machine vulnerabilities, thereby rendering it a lot simpler to conduct an effective assault.[27] The impact of the attacks follows a pattern seen in existing domains: the initial sea conflict was primarily minor skirmishes, whereas today we are currently in a comparable phase in the cyber domain, with a grander, decisive cyber-Trafalgar arriving earlier than expected, resulting in more economic, physical, and logical destruction than any of the previous occurrences.[28]

In addition, NATO's attitude toward cyber challenges has changed over the last fifteen years, from treating cyber defence in strictly technical terms to recognizing it as critical to the alliance's strategic framework.[29] Due to the fact that cyberattacks are not by definition "armed attacks," alliance member nations frequently take various approaches to information security, especially with regard to the widely accepted notions of what qualifies as an armed attack under the rules of international law.[30] The repercussions of cyberattacks can be just as catastrophic as those of a conventional strike, according to some observers, while others contend that a cyberattack is only a "cyber war" if it is paired with regular military operations and results in extensive damage instead of solely discomfort.[31] This terminology posed significant challenges to the *jus ad bellum* because cyber-attacks frequently occur in cyberspace and might lack the tangible effect of conventional kinetic assaults, making them challenging to negotiate with Article 51's "territorial integrity," "political independence," and the exercise of self-defense by

---

[26] United States. Government Accountability, Norwood, and Catwell, *Cybersecurity, Cyberanalysis and Warning*, 10.

[27] "What Is a Cyber War – Explained."

[28] K. J. Andreasson, *Cybersecurity: Public Sector Threats and Responses*, Public Administration and Public Policy, (Taylor & Francis, 2011), 312.

[29] "Inside NATO's Cyber Range: How armies prepare against attack and why nations must work together," 2022, accessed October 12, 2022, https://www.euronews.com/next/2022/12/09/inside-natos-cyber-range-how-armies-prepare-for-attack-and-why-nations-must-work-together2.

[30] "Would NATO Go to War Over a Cyberattack?," 2014, accessed October 30, 2022, https://nationalinterest.org/feature/would-nato-go-war-over-cyberattack-11199.

[31] N. Kshetri, *The Global Cybercrime Industry: Economic, Institutional and Strategic Perspectives* (Springer Berlin Heidelberg, 2010), 4.

States.[32] Applying *jus in bello* to the real-world utilization of digital weaponry and targets poses major difficulties, such as the inability to differentiate among civilian and military targets, the unique difficulty of controlling the impact of cyberattacks, and the inability to meet the requirements of the concept of proportionality with adequate certainty.[33] The difficulties in identifying attackers, the possibility of unexpected consequences, and the requirement for military response call into question the execution of Article 5, also limiting NATO to a support component for its member states' national systems.[34] After cyberattacks on Estonia's digital infrastructure in 2007, NATO accepted that a conflict between states could have a cyber dimension, and at the Bucharest Summit in 2008, it issued its first cyber-defense policy. Therefore, as cyber capabilities develop within the Alliance, they will form part of the military aid package supplied by allies in non-NATO conflicts, alongside conventional weapons. Nonetheless, some authors also highlighted the importance of Russian cyberattacks.

2) Significance of Russian cyberattacks

The majority of the literature on Russia's cyberattacks has emphasized Russia's growing cyber capabilities and threat as Russia's military and intelligence apparatus have honed their cyber warfare skills. The Russian Federation's 2010 Military Doctrine defined "information warfare" as a device for "obtaining political goals without the use of armed force" as well as an instrument for acquiring a "favorable reaction."[35] Russia's views on "information security" and the "use of information operations" have consolidated, and it has begun to concentrate on using information operations for accomplishing political goals.[36] Russia has already proven significant capability in this area, including the ability to combine technical and misinformation assaults,[37] and conducted multiple kinds of "quasi-military cyber operations" targeting various countries, including Ukraine,

[32] M. Taddeo and L. Glorioso, *Ethics and Policies for Cyber Operations: A NATO Cooperative Cyber Defence Centre of Excellence Initiative*, Philosophical Studies Series, (Springer International Publishing, 2016), 90-91.

[33] Ibid., 93-94.

[34] Jordan, "Would NATO Go to War Over a Cyberattack?."

[35] T. Maurer, *Cyber Mercenaries: The State, Hackers, and Power* (Cambridge University Press, 2018), 60.

[36] Ibid., 61.

[37] Mirosław Maj, "Cyber Conflict During the War in Ukraine," *European Cybersecurity Journal* 8, no. 1 (2022), https://cybersecforum.eu/wp-content/uploads/2022/06/ECJ_vol8_issue1.pdf.

Georgia, Estonia, and the United States.[38] Prime Minister Putin has also learned to utilize crowdsourcing to plan enormous DoS strikes capable of taking down a country's internet access.[39] Russia has a robust cyberwarfare model and doctrine, and it was abundantly clear during the conflict between Russia and Estonia that the capabilities exhibited during that cyber campaign effectively shut down the whole country of Estonia by denying access to the Internet.[40]

In addition, in response to the US's strengths and weaknesses, Russia and China have collaborated to develop capabilities and tactics so that, instead of viewing "cyberwar" as a separate field of military operations, it is included within the wider field of "information warfare," which involves psychological operations and propaganda.[41] The Russians are also interested in bilateral information security agreements with China, such as the shared definition of a cyberattack,[42] since they both have the technological capacity to target and disrupt components of the US information infrastructure as well as for intelligence collection.[43] Both nations are undoubtedly the most aggressive in carrying out covert cyberwarfare operations against other countries.[44] Because over-educated students who are skilled in mathematics, physics, and computer science are having problems obtaining employment, and the 1998 Russian financial crisis left a number of software developers unemployed, Russia and Eastern Europe are likewise rich grounds for cybercriminals.[45]

Furthermore, the continuing Ukraine-Russia conflict highlights the critical necessity for NATO to lead in forging shared rules among NATO Allies for engaging in offensive cyberspace in the new threat environment.[46] Although the cyberattacks on Estonia in 2007 did not physically

---

[38] "Russia's cyber capabilities, explained," 2022, accessed May 6, 2023, https://news.northwestern.edu/stories/2022/02/russias-cyber-capabilities-explained/?fj=1.

[39] Stiennon, *Surviving Cyberwar*, 75.

[40] W. Gragido and J. Pirc, *Cybercrime and Espionage: An Analysis of Subversive Multi-Vector Threats* (Elsevier Science, 2011), 130.

[41] Dyer-Witheford and Matviyenko, *Cyberwar and Revolution: Digital Subterfuge in Global Capitalism*, 44.

[42] Stiennon, *Surviving Cyberwar*, 49.

[43] Maurer, *Cyber Mercenaries: The State, Hackers, and Power*, 64.

[44] Taddeo and Glorioso, *Ethics and Policies for Cyber Operations: A NATO Cooperative Cyber Defence Centre of Excellence Initiative*, 227.

[45] Kshetri, *The Global Cybercrime Industry: Economic, Institutional and Strategic Perspectives*, 178-79.

[46] Olesya Tkacheva and Martin C. Libicki, "NATO as a Norm Entrepreneur on Cyber Engagement in a Third-Party Conflict," *European Cybersecurity Journal* 8, no. 1 (2022), https://cybersecforum.eu/wp-content/uploads/2022/06/ECJ_vol8_issue1.pdf.

destroy anything, they "captured the world's attention" because Estonia was a NATO member.[47] This implies that Estonia could invoke Article 5 and invoke collective self-defense in response to the cyberattacks, but according to another report, this was not invoked and was never seriously considered, even though there were suspicions that the hackers who had perpetrated the attacks were connected to the Russian state, but this was never proven.[48] The interruption of the electric power infrastructure for a few days or even months would almost certainly be devastating, just as a computer virus might wreak havoc on the economy and a biological weapon could send off an earthquake in world politics, changing our entire patterns of life forever.[49] Russia, perhaps the most skilled manipulator of global opinion, continues to deny all responsibility for its well-orchestrated attacks against Estonia and Ukraine, though a Nashi youth has claimed credit for the Estonian attacks, which have not only brought down immediate targets, such as government agency websites, but have effectively halted Internet traffic.[50] As a result, both incidents emphasize the importance and threat of Russian cyberattacks.

1.4 Hypothesis

According to a series of attacks on Estonian critical information infrastructure and Ukrainian electrical distribution breaches, Russia appears to be using cyberattacks to affect both domestic and international issues in neighboring countries. The Russian cyber activities are motivated by four major factors: 1) to survive amid the international system's instability; 2) to reassert its regional dominance and rebuild the Great Russian Empire; 3) to limit Western impact on neighboring countries and prevent the spread of NATO installations towards the Russian border, as well as to limit adjacent countries' economic, political, and military tilt towards the EU and NATO; and 4) to demonstrate their capabilities to influence or deter adversaries in the global arena. The acts of Estonia and Ukraine, as well as NATO's ambitions and efforts to intervene, expand, and achieve dominance in Russia's sphere of influence, would be the most threatening to Russia's survival. Russia does not think that nations can ever trust each other and

---

[47] L. J. M. Boer, *International Law as We Know it: Cyberwar Discourse and the Construction of Knowledge in International Legal Scholarship* (Cambridge University Press, 2021), 28.

[48] Ibid.

[49] P. W. Singer and A. Friedman, *Cybersecurity: What Everyone Needs to Know*, Business book summary, (OUP USA, 2014), 98-99.

[50] Stiennon, *Surviving Cyberwar*, 78.

must rely on themselves, according to offensive realism, which holds that anarchy is accountable for the development of belligerent state action. Because Russia is in a scenario that many other European nations are not, Russia's cyber strategy is therefore highly affected not just by Russia's history but also by perceived physical and ideological threats.

Furthermore, cyberattacks are a preferred method of achieving its objectives because they provide a more comfortable and cost-effective course of action and are regarded as a fifth domain of operation driven by essential elements of this power to capture and use other computers, including 1) the covert nature; 2) no geographical limits; 3) their relatively low costs; and 4) the strategic advantage they provide over conventional warfare. In the early phases of contemporary warfighting strategies, cyberpower could potentially be used to raise awareness of a potential enemy's objectives, capabilities, and behavior, reducing the uncertain nature of military operations. It can additionally disrupt, disable, or destroy an opponent's computer systems or networks, as well as steal or corrupt important data. It can also be selectively controlled and executed in a completely painless manner, avoiding violations of morality and obligations that would be penalized under international law if Russia does not want to provoke a third world war or considerably increase the likelihood of direct armed conflict with NATO. While the Estonian disruption in 2007 resulted in the establishment of a cyber defense policy, the "NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE)," and the "Tallinn Manual on International Law Applicable to Cyberwarfare," the 2015 Ukraine electrical system attack emphasizes the necessity for vigilance and a greater effort in power grid cybersecurity as our nation's security is threatened.

1.5 Theoretical framework

Offensive realism, a neorealist structural theory presented in opposition to defensive realism by political theorist John Mearsheimer, proposes that the anarchic nature of the international system encourages aggressive state engagement in international affairs.[51] It reasoned that without the capacity to execute agreements, governments could never be convinced that any peace-causing condition in place now will continue to exist in the future; therefore, states can

[51] P. Toft and Statskundskab Københavns Universitet. Institut for, *Arbejdspapir: John J. Mearsheimer : an Offensive Realist Between Geopolitics & Power. 2003/01* (2003).

rarely be secure in their security and must constantly look at other states' growth in power with distrust.[52] Its attitude towards power is more focused on power expansion than defensive realism, which is primarily concerned with power preservation.[53] States, rather than "security maximizers," seek opportunities to "gain more power," because security for a nation is a consequence of power, it is readily apparent that being the most powerful state is the best way to accomplish it; more powerful governments tend to be less susceptible to assault than less powerful ones.[54] The theory differs fundamentally from defensive realism in that it depicts states as power-maximizing revisionists[55] who priorities buck-passing and self-promotion over balancing strategies, and it also criticizes the "false promise" of liberal institutionalists' prescriptions for peace.[56] While liberals see increased opportunities for cooperation, realists criticize collective security measures for underestimating the extent to which greater powers are going to reject these treaties in order to obtain greater power, while smaller nations will disregard them in order to avoid losing power during what will undoubtedly be a crippling dispute.[57] Governments are prone to rivalry and conflict because they are self-interested, power-hungry, and fearful of other nations, which are required to act in this manner in order to maintain their existence in the international system.[58] As a result, offensive realism's ultimate objective is to "achieve hegemony" as the greatest way to retain stability in an unstable international system by chasing as much power as possible,[59] driving the state into egoist conduct, and necessitating self-help. In practice, the most powerful state thus creates hegemony inside its territorial boundaries while preventing other superpowers from gaining influence in other regions.

---

[52] S. Smith, A. Hadfield, and T. Dunne, *Foreign Policy: Theories, Actors, Cases* (Oxford University Press, 2016), 39.

[53] S. Molloy, *The Hidden History of Realism: A Genealogy of Power Politics*, The Palgrave Macmillan History of International Thought, (Palgrave Macmillan US, 2006), 122-23.

[54] Smith, Hadfield, and Dunne, *Foreign Policy: Theories, Actors, Cases*, 211.

[55] M. Williams, *Realism Reconsidered: The Legacy of Hans Morgenthau in International Relations* (OUP Oxford, 2007), 139.

[56] J. A. Vasquez, *The Power of Power Politics: From Classical Realism to Neotraditionalism*, Cambridge Studies in International Relations, (Cambridge University Press, 1998), 5.

[57] M. D. Gismondi, *Ethics, Liberalism and Realism in International Relations*, Routledge Advances in International Relations and Global Politics, (Taylor & Francis, 2007), 24.

[58] J. J. Mearsheimer, *The Tragedy of Great Power Politics (Updated Edition)* (W. W. Norton, 2003), 21-22.

[59] J. J. Mearsheimer, *The False Promise of International Institutions*, Working paper (John M. Olin Institute for Strategic Studies. Project on the Changing Security Environment and American National Interests), (Harvard University, John M. Olin Institute for Strategic Studies, 1994), 11–12.

Therefore, on a case-by-case basis, this individual research employs offensive realism to investigate Russian intentions in cyberattacks in Estonia and Ukraine. Although it appears that a single IR theory is unlikely to fully explain cyberconflicts and that incorporating these attacks into traditional IR paradigms is difficult due to the characteristics of cyberspace being too technological and being studied only by those with technical knowledge, realism approaches cybersecurity from a state-centric perspective, providing a useful lens for analyzing cyberattacks due to its natural focus on inter-state conflict and the use of cyberattacks. However, it has limits in that it cannot explain the participation of non-state actors; consequently, this study will analyze the idea that the state is a primary aggressor or sponsor of the event in order to capture the context of Russian cyberattacks.

1.6 Objectives

This paper aims to examine Russian motives in cyberattacks in Estonia and Ukraine in 2007 and 2015. It also analyses the aftermath and outcome of the attack, as well as efforts to address the issues.

1.7 Methodology

This independent study is qualitative research that uses the "cause-and-effect method" to explain specific outcomes because cyberattack analysis is still a developing subject and executing an effects-of-causes method or quantitative analysis will be difficult due to the lack of measurable data. Rather than doing research on big n-cases, this study focuses on small n-research or case study methodologies that perform better with cyberattacks by concentrating on the Estonian in 2007 and the Ukraine in 2015. Finding data is frequently challenging for two main reasons. Firstly, the secrecy of cyberconflicts, as well as the difficulty of verifying who carried out the assaults and from where, limit data collection, as does the fact that once an attack happens, governments or organizations attempt to keep the details of the attack concealed for fear of revealing their flaws. Secondly, because of the disagreement between Russia and the targeted nations, or NATO, there will be some prejudice towards Russia as well as bias towards the latter when analyzing public information. As a result, to overcome data collection restrictions and the debate around the likely culprit, a vast number of primary and secondary English materials available online or in published publications will be gathered and used to construct a picture of

the motives. In order to eliminate prejudice, third-party and cyber-security organizations that examined the assaults will be highlighted.

Primary sources are: 1) Official documents and statements 2) International and multilateral agreement or documents 3) National laws, regulations, measures or policies and 4) Statistical data collected by NATO, international organizations, and non-profit organization.

Secondary sources are: 1) Academic researches 2) Academic journals 3) Thesis 4) Analyzed articles and 5) News, articles and personal opinions.

These data are selected as essential, will take various forms for answering predefined questions, and will be obtained from diverse information sources in a qualitative scenario. To avoid tainting analysis with inaccuracies, the relevant data will be cleaned and prepared for analysis by deleting any duplicate or irrelevant records, and grouping will be examined and modified to extract relevant findings, trends, correlations, variances, and patterns that can help answer the questions posed in the identification step. Finally, the data from the case studies will be analyzed to generate an overall conclusion on the application of offensive realism in the investigation of Russian cyberattacks.

1.8 Structure

This study will look at two nations that were victims of Russian cyberattacks, which are considered watershed moments in cyberattack history and were chosen for four major reasons. Firstly, they have a history of sharing borders with Russia as former Soviet republics. Second, both countries have difficult relations and have recently struggled with Russia. Third, Russia was suspected of being the major perpetrator of the assaults. Fourth, Estonia is a member of both NATO and the EU, whereas Ukraine is not a member of either but is in the process of applying for NATO membership. As a result, these case studies will be utilized to investigate various aspects of the motive behind the Russian cyberattacks.

This independent study will investigate the motives behind Russian cyberattacks in Estonia and Ukraine. The structure of this study is comprised of:

1) Introduction – this chapter states the problems of Russian cyberpower in Estonia and Ukraine, briefly explains the background and motivation to employ cyberspace as a tool, and reviews related literature and the theoretical framework of this study;

2) The background of Russian cyber strategy and tactics – this chapter explains the significance of Russian offensive cyberattacks in Estonia and Ukraine and explores the background of Russia's policies, cyber capabilities, and cyberattacks;

3) Analysis of Mearsheimer's theory of offensive realism for Russian cyberattacks – this chapter will investigate the reasons for and variables of Russian cyber actions using Mearsheimer's theory of offensive realism in two dimensions, including internal and foreign factors impacting Russia;

4) An analysis of the motives behind Russia's cyberattacks on Estonia and Ukraine – this chapter examines hypotheses about Russian cyberattacks, based on internal and external variables impacting Russia, starting with Estonia and progressing through Ukraine;

5) Conclusion – this chapter reviews and responds to research questions.

CHAPTER 2

THE BACKGROUND OF RUSSIAN CYBER STRATEGY AND TACTICS

The willingness of the Russians to engage in cyberattacks has resulted in massive financial losses, disruptions to critical infrastructure operations, and disruptions to critical software supply chains. This chapter will explain the overview of Russian cyberattacks in three parts. Firstly, this chapter will examine the consequences of cybersecurity breaches, with a focus on how the complex cyberspace regime impacts Estonia and Ukraine. In the second part, this chapter will discuss how Russia's cyber capabilities and tactics continue to evolve and adapt as Russian cyberattacks remain a critical issue for the future administration and have grown in potency. The last part is the conclusion.

2.1 The significance of Russian cyberattacks in Estonia and Ukraine

Firstly, one of the most significant Russian cyber incidents that caused serious damage was a series of DoS operations targeting Estonians following disagreements between the two nations.[60] In April 2007, protests erupted in both Estonia and Russia as a result of the relocation of the Bronze Soldier, a memorial to Soviet troops slain during WWII, from Tallinn's center to a graveyard outside of town. In reaction, the Russian parliament demanded that the Estonian government resign and halted rail service from St. Petersburg, oil train shipments through Estonia, and even heavy trucks from crossing a key bridge from Russia into Estonia.[61] At the same time, many computer-based services, including government and commercial websites, as well as ATMs and other means of communication, suffer from DoS attacks that flood their servers with traffic until they can no longer respond to genuine requests.[62] While Estonia was thought to be well-connected to the internet at the time and was especially symbolic because more than 90% of its banking operations were conducted online, these attacks show that cyberattacks do not have to be sophisticated and that a simple method of flooding networked

[60] United States. Government Accountability, Norwood, and Catwell, *Cybersecurity, Cyberanalysis and Warning*, 10.

[61] J. Joque and C. Malabou, *Deconstruction Machines: Writing in the Age of Cyberwar*, Electronic Mediations, (University of Minnesota Press, 2018), 38-39.

[62] Ghernaouti, "Cyber power : Crime, conflict and security in cyberspace ", 150.

computers with information requests can drive them offline.[63] Because of Estonia's small population and reliance on electronic communications, the impact of the strikes was enormous; many other nations would have been able to fight against a comparable attack more readily.[64]

Furthermore, the cyberattack on Estonia was generally recognized as the first real cyberwar against a state for a variety of reasons.[65] First, it marked the greatest DoS assault, involving a significant number of computers targeting banking, commercial, and communication systems across the country. Second, most DoS assaults last only a few days, but this one lasted many weeks. Third, this attack is also regarded as "politically motivated," as its purpose is to interrupt functions, either with or without the aim of inflicting bodily harm, utilizing a botnet, which is a network of infected computers that enables systems to be remotely managed.[66] Fourth, this was the "actual event," and it was regarded as the one that came closest to, or crossed, the "use of force" boundary specified by Article 2(4) and so served as a standard reference point.[67] Fifth, it resulted in the NATO creating a "Cyber Defence Centre" in Tallinn, Estonia, by 2008. Although these early outbreaks of cyberwar have resulted mainly in temporary inconveniences, as militaries invest in the ability to destroy physical infrastructure through networked attacks and governments attempt to subvert other states, future cyberwars threaten massive destruction and destabilization.[68]

Following the attack, the Estonian government has accused the Kremlin of direct involvement in the attack, but Russia has said its allegations of involvement are baseless, and neither NATO nor European Commission experts have confirmed official involvement by the Russian government.[69] It is a classic example of cyberattacks occurring between non-traditional adversaries, as opposed to cyberwarfare that accompanies recognized warfare.[70] The entire-nation

---

[63] Taddeo and Glorioso, *Ethics and Policies for Cyber Operations: A NATO Cooperative Cyber Defence Centre of Excellence Initiative*, 19.

[64] Andreasson, *Cybersecurity: Public Sector Threats and Responses*, 312.

[65] Johnson, *Cybersecurity: Protecting Critical Infrastructures from Cyber Attack and Cyber Warfare*, 177-78.

[66] Andreasson, *Cybersecurity: Public Sector Threats and Responses*, XVII.

[67] Boer, *International Law as We Know it: Cyberwar Discourse and the Construction of Knowledge in International Legal Scholarship*, 28.

[68] Joque and Malabou, *Deconstruction Machines: Writing in the Age of Cyberwar*, 1.

[69] Singer and Friedman, *Cybersecurity: What Everyone Needs to Know*, 110.

[70] E. Van Wie Davis, *Shadow Warfare: Cyberwar Policy in the United States, Russia and China*, Security and Professional Intelligence Education Series, (Rowman & Littlefield Publishers, 2021), 4.

approach was clear, with several stakeholders working together to protect themselves and minimize the impact of the attacks by providing important equipment, machinery, and details regarding the attack's scope, nature, and technical aspects.[71] While the attack did not cause long-term property damage, deaths, or significant economic loss, it has highlighted that cyberattacks have the capability to endanger national security. This resulted in a noticeable shift in strategic mindset with improved network protection and response procedures, and cybersecurity has been considered of greater strategic importance.[72] To protect Estonia from future cyberattacks, NATO performed a comprehensive inspection of infrastructure security measures, which led to a document submitted to the Allied Defense Ministers in October 2007, which was later expanded into the establishment of a cyber defense policy and the NATO CCDCOE in May 2008. The Tallinn Manual on International Law was additionally produced to outline the law that may apply in cyberspace and overhaul existing law to establish new global norms.[73]

Furthermore, another important Russian cyber operation was the 2015 hack on Ukraine's electrical infrastructure, which was launched from Russian IP addresses and used malware known as BlackEnergy.[74] On December 23, 2015, malicious actors were able to hack the controlling systems of Ukrainian power distribution, gaining command of the facilities' Supervisory Control and Data Acquisition (SCADA) systems and releasing circuit breakers at about 30 substations in Kiev and the western Ivano-Frankivsk region.[75] Hackers exploited compromised user accounts and altered machinery control systems, causing 225,000 Ukrainian electricity consumers to lose power for six hours.[76] Although the electricity blackout happened due to credential theft, the attack also utilized malware to slow recovery efforts, and a concerted attempt to interfere with communications indicates a closer relationship with the state. Ukraine has identified Russia as the apparent perpetrator, citing their disagreement over Crimea, while US authorities allege that the

---

[71] Taddeo and Glorioso, *Ethics and Policies for Cyber Operations: A NATO Cooperative Cyber Defence Centre of Excellence Initiative*, 192-93.

[72] Ibid., 191.

[73] Ibid., 91.

[74] Dyer-Witheford and Matviyenko, *Cyberwar and Revolution: Digital Subterfuge in Global Capitalism*.

[75] "Cyberattack on Ukraine grid: here's how it worked and perhaps why it was done," 2016, accessed March 22, 2023, https://theconversation.com/cyberattack-on-ukraine-grid-heres-how-it-worked-and-perhaps-why-it-was-done-52802.

[76] "Lessons from The Ukraine Electric Grid Hack," 2016, accessed March 23, 2023, https://www.darkreading.com/vulnerabilities-threats/lessons-from-the-ukraine-electric-grid-hack.

attack was the result of a Russian state-led initiative.[77] It is widely assumed to be an act of Russian government or well-funded non-government team hostility; however, the attribution, as always, is inconclusive.

The cyberattack on Ukraine's power grid was the earliest officially recognized successful cyberattack on the nation's electrical network, and cyberattacks aimed at shutting down power grids have long been a key source of concern for security professionals. It exposed the protection system's flaws because the present-day electricity network consists of more than just a physical infrastructure comprised of generators, transmission lines, and other electrical components; it is also vulnerable to cyberattacks due to its reliance on advanced communication networks and a more open operational environment.[78] In addition, because their power plants were built during the Soviet period, Ukrainians are anxious about their safety, as Russia is well-versed in the construction of such facilities, resulting in it being simpler to launch effective cyberweapons.[79] Much of the concern is focused on potential assaults on SCADA systems, which rely heavily on the safe, reliable, and secure functioning of the power grid and crucial data for operations, automation, and remote control. Despite successfully blacking out hundreds of cities and villages, except for the power station's security, administration, and technical personnel, many people had mistaken the outages for a normal power cut, which is a nationally organized practice intended to conserve electricity. It is also only one of many cyberattacks, generally scattered and low-level, that accompany physical attacks in Ukraine, indicating that cyberattacks have become a more conspicuous part of civil and interstate conflict.[80] This event emphasizes the necessity of vigilance and greater cybersecurity initiatives across the government and business sectors as our reliance on the electrical grid grows, necessitating the inclusion of cybersecurity in the design of all new systems.

The mentioned case studies of Russian cyberattack in Estonia and Ukraine led both countries to perceive these actions as a threat and prompt reactionary measures. The capacity to

---

[77] "U.S. firm blames Russian 'Sandworm' hackers for Ukraine outage," 2016, accessed March 24, 2023, https://www.reuters.com/article/us-ukraine-cybersecurity-sandworm-idUSKBN0UM00N20160108.

[78] Y. Cao et al., *Cyber-Physical Energy and Power Systems: Modeling, Analysis and Application* (Springer Nature Singapore, 2019), 177.

[79] Taddeo and Glorioso, *Ethics and Policies for Cyber Operations: A NATO Cooperative Cyber Defence Centre of Excellence Initiative*, 227.

[80] Nadiya Kostyuk and Yuri M. Zhukov, "Invisible Digital Front: Can Cyber Attacks Shape Battlefield Events?," *Journal of Conflict Resolution* 63, no. 2 (2017), https://doi.org/10.1177/0022002717737138.

launch a series of cyberattacks on Estonian organizations' websites as well as get into a Ukrainian utility to throw switches or breakers at substations opens the door to more destructive types of attacks. The number of cyberattacks is growing, and the most sophisticated have been linked to nation-state actors. Experts participating in the investigation have thus warned that other nations may be exposed to similar assaults.

2.2. The background of Russia's cyber capabilities and cyberattacks

Russia, along with China and the US, is regarded as one of the world's most technologically sophisticated and dominant countries in terms of its ability to hack into government networks, steal data, and deface websites.[81] Russia has an established cyberwarfare model and doctrine, is extremely proficient in information technology, and, like China, has a significant number of institutions from which to recruit engineers.[82] Russia is also known for producing some of the best cybercriminals because of its well-educated workers, computing abilities, and hacker-friendly atmosphere, which enables complex assaults to be carried out with little computer power and low-cost software.[83] According to a self-identified hacker from Russia, "hacking happens to be one of the few employment opportunities left here."[84] As of May 2008, Russia was ranked fourth in the world for cyber capabilities, with a cyber warfare budget of 127 million USD and superior offensive cyber capabilities.[85] Russian cyber strategy mixes old Russian misinformation with present-day digital technology, which is obviously a technique not only within Russia but also in the approach against democratic liberals in the US and Europe, as well as neighboring countries.[86] Whereas the US has built a reputation in cyberspace since the early 1990s, Russian political and military leaders believe they will lose the cyber war from 1991 to 2001 to the US because they lack the credibility to consider themselves among the world's most advanced and sophisticated nations, particularly in terms of supercomputer use.[87] After a

---

[81] R. Maness and B. Valeriano, *Russia's Coercive Diplomacy: Energy, Cyber, and Maritime Policy as New Sources of Power* (Palgrave Macmillan UK, 2015), 12-13.

[82] Gragido and Pirc, *Cybercrime and Espionage: An Analysis of Subversive Multi-Vector Threats*, 130.

[83] Kshetri, *The Global Cybercrime Industry: Economic, Institutional and Strategic Perspectives*, 144-45.

[84] Ibid.

[85] Gragido and Pirc, *Cybercrime and Espionage: An Analysis of Subversive Multi-Vector Threats*, 130.

[86] Van Wie Davis, *Shadow Warfare: Cyberwar Policy in the United States, Russia and China*, 110.

[87] Kshetri, *The Global Cybercrime Industry: Economic, Institutional and Strategic Perspectives*, 130.

slow start since the Soviet Union's fall, at least fifteen years are needed to master the technique of "shadow warfare."[88] This demonstrates Russia's willingness to utilize cyber weapons, notably cyberespionage and disinformation operations, for which it has since been confirmed to be a pioneer in cyberwarfare, with Russian hacktivists demonstrating convincingly their ability to attack and damage computer and communications infrastructure.

In addition, Russia has dedicated cyberwarfare units as well as strategy institutes for infiltrating an opponent's society. Although Russia's cyber strategy is aggressive, it is more about enhancing its influence by exploiting social fractures using deception to dissuade those who would ignore or insult Russia, degrade opponents while getting ready for kinetic digital warfare, and, perhaps, boost domestic morale by demonstrating that Russian leadership is on par with or superior to that of the opponents. In response to NATO expansion, for example, Russia's General Staff, General Valery Gerasimov, proposed that the Russian development of technologically advanced weaponry should be comparable to that of the US, with a greater focus on integrating traditional warfare with special operations, diplomatic and economic pressures, and information-space activities rather than utilizing solely military operations.[89] Russian cyberattacks are aimed at its neighbors, particularly countries that were originally part of the Soviet Union but have since become vocal opponents, such as Estonia, Georgia, and Ukraine.[90] Estonia in 2007, Lithuania in 2008, and Georgia in 2009 are examples of large-scale cyberattacks in which numerous significant internet pages were taken down as a consequence of Russian strikes; however, this does not always indicate that the Russian government was responsible for the attacks.[91] Estonia's government websites and private sectors, as well as Ukraine's power grid, are thus key examples of how Russia frequently combines disinformation initiatives with cyberattacks on critical infrastructure, whereas Russian attacks on Europe and the US are frequently launched in order to particularly impact presidential elections and domestic viewpoints.

---

[88] Reveron, *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World*, 173.

[89] Dyer-Witheford and Matviyenko, *Cyberwar and Revolution: Digital Subterfuge in Global Capitalism*, 48.

[90] Van Wie Davis, *Shadow Warfare: Cyberwar Policy in the United States, Russia and China*, 22-23.

[91] Andreasson, *Cybersecurity: Public Sector Threats and Responses*, 60.

2.3 Conclusion

The history of cybersecurity breaches in Estonia and Ukraine is examined in this chapter. Following the moving of the Bronze Soldier of Tallinn, the Estonian attack targeted websites and organizations such as the Estonian parliament, banks, and newspapers, whereas the Ukraine case breached the transmission of electricity in western Ukraine, resulting in a loss of electricity. Both incidents show Russia's status as a cyber powerhouse, with a powerful arsenal of cyber tools and hackers capable of conducting disruptive and perhaps devastating assaults. Russia's cyber strategy and methods are aggressive, evolving, and increasing their impact by exploiting societal fissures through misinformation to dissuade those who would ignore or disparage Russia, perhaps posing a key challenge for Estonia and Ukraine. Therefore, as cyberattacks are immensely useful to criminals and spies, their frequency increases, and they have been linked to states, a conceptual framework is required to understand how these attacks worked and, presumably, why they were carried out.

CHAPTER 3

ANALYSIS OF MEARSHEIMER'S THEORY OF OFFENSIVE REALISM FOR RUSSIAN CYBER ATTACKS

The execution of Russian foreign policy is critical, and there are many degrees of policy implementation, which include internal and external risks to Russian foreign policy implementation. This chapter will use Mearsheimer's concept of offensive realism in two dimensions to examine the reasons for and variables of Russian cyber activities. Firstly, it will examine internal actors affecting motives for cyberattacks and foreign policy implementation, including: 1) leader and government factors; and 2) economic and energy security factors. In the second part, this chapter will discuss external factors, including: 1) Russia's interest in Ukraine and Estonia; and 2) the intervention by foreign powers, with emphasis on NATO. The last part is the conclusion.

3.1 Internal factors affecting Russian motives for cyberattacks and foreign policy implementation.

3.1.1 leader and government factors

The Russia of the twenty-first century, commonly known as "Putin's Russia," rapidly emerged with a "new realism," which was a far sharper realization of Russian power's constraints, most notably economic weakness.[92] It doesn't constitute the military juggernaut that the former USSR was, and its power is limited since the number of its citizens was reduced by fifty percent as a result of the dissolution of the Soviet Union and a number of factors, including increased immigration, a lower fertility rate, and a shorter lifespan, lowering the pool of military-eligible males.[93] Russia's main ideological strategy is to persuade people that any kind of uprising in the country will be linked to the US, with Putin portrayed as the sole leader capable of confronting US interference in Russian internal affairs and defending the imperial legacy.[94] Putin's policies were neither totally pro-West nor purely anti-West, as he opposed the US on numerous key

---

[92] R. Sakwa, *Putin: Russia's Choice* (Taylor & Francis, 2007), 210.

[93] Maness and Valeriano, *Russia's Coercive Diplomacy: Energy, Cyber, and Maritime Policy as New Sources of Power*, 5.

[94] Vladimir Shlapentokh, "Are today's authoritarian leaders doomed to be indicted when they leave office? The Russian and other post-Soviet cases," *Communist and Post-Communist Studies* 39, no. 4 (2006/12/01/ 2006): 462-63, https://doi.org/https://doi.org/10.1016/j.postcomstud.2006.08.001.

issues, most notably his opposition to national missile defence and NATO expansion, while still attempting to retain Yeltsin's cooperation with the West.[95] According to him, "the only feasible option is to be a nation that is strong and confident in its strength, not in spite of the world community or against other strong states, but together with them."[96] Under his leadership, China, for example, is required as an ally to counterbalance the West, not because of any new Chinese effort but because of Russia's shifting relationship with the West, which has been extremely beneficial to China.[97]

In addition, a conceptual framework early in his presidency underlined huge disparities with the West and two fundamentally distinct models of a new global order, identifiable by their degree of polarity.[98] Whereas a "unipolar" world based on the US's economic and military strength on the concept of "might makes right" and substitutes new doctrines of "limited sovereignty" and "humanitarian intervention" for traditional international law principles, Russia advocates for "multipolarity," in which no state or bloc should be hegemonic.[99] The new Foreign Policy Concept, released on June 28, 2000, emphasized the importance of Russia's policy being reasonable and feasible in order to serve Russian economic and political interests by encouraging its lead in the creation of a multipolar world, a policy specifically aimed at addressing the growing danger of US dominance.[100] Initially, Putin proposed the Organization for Security and Cooperation in Europe (OSCE) as the primary authority for continental security rather than NATO, and Russia's preferred model for sustaining international security was based on the United Nations.[101] Following Russian national elections in late 2003 and early 2004, Putin gained his second term with a wholly obedient parliament and an improved Russian foreign policy that became considerably more assertive and hardline. By criticizing his predecessor Boris Yeltsin's

---

[95] R. H. Donaldson, J. L. Nogee, and V. Nadkarni, *The Foreign Policy of Russia: Changing Systems, Enduring Interests* (Taylor & Francis Group, 2014), 365.

[96] Sakwa, *Putin: Russia's Choice*, 207.

[97] S. Blank and Institute Army War College . Strategic Studies, *Towards a New Russia Policy*, Global security challenges to U.S. interests, (Strategic Studies Institute, U.S. Army War College, 2008), 27.

[98] Donaldson, Nogee, and Nadkarni, *The Foreign Policy of Russia: Changing Systems, Enduring Interests*, 364.

[99] Ibid.

[100] Sakwa, *Putin: Russia's Choice*, 214.

[101] Ibid., 364.

cooperative approach, he urged that Russia be acknowledged as a significant state with geopolitical equals to the US and Europe and be given fair weight in settling world crises.[102] As a result, Putin's and his government's worldviews are crucial to Russian policymaking.

3.1.2 economic and energy security factors;

One of Russia's national interests is energy security, as it was used to boost its economic position, mostly through cooperative groups, and promote its role as the world's center of influence. Because it possesses natural gas and pipeline power over most post-Soviet nations, Russia has the capacity to push other states into doing things they would not do otherwise through its coercive energy policy.[103] Because the EU imports more than half of its natural gas and one-third of its oil from Russia via ships and pipelines built by Russia, political events affecting the EU-Russia relationship will have an influence on the import and export of oil and natural gas. During the 2006 and 2009 gas crises, for example, tensions between Russia and Ukraine erupted over debts, pricing, and transit fees, resulting in gas supplies being cut off to Ukraine, with the repercussions instantly reverberating throughout Europe for two weeks in the middle of winter.[104] This event reflected Russia's influence on Eastern and Central European countries that continue to rely on Russian gas, which contributes greatly to European energy supplies via a number of important pipelines, the largest of which runs through Ukraine and has grown into an obstacle for both countries in their attempts to prevent the escalating conflict.[105] As a result, because energy is vital to driving the economic and political systems, Russia must secure oil and natural gas transit routes while also gaining as many natural resources as feasible.

In addition, aside from the geopolitical implications of Putin's worldwide diplomacy in the early years of his administration, economics was an essential consideration for the new Russian leader.[106] Putin worked hard to expand Russian markets and ensure, to the greatest extent

---

[102] Ibid., 383.

[103] Maness and Valeriano, *Russia's Coercive Diplomacy: Energy, Cyber, and Maritime Policy as New Sources of Power*, 11.

[104] S. Pirani et al., *The Russo-Ukrainian Gas Dispute of January 2009: A Comprehensive Assessment* (Oxford Institute for Energy Studies, 2009), 60.

[105] "The Ukraine crisis and Russia's gas threat in Europe," accessed April 26, 2023, https://www.reuters.com/graphics/UKRAINE-CRISIS/GAS/gdpzynlxovw/.

[106] Donaldson, Nogee, and Nadkarni, *The Foreign Policy of Russia: Changing Systems, Enduring Interests*, 369.

feasible, repayment of Russian loans, and he loosened some of the laws limiting the export of armaments to Iran.[107] Russia's economic power is essentially restricted to the former USSR and areas of Europe where it can apply pressure, and it is economically and militarily outmatched by the US.[108] Under President Putin, the Russian economy went through two distinct phases: from 1999 to 2008, Russia profited with an average annual growth of 7%, and since 2009, it has stalled at 1%.[109] Putin, unable to please people with strong economic development and higher standards of living, chose minor triumphs, including the 2008 Georgia-Russia conflict and the 2014 Crimean Status Referendum.[110] As a result, Russia is attempting to preserve regional leadership in energy and economy, and any disturbance is seen as damaging to Russia's national interest.

3.2 External factors affecting Russian motives for cyberattacks and foreign policy implementation.

3.2.1 Russia's interest in Ukraine and Estonia

Firstly, Estonia, the northernmost of the three Baltic republics, rose to prominence after regaining independence following the fall of the Soviet Union and is well-known for its huge success in implementing digital technology into the country's structure.[111] For much of its history, it was governed by foreign powers until 1991, when it proclaimed independence alongside the other Baltic republics, sought integration with a larger Europe, and ultimately achieved its long-standing geopolitical aims by joining NATO and the EU in 2004. Estonia, formerly colonized by the Soviet Union, is today a model democracy, a critical partner in confronting global and regional security challenges, and a global pioneer in cybersecurity and e-governance. Estonia's electric power output is also crucial for supplying sections of northern Russia and the Baltic republics, notably two power plants in Narva, which is flanked by Russia to the east. Because Estonia, Latvia, and Lithuania perceived the Soviet Union as dictatorial and the forcible annexation as coercive, the choice of a declaration of independence after the Cold War plainly

---

[107] Ibid.

[108] Maness and Valeriano, *Russia's Coercive Diplomacy: Energy, Cyber, and Maritime Policy as New Sources of Power*, 14.

[109] "The Russian economy in health, oil, and economic crisis," 2020, accessed April 25, 2023, https://www.atlanticcouncil.org/commentary/long-take/the-russian-economy-in-health-oil-and-economic-crisis/.

[110] Ibid.

[111] "Cyberattack on Critical Infrastructure: Russia and the Ukrainian Power Grid Attacks," 2017, accessed May 1, 2023, https://jsis.washington.edu/news/cyberattack-critical-infrastructure-russia-ukrainian-power-grid-attacks/.

showed the attitude of an independent nation threatened by Russia by using the phrase "reindependence." Instead, Russia saw the three Baltic republics as being of great strategic importance to the USSR's security, referring to them as "the backyard" and seeing itself as protecting these countries from the effects of the Second World War and the Nazi invasion. As a result, the three Baltic nations and Russia have quite distinct sets of Cold War memories, making both parties adversaries.

In addition, there are three primary reasons why Russia regards Ukraine as an important strategic position that it wishes to possess. Firstly, because of its location in the center between Russia on the east and EU nations on the west, Ukraine serves as an essential buffer zone for the two superpowers. Ukraine's Black Sea and Azov Sea coasts were both important port cities and naval bases in the former Soviet Union, particularly in the city of Sevastopol, located in Crimea, which has now been controlled by Russia since 2014[112] and is a popular vote for Putin, used as a symbol of rejection by Western mandates. Secondly, Ukraine has abundant natural resources and has been dubbed the "bread basket" of Europe because it is a large agricultural region that grows wheat, corn, barley, and sunflowers, all of which are important exports for the country. It also houses a natural gas pipeline that transports gas from Russia to EU nations, although the gas pipeline via Ukraine is currently less vital due to the construction of a new gas pipeline to the north. Thirdly, Ukraine was referred to as "Little Russia" from Russia's perspective since there was no distinction because some Russians were transported to Ukraine during the time when Ukraine was a part of the Soviet Union, particularly in the country's eastern and southern cities. Around 10 million people, or 20% of Ukraine's total population, are considered the largest group of Russians outside Russia and support the president on Russia's side. Ukraine is highly significant for these three reasons, and thus Russia and the EU nations are at odds with each other until the conflict grows into a twenty-first century war. As a result, because Ukraine is so important, its western allies sought to prevent Russia from repeating the events in Crimea, as Ukraine is UN-recognized nation with the right to select its own destiny and to prevent Russia from violating its sovereignty.[113]

---

[112] "Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid," 2016, accessed May 15, 2023, https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/.

[113] Maness and Valeriano, *Russia's Coercive Diplomacy: Energy, Cyber, and Maritime Policy as New Sources of Power*, 110.

3.2.2 the intervention by foreign powers, with emphasis on NATO.

There are three foreign powers that could intervene in Russia's national interests, including NATO, the EU, and the US. Firstly, NATO was founded in 1949 by a coalition of 12 Western countries to provide mutual aid in the event of an armed attack in reaction to the Soviet Union's expanding dominance in Europe after World War II. To counter NATO, the Warsaw Pact Organization was formed in 1955 by communist states in Eastern Europe. By late 1991, the presidents of three of the USSR's founding countries had proclaimed that the USSR no longer existed, and a number of countries turned away from Warsaw to join NATO instead. Over the course of the 1990s and the early 2000s, NATO expanded three times, the second time in 2004 adding seven new nations, some of which were former Soviet republics such as Estonia, Latvia, and Lithuania. The May 1997 agreement between Russia and NATO[114] contained language relating to future membership, and Russian President Boris Yeltsin made it plain in his December 1997 National Security Blueprint that NATO enlargement was "unacceptable" and a danger to Russian security.[115] In the preceding decade, Russian military concerns about US expansion were consolidated by General Valery Gerasimov, who depicted it not solely by means of programs in Yugoslavia in 1991, Afghanistan in 2001, and Iraq in 2003 but also by means of "color revolutions," in which pro-Russians were deposed by nationalist, pro-Western, and liberal uprisings.[116] Although Western officials, including the leaders of those "new NATO" countries, see NATO membership as purely defensive and see no threat to Russia, they note that Putin is not the type of leader who makes neighbors feel at ease, as he considers the regathering of Russian lands, particularly Ukraine, to be part of his legacy.[117]

Furthermore, comparisons of European power in the twenty-first century, particularly considering the fundamental assets that Russia and NATO partners may deploy to accomplish what they desire, are crucial for understanding the context of European strategic rivalry.

---

[114] "Founding Act on Mutual Relations, Cooperation and Security between NATO and the Russian Federation signed in Paris, France," 2009, accessed April 20, 2023, https://www.nato.int/cps/en/natohq/official_texts_25468.htm.

[115] "Russian National Security Blueprint," 1997, accessed April 24, 2023, https://nuke.fas.org/guide/russia/doctrine/blueprint.html.

[116] Dyer-Witheford and Matviyenko, *Cyberwar and Revolution: Digital Subterfuge in Global Capitalism*, 48.

[117] "Russia feels threatened by NATO. There's history behind that," 2021, accessed April 25, 2023, https://www.latimes.com/politics/story/2021-12-19/russia-feels-threatened-by-nato-theres-history-behind-that.

Russia's relative power in Europe is less than it was for the majority of the previous two centuries, owing to its political and diplomatic influence still not fully recovered after the collapse of the USSR. It has an economy burdened with structural problems, which are exacerbated by a relatively small population and traditional armed forces, both of which have a restricted capacity for significant development owing to escalating economic and political constraints. NATO's combined military force structure, on the other hand, is much greater, with North American armed forces totaling 1.4 million soldiers and the remaining partners totaling 1.8 million, while Russia has 850 thousand active-duty soldiers. On a technical basis, Russia has developed a number of the most advanced weapons platforms; nevertheless, due to financial constraints, it lacks the ability to deploy a substantial amount of its armed forces, making any damage in an important dispute operationally or even strategically critical. As a result, the extension of military-political blocs and alliances, notably NATO's enlargement, the establishment of military bases, and NATO's presence near its territory, have become threats to Russian national security.[118]

3.3 Conclusion

In two dimensions, to understand the motivations that are likely behind Russian cyber activities, this chapter applied Mearsheimer's concept of offensive realism, which believes that anarchy is contributing to violent state conduct. Firstly, when it comes to internal variables, Putin's and his government's worldviews are critical to Russian strategy because he supports multipolarity, which holds that no state or bloc should be hegemonic in order to oppose US humanitarian intervention. He pushed harder for Russia to be acknowledged as a major superpower, striving to preserve regional leadership in energy and economy, and any disturbance is viewed as a threat. Second, in terms of external forces, Russia's interest in Ukraine and Estonia is significant, since Russia sees them as crucial strategic locations that it would want to hold. Military-political blocs and alliances, particularly NATO's enlargement, pose significant dangers to Russian security. As a result, all of these considerations play a part in Russian's motivations, which are believed to be driving Russia's cyber actions.

[118] "2000 Russian National Security Concept." https://www.bits.de/EURA/natsecconc.pdf.

CHAPTER 4

AN ANALYSIS OF THE MOTIVES BEHIND RUSSIA'S CYBER ATTACKS IN ESTONIA AND UKRAINE

Since Russia is recognized as one of the most technologically competent and powerful nations, it has been accused of a number of cyberattacks. Considering the previous chapter's internal and external factors influencing Russia, the following four assumptions about Russian cyber activities are made: 1) to survive in the anarchy of the international system; 2) to reestablish its regional dominance and reconstruct the Great Russian Empire; 3) to restrict Western influence on surrounding nations and prevent the growth of NATO installations towards the Russian border, as well as to limit neighboring countries' economic, political, and military ties to the EU and NATO; and 4) to demonstrate their power to influence or deter adversaries, as well as their effectiveness against a country that cannot react in kind. Based on the internal and external factors, this chapter examines these four assumptions, beginning with Estonia, moving on to Ukraine, and eventually concluding.

4.1 The Estonia Case

To begin, the cyberattacks on Estonia in 2007 were an allegation that Russian recruited hackers to carry out attacks, flooding Estonian government websites and private sector institutions, although the Russian authorities consistently denied this. Estonia was the target of the first massive and organized cyberattack on a sovereign nation, which is seen as a true wake-up call for the rest of the world about the use of cybercrime as a weapon in political and diplomatic squabbles. From a narrow perspective, this incident is supposedly related to Russia since it followed decisions to relocate Soviet war memorials, which Estonians see as a reminder of 50 years of Soviet domination, which enraged some Russian speakers who protested against relocating the monument. It emphasizes the need for Russia to respond to Estonia's actions and reintegrate it into its orbit. Additionally, because it was the first significant and coordinated cyberattack campaign against a sovereign state, it is clear that Russia is also using this chance to find vulnerabilities and has proven its ability to sway or deter adversaries on a global scale. Despite the fact that this Estonian incident may be considered an example of international response, it showed the infrastructure's incapacity to quickly identify and block a relatively

simple type of attack. Therefore, Russia attracted worldwide attention as suspicions surfaced that it was responsible for a series of cyberattacks.

Furthermore, from a broader perspective, it is evident that the attack was done for political purposes, since Russia has had strained relations with Estonia since the Soviet Union's demise in 1991. Russia responded furiously to the monument's relocation, and its upper chamber of parliament voted to request that Putin break relations with the Baltic state and take strong actions to counter Russia's power. Because the Baltic Sea region was part of the Iron Curtain, which was critical to the security of the former Soviet Union and served as a home for many Russian residents, these nations are also subject to European Union and NATO security rules that collide with Russia's sphere of influence. The assumption that Russian authorities hired cybercriminals to carry out strikes and conduct the state-sponsored offensive appears most likely, as Russia wanted to punish Estonia but couldn't because it is a NATO member, so it was convenient to hire cybercriminals who carried out the offensive campaign on Russian authorities' behalf. Through the perspective of offensive realism, Russia strives to become a great power and is unsure about Estonia's intentions, which, along with NATO, might threaten Russia's security and possess some offensive military capabilities. When Russia's primary purpose is survival, it is a rational actor capable of devising effective tactics to optimize its chances of survival. As a result, cyberpower was used to retaliate against the Estonian movement in 2007, which was regarded as a watershed moment in offensive nation-state activities and spurred Estonia to enhance its cybersecurity.

4.2 The Ukrainian Case

Firstly, the 2015 Ukrainian electrical infrastructure strike was the first publicly recorded use of a digital weapon to completely disrupt a power grid and cause a power outage. The Sandworm Group was designated as the most likely perpetrator, and Russia was suspected of carrying out the attack. The multiple phases of the operation, demonstrating that various categories of players engaged in various components of the assault, raise the idea that the attack entailed coordination between entirely distinct participants, perhaps nation-state actors alongside well-funded, well-trained cybercriminals. As such attacks necessitate extensive planning and no customer records or extortion demands were made, governments rather than cybercriminals are

commonly implicated, or it might have begun with hackers acquiring early network access and then passing it on to nation-state operators, who performed the rest. Therefore, it implies that Ukraine has been compared to a "playground" for Russian hackers, who sought to test a distant cyber operation on Ukraine's crucial energy infrastructure.

In a broader perspective, when Yushchenko became president, there was a push for Ukraine to join NATO until it was granted the title of partner country," and it currently maintains this status today and may be able to participate in the future. Although Ukraine is not yet a member, it began formalizing relations with NATO in 1992, when Ukraine's first president, Leonid Kravchuk, visited NATO headquarters in Brussels, Belgium, and the NATO Secretary General, who visited Kiev. Political tensions between the two nations have escalated since the 'Euromaidan' movement for closer EU integration and Russia's invasion of Crimea, when Ukrainian-owned energy companies were nationalized by Crimean officials, aggravating Ukrainian ownership. The subsequent blackouts in Ukraine served as punishment for a pro-Ukrainian assault on Crimean substations, which had left two million Crimean citizens lacking electricity in the territory that Russia had seized, as well as a Russian naval base. It was therefore urged that NATO refuse Ukraine permanent membership and remove soldiers stationed in all 14 countries that joined NATO after 1997, fearing that the West was attempting to encircle Russia by enlisting all Eastern European nations as members.

4.3 Conclusion

This chapter investigates four hypotheses on Russian cyberattacks based on internal and external variables in Estonia and Ukraine. When evaluated through the lens of offensive realism, it is clear that the reasons driving both Russian cyberattacks are consistent with the premise. They were done for political reasons, as Russia has had strained relations with both nations since the breakup of the USSR, which erupted in response to the removal of the Bronze Soldier of Tallinn and the pro-Ukrainian attack on Crimean substations. Russia must respond to the acts of Estonia and Ukraine since both are essential to its security, and NATO appears to be expanding and gaining influence in the region. As a result, cyberpower has been employed in retaliation as well as exploiting these possibilities to uncover their weaknesses, and it has demonstrated its capacity to affect or deter opponents.

CHAPTER 5

CONCLUSION

This chapter summarize the findings of this study's research question, "How motivated was Russia to launch cyberattacks in Estonia and Ukraine in 2007 and 2015? What are the outcomes and consequences of the attack?" The majority of cyberattacks that occurred during this period have many similarities: 1) the aggressor's techniques; 2) the political context; and 3) the suspected perpetrators. While both events are examples of massive cyberattacks aiming at disabling state infrastructure, there are also a few differences, such as the major goals, the outcome, and the consequences of the attack.

5.1 The conclusion of the findings in this study

To answer the first part of the question, it is preferable to begin with the second component of results and effects, as well as by analyzing the similarities and contrasts between the attacks. To begin, in terms of aggressor techniques, there were attacks that used cyberspace as a tool, but the manner was slightly different. It was a widespread DoS attack in Estonia, employing various means such as ping floods and botnets commonly used for spam dissemination. The case of Ukraine was more complex, as hackers using the "BlackEnergy 3 malware" distantly undermined electricity distribution systems, including seizing control of SCADA, switching off substations, blocking or ruining IT infrastructure elements, and launching a DoS attack on the call center to prevent clients from receiving current updates on the power outage. Secondly, in terms of the political environment, Russia has had tense ties with Estonia and Ukraine since the breakup of the USSR, and in particular since Estonia's relocation of the Bronze Soldier and the pro-Ukrainian attack on Crimean substations. Third, in terms of alleged perpetrators, although in the case of Estonia, the Kremlin was quick to accuse without any official proof, and in the case of Ukraine, the persistent threat group known as Sandworm, both attacks were likely state-sponsored by Russia. Fourth, the primary goals of the attack were slightly different: the transfer of the Bronze Soldier and the pro-Ukrainian attack on Crimean substations. Fifth, as a result of the assault, while enormous amounts of internet traffic shut down the websites of Estonian banks, media, and government institutions, the situation in Ukraine is more serious, with a power outage impacting the residents. Both acts, which may be viewed as exemplary examples of international reaction, exposed a lack of infrastructure to quickly identify

and counter an assault. Sixth, in terms of the consequences of the attack, in the case of Estonia, NATO performed an internal assessment of cyber security and infrastructure measures, and the Tallinn Manual on International Law Applicable to Cyber Warfare was developed. However, because Ukraine is not yet a member of NATO, any reactions from NATO will be questioned by Russia. As a result, the similarities and differences between the attacks aid in determining the broader purpose of Russian cyber activities.

Furthermore, when looking back to address the first part of the question, Russia conducts its diplomatic activities primarily on the basis of its view of current circumstances and their influence on its interests. Through the prism of offensive realism, great powers are represented as power-maximizing and self-promotional, with the anarchic character of the international system accountable for aggressive state conduct. Estonia and Ukraine's actions, as well as NATO's intentions and efforts to intervene, expand, and gain supremacy in Russia's sphere of influence, would suffer harsh retaliation from Russia since the deeds of the US hegemon, who believed himself to be the lone superpower, would be the most threatening to Russia's survival. Hence, The Russians' primary objective in cyberattacks is most likely to survive the anarchy of the international system, in which realists do not believe governments can ever trust one another and must rely on themselves. This could be accomplished by reclaiming regional dominance and rebuilding the Great Russian Empire in order to re-enter Estonia and Ukraine into its orbit and utilize their strategic location and energy supplies for economic and security reasons. Russia must respond to threats from Estonia and Ukraine, prevent NATO installations from spreading along its border, limit Western influence on neighboring nations, and demonstrate its potential to influence or dissuade adversaries on an international level.

In addition, to achieve its aims, Russia appears to be employing a variety of strategies to shape the direction taken by its neighbors, including, among other things, a mix of invisible military operations on the battlefield and in cyberspace. Cyberattacks are a preferred method as they enable a more convenient and cost-effective course of action, particularly the employment of network warfare and cyber espionage in the early stages of modern warfighting strategies. As political uncertainty causes military uncertainty, utilizing cyberspace to gather intelligence and perform surveillance, or spying, against essential infrastructure gives an awareness of a

prospective enemy's intentions, capabilities, and behavior. This intelligence collection is critical to reducing the unpredictability of military operations and obtaining and sustaining military aggressive and defensive tools toward the possibility of war or efforts to compel or influence enemy courses of action. Moreover, the ability of a cyberattack to interrupt, malfunction, or damage a competitor's technological infrastructure or systems, or gain access to or alter private information, shatters the conventional war by permitting nations to bypass breaches of ethics and legal responsibilities that could be penalized according to conventional principles of engagement in warfare. Because cyberattacks have no boundaries in geography, low costs, and distinctive fields above the scope of conventional standards like the Geneva Convention, Russia has disseminated pro-Russian and anti-Western propaganda while putting forth dominance over Eastern European states.

In conclusion, Russian cyberattacks are most likely driven by a desire to survive the world system's anarchy, in which Russia lacks trust in others. Cyberattacks are frequently used because they allow for a more convenient, cost-effective course of action while avoiding ethical infractions and legal obligations that would be punishable under international conventions, especially in the early stages of military operations or information collection. Indeed, even if Russia claims survival, its aggressive course of action is unlikely to be peaceful, and Estonia, Ukraine, and NATO, which symbolize US and European military might, would not allow Russia to interfere and dominate in their affairs. To avoid a confrontation, the US must "accept" and "respect" Russia as a superpower with military force and prestige similar to the US, including refusing to accept a unipolar system and ceasing support for anything that would jeopardize its national security. Therefore, the activities of Estonia and Ukraine, as well as NATO's efforts to maintain political unity, military interoperability, and readiness in the region, must not precipitate a war with Russia.

REFERENCES

"2000 Russian National Security Concept." Accessed April 25. https://www.bits.de/EURA/natsecconc.pdf.

"Russia's Cyber Capabilities, Explained." 2022, accessed May 6, 2023, https://news.northwestern.edu/stories/2022/02/russias-cyber-capabilities-explained/?fj=1.

"Cyberattack on Ukraine Grid: Here's How It Worked and Perhaps Why It Was Done." 2016, accessed March 22, 2023, https://theconversation.com/cyberattack-on-ukraine-grid-heres-how-it-worked-and-perhaps-why-it-was-done-52802.

Andreasson, K. J. *Cybersecurity: Public Sector Threats and Responses.* Public Administration and Public Policy. Taylor & Francis, 2011.

Applegate, S. D. "The Dawn of Kinetic Cyber." Paper presented at the 2013 5th International Conference on Cyber Conflict (CYCON 2013), 4-7 June 2013 2013.

"The Russian Economy in Health, Oil, and Economic Crisis." 2020, accessed April 25, 2023, https://www.atlanticcouncil.org/commentary/long-take/the-russian-economy-in-health-oil-and-economic-crisis/.

Blank, S., and Institute Army War College . Strategic Studies. *Towards a New Russia Policy.* Global Security Challenges to U.S. Interests. Strategic Studies Institute, U.S. Army War College, 2008.

Boer, L. J. M. *International Law as We Know It: Cyberwar Discourse and the Construction of Knowledge in International Legal Scholarship.* Cambridge University Press, 2021.

Cao, Y., Y. Li, X. Liu, and C. Rehtanz. *Cyber-Physical Energy and Power Systems: Modeling, Analysis and Application.* Springer Nature Singapore, 2019.

Council, N. R., D. E. P. Sciences, and C. S. T. Board. *Cybersecurity Today and Tomorrow: Pay Now or Pay Later.* National Academies Press, 2002.

"Inside Nato's Cyber Range: How Armies Prepare against Attack and Why Nations Must Work Together." 2022, accessed October 12, 2022, https://www.euronews.com/next/2022/12/09/inside-natos-cyber-range-how-armies-prepare-for-attack-and-why-nations-must-work-together2.

Donaldson, R. H., J. L. Nogee, and V. Nadkarni. *The Foreign Policy of Russia: Changing Systems,*

Enduring Interests. Taylor & Francis Group, 2014.

"Cyberattack on Critical Infrastructure: Russia and the Ukrainian Power Grid Attacks." 2017, accessed May 1, 2023, https://jsis.washington.edu/news/cyberattack-critical-infrastructure-russia-ukrainian-power-grid-attacks/.

Dyer-Witheford, N., and S. Matviyenko. *Cyberwar and Revolution: Digital Subterfuge in Global Capitalism.* University of Minnesota Press, 2019.

"U.S. Firm Blames Russian 'Sandworm' Hackers for Ukraine Outage." 2016, accessed March 24, 2023, https://www.reuters.com/article/us-ukraine-cybersecurity-sandworm-idUSKBN0UM00N20160108.

"The Phases of War: Thoughts in and around Geopolitics.", 2022, https://geopoliticalfutures.com//pdfs/the-phases-of-war-geopoliticalfutures-com.pdf.

"Russian National Security Blueprint." 1997, accessed April 24, 2023, https://nuke.fas.org/guide/russia/doctrine/blueprint.html.

Ghernaouti, Solange. "Cyber Power : Crime, Conflict and Security in Cyberspace ", CRC Press, 2013.

Gismondi, M. D. *Ethics, Liberalism and Realism in International Relations.* Routledge Advances in International Relations and Global Politics. Taylor & Francis, 2007.

Gragido, W., and J. Pirc. *Cybercrime and Espionage: An Analysis of Subversive Multi-Vector Threats.* Elsevier Science, 2011.

"Lessons from the Ukraine Electric Grid Hack." 2016, accessed March 23, 2023, https://www.darkreading.com/vulnerabilities-threats/lessons-from-the-ukraine-electric-grid-hack.

"Fact Sheet: Imposing Costs for Harmful Foreign Activities by the Russian Government." The White House, accessed 15 November, 2022, https://www.whitehouse.gov/briefing-room/statements-releases/2021/04/15/fact-sheet-imposing-costs-for-harmful-foreign-activities-by-the-russian-government/?utm_source=link.

Johnson, T. A. *Cybersecurity: Protecting Critical Infrastructures from Cyber Attack and Cyber Warfare.* Zones of Religion. Taylor & Francis, 2015.

"The Ukraine Crisis and Russia's Gas Threat in Europe." accessed April 26, 2023, https://www.reuters.com/graphics/UKRAINE-CRISIS/GAS/gdpzynlxovw/.

Joque, J., and C. Malabou. *Deconstruction Machines: Writing in the Age of Cyberwar.* Electronic Mediations. University of Minnesota Press, 2018.

"Would Nato Go to War over a Cyberattack?", 2014, accessed October 30, 2022, https://nationalinterest.org/feature/would-nato-go-war-over-cyberattack-11199.

Kostyuk, Nadiya, and Yuri M. Zhukov. "Invisible Digital Front: Can Cyber Attacks Shape Battlefield Events?". *Journal of Conflict Resolution* 63, no. 2 (2017): 317-47. https://doi.org/10.1177/0022002717737138.

Kshetri, N. *The Global Cybercrime Industry: Economic, Institutional and Strategic Perspectives.* Springer Berlin Heidelberg, 2010.

Lehto, M., and P. Neittaanmäki. *Cyber Security: Power and Technology.* Intelligent Systems, Control and Automation: Science and Engineering. Springer International Publishing, 2018.

Libicki, Olesya Tkacheva and Martin C. "Nato as a Norm Entrepreneur on Cyber Engagement in a Third-Party Conflict." *European Cybersecurity Journal* 8, no. 1 (2022). https://cybersecforum.eu/wp-content/uploads/2022/06/ECJ_vol8_issue1.pdf.

"Nato's Role in Global Cyber Security." 2022, accessed October 2, 2022, https://www.gmfus.org/news/natos-role-global-cyber-security.

Maj, Mirosław. "Cyber Conflict During the War in Ukraine." *European Cybersecurity Journal* 8, no. 1 (2022). https://cybersecforum.eu/wp-content/uploads/2022/06/ECJ_vol8_issue1.pdf.

Maness, R., and B. Valeriano. *Russia's Coercive Diplomacy: Energy, Cyber, and Maritime Policy as New Sources of Power.* Palgrave Macmillan UK, 2015.

Maurer, T. *Cyber Mercenaries: The State, Hackers, and Power.* Cambridge University Press, 2018.

"Russia Feels Threatened by Nato. There's History Behind That." 2021, accessed April 25, 2023, https://www.latimes.com/politics/story/2021-12-19/russia-feels-threatened-by-nato-theres-history-behind-that.

McQuade, S. C. *Encyclopedia of Cybercrime.* Non-Series. ABC-CLIO, 2008.

Mearsheimer, J. J. *The False Promise of International Institutions.* Working Paper (John M. Olin Institute for Strategic Studies. Project on the Changing Security Environment and American National Interests). Harvard University, John M. Olin Institute for Strategic Studies, 1994.

———. *The Tragedy of Great Power Politics (Updated Edition).* W. W. Norton, 2003.

Molloy, S. *The Hidden History of Realism: A Genealogy of Power Politics.* The Palgrave Macmillan

History of International Thought. Palgrave Macmillan US, 2006.

"Founding Act on Mutual Relations, Cooperation and Security between Nato and the Russian Federation Signed in Paris, France." 2009, accessed April 20, 2023, https://www.nato.int/cps/en/natohq/official_texts_25468.htm.

Pirani, S., J. P. Stern, K. Yafimava, Studies Oxford Institute for Energy, and Staff Oxford Institute for Energy Studies. *The Russo-Ukrainian Gas Dispute of January 2009: A Comprehensive Assessment.* Oxford Institute for Energy Studies, 2009.

Reveron, D. S. *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World.* Cyberspace and National Security. Georgetown University Press, 2012.

Sakwa, R. *Putin: Russia's Choice.* Taylor & Francis, 2007.

Schmitt, M. N., and Nato Cooperative Cyber Defence Centre of Excellence. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations.* Cambridge University Press, 2017.

Sciarrone, Marie O'Neill. "Cyber Warfare: The New Front." *The Catalyst*, no. 6 (2017). https://www.bushcenter.org/catalyst/modern-military/sciarrone-cyber-warfware.

Scott, J. *Metadata: The Most Potent Weapon in This Cyberwar: The New Cyber-Kinetic-Meta War.* CreateSpace Independent Publishing Platform, 2017.

Shlapentokh, Vladimir. "Are Today's Authoritarian Leaders Doomed to Be Indicted When They Leave Office? The Russian and Other Post-Soviet Cases." *Communist and Post-Communist Studies* 39, no. 4 (2006/12/01/ 2006): 447-73. https://doi.org/https://doi.org/10.1016/j.postcomstud.2006.08.001.

Singer, P. W., and A. Friedman. *Cybersecurity: What Everyone Needs to Know.* Business Book Summary. OUP USA, 2014.

Smith, S., A. Hadfield, and T. Dunne. *Foreign Policy: Theories, Actors, Cases.* Oxford University Press, 2016.

Stiennon, R. *Surviving Cyberwar.* Government Institutes, 2010.

Taddeo, M., and L. Glorioso. *Ethics and Policies for Cyber Operations: A Nato Cooperative Cyber Defence Centre of Excellence Initiative.* Philosophical Studies Series. Springer International Publishing, 2016.

Toft, P., and Statskundskab Københavns Universitet. Institut for. *Arbejdspapir: John J. Mearsheimer : An Offensive Realist between Geopolitics & Power. 2003/01.* 2003.

United States. Government Accountability, Office, K. T. Norwood, and S. P. Catwell. *Cybersecurity, Cyberanalysis and Warning.* Nova Science Publishers, 2009.

Van Wie Davis, E. *Shadow Warfare: Cyberwar Policy in the United States, Russia and China.* Security and Professional Intelligence Education Series. Rowman & Littlefield Publishers, 2021.

Vasquez, J. A. *The Power of Power Politics: From Classical Realism to Neotraditionalism.* Cambridge Studies in International Relations. Cambridge University Press, 1998.

"What Is a Cyber War – Explained." accessed April 31, 2023, https://www.neit.edu/blog/what-is-a-cyber-war-explained#:~:text=Cyber%20espionage%20can%20gather%20intelligence,and%20aid%20conventional%20warfare%20efforts.

Williams, M. *Realism Reconsidered: The Legacy of Hans Morgenthau in International Relations.* OUP Oxford, 2007.

Zetter, K. *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon.* Crown, 2014.

"Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid." 2016, accessed May 15, 2023, https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/.

VITA

NAME	Sub.Lt.Theeratiphong Pannil, RTN
DATE OF BIRTH	1 July 1996
PLACE OF BIRTH	Khon Kaen, Thailand
INSTITUTIONS ATTENDED	2021 - 2023, Master of Arts (International Relations), Faculty of Political Science, Chulalongkorn University 2017 - 2019, Bachelor of Science in Computer Science and Mathematics and Statistics, School of Science, University of New South Wales, Australia
HOME ADDRESS	123/132 Ekachai Road, Chom Thong, Bang Khun Thian, Bangkok 10150
AWARD RECEIVED	Bachelor of Science in Computer Science and Mathematics and Statistics with Distinction