



NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

**RUSSIAN CYBER OPERATIONS TO
DESTABILIZE NATO**

by

Joshua D. Christian

June 2020

Thesis Advisor:
Second Reader:

Scott E. Jasper
Wade L. Huntley

Approved for public release. Distribution is unlimited.

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			<i>Form Approved OMB No. 0704-0188</i>	
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington, DC 20503.				
1. AGENCY USE ONLY (Leave blank)	2. REPORT DATE June 2020	3. REPORT TYPE AND DATES COVERED Master's thesis		
4. TITLE AND SUBTITLE RUSSIAN CYBER OPERATIONS TO DESTABILIZE NATO			5. FUNDING NUMBERS	
6. AUTHOR(S) Joshua D. Christian				
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000			8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A			10. SPONSORING / MONITORING AGENCY REPORT NUMBER	
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.				
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release. Distribution is unlimited.			12b. DISTRIBUTION CODE A	
13. ABSTRACT (maximum 200 words) Cyber operations are constantly evolving as states discover new tactics to achieve strategic goals. Thus far, they have remained below the threshold for armed conflict by operating within the gray zone. Since 2008, Russia has demonstrated a preference for using cyber operations with the primary goal to weaken enemies of the state and achieve strategic objectives delineated in Russian grand strategy. This thesis examines the intersection between Russian cyber operations and grand strategy to weaken NATO. Russian grand strategy attempts to strengthen its position as a world power, in part, by utilizing cyber operations as a tool to destabilize adversaries. Specifically, their cyber operations fundamentally changed the way information is disseminated to sow discord in NATO societies, with the ultimate goal of sabotaging elections and democratic processes. Russian cyber operations also attempt to destabilize the security of NATO member states through cyberattacks against critical infrastructure. Russia's advances to grow its power have put it on a path to directly challenge the regional power balance with itself, NATO, and other European states. Russia's hegemonic goals and threat perceptions of NATO as a potential cyber target are critical developments to recognize and respond to present and future cyber operations. It is essential that NATO policymakers understand the ramifications of these cyber operations in order to preserve NATO security and stability.				
14. SUBJECT TERMS Russia, NATO, cyber, cyberattack, cyber operation, critical infrastructure, disinformation, grand strategy, gray zone			15. NUMBER OF PAGES 95	
			16. PRICE CODE	
17. SECURITY CLASSIFICATION OF REPORT Unclassified	18. SECURITY CLASSIFICATION OF THIS PAGE Unclassified	19. SECURITY CLASSIFICATION OF ABSTRACT Unclassified	20. LIMITATION OF ABSTRACT UU	

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release. Distribution is unlimited.

RUSSIAN CYBER OPERATIONS TO DESTABILIZE NATO

Joshua D. Christian
Ensign, United States Navy
BS, Embry-Riddle Aeronautical University, 2019

Submitted in partial fulfillment of the
requirements for the degree of

**MASTER OF ARTS IN SECURITY STUDIES
(STRATEGIC STUDIES)**

from the

**NAVAL POSTGRADUATE SCHOOL
June 2020**

Approved by: Scott E. Jasper
Advisor

Wade L. Huntley
Second Reader

Afshon P. Ostovar
Associate Chair for Research
Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Cyber operations are constantly evolving as states discover new tactics to achieve strategic goals. Thus far, they have remained below the threshold for armed conflict by operating within the gray zone. Since 2008, Russia has demonstrated a preference for using cyber operations with the primary goal to weaken enemies of the state and achieve strategic objectives delineated in Russian grand strategy. This thesis examines the intersection between Russian cyber operations and grand strategy to weaken NATO. Russian grand strategy attempts to strengthen its position as a world power, in part, by utilizing cyber operations as a tool to destabilize adversaries. Specifically, their cyber operations fundamentally changed the way information is disseminated to sow discord in NATO societies, with the ultimate goal of sabotaging elections and democratic processes. Russian cyber operations also attempt to destabilize the security of NATO member states through cyberattacks against critical infrastructure. Russia's advances to grow its power have put it on a path to directly challenge the regional power balance with itself, NATO, and other European states. Russia's hegemonic goals and threat perceptions of NATO as a potential cyber target is a critical development to recognize and respond to present and future cyber operations. It is essential that NATO policymakers understand the ramifications of these cyber operations in order to preserve NATO security and stability.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

I.	RUSSIAN CYBER OPERATIONS: AN ENABLER OF GRAND STRATEGY.....	1
A.	INTRODUCTION.....	1
B.	SIGNIFICANCE.....	2
C.	LITERATURE REVIEW	4
	1. Russian Grand Strategy	4
	2. Cyber Operations.....	10
D.	POTENTIAL EXPLANATIONS AND HYPOTHESES	14
E.	RESEARCH DESIGN.....	16
F.	THESIS OVERVIEW AND CHAPTER DESIGN.....	17
II.	GRAND STRATEGY: RUSSIAN GOALS AND CYBER OPERATIONS	19
A.	RUSSIAN GRAND STRATEGY	19
	1. NATO Containment.....	23
	2. World Power Status.....	25
	3. Greater Sphere of Influence in Europe.....	26
B.	CYBER TO ACHIEVE GRAND STRATEGY	28
	1. Cyber Actors.....	31
	2. Political Fracturing.....	32
	3. Diminish NATO Capacity to Respond.....	33
C.	CONCLUSION: RUSSIA’S GRAND STRATEGY AND CYBER OPERATIONS AS A TOOL	34
III.	CASE STUDIES: RUSSIAN CYBER OPERATIONS AGAINST NATO STATES.....	37
A.	2016 U.S. PRESIDENTIAL ELECTION	38
	1. Overview	38
	2. Contextual Analysis	39
	3. Event Timeline	40
	4. Findings and Implications.....	43
B.	2017 FRENCH PRESIDENTIAL ELECTION.....	45
	1. Overview	45
	2. Contextual Analysis	46
	3. Event Timeline	47
	4. Findings and Implications.....	49
C.	DRAGONFLY CAMPAIGNS.....	50

1.	Overview	50
2.	Contextual Analysis	51
3.	Event Timeline	52
4.	Findings and Implications.....	54
D.	NOTPETYA	55
1.	Overview	55
2.	Contextual Analysis	56
3.	Event Timeline	56
4.	Findings and Implications.....	59
E.	CONCLUSION	60
IV.	COUNTERING RUSSIAN CYBER OPERATIONS	63
A.	RESEARCH SUMMARY	63
B.	POLICY CONSIDERATIONS.....	65
1.	Evaluate NATO Attribution for Cyber Operations	65
2.	Determine NATO Threshold for Response and Retaliation.....	66
3.	Strengthen Intelligence Sharing Cooperation	67
4.	Develop NATO Cybersecurity Tactics, Training, and Procedures	68
	LIST OF REFERENCES	71
	INITIAL DISTRIBUTION LIST	81

LIST OF ACRONYMS AND ABBREVIATIONS

ANSSI	National Cybersecurity Agency of France
APT	Advanced Persistent Threat
CCDCOE	Cooperative Cyber Defence Centre of Excellence
CIA	Central Intelligence Agency
CISA	Cybersecurity and Infrastructure Security Agency
CSIS	Center for Strategic and International Studies
DHS	Department of Homeland Security
DIA	Defense Intelligence Agency
DNC	Democratic National Committee
EU	European Union
FBI	Federal Bureau of Investigation
GRU	Main Intelligence Directorate
ICA	Intelligence Community Assessment
ICS	Industrial Control System
IRA	Internet Research Agency
JAR	Joint Analysis Report
NATO	North Atlantic Treaty Organization
NSA	National Security Agency
NSS	National Security Strategy
SVR	Russian Foreign Intelligence Service
U.S.	United States
USIC	U.S. Intelligence Community

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

I would like to thank my thesis advisor, Dr. Scott Jasper, for all of his continued support and guidance throughout this process. Without his prying questions and expertise this thesis would have never progressed, and I have greatly enjoyed working with him. I would also like to thank Dr. Wade Huntley for his insight and time as my second reader. These two gentlemen provided superb insight while also challenging me to grow in my analytical abilities as a research writer.

I would also like to thank Colette O'Connor and the Graduate Writing Center for the outstanding advice and support during the revision process. Colette's guidance and ability to correctly utilize commas greatly improved the grammar and flow of this thesis. Her expertise and direction throughout my time at the Naval Postgraduate School has helped me improve exponentially as a writer.

Finally, to my mother, Dr. Ginger Christian, thank you for the hours of support you provided. You pushed me to think as a researcher and continued to challenge my analytical abilities, which greatly improved my research understanding. I could not have done this without your love and support as well as your teaching and encouragement. Thank you to all of my professors, peers, and friends who encouraged me and shaped my thinking during this academic journey. I cannot thank you enough for your guidance during this experience.

—ENS Joshua Christian, USN

THIS PAGE INTENTIONALLY LEFT BLANK

I. RUSSIAN CYBER OPERATIONS: AN ENABLER OF GRAND STRATEGY

A. INTRODUCTION

Cyberspace is a constantly expanding resource for state and commercial sectors that enables increased productivity, connectivity, and more efficient operations. While cyberspace is an effective medium to maximize operations it also creates a new opportunity for exploitation by adversaries. Of particular interest is the recent increase in the use of cyber operations by Russia as an emerging enabler of strategy.¹ In order to investigate potential threats with regard to cyber operations, this research investigates Russian cyber operations and subsequent impacts on state security. Critical to this thesis is the identification of Russian grand strategy, previous cyber operations, and reported impacts on member states within the North Atlantic Treaty Organization (NATO). This research should answer the question: What is the intersection between Russian cyber operations and grand strategy to weaken the NATO Alliance?

Russia utilizes cyber operations as a major component of its information warfare strategy. Areas of focus for this research include the manner in which Russia utilizes cyber operations and the interconnections of political and strategic goals for the state. The purpose of this thesis is to investigate previous Russian cyber operations as it relates to possible political influences within the NATO Alliance. The connection between political goals and strategic policy is important for analyzing and addressing the strategic purpose associated with Russian actions. Historically, priorities for Russia encompass increasing economic prosperity, geographical power, military power, and state power. Three main tenets of grand strategy that Russia prioritizes are: establishing a greater sphere of influence across former territory of the Soviet Union, attaining great power status in the eyes of the world, and containing the United States' (U.S.) and NATO global interests.²

¹ Keir Giles, *Handbook of Russian Information Warfare*, Fellowship Monograph No. 9 (Italy: NATO Defense College, 2016).

² Robert Person, "Russian Grand Strategy in the 21st Century" (Presentation, NSI SMA Speaker Series, Boston, MA, May 3, 2019), <https://nsiteam.com/russian-grand-strategy-in-the-21st-century/>.

Important for developing a detailed answer to the research question is understanding Russian political influence within its grand strategy, defining cyber operations within information warfare, and how Russia is utilizing its resources within that domain. This research also raises two sub-questions. First, what is the relationship of Russian grand strategy to the NATO Alliance? Second, what is the impact of Russian cyber operations on the NATO Alliance? In order to answer these sub-questions this research analyzes a historical shift of Russian and NATO relations from 2000 to 2020. It also reviews Russian political, military, and state leaders' views on grand strategy in relation to NATO. Reviewing Russian strategy, analyzing the scope of cyber operations, and identifying case studies provides insight on factors that have shaped and directed Russia's use of cyber operations to attain state goals.

B. SIGNIFICANCE

This research is crucial for three reasons. First, it analyzes case studies in order to create a greater understanding of Russian reactions to NATO expansion. NATO's growth in the post-Cold War era has placed added strain on its relationship with Russia due to NATO's borders encroaching on Russia. Russia views NATO expansion through a lens of containment, and therefore the need to prevent the NATO Alliance from gaining more members, as displayed by its strategy and political actions toward the NATO Alliance.³ Russia utilizes cyber operations to hamper NATO expansion by creating conflict. Russia's advances to grow its power have put it on a path to directly challenge the regional power balance among itself, NATO, and other European states. Russia's hegemonic goals and threat perceptions of its European neighbors are critical aspects to know and understand as drivers of Russian strategic views.⁴

Second, this thesis analyzes Russian aims to capitalize on the lack of political cohesion within NATO through attempts to politically fracture the Alliance. Many NATO states view political interference as a real threat that Russia poses to their people and

³ Michael Rühle, "NATO Enlargement and Russia: Die-Hard Myths and Real Dilemmas," NDC Research Report (Italy: NATO Defense College, May 15, 2014).

⁴ Ibid.

democratic processes. Russia's public interference in the democratic processes of elections works to undermine the faith of the people in the democratic processes of their state.⁵ Russian interference in political events within states undermines each state's power, potentially affecting the power and legitimacy of the Alliance as a whole. Greater member coordination within the Alliance that identifies interference operations and ends the operations before they can affect the legitimacy of the state will be crucial to countering Russian grand strategy and cyber operations. Understanding the political as well as military strategic goals of Russian interference is important to developing a coherent strategy within the Alliance to counter this threat.

Third, it analyzes how Russian cyber operations against the civil preparedness of NATO diminish the capacity for NATO to respond in a crisis. NATO identifies civil preparedness as, "aspects of national planning that affect the ability to contribute to Allied efforts in continuity of government, continuity of essential services to the population and civil support to military operations."⁶ Civil preparedness is critical to a state's ability to respond after an attack against a member state. NATO identifies resilience as, "society's ability to resist and recover easily and quickly from such shocks [natural disaster, critical infrastructure, hybrid or armed attack] and combines civil preparedness with military capacity."⁷ Cyber operations are capable of targeting and crippling critical infrastructure, thus greatly diminishing the ability for a state to respond in crisis. Acknowledging and planning, appropriately, for this cyber threat is critical to the security of Alliance states.

A clear analysis of elements that have led to Russia's increased use of cyber operations within its grand strategy will assist policy, strategy, and military planners within NATO in addressing Russian actions. Specifically, this analysis provides potential counter-strategies to mitigate Russian future cyber operations. This thesis will provide leaders with

⁵ Geir Hågen Karlsen, "Divide and Rule: Ten Lessons about Russian Political Influence Activities in Europe," *Palgrave Communications* 5, no. 1 (February 8, 2019): 1–14, <https://doi.org/10.1057/s41599-019-0227-8>.

⁶ NATO, "Civil Preparedness," NATO, March 31, 2020, http://www.nato.int/cps/en/natohq/topics_49158.htm.

⁷ NATO, "Resilience and Article 3," NATO, March 31, 2020, http://www.nato.int/cps/en/natohq/topics_132722.htm.

case studies and research that identify Russian operations at the political and strategic levels.

C. LITERATURE REVIEW

1. Russian Grand Strategy

a. *Grand Strategy Defined*

Grand strategy is used repeatedly when states are attempting to understand the motivating factors that drive a state to act in the way it does. Andrew Monaghan defines grand strategy as, “the art of bringing together and using all the resources of a nation to promote the vital interests of the state ... It is thus about the relationship between political ends and military, economic, political and cultural means—the ‘art of creating power.’”⁸ Peter Feaver asserts that grand strategy is, “the collection of plans and policies that comprise the state’s deliberate effort to harness political, military, diplomatic, and economic tools together to advance that state’s national interest.”⁹

Scholars are generally in agreement about the scope of the definition for grand strategy. Robert Person briefly defines grand strategy as, “the coordinated and comprehensive integration of ways and means to achieve national strategic ends.”¹⁰ Colin Gray states, “strategy is the bridge that relates military power to political purpose.”¹¹ The scope of grand strategy encompasses political and military means as a way of achieving the objectives of the state. Grand strategy is long-term focused planning for the role of the state years into the future.

⁸ Andrew Monaghan, “Putin’s Russia: Shaping a ‘Grand Strategy’?,” *International Affairs (Royal Institute of International Affairs 1944-)* 89, no. 5 (2013): 1226–27.

⁹ Peter Feaver, “What Is Grand Strategy and Why Do We Need It?,” *Foreign Policy*, April 8, 2019, <https://foreignpolicy.com/2009/04/08/what-is-grand-strategy-and-why-do-we-need-it/>; Person, “Russian Grand Strategy in the 21st Century,” May 3, 2019, 2.

¹⁰ Person, “Russian Grand Strategy in the 21st Century,” May 3, 2019, 4.

¹¹ Colin S. Gray, *Modern Strategy* (New York: Oxford University Press, 1999), 17.

b. History of NATO

In order to recognize the importance of the NATO-Russian relationship it is necessary to analyze the historical purpose of the NATO Alliance. The North Atlantic Treaty was signed on April 4, 1949, and within that treaty there are fourteen articles defining the duties of each Allied state for collective defense.¹² According to NATO, the Alliance was founded for the strategic purposes of, “deterring Soviet expansionism, forbidding the revival of nationalist militarism in Europe through a strong North American presence on the continent, and encouraging European political integration.”¹³ Of the fourteen articles in the treaty, Article 3 and Article 5 are relevant to the security of NATO in the cyber domain. NATO Article 3 declares, “the Parties, separately and jointly, by means of continuous and effective self-help and mutual aid, will maintain and develop their individual and collective capacity to resist armed attack.”¹⁴ A recent NATO publication notes resilience and Article 3 are closely tied in that, “resilience reduces the vulnerability of NATO as a whole,” which further strengthens the Alliance’s capacity to respond.¹⁵ Tim Prior asserts that, “Global connectivity presents new security challenges for NATO, especially in relation to critical infrastructure interdependence. Building resilience though civil preparedness will be a paradigm changer for deterrence.”¹⁶ Prior highlights the importance of strong civil preparedness in order to effectively carry out collective defense, as stated in Article 5, due to the reliance on a capable critical infrastructure to support military operations.¹⁷ Article 5 is the article surrounding the principle of collective defense which states, “an armed attack against one or more of them... shall be considered an attack against them all’ and that following such an attack, each Ally would take ‘such action as it

¹² NATO, “The North Atlantic Treaty,” NATO, accessed January 28, 2020, http://www.nato.int/cps/en/natohq/official_texts_17120.htm.

¹³ NATO, “A Short History of NATO,” NATO, accessed January 28, 2020, http://www.nato.int/cps/en/natohq/declassified_139339.htm.

¹⁴ NATO, “The North Atlantic Treaty.”

¹⁵ NATO, “Resilience and Article 3.”

¹⁶ Tim Prior, “NATO: Pushing Boundaries for Resilience,” *CSS Analyses in Security Policy*, no. 213 (September 2017): 1.

¹⁷ *Ibid.*, 3.

deems necessary, including the use of armed force' in response."¹⁸ Bruno Tertrais notes, "Article 5 is meant as an exceptional and temporary measure to deal with military threats."¹⁹ Tertrais also acknowledges that Article 5 has worked as a deterrent because there has not been any country that has undertaken a large military operation against a NATO member.²⁰ Additionally, Article 5 has only been invoked once, which was on October 2, 2001 in response to the 9/11 attacks against the United States.²¹

Throughout NATO's formative years, the late 1940s through the 1950s, its priority was on defense. NATO history states, "only a truly transatlantic security agreement could deter Soviet aggression while simultaneously preventing the revival of European militarism and laying the groundwork for political integration."²² Initially, there was not a coordinated military structure within NATO, but the Soviet Union was growing militaristically and the Alliance adapted to the growing Soviet threat. This security cooperation helped bring about political stability in post-WWII Western Europe. Diego Ruiz Palmer notes that NATO began its shift in posture toward "massive retaliation" with nuclear capabilities in 1952 in order to counter the Russian atomic bomb threat.²³ This new approach shifted the collective defense theory toward a nuclear defense and nuclear retaliation posture. Ruiz Palmer explains that NATO shifted again from 1957–1967 to a "Flexible Response," or *détente*, which focused more on conventional defense rather than an all or nothing nuclear strike.²⁴ NATO's goal was to force an arms control agreement that would eliminate such weaponry. This did not happen until 1987 when the Intermediate-Range Nuclear Forces (INF) treaty was established between the United States

¹⁸ NATO, "A Short History of NATO."

¹⁹ Bruno Tertrais, "Article 5 of the Washington Treaty: Its Origins, Meaning and Future," no. 130 (2016): 2.

²⁰ *Ibid.*, 4.

²¹ *Ibid.*

²² NATO, "A Short History of NATO."

²³ Diego Ruiz Palmer, "A Strategic Odyssey: Constancy of Purpose and Strategy-Making in NATO, 1949–2019," NDC Research Paper (Italy: NATO Defense College, June 2019), 28, <http://www.ndc.nato.int/news/news.php?icode=1330>.

²⁴ *Ibid.*, 33–34.

and the Soviet Union. Many experts believed this signaled the end of the Cold War, which happened when the Berlin Wall fell in 1989.²⁵

Following the Cold War and the subsequent break-up of the Soviet Union, NATO was left to find its new place in the international order. The Alliance had been founded in part to balance against the Soviet threat and had done so for over forty years. During the 1990s many experts expected NATO to disappear due to the lack of a Soviet threat; however, the Alliance survived because it still had two other original missions: “to deter the rise of militant nationalism and to provide the foundation of collective security that would encourage democratisation and political integration in Europe.”²⁶ John Duffield highlights that, due to NATO’s ability to adapt fundamentally, the need for a unified response to external threats, and the value of the intra-Alliance ability to cooperate, that the Alliance had significant purpose to stay in place.²⁷ Duffield argues that NATO was necessary following the end of the Cold War in order to counter any residual military power of Russia in order to bring stability to Central and Eastern Europe.²⁸ NATO brought increased security to former Soviet states in order to promote the new political reform these states were facing following the collapse of the Soviet Union.²⁹ NATO’s shift from prioritizing the Soviet threat to taking a proactive stance against external threats abroad displayed a fundamental change within the Alliance that was still committed to the security of all member states.³⁰ Additionally, NATO views expansion as a tool, “NATO enlargement has helped increase stability and prosperity in Europe. It is aimed at promoting stability and cooperation, and at building a Europe united in peace, democracy and

²⁵ NATO, “A Short History of NATO.”

²⁶ NATO.

²⁷ John S. Duffield, “NATO’s Functions after the Cold War,” *Political Science Quarterly* 109, no. 5 (1994): 766–67, <https://doi.org/10.2307/2152531>.

²⁸ *Ibid.*, 768–769.

²⁹ *Ibid.*, 771.

³⁰ *Ibid.*

common values.”³¹ Stability and prosperity are key beliefs of NATO that the Alliance wishes to share with other European states.

c. *NATO-Russian Relations—2000 to Today*

Following the collapse of the Soviet Union, the new Russian Federation attempted to create closer ties to the NATO Alliance to move on from the past. Robert Person highlights three distinct phases of Russian grand strategy and relationship with the NATO Alliance. He notes that these are “Pragmatic Accommodation” from 2000–2003, “Soft Balancing” from 2003–2007, and “Asymmetric Balancing” from 2007–present.³² These three phases display the shift of the events that led to increased tensions between NATO and Russia.

In his lecture, Robert Person highlights the key events of the first phase of pragmatic accommodation in Russian strategy.³³ He notes that the Russian position was weak compared to its competitors due to the economic and political recovery the state went through during the decade following the collapse of the Soviet Union. He continues on, stating that Russian attempts to increase its influence through bargaining and concessions in order to secure more Russian interests. One example of this was Russian support of the United States following the 9/11 terrorist attack.³⁴ Essentially, Russia gave approval for central Asian states to support U.S. intervention in Afghanistan without Russia creating issues. In return, Russia expected to secure concessions from the United States to preserve the Anti-Ballistic Missile Treaty (ABM), a treaty the United States withdrew from in November of 2001.³⁵ Russia also sought to limit NATO expansion of the Baltic states of Estonia, Latvia, and Lithuania, but NATO also went through with this expansion toward

³¹ NATO, “NATO Enlargement & Open Door,” NATO, 2017, https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2017_11/20171130_1711-factsheet-enlargement-eng.pdf.

³² Person, “Russian Grand Strategy in the 21st Century,” May 3, 2019, 11.

³³ Robert Person, *Russian Grand Strategy in the 21st Century*, Lecture, Future of Global Competition & Conflict (NSI SMA Speaker Series, Boston, MA, 2019), <https://nsiteam.com/russian-grand-strategy-in-the-21st-century/>.

³⁴ Ibid.

³⁵ Person, “Russian Grand Strategy in the 21st Century,” May 3, 2019, 12.

the Russian border. These events led Russia to abandon pragmatic accommodation for a stronger stance to secure the interests of the state.³⁶

Russia shifted its strategy to focus on soft-balancing in order to achieve its goals. Robert Pape states that soft-balancing focuses prioritizes, “to demonstrate resolve in a manner that signals a commitment to resist the superpower’s future ambitions” in order to set the stage for hard balancing in the future.³⁷ Person asserts that this focus is less militaristic and more on the political and diplomatic challenging of adversaries in order to slow down a unipolar country.³⁸ Person believes that this strategy is meant to slow down a larger state to prevent them from efficiently carrying out tasks that are in the interests of that state.³⁹ This phase ended when Russia took a harder stance against its adversaries and carried out a cyberattack against Estonia in 2007.⁴⁰

The third phase of asymmetric balancing started in 2007 and is still ongoing with distinct shifts of Russian use of power to be more assertive and directed. Person defines asymmetric balancing tactics as “efforts to balance and contain indirect threats by using unconventional means.”⁴¹ Bettina Renz and Hanna Smith note that Russia is “more aggressive, assertive and frustrated with Western countries” and uses these asymmetric tactics as a means to achieve its ends.⁴² They note that Russian grand strategy seeks to “maintain its status as a Great Power” and the use of asymmetric and gray zone tactics assist in achieving this goal.⁴³ Person notes that regional powers are more likely to utilize

³⁶ Person, *Russian Grand Strategy in the 21st Century*, 2019.

³⁷ Robert A. Pape, “Soft Balancing against the United States,” *International Security* 30, no. 1 (July 2005): 37, <https://doi.org/10.1162/0162288054894607>.

³⁸ Person, *Russian Grand Strategy in the 21st Century*, 2019.

³⁹ Ibid.

⁴⁰ Rain Ottis, “Analysis of the 2007 Cyber Attacks against Estonia from the Information Warfare Perspective,” *Cooperative Cyber Defence Centre of Excellence*, 2008, 1.

⁴¹ Person, *Russian Grand Strategy in the 21st Century*, 2019.

⁴² Bettina Renz and Hanna Smith, “Russia and Hybrid Warfare—Going Beyond the Label,” *Aleksanteri Papers*, January 2016, 23.

⁴³ Ibid.

asymmetric balancing against hegemonic powers.⁴⁴ Examples of tactics that fall under asymmetric balancing also fall under the purview of “gray zone” tactics. These are: cyber and information operations, propaganda, manipulation and discrediting democratic institutions, calculated ambiguity, and deception and denial.⁴⁵ Gray zone tactics play a large role in how Russia carries out operations against its adversaries in order to achieve its end goal. Rod Thornton argues that the goal of these unconventional means is to use asymmetric tools and tactics to “defeat an adversary from the *inside* out.”⁴⁶ Person notes instances such as Estonia in 2007 and the warfare against the state over the removal of a Russian statue, the illegal annexation of Crimea in 2014, and election interference in the 2016 U.S. presidential election.⁴⁷

2. Cyber Operations

a. Cyber Operations Defined

The U.S. Joint Chiefs of Staff (JCS) defines cyberspace as, “a global domain within the information environment consisting of the interdependent networks of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.”⁴⁸ In reference to cyberspace, the JCS defines a cyberspace attack as, “actions taken in cyberspace that create noticeable denial effects (i.e., degradation, disruption, or destruction) in cyberspace or manipulation that leads to denial that appears in a physical domain, and is considered a form of fires.”⁴⁹ The United States has clear definitions in regard to cyberspace; recently NATO has begun to address the cyber domain as well. During the Wales Summit in 2014, the Alliance formally added cyber defense into NATO’s task structure for collective

⁴⁴ Person, “Russian Grand Strategy in the 21st Century,” May 3, 2019, 16.

⁴⁵ Ibid., 18.

⁴⁶ Renz and Smith, “Russia and Hybrid Warfare—Going Beyond the Label,” 55.

⁴⁷ Person, *Russian Grand Strategy in the 21st Century*, 2019, 19.

⁴⁸ Joint Chiefs of Staff, *Cyberspace Operations*, JP 3-12 (Washington, DC: Joint Chiefs of Staff, 2018), https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf, GL-3.

⁴⁹ Ibid.

defense, meaning cyberattacks could warrant an Article 5 response.⁵⁰ During the following meeting, the Warsaw Summit in 2016, NATO reaffirmed that decision and recognized cyberspace as an operational domain in which NATO will defend itself.⁵¹

b. *Gray Zone Defined*

Gray zone warfare is increasingly used by countries that seek to disrupt international order and rise to power. The Center for Strategic and International Studies (CSIS) defines gray zone as, “actions, which seek to gain advantage without provoking a conventional military response, are often difficult for free-market democracies to counter.”⁵² CSIS highlights how countries such as Russia and China “increasingly use non-military means to achieve their objectives. These gray zone actions include election meddling, economic coercion, and the ambiguous use of unconventional force. Below the level of war...”⁵³ Gray zone operations allow a state to operate in an area that falls below the threshold for armed attack. Hal Brands points out that “cyberattacks have proven to be a potent component of gray zone challenges in areas like Eastern Europe...spreading black propaganda and misinformation.”⁵⁴ Michael Mazarr believes that gray zone operations are used by “revisionist states with grand geopolitical ambitions.”⁵⁵ Mazarr argues, “Gray zone strategies pursue political objectives through calculated and integrated campaigns to achieve specific and often quite ambitious goals within a certain period of time.”⁵⁶

⁵⁰ NATO, “Wales Summit Declaration Issued by the Heads of State and Government Participating in the Meeting of the North Atlantic Council in Wales,” NATO, September 5, 2014, http://www.nato.int/cps/en/natohq/official_texts_112964.htm.

⁵¹ NATO, “Warsaw Summit Communiqué—Issued by the Heads of State and Government Participating in the Meeting of the North Atlantic Council in Warsaw, 8–9 July 2016,” NATO, July 9, 2016, http://www.nato.int/cps/en/natohq/official_texts_133169.htm.

⁵² “Competing in the Gray Zone,” accessed February 6, 2020, <https://www.csis.org/features/competing-gray-zone>.

⁵³ Ibid.

⁵⁴ Hal Brands, “Paradoxes of the Gray Zone,” *Foreign Policy Research Institute*, February 5, 2016, <https://www.fpri.org/article/2016/02/paradoxes-gray-zone/>.

⁵⁵ Michael J. Mazarr, “Struggle in the Gray Zone and World Order,” *War on the Rocks*, December 22, 2015, <https://warontherocks.com/2015/12/struggle-in-the-gray-zone-and-world-order/>.

⁵⁶ Ibid.

Lyle Morris et al., in a RAND study, highlights multiple important points about gray zone activities with the first being, “gray zone elements remain below the threshold that would justify a military response.”⁵⁷ The second point that the study notes is that gray zone activities, “unfold gradually over time rather than involving bold, all-encompassing actions to achieve objectives in one step.”⁵⁸ The third point is that the aggressor looks for a, “lack of attributability” in order to disguise the role of the state in the action.⁵⁹ Morris et al. highlights a total of eight characteristics that encompasses using international law to justify gray zone actions, ensuring they do not threaten a vital interest to avoid conflict, escalatory risk to coerce, uses nonmilitary tools to remain below the threshold for military response, and targeting specific vulnerabilities within a country.⁶⁰ Essentially, the objective for the aggressor state is that a gray zone, “takes advantage of strategic ambiguity to achieve gradual gains.”⁶¹

c. Information Warfare

Information warfare strategy is the Western terminology for its view on Russia’s use of different cyber tools to compete in the information space. The Congressional Research Service (CRS) defines information warfare as, “strategy for the use and management of information to pursue a competitive advantage, including both offensive and defensive operations.”⁶² The Western definition of information warfare is similar to Russian “information confrontation [*informatsionnoe protivoborstvo*], or IPb” which Lesley Kucharski explains is what Russia uses as a major strategy against NATO and other

⁵⁷ Lyle Morris et al., *Gaining Competitive Advantage in the Gray Zone: Response Options for Coercive Aggression Below the Threshold of Major War* (RAND Corporation, 2019), 8, <https://doi.org/10.7249/RR2942>.

⁵⁸ Ibid., 9.

⁵⁹ Ibid.

⁶⁰ Ibid., 8–11.

⁶¹ Ibid., 12.

⁶² Catherine A Theohary, “Defense Primer: Information Operations,” CRS In Focus (Washington, DC: Congressional Research Service, December 18, 2018), 1.

adversaries.⁶³ Khatuna Mshvidobadze further explains information confrontation: “Russia views cyber-capabilities as tools of information warfare, which combines intelligence, counterintelligence, maskirovka, disinformation, electronic warfare, debilitation of communications, degradation of navigation support, psychological pressure, and destruction of enemy computer capabilities.”⁶⁴ Information confrontation is a very broad strategy; Keir Giles points to how Russia utilizes cyber as a tool for achieving smaller more diverse information operational goals.⁶⁵ Kucharski notes that Russian views on information confrontation differ from Western state views in that Russia considers not just technology and infrastructure, but also human emotions and responses which Western states do not consider as information.⁶⁶

The Defense Intelligence Agency (DIA) recently published *Russia Military Power Report 2017*, a report in which the DIA recognizes that Russia uses cyber and information confrontation as means to control adversaries without escalation to kinetic military conflict.⁶⁷ Giles notes that it is important to understand that Russia does not differentiate cyberspace from the information space, in Russian strategy they are the same.⁶⁸ Due to this, the scope of cyber in Russian strategy enables Russia to break down this space to include “information-technical” and “information-psychological” as the two areas of Russian focus.⁶⁹ Timothy Thomas uses P. Koayesov’s definition of information-technical as, “blocking the operation of the enemy’s state and military command and control

⁶³ Lesley Kucharski, “Russian Multi-Domain Strategy against NATO: Information Confrontation and U.S. Forward-Deployed Nuclear Weapons in Europe” (The Center for Global Security Research: Lawrence Livermore National Laboratory, 2018), 2, https://cgsr.llnl.gov/content/assets/docs/4Feb_IPb_against_NATO_nuclear_posture.pdf.

⁶⁴ Khatuna Mshvidobadze, “The Battlefield on Your Laptop,” RadioFreeEurope/RadioLiberty, March 21, 2011, https://www.rferl.org/a/commentary_battlefield_on_your_desktop/2345202.html.

⁶⁵ Giles, *Handbook of Russian Information Warfare*, 2016, 7.

⁶⁶ Kucharski, “Russian Multi-Domain Strategy against NATO: Information Confrontation and U.S. Forward-Deployed Nuclear Weapons in Europe,” 2018, 4.

⁶⁷ Defense Intelligence Agency, *Russia Military Power Building a Military to Support Great Power Aspirations* (Washington, DC: Defense Intelligence Agency, 2017), <https://www.dia.mil/Portals/27/Documents/News/Military%20Power%20Publications/Russia%20Military%20Power%20Report%202017.pdf>.

⁶⁸ Giles, *Handbook of Russian Information Warfare*, 2016, 9.

⁶⁹ Ibid.

systems.”⁷⁰ Thomas also uses Koayesov’s definition of information-psychological which is, “exerting psychological information pressure on its leaders, Armed Forces personnel, and the population.”⁷¹ According to Giles, these two areas allow Russia to target information in order to disinform populations (psychological) and to target systems that collect, receive, and disseminate information (technical).⁷² Chief of Strategic Communications, Supreme Headquarters Allied Powers Europe (SHAPE), Mark Laity stated:

The Russians use information from a covert stage through six phases of warfare to the re-establishment of victory. Information confrontation is conducted in every phase, including covertly, in peace and in war. Our doctrines do not allow us to do a lot of this stuff till the fighting basically starts.⁷³

D. POTENTIAL EXPLANATIONS AND HYPOTHESES

The use of information confrontation is directly tied to gray zone strategies and is tightly woven into Russian operations in the cyber domain. Russian cyber operations have operated within the gray zone area targeting adversary institutions in order to achieve state objectives.⁷⁴ This is the foundation for the first hypothesis, which is Russia’s strategic goals, within the grand strategy, are to create political destabilization and threaten critical infrastructure sectors and ultimately hinder the Alliance’s ability to respond to a cyberattack. Michael Connell and Sarah Vogler note that Russian cyber operations fall outside of the established norms and laws for the cyber domain.⁷⁵ They highlight that these norms have a legal precedence that states are supposed to follow which makes it more

⁷⁰ Timothy Thomas, “Russian Information Warfare Theory: The Consequences of August 2008,” in *The Russian Military Today and Tomorrow: Essays in Memory of Mary Fitzgerald* / (Carlisle, PA, 2010), 284, <http://hdl.handle.net/2027/mdp.39015085911041>.

⁷¹ Thomas, 284.

⁷² Giles, *Handbook of Russian Information Warfare*, 2016, 10.

⁷³ House of Commons Defence Committee, “Russia: Implications for UK Defence and Security” (London, England: House of Commons Defence Committee, June 28, 2016), 17, <https://publications.parliament.uk/pa/cm201617/cmselect/cmdfence/107/107.pdf>.

⁷⁴ Giles, *Handbook of Russian Information Warfare*, 2016.

⁷⁵ Michael Connell and Sarah Vogler, “Russia’s Approach to Cyber Warfare,” Final (Arlington, VA: Center for Naval Analyses, September 2016), https://www.cna.org/CNA_files/PDF/DOP-2016-U-014231-1Rev.pdf.

difficult for states to legally respond to Russia. Additionally, the second hypothesis identifies the impact of cyber operations and the potential to destabilize the NATO Alliance. Specifically, Russia utilizes cyber operations are continually adapting and changing in order to create a weakness within the Alliance posing a long-term risk to the Alliance, its member states' security, and regional stability.

In the *2017 Russian military power report* published by the DIA, the report states that Russia sees the United States and its NATO Allies as a roadblock to achieving world power status and the respect the state deserves.⁷⁶ Russia states in its 2015 National Security Strategy that the NATO Alliance's buildup of military forces near Russia's border was a direct threat to its national security.⁷⁷ Russia's views of NATO and its member states demonstrates that Russia wants to change the current relationship between NATO and itself. The DIA highlights, "Moscow perceives the information domain as strategically decisive and critically important to control its domestic populace and influence adversary states."⁷⁸ Russia's use of information operations against adversary states and its willingness to do so highlights the need for NATO to be prepared to defend itself against information operations by Russia. Recent attacks also highlight the need to investigate Russia's original intention behind cyberattacks and is the foundation for the third hypothesis: Regardless of true intentions, it is in Russia's interest to portray their actions as defensive, and therefore to portray NATO expansion as the origin of aggression. If this hypothesis is plausible, then NATO may at least doubt the veracity of such protestations, and does not have to accept at face value that Russian leaders genuinely believe they are merely defensive actors.

⁷⁶ Defense Intelligence Agency, *Russia Military Power Building a Military to Support Great Power Aspirations*.

⁷⁷ Kremlin, *Russian National Security Strategy* (Moscow, Russia: The Kremlin, 2015), <http://www.ieee.es/Galerias/fichero/OtrasPublicaciones/Internacional/2016/Russian-National-Security-Strategy-31Dec2015.pdf>.

⁷⁸ Defense Intelligence Agency, *Russia Military Power Building a Military to Support Great Power Aspirations*.

E. RESEARCH DESIGN

This thesis utilizes strategy documents, joint publications, and scholarly writing on Russian strategy to assist in outlining Russian grand strategy. Scholarly writing as well as strategy documents will be used to analyze cyber operations and the role they play in Russian grand strategy. Expert reviews and government reports will be utilized to analyze case studies of Russian cyber incidents. These documents are used to create the best understanding of how Russia utilizes cyber as a tenet of information confrontation in order to achieve grand strategy. The white papers and scholarly writing on Russian information confrontation all follow a similar narrative that explains how Russian strategy is carried out and the potential effects it has. These documents are key pillars to the main argument for this thesis.

This thesis uses a case study analysis to better understand the effects of Russian cyber operations. This approach is best to grasp how the cyber operations have become more effective and efficient over time. This has enabled Russia to conduct operations of similar ends against multiple states in order to further its own objectives. Russia views NATO expansion as a direct threat to Russia and reasoning behind this will be analyzed to discover where it fits into Russian grand strategy. Lack of political cohesion within the NATO Alliance creates a vulnerability for Russia to exploit. Political instability and distrust in the government can be analyzed through the 2016 presidential election, as well as the election tampering in Europe, because both are important case studies to showcase how Russia has adapted the use of cyber and technology to further the effectiveness of its activities. Civil preparedness and resiliency are key parts of NATO strength that Russia has attempted to exploit to diminish NATO's capacity to respond during a crisis. Dragonfly and NotPetya displayed the progression of Russian cyber capabilities against critical infrastructure in a short period of time. The effectiveness and concerns highlighted by these cases are important to analyze in order for NATO states to better prepare to defend against cyber operations of this type. The disruption and damage that can be caused through critical infrastructure attacks has a global impact that far exceeds that of the United States and NATO.

F. THESIS OVERVIEW AND CHAPTER DESIGN

The second chapter examines Russian grand strategy and cyber operations. It analyzes what Russian grand strategy is as well as what role and impact cyber operations have on the strategy. This chapter discusses cyber as a tenet of information confrontation and what Russia is attempting to achieve with these operations.

The third chapter reviews three case studies for Russian election interference in NATO states and the United States in order to demonstrate the goals of the Russian grand strategy and cyber operations. The first case study is focused on election interference due to how directly attacking democratic states creates a distrust in the governmental processes that strengthen these states. Weakening states internally has the ability to weaken the Alliance as a whole.⁷⁹ The third chapter also assesses Russian cyber operations against critical infrastructure and energy sectors in the United States and NATO. The second case study is the Dragonfly operation against U.S. and European energy sectors. Globalization and technology rely on power provided by the energy sector in order to carry out daily operations. Without power or technology most organizations come to halt or are greatly slowed as seen with the NotPetya cyberattack.⁸⁰ The third case study is focused on the NotPetya cyberattack. While NotPetya did not target a NATO state directly, it did affect multiple NATO states in the process. It is important to grasp the effects of that operation due to the fact that this attack highlights the potential damage cyber operations can create.

The fourth chapter contains the findings and suggestions. Chapter V focuses on what the evidence presented by the case studies shows about Russia's grand strategy. The findings and implications will analyze what the role of these cyber operations are and what Russia is attempting to achieve through its use of information confrontation. While examining the strategy it is critical to recognize the appropriate responses of NATO states and their allies in order to prevent Russia from exploiting its cyber capabilities further. Thorough analysis of the strategy and case studies will assist NATO leaders in creating

⁷⁹ Karlsen, "Divide and Rule," February 8, 2019.

⁸⁰ Andy Greenberg, "The Untold Story of NotPetya, the Most Devastating Cyberattack in History," *Wired*, August 22, 2018, <https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/>.

strategy and policy that will further strengthen the Alliance against Russian cyber operations. Greater understanding will assist these leaders in effectively defending their states from Russian cyber operations that could potentially destabilize NATO.

II. GRAND STRATEGY: RUSSIAN GOALS AND CYBER OPERATIONS

This chapter is divided into two distinct sections. First, it explores Russian grand strategy and key goals and related objectives defined in Russian policy documents. Second, this chapter analyzes cyber operations as a tool to assist in achieving grand strategy objectives. This chapter provides analysis of Russian strategic documents in order to determine broader Russian strategic goals. In addition, the grand strategy section defines the Russian views on U.S. and NATO expansion, world power status, and the expansion of Russia's sphere of influence in Europe. The second section focuses on cyber operations as a key part of Russian information operations. It examines the actors Russia utilizes for cyber operations, to politically fracture NATO, and diminish NATO's capacity to respond in crisis. Chapter II begins the process of answering the first sub-question: What is the relationship of Russian grand strategy to the NATO Alliance? Defining grand strategy goals as well as Russia's goals through cyber operations is critical to the upcoming case study chapter.

A. RUSSIAN GRAND STRATEGY

Robert Person highlights the three goals of Russian grand strategy as follows: containing U.S. and NATO expansion, achieving world power status, and creating a greater sphere of influence in Europe.⁸¹ According to Geir Karlsen, it is critical to synthesize Russian policies to better understand how Russian strategies have long-term objectives.⁸² The 2016 Russian Foreign Policy Concept delineates five objectives and principles of importance to Russia with specific regard to its position with other states.⁸³ These five are: "General Provisions;" "Modern World and Foreign Policy of the Russian Federation;" "Priorities of the Russian Federation and Overcoming Global Challenges Shaping a Fair

⁸¹ Person, "Russian Grand Strategy in the 21st Century," May 3, 2019, 5.

⁸² Karlsen, "Divide and Rule," February 8, 2019.

⁸³ Kremlin, *Foreign Policy Concept of the Russian Federation* (Moscow, Russia: Kremlin, 2016), https://www.mid.ru/en/foreign_policy/official_documents//asset_publisher/CptICkB6BZ_29/content/id/2542248.

and Sustainable World Order;” “Regional Foreign Policy Priorities of the Russian Federation;” and “Russian’s Foreign Policy Formulation and Implementation.”⁸⁴ These priorities provide specific guidance with regard to national and international cyber operations.⁸⁵ Russia utilizes a myriad of tools and tactics in order to attempt to strengthen its position as a strong state in the competitive global sphere. The Russian Foreign Policy concept notes that the use of military, information technology, and soft power such as information and communication are important tools for achieving the objectives of the state.⁸⁶ Russian grand strategy goals are prioritized by aligning the doctrine and different areas of the state to focus on important objectives. Russia utilizes its National Security Strategy (NSS) and the Military Doctrine in combination with the Foreign Policy Concept to create a consensus within the state policy.

The current NSS of Russia highlights six key areas of concern and priorities of focus for the Russian Federation.⁸⁷ These six are: “General Provisions;” “Russia in the Modern World;” “National Interests and Strategic Priorities;” “Ensuring National Security;” “Organizational, Regulatory-Legal, and Information Foundations for Implementing This Strategy;” and “Main Indicators of the State of National Security.”⁸⁸ Within the NSS, Russia states the United States and its allies, such as NATO, seek to contain Russia in order to preserve the global dominance of these states. The NSS also highlights NATO, specifically, as a threat to Russian national security due to the expansion of the Alliance and military tools to states closer to Russian borders.⁸⁹ Julien Nocetti notes that Russian decision-makers take a defensive approach when creating strategy in order to

⁸⁴ Ibid.

⁸⁵ Ibid.

⁸⁶ Ibid.

⁸⁷ Kremlin, *Russian National Security Strategy* (Moscow, Russia: Kremlin, 2015), <http://www.ieee.es/Galerias/fichero/OtrasPublicaciones/Internacional/2016/Russian-National-Security-Strategy-31Dec2015.pdf>.

⁸⁸ Ibid.

⁸⁹ Ibid.

counter a perceived offensive threat.⁹⁰ The 2014 Military Doctrine of the Russian Federation also highlights NATO build-up of forces and expansion near Russian borders as an external military risk to its sovereignty.⁹¹ The Russian Foreign Policy concept describes the Russian understanding on issues it views as critical:

The Russian Federation maintains its negative perspective toward NATO's expansion, the Alliance's military infrastructure approaching Russian borders, and its growing military activity in regions neighbouring Russia, viewing them as a violation of the principle of equal and indivisible security and leading to the deepening of old dividing lines in Europe and to the emergence of new ones.⁹²

Russia's belief that it needs to respond defensively to NATO further exacerbates the current NATO-Russian relationship.

The defensive mindset of Russian policy-makers concerning what is perceived as a larger threat, NATO, has shaped the way policy-makers define Russian strategy. Lesley Kucharski states that Russia is falling back on a Soviet Union style of planning and thinking.⁹³ Kucharski lists six non-military instruments Russia adapted from Soviet techniques as: "political influence operations," "disinformation," "propaganda," "media manipulation and control," "front organizations," and "non-ruling communist parties."⁹⁴ Along with adapting this Soviet style of thinking, Russia aims to avoid costly confrontation when protecting its national interests.⁹⁵ According to Stacie Pettyjohn and Becca Wasser, "gray zone tactics are cheap in terms of cost and risk, Russia is willing to liberally use them even when the prospect of success is low."⁹⁶ The gray zone has become an essential part

⁹⁰ Andrei P. Tsygankov, ed., *Routledge Handbook of Russian Foreign Policy* (London; New York: Routledge, Taylor & Francis Group, 2018).

⁹¹ Kremlin, *The Military Doctrine of the Russian Federation* (Moscow, Russia: Kremlin, 2014), <http://rusemb.org.uk/press/2029>.

⁹² Kremlin, Foreign Policy Concept of the Russian Federation.

⁹³ Kucharski, "Russian Multi-Domain Strategy against NATO: Information Confrontation and U.S. Forward-Deployed Nuclear Weapons in Europe," 2018, 13.

⁹⁴ Ibid.

⁹⁵ Kremlin, Russian National Security Strategy.

⁹⁶ Stacie Pettyjohn and Becca Wasser, *Competing in the Gray Zone: Russian Tactics and Western Responses* (RAND Corporation, 2019), 32, <https://doi.org/10.7249/RR2791>.

of Russian Military Doctrine, and the Gerasimov Doctrine, named after General Valery Gerasimov, further explains the role asymmetric tactics, gray zone operations, play in achieving the goals of Russia. General Gerasimov, Chief of the General Staff of the Russian Federation Armed Forces, wrote an article explaining the new way of modern warfare in which he stated, “The very ‘rules of war’ have changed. The role of nonmilitary means of achieving political and strategic goals has grown, and, in many cases, they have exceeded the power of force of weapons in their effectiveness.”⁹⁷ Russia has shifted from using purely conventional forces to prioritizing asymmetric political and informational activities to further achieve the state’s strategic objectives without resorting to force-on-force conflict.

Russia’s grand strategy is driven in part by Russian President Vladimir Putin, who stated, “the demise of the Soviet Union was the greatest geopolitical catastrophe of the [20th] century.”⁹⁸ This statement explains President Putin’s personal views on the current state of affairs within Russia and helps NATO understand the direction President Putin has for the Russian Federation. The collapse of the Soviet Union saw Russia attempt to reform the government toward democracy, but the state struggled to accept democracy.⁹⁹ Russia has been shifting away from democracy and toward autocracy with President Putin as the leader and driver of Russia’s future.¹⁰⁰ Fiona Hill contends that this leaves Russia and President Putin with a strategic advantage over democratic institutions:

[President Putin’s] ability to translate quick thinking into action and change course at the last minute gives him a significant advantage over Western

⁹⁷ Valery Gerasimov, “The Value of Science Is in the Foresight New Challenges Demand Rethinking the Forms and Methods of Carrying out Combat Operations,” *Military Review*, February 2016, 24, https://www.armyupress.army.mil/Portals/7/military-review/Archives/English/MilitaryReview_20160228_art008.pdf.

⁹⁸ Associated Press, “Putin: Soviet Collapse a ‘Genuine Tragedy,’” NBCNEWS, April 25, 2005, http://www.nbcnews.com/id/7632057/ns/world_news/t/putin-soviet-collapse-genuine-tragedy/.

⁹⁹ Michael McFaul, “Russia’s Transition to Democracy and U.S.-Russia Relations: Unfinished Business,” § U.S. Congress (2003), <https://carnegieendowment.org/2003/09/30/russia-s-transition-to-democracy-and-u.s.-russia-relations-unfinished-business-pub-1363>.

¹⁰⁰ Fiona Hill, “Putin: The One-Man Show the West Doesn’t Understand,” *Bulletin of the Atomic Scientists* 72, no. 3 (May 3, 2016): 140–44, <https://doi.org/10.1080/00963402.2016.1170361>.

leaders, who are always institutionally constrained in their decision-making, and usually have limits on the methods they can use to respond to a crisis.¹⁰¹

Hill argues that the autocratic state of ruling within Russia has enabled it to be able to make strategic moves that are more difficult for democratic Western states and institutions to navigate.¹⁰²

Success of Russian grand strategy is dependent on its execution and long-term commitment to Russian strategic goals. Karlsen notes that Russia has a strategy of “Divide and Rule” to achieve Russian goals in regard to Western states and institutions.¹⁰³ Karlsen further explains, based on evidence compiled by Western security institutions, that Russia has three levels of divide and rule which are to: divide European alliances such as NATO and the European Union (EU), create distrust and division between states, and to create internal division within a state.¹⁰⁴ Divide and Rule is critical to Russia’s success in achieving its three grand strategy goals. In order to achieve these goals Russia understands the importance of weakening its adversaries and further bolstering its own strength.

1. NATO Containment

Russia’s 2015 NSS highlights the belief that NATO is expanding in order to contain Russian influence. In addition, the Russian Foreign Policy Concept states, “Systemic problems in the Euro-Atlantic region that have accumulated over the last quarter century are manifested in the geopolitical expansion pursued by [NATO].”¹⁰⁵ This policy continues, stating that containment policies used by NATO undermine Russia and are detrimental to long-term stability and cooperation.¹⁰⁶ Russian leaders echo these concerns when questioned about NATO expansionism. During an interview about the Ukrainian conflict, Secretary of the Russian Security Council Nikolay Patrushev stated in regard to

¹⁰¹ Ibid.

¹⁰² Ibid.

¹⁰³ Karlsen, “Divide and Rule,” February 8, 2019.

¹⁰⁴ Ibid., 6.

¹⁰⁵ Kremlin, Foreign Policy Concept of the Russian Federation.

¹⁰⁶ Ibid.

NATO responses to the conflict, “If the catastrophe in Ukraine had not happened some other grounds would have been found to step up the policy of ‘containment’ of our country [Russia].”¹⁰⁷ Michael Rühle notes that Russia views NATO “as a hostile alliance” which has a large role in Russian politics and decision-making.¹⁰⁸ Russian views of NATO as a hostile organization echo the defensive posturing and external beliefs that are found within Russia’s greater strategic and policy documents.

NATO expansion has been a historically contentious topic between Russia and the West since the fall of the Soviet Union. During the 43rd Munich Conference on Security Policy, President Putin stated his belief that NATO expansion is a provocation that goes against assurances made by Western states when the Warsaw Pact dissolved in 1990.¹⁰⁹ In March of 2014 President Putin addressed Russian Parliament, stating, “On the contrary, they [NATO] have lied to us many times, made decisions behind our backs, placed us before an accomplished fact. This happened with NATO’s expansion to the East, as well as the deployment of military infrastructure at our borders.”¹¹⁰ Mark Kramer explained that there is a belief within Russia that when NATO and Russia negotiated German reunification, NATO expansion was addressed and promises were made not to expand eastward.¹¹¹ However, scholars have analyzed recently declassified documents related to this negotiation and have found no formal commitment in regard to expansion of NATO eastward.¹¹² Russia firmly states that a promise was made not to expand the Alliance and

¹⁰⁷ Nikolay Patrushev and Ivan Yegorov, Cold War II: Interview with Nikolay Patrushev, Secretary of the Russian Security Council, October 15, 2014, <https://mideastshuffler.com/2014/10/22/cold-war-ii-interview-with-nikolay-patrushev-secretary-of-the-russian-security-council/>.

¹⁰⁸ Rühle, “NATO Enlargement and Russia: Die-Hard Myths and Real Dilemmas,” 4.

¹⁰⁹ Vladimir Putin, “Putin’s Prepared Remarks at 43rd Munich Conference on Security Policy,” February 12, 2007, <http://www.washingtonpost.com/wp-dyn/content/article/2007/02/12/AR2007021200555.html>.

¹¹⁰ Team of the Official website of the President of Russia, “Address by President of the Russian Federation,” President of Russia, March 18, 2014, <http://en.kremlin.ru/events/president/news/20603>.

¹¹¹ Mark Kramer, “TWQ: The Myth of a No-NATO-Enlargement Pledge to Russia—Spring 2009,” *Center for Strategic & International Studies*, April 1, 2009, <https://www.csis.org/analysis/twq-myth-no-nato-enlargement-pledge-russia-spring-2009>.

¹¹² Ibid.

consequently views current NATO expansion as a strategy of containment meant to hold Russia back from rising to power.¹¹³

2. World Power Status

The definition of power is widely debated among scholars within international relations and Joseph Nye states “Power, like love, is easier to experience than to define or measure.”¹¹⁴ He defines power as “the ability to achieve one’s purpose or goals.”¹¹⁵ Nye narrows the definition of power to “the ability to influence the behavior of others to get the outcomes one wants.”¹¹⁶ Kenneth Waltz defines power simply as the “notion that an agent is powerful to the extent that he affects others more than they affect him.”¹¹⁷ For the purpose of this research, power encompasses the ability to influence other states as a crucial part of a state’s ability to gain respect and control on the international scale.¹¹⁸ Russia’s Foreign Policy Concept states that a main objective of Russia is: “to consolidate the Russian Federation’s position as a centre of influence in today’s world.”¹¹⁹ States at the center of influence have the most power and say over the changing international environment. Nikolay Patrushev stated that following the Russian intervention in Ukraine, the United States “was clearly alarmed by Russia’s obvious intention to take its place among the world powers of the 21st century and uphold the principle of equal opportunities and full autonomy in global politics.”¹²⁰ Patrushev made this statement in regard to Russia’s plan to sculpt a multipolar world in which Russia competes against world power’s such as the United States for a voice on international issues. This plan falls in line with the

¹¹³ Jonathan Masters, “An Unsettled Alliance,” Council on Foreign Relations, December 3, 2019, <https://www.cfr.org/background/north-atlantic-treaty-organization-nato>.

¹¹⁴ Joseph S. Nye, *Power in the Global Information Age: From Realism to Globalization* (London ; New York: Routledge, 2005), 53.

¹¹⁵ Ibid., 53.

¹¹⁶ Joseph S. Nye, *Soft Power: The Means to Success in World Politics*, 1st ed (New York: Public Affairs, 2004), 1.

¹¹⁷ Kenneth Neal Waltz, *Theory of International Politics*, Reissued (Long Grove, Ill: Waveland Press, 2010), 192.

¹¹⁸ Waltz, *Theory of International Politics*.

¹¹⁹ Kremlin, Foreign Policy Concept of the Russian Federation.

¹²⁰ Patrushev and Yegorov, Cold War II.

balance-of-power theory of international relations. Kenneth Waltz explains that in balance-of-power politics, two or more states exist in a system of self-help, with one being superior and the other having to help themselves in order to compete, survive, and gain power.¹²¹ Balance-of-power theory aligns with Russia's views that NATO is attempting to contain Russia and therefore Russia needs more power to survive in the international system.

Russia's policy delineates a clear position for the state to obtain status as a global power. Andrei Tsygankov states that Russian leaders are continually shaping the political landscape so Russia can be recognized as a world power in the eyes of the West.¹²² The 2015 NSS states that Russia seeks to consolidate its role as a leading world power in order to shape a polycentric world.¹²³ Gray zone tactics are useful for Russia to shape and achieve its world power goal. Russia is perceived as a weaker state in the international order; however, these tactics allow Russia to position itself competitively against stronger states and institutions such as the United States and NATO.¹²⁴ Greg Simons notes that Russia has had success in Foreign Policy due to the state's ability to utilize asymmetric tools that are difficult for a democratic state or institution to respond to.¹²⁵

3. Greater Sphere of Influence in Europe

Several Russian experts have highlighted that Russia wants to expand its influence over former states of the Soviet Union. In particular, Michael Kofman notes that Russia has a "drive to restore a privileged sphere of influence in the former Soviet Union."¹²⁶ Kofman argues that Russia views these states as a buffer zone against NATO and that NATO wants to use them as a buffer zone against Russia. He continues, stating that Russian leaders see these buffer states as an extended security zone needed to create space against

¹²¹ Waltz, *Theory of International Politics*, 118.

¹²² Andrei P. Tsygankov, "Preserving Influence in a Changing World: Russia's Grand Strategy," *Problems of Post-Communism* 58, no. 2 (March 2011): 33–34, <https://doi.org/10.2753/PPC1075-8216580203>.

¹²³ Kremlin, Russian National Security Strategy.

¹²⁴ Person, *Russian Grand Strategy in the 21st Century*, 2019.

¹²⁵ Tsygankov, *Routledge Handbook of Russian Foreign Policy*, 204.

¹²⁶ Michael Kofman, "Drivers of Russian Grand Strategy" (Stockholm: Frivärld, April 23, 2019), <https://frivarld.se/rapporter/drivers-of-russian-grand-strategy-2/>.

its perceived Western adversaries. The Russian Federation views its neighboring states as a strategic necessity to maintain security and control of its borders. Kofman also states, that while Russia views these states from a security standpoint, it also believes that it is the “rightful hegemon in its own region, and [needs to] reintegrate the former Soviet space to the extent possible around its own leadership.”¹²⁷ Through the reintegration of former Soviet states, Russia envisions its ability to increase regional influence in Europe as well as create a greater buffer zone with NATO.

Several military and academic experts have analyzed Russian actions to determine what ends Russian strategy is trying to achieve through expanding influence in Europe. John Allen, Philip Breedlove, Julian Lindley-French, and George Zambellas co-authored a paper concerning NATO strategy in future war with Russia.¹²⁸ These authors argue that post-Cold War Russia intends to rewrite European borders to create a “more Russia-friendly balance of power in Europe” in order to destabilize Western European states.¹²⁹ They state that Russia seeks to “compel the rest [Western European states] to comply with Russian strategic interests.”¹³⁰ With a restructured security framework in Europe, Russia can sow division and destabilize the NATO Alliance in order to expand Russian interests. Thomas Graham argues that Russia views itself surrounded by countries that are economically, politically, or demographically more dynamic than it is.¹³¹ He notes that due to this, “Russian leaders fear for the survival and territorial integrity of their country.”¹³² Russia’s defensive mindset in regard to its geographical and geopolitical position within Europe is a consistent driver of its grand strategy and strategic objectives.

¹²⁷ Kofman, 3.

¹²⁸ John Allen et al., *Future War NATO? From Hybrid War to Hyper War via Cyber War*, (Bratislava, Slovakia: Globsec, 2017), <https://www.globsec.org/wp-content/uploads/2017/10/GNAI-Future-War-NATO-JLF-et-al.pdf>.

¹²⁹ Ibid., 11.

¹³⁰ Ibid.

¹³¹ Thomas Graham, “The Sources of Russia’s Insecurity,” *Survival* 52, no. 1 (March 2010): 62, <https://doi.org/10.1080/00396331003612471>.

¹³² Ibid., 55.

B. CYBER TO ACHIEVE GRAND STRATEGY

Western views of cyber operations and the cyber realm parallel Russian information warfare and tactics. Information warfare, or information confrontation, as Russia calls it, utilizes cyber as an avenue to carry out operations that are in line with the goals of the state.¹³³ Russia's Foreign Policy concept states that information technical capabilities used in coordination with the military can influence states and international politics.¹³⁴ With this in mind, Russia has established a Doctrine of Information Security of the Russian Federation, defining "the strategic objectives and key areas of information security taking into account the strategic national priorities of the Russian Federation."¹³⁵ Nocetti states that, "The Kremlin fully considers the Internet as a foreign policy item," and due to this, Russia realizes the effect the cyber and information operations conducted over the internet has on national security.¹³⁶

Russian information operations have embraced ambiguity through gray zone activities in order to further Russian strategic goals. Russian literature refers to cyberspace and cyber operations when referring to Western state activities, but utilizes information operations or information confrontation in regard to Russian cyber operations.¹³⁷ The 2010 Russian Military Doctrine highlights how modern military conflicts rely on information confrontation to be used to achieve a political objective without using military force to shape responses from adversary states.¹³⁸ The Military Doctrine was updated in 2014 and it highlights the importance of utilizing asymmetric and indirect methods to achieve a favorable response.¹³⁹ The 2014 Military Doctrine also highlights "the development of

¹³³ Kucharski, "Russian Multi-Domain Strategy against NATO: Information Confrontation and U.S. Forward-Deployed Nuclear Weapons in Europe," 2018.

¹³⁴ Kremlin, Foreign Policy Concept of the Russian Federation.

¹³⁵ Kremlin, *Doctrine of Information Security of the Russian Federation*, (Moscow, Russia: Kremlin, 2016), https://www.mid.ru/foreign_policy/official_documents/-/asset_publisher/CptICk6B6BZ29/content/id/2563163.

¹³⁶ Tsygankov, *Routledge Handbook of Russian Foreign Policy*, 186.

¹³⁷ Giles, *Handbook of Russian Information Warfare*, 2016, 9.

¹³⁸ Kremlin, *The Military Doctrine of the Russian Federation*, (Moscow, Russia: Russian Federation, 2010), https://carnegieendowment.org/files/2010russia_military_doctrine.pdf.

¹³⁹ Kremlin, *The Military Doctrine of the Russian Federation*.

forces and means of information warfare” as an important task that the Russian military needs to be equipped to handle. Russia’s focus on strengthening its information warfare and operations capabilities is critical to growing its influence.

Russia utilizes cyber as a way to maintain its defensive posture against the perceived threat by Western institutions.¹⁴⁰ Greg Simons states that, “Russia maintains that it is fighting a defensive informational war in its foreign policy, which contradicts the mainstream Western political narrative that it is fighting an offensive war.”¹⁴¹ Russia’s foreign policy decisions and actions are tied to the achievement of its grand strategy. Nocetti highlights that Russia’s defensive mindset has led to changes in Russian foreign policy and security, utilizing cyber “as an asymmetric weapon, in an unequal balance of power as Russia’s conventional means remain inferior to NATO’s.”¹⁴² Ambiguity is one of the hallmark tools of gray zone tactics, making it more difficult to attribute blame and surmise the true intent of an information operation. Connell and Vogler note that Russia has further developed a way to carry out cyber operations against Western states that allow the state to avoid attribution for the attack.¹⁴³ These authors highlight how Russia has efficiently utilized hackers-for-hire to enable the state’s gray zone activities and maintain anonymity. Gray zone operations and anonymity allow Russia and other states to maintain a level of ambiguity that enables the state to effectively avoid direct blame for an incident. Connell and Vogler note that “plausible deniability with regard to disinformation campaigns” is critical to the achievement of Russian objectives.¹⁴⁴

Information operations utilized through the cyber domain play a key role in the achievement of strategic ends. Margarita Jaitner quotes Colonel Sergei Chekinov and Lieutenant General Sergei Bogdanov, who stated in 2010 that “Today the means of

¹⁴⁰ Tsygankov, *Routledge Handbook of Russian Foreign Policy*.

¹⁴¹ *Ibid.*, 209.

¹⁴² *Ibid.*, 189.

¹⁴³ Connell and Vogler, “Russia’s Approach to Cyber Warfare,” 9.

¹⁴⁴ *Ibid.*, 4.

information influence reached such perfection that they can tackle strategic tasks.”¹⁴⁵ Jaitner highlights another important quote from Chekinov and Bogdanov: “It is critical that such activities [information operationa] begin prior to the onset of traditional military operations.”¹⁴⁶ The introduction of influence operations before a wartime operation allows Russia to attempt to weaken an adversary before traditional conflict ensues. Nocetti notes that an interesting aspect of Russian information confrontation is that these operations are carried out consistently during peacetime as well as wartime.¹⁴⁷

Cyber is an effective tool that Russia has adapted into its military and political arsenal to enable successful achievement of its grand strategy. Cyber has multiple roles when it comes to achieving a strategic interest. Karlsen highlights the role that cyber plays in dividing a population internally via disinformation and misinformation as a covert means to influence the population.¹⁴⁸ He continues stating that Russia also utilizes overt force or coercion in the energy and critical infrastructure sectors to influence an adversary state. Karlsen states that a specific long-term strategic goal for Russia is to utilize information and influence operations to weaken NATO and its security position in the international order. Giles states that a key strategic goal for Russia would be to destabilize NATO, through information operations, to the point where if the Alliance needed to invoke an Article 5 commitment that it would be unable to reach a consensus decision.¹⁴⁹ Destabilizing NATO at this level requires long-term commitment to degrading relationships within not only the Alliance but also within individual states of the Alliance which Karlsen notes is what Western security institutions believe to be a key goal of Russian cyber operations to divide the Alliance.¹⁵⁰

¹⁴⁵ Kenneth Geers and NATO Cooperative Cyber Defence Centre of Excellence, *Cyber War in Perspective: Russian Aggression against Ukraine*, 2015, 89, <https://www.ccdcoe.org/library/publications/cyber-war-in-perspective-russian-aggression-against-ukraine/>.

¹⁴⁶ Ibid., 89.

¹⁴⁷ Tsygankov, *Routledge Handbook of Russian Foreign Policy*, 185.

¹⁴⁸ Karlsen, “Divide and Rule,” February 8, 2019.

¹⁴⁹ Giles, *Handbook of Russian Information Warfare*, 2016, 5.

¹⁵⁰ Karlsen, “Divide and Rule,” February 8, 2019.

1. Cyber Actors

Russia uses a myriad of different actors in order to further the ambiguity of its gray zone operations as well as attribution avoidance. Giles describes so-called “Information Troops,” who are a type of “Information Special Forces” within the military, that Russia utilizes to carry out its information cyber operations:

To construct information countermeasures, it is necessary to develop a centre for the determination of critically important information entities of the enemy, including how to eliminate them physically, and how to conduct electronic warfare, psychological warfare, systemic counterpropaganda, and net operations to include hacker training.¹⁵¹

Giles lists the personnel necessary to carry out this order as “diplomats, experts, journalists, writers, publicists, translators, operators, communications personnel, web designers, hackers, and others.”¹⁵² This diverse group is what enables Russia to covertly carry out its information operations as an aspect of gray zone that allows for the necessary level of ambiguity.

Russia’s broad use of actors to carry out these operations sets them apart from most other state actors in cyberspace. Connell and Vogler describe how Russia uses nonstate actors, such as hackers-for-hire, in order to carry out operations.¹⁵³ Another group of nonstate hackers is called “hacktivists,” who for political or nationalist reasons will undertake cyber operations on Russia’s behalf.¹⁵⁴ These hacktivists are a cost effective way for Russia to achieve strategic ends due to the hackers providing their own resources to successfully carry out an operation. They also provide the added benefit of anonymity and attribution difficulties due to the fact they are not directly tied to the state and appear to be operating on their own accord.¹⁵⁵ President Putin has denounced the actions of these

¹⁵¹ Keir Giles, “Information Troops”—*A Russian Cyber Command?*, 2011, 52.

¹⁵² *Ibid.*, 52.

¹⁵³ Connell and Vogler, “Russia’s Approach to Cyber Warfare,” 7.

¹⁵⁴ *Ibid.*, 9.

¹⁵⁵ *Ibid.*

hacktivists as not being guided by the state, but he has still titled them “patriotic hackers” who are free to act in the best interests of the Russian Federation.¹⁵⁶

2. Political Fracturing

NATO is a strong alliance that evinces the political ideals of free democracy, security, and a voice for the people. Russia by contrast is an autocratic state with policy and decision-making driven by the top leaders. Anne Applebaum explains that democracy threatens President Putin and Russia’s way of operating, and democracy cannot be allowed in Russia.¹⁵⁷ She continues, stating that, because of this threat, Russia is devoting extensive resources to “a political and information war designed to undermine and eventually destroy Western democracies as well as Western institution.”¹⁵⁸ Lesley Kucharski highlights that Russia exploits “perceived vulnerabilities of these democratic societies...in order to exacerbate pre-existing societal, political, and military divisions, thereby degrading NATO cohesion.”¹⁵⁹ Kucharski argues that Russia is able to utilize cyber and information in order to influence government officials as well as populations within a state in order to further spread Russian goals.¹⁶⁰ Russia actively uses propaganda to spread its interests globally and has even spread disinformation to attempt to influence populations globally through the use of the internet and social medias.¹⁶¹ Influence operations against a state’s population can spread decisive views with social media with the ability to further divide a state; this is a part of Karlsen’s findings that Russia is attempting to target populations to divide and rule.¹⁶²

¹⁵⁶ Mary Ilyushina and Euan McKirdy, “Putin: ‘Patriotic’ Russian Hackers May Have Targeted U.S. Election,” June 2, 2017, <https://www.cnn.com/2017/06/01/politics/russia-putin-hackers-election/index.html>.

¹⁵⁷ Anne Applebaum, “Putin’s Grand Strategy,” *South Central Review* 35, no. 1 (April 17, 2018): 28, <https://doi.org/10.1353/scr.2018.0001>.

¹⁵⁸ *Ibid.*, 28.

¹⁵⁹ Kucharski, “Russian Multi-Domain Strategy against NATO: Information Confrontation and U.S. Forward-Deployed Nuclear Weapons in Europe,” 2018, 2.

¹⁶⁰ *Ibid.*, 3.

¹⁶¹ Elizabeth Bodine-Baron et al., *Countering Russian Social Media Influence* (RAND Corporation, 2018), 1, <https://doi.org/10.7249/RR2740>.

¹⁶² Karlsen, “Divide and Rule,” February 8, 2019, 6.

A state that is embroiled with internal issues is slower to respond to external issues, such as a threat to the NATO Alliance.¹⁶³ World leaders are beginning to recognize the dangers of a divided NATO and its ability to respond to external threats. For instance, Polish President Andrzej Duda recently referenced Russia's goal to "pit NATO members against one another, to incite discord and doubts among states, between us and our neighbours."¹⁶⁴ Russia's attempts to divide the NATO Alliance place it in a more secure position of power. Kucharski finds that, based on Russian information operational goals, Russia seeks to gain strategic victory through subversive actions to destabilize foreign governments while maintaining stability in Russia.¹⁶⁵ Giles notes the multitude of ways that Russia uses information operations through social media to destabilize and delegitimize adversaries through the spread of disinformation and propaganda that damages adversaries while strengthening Russia's position.¹⁶⁶

3. Diminish NATO Capacity to Respond

NATO resiliency and civil preparedness are important factors when it comes to NATO's ability to respond during a crisis, such as a critical infrastructure failure due to a cyberattack. Allen, Breedlove, Lindley-French, and Zambellas argue that a weaker state, such as Russia, can utilize the internet, technology, and other cyber tools to weaken a far stronger opponent and cause disproportionate damage to an adversary.¹⁶⁷ These authors highlight how cyber operations have the ability to disrupt energy, the telephone, computer systems, transportation operations, TV, and social media to create chaos and push propaganda that creates a divide and slows the response of the victim state.¹⁶⁸ The growth

¹⁶³ Ibid.

¹⁶⁴ "Russia Seeking to Sow Discord, NATO Must React: Polish President," *Polskie Radio dla Zagranicy*, accessed November 21, 2019, <http://archiwum.thenews.pl/1/10/Artykul/410646,Russia-seeking-to-sow-discord-NATO-must-react-Polish-president>.

¹⁶⁵ Kucharski, "Russian Multi-Domain Strategy against NATO: Information Confrontation and U.S. Forward-Deployed Nuclear Weapons in Europe," 2018, 13.

¹⁶⁶ Keir Giles, James Sherr, and Anthony Seaboyer, "Russian Reflexive Control," *Royal Military College of Canada*, (October 2018), 28–42.

¹⁶⁷ Allen et al., *Future War NATO? From Hybrid War to Hyper War via Cyber War*, 5.

¹⁶⁸ Ibid., 7.

of cyber and connectivity into everyday lives of citizens creates a target of opportunity for a weaker state such as Russia.¹⁶⁹ Ambiguity and relative cost effectiveness of cyber and information operations creates an easier way to disrupt and divide a population from within.¹⁷⁰

James Wirtz argues that Russia is using cyber to diminish NATO's ability to respond by continually carrying out cyber and information operations that produce minimal destruction but create issues for the Alliance. He writes that, "In effect, the Russians seem to have realized that by defeating NATO's strategy at the outset of a confrontation, they can actually alter political perceptions within the Alliance in a way that suits their objectives."¹⁷¹ Similarly, Nocetti highlights that Russia is combining cyber and foreign policy to achieve its strategic goals. She states in regard to cyber that, "Russia is eager to challenge NATO member states' reactions and capacities, while blurring the lines between cybersecurity and the Russian concept of information security."¹⁷² A fractured NATO Alliance is slower to respond in crisis, a situation which Russia understands, and due to this, it uses a multitude of cyber and information tools to further destabilize the Alliance's ability to respond quickly.¹⁷³

C. CONCLUSION: RUSSIA'S GRAND STRATEGY AND CYBER OPERATIONS AS A TOOL

Russian grand strategy utilizes a vast array of tools available to the state in order to further the power and position of the state. Asymmetric gray zone operations utilizing cyber are a main tool that Russia employs to achieve grand strategy objectives. Cyber plays a crucial role in wearing down NATO over time in order to strengthen Russia's position. Russian information operations thrive on ambiguity and attribution difficulties, which is

¹⁶⁹ Giles, *Handbook of Russian Information Warfare*, 2016.

¹⁷⁰ Karlsen, "Divide and Rule," February 8, 2019.

¹⁷¹ James J Wirtz, "Cyber War and Strategic Culture: The Russian Integration of Cyber Power into Grand Strategy," in *Cyber War in Perspective: Russian Aggression Against Ukraine* (Estonia: CCDCOE, 2015), 34.

¹⁷² Tsygankov, *Routledge Handbook of Russian Foreign Policy*, 183.

¹⁷³ Karlsen, "Divide and Rule," February 8, 2019.

why they are so useful for Russia to remain under the radar of other states. This ambiguity gives Russia more latitude to avoid direct blame for these operations, and therefore more freedom to operate without triggering a direct response from NATO.

The reach of the internet and connected resources online enables Russia to carry out operations globally utilizing a variety of its “Information Troops” to achieve strategic objectives. Russian views of the outside world and competitive sphere against NATO are driving factors for Russia’s actions, with Putin recently stating his concern that continued NATO expansion posed a threat to Russia.¹⁷⁴ Putin’s statement points to the defensive posturing that Russia is currently undertaking through the use of information operations in order to strengthen its position. Achievement of grand strategy focuses on long-term goals with Russian operations piling up over time to slowly change the international sphere in its favor.

The following chapter will explore the role cyber operations play in achieving Russian grand strategy. Analysis will focus on four case studies, with two focusing on sowing discord within adversary states and two focusing on the ability to target critical infrastructure to slow an adversary’s ability to respond in a crisis. In keeping with the theme of gray zone and ambiguity, the case studies display the attribution issues, motivating factors, and delivery methods of cyber operations in order to achieve Russian grand strategy over time.

¹⁷⁴ Reuters, “Putin Criticizes NATO Expansion,” The Moscow Times, December 3, 2019, <https://www.themoscowtimes.com/2019/12/03/putin-criticizes-nato-expansion-as-alliance-holds-london-summit-a68457>.

THIS PAGE INTENTIONALLY LEFT BLANK

III. CASE STUDIES: RUSSIAN CYBER OPERATIONS AGAINST NATO STATES

This chapter examines four incidents involving Russian cyber operations and subsequent impact on NATO members and partners—the 2016 U.S. presidential election interference, the 2017 French presidential election interference, the Dragonfly operations from 2013–2017, and the 2017 NotPetya cyberattack on Ukraine. It should be noted that although it is difficult to attribute blame for a cyberattack, the United States is the prominent global leader that openly contends Russia’s cyber actors are responsible for these incidents.

The case studies were selected for several analytical reasons to best address this thesis’ primary research question—what is the intersection between Russian cyber operations and grand strategy to weaken the NATO Alliance? First, these cases were sourced from a multitude of state and expert scholarly research on Russian cyber activities. Secondly, these four cases demonstrate the scope of Russian cyber activities intended to sow discord as well as disrupt operations within NATO states. Thirdly, these four cases show an increase in ability and effectiveness suggesting that Russia is continually learning from previous cyber operations to structure future operations. Additionally, these cases analyze Russian cyber operations targeting political cohesion as well as the critical infrastructure resiliency of NATO states.

Russia uses a multitude of cyber actors known as Advanced Persistent Threat (APT) groups in state sponsored cyber operations.¹⁷⁵ Two well-known APT actors are APT28 and APT29 which are also associated with a myriad of other names. APT28 is known as “Fancy Bear, Pawn Storm, Sofacy Group, Sednit and STRONTIUM” while APT29 is known as “Cozy Bear, Office Monkeys, CozyCar, The Dukes, and

¹⁷⁵ Department of Homeland Security, *GRIZZLY STEPPE—Russian Malicious Cyber Activity*, (Washington, DC: Department of Homeland Security, 2016), https://www.us-cert.gov/sites/default/files/publications/JAR_16-20296A_GRIZZLY%20STEPPE-2016-1229.pdf, 2.

CozyDuke.”¹⁷⁶ Several of these names will be referenced throughout these case studies in regard to APT28 and APT29.

A. 2016 U.S. PRESIDENTIAL ELECTION

1. Overview

The Intelligence Community Assessment (ICA) joint report, published on January 7, 2017, by the National Security Agency (NSA), the Central Intelligence Agency (CIA), and the Federal Bureau of Investigation (FBI), discovered that in June 2014, the Internet Research Agency (IRA) located in St. Petersburg sent two employees to begin reconnaissance and intelligence gathering for the organization to carry out “information warfare against the United States.”¹⁷⁷ This early reconnaissance operation was used to refine IRA tactics to advance its information influence operations in the US.¹⁷⁸

These influence operations were utilized, as the ICA claimed, to “undermine public faith in the U.S. democratic process” through the use of social media “trolls” to spread disinformation throughout the election season and after.¹⁷⁹ Brian Barrett reports that as early as June 27, 2015, “Russian Intelligence group Cozy Bear ... also known as APT29—infiltrated the DNC [Democratic National Committee] network.”¹⁸⁰ APT29 has been linked to the SVR which is Russia’s Foreign Intelligence Service.¹⁸¹ CrowdStrike, the cybersecurity firm that discovered the DNC hack, reports that Fancy Bear, APT28,

¹⁷⁶ Pierluigi Paganini, “FBI-DHS JAR Report Links Russian Hackers to Presidential Election Hacks,” Security Affairs, December 31, 2016, <https://securityaffairs.co/wordpress/54900/cyber-warfare-2/fbi-dhs-jar-report.html>.

¹⁷⁷ Director of National Intelligence, Background to “Assessing Russian Activities and Intentions in Recent U.S. Elections”: The Analytic Process and Cyber Incident Attribution, (Washington, DC: Director of National Intelligence, 2017), https://www.dni.gov/files/documents/ICA_2017_01.pdf, 30.

¹⁷⁸ Ibid.

¹⁷⁹ Ibid., ii.

¹⁸⁰ Brian Barrett, “DNC Lawsuit Against Russia Reveals New Details About 2016 Hack,” *Wired*, April 20, 2018, <https://www.wired.com/story/dnc-lawsuit-reveals-key-details-2016-hack/>.

¹⁸¹ Andy Greenberg, “Russia’s Cozy Bear Hackers Resurface with Clever New Tricks,” *Wired*, October 17, 2019, <https://www.wired.com/story/cozy-bear-dukes-russian-hackers-new-tricks/>.

infiltrated the DNC in April 2016 separately from Cozy Bear.¹⁸² CrowdStrike notes that these two actors appeared to operate independently of each other to achieve the same objective. These hacks lead to the leaking of close to 20,000 emails through WikiLeaks with the intent to disrupt the political process.¹⁸³ Pawn storm, APT28, released these documents to the mainstream media as “exclusive access” in order to “publicize their attacks and influence public opinion.”¹⁸⁴

2. Contextual Analysis

This case is crucial to understanding the effects influence operations can have on a population through disinformation as well as sowing discord. Central to the incident’s repercussions is the consistent message that multiple Russia state actors have been blamed for cyber operations and disinformation campaigns during the 2016 U.S. presidential election. The ICA report assessed that “Moscow will apply lessons learned from its campaign aimed at the U.S. presidential election to future influence efforts in the United States and worldwide, including against U.S. allies and their election processes.”¹⁸⁵ The recent Select Committee on Intelligence U.S. Senate report on “Russian Active Measures Campaigns and Interference in the 2016 U.S. Election” stated that Russia’s influence in the election was an attack on U.S. democracy, but it was not the first time Russia used “asymmetric warfare against America.”¹⁸⁶ This report establishes that Russia favors information operations due to the difficulty of defending against them. More narrowly, it is relevant to recognize how cost-effective cyber and information operations are compared

¹⁸² Dmitri Alperovitch, “Bears in the Midst: Intrusion into the Democratic National Committee,” June 14, 2016, <https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/>.

¹⁸³ April Glaser, “Here’s What We Know About Russia and the DNC Hack,” *Wired*, July 27, 2016, <https://www.wired.com/2016/07/heres-know-russia-dnc-hack/>.

¹⁸⁴ Feike Hacquabord, “Two Years of Pawn Storm Examining an Increasingly Relevant Threat,” (Manilla: Trendlabs, 2017), 5.

¹⁸⁵ Director of National Intelligence, Background to “Assessing Russian Activities and Intentions in Recent U.S. Elections”: The Analytic Process and Cyber Incident Attribution, 5.

¹⁸⁶ Select Committee on Intelligence, Russian Active Measures Campaigns and Interference in the 2016 U.S. Election Volume 2: Russia’s Use of Social Media with Additional Views (Washington, DC: United States Senate, 2019), https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume2.pdf, 11.

to conventional military operations.¹⁸⁷ Not only are information operations cost effective, but the U.S. Senate report found that they also pose a difficult threat for “military alliances like NATO” to effectively respond and prepare for strategic defenses.¹⁸⁸

3. Event Timeline

According to the U.S. Senate Report and the Special Counsel’s Office, “by April 2014, the IRA had formed a new department inside the larger organization that was focused solely on the U.S. population.”¹⁸⁹ This department was referenced “as the ‘translator project,’” which continued to grow in size and presence as the election season picked up in 2016.¹⁹⁰ After the translator project was started, the IRA sent employees to the United States in June of 2014 to refine social media tactics, study societal issues, political views, and online activities in the US.¹⁹¹ This early reconnaissance was used to tailor the IRA’s activities to most effectively carry out information warfare operations within the US.¹⁹² The purpose of the IRA was to use “trolls,” which are paid social media users, to further spread disinformation, propaganda, and societal division.¹⁹³

The DNC believes that by July 27, 2015, Cozy Bear (APT29) hacked into the DNC’s systems.¹⁹⁴ The Joint Analysis Report (JAR) published by the FBI states that Cozy Bear gained access to the systems using a targeted spearphishing campaign that sent malicious email links to 1,000 people with ties to the DNC and U.S. government.¹⁹⁵

¹⁸⁷ Ibid., 13.

¹⁸⁸ Ibid.

¹⁸⁹ Select Committee on Intelligence, Russian Active Measures Campaigns and Interference in the 2016 U.S. Election Volume 2: Russia’s Use of Social Media with Additional Views, 30; Robert Mueller, Report On The Investigation Into Russian Interference In The 2016 Presidential Election, Volume I of II (Washington, DC: U.S. Department of Justice, 2019), <https://www.justice.gov/storage/report.pdf>.

¹⁹⁰ Select Committee on Intelligence, Russian Active Measures Campaigns and Interference in the 2016 U.S. Election Volume 2: Russia’s Use of Social Media with Additional Views, 30.

¹⁹¹ Ibid.

¹⁹² Ibid.

¹⁹³ Director of National Intelligence, Background to “Assessing Russian Activities and Intentions in Recent U.S. Elections”: The Analytic Process and Cyber Incident Attribution, 2.

¹⁹⁴ Barrett, “DNC Lawsuit Against Russia Reveals New Details About 2016 Hack.”

¹⁹⁵ Department of Homeland Security, GRIZZLY STEPPE—Russian Malicious Cyber Activity, 2.

Spearphishing uses fake emails with attachments or links used to attempt to trick an individual into providing credentials that are needed to login to a system.¹⁹⁶ The JAR states that throughout the spearphishing campaign, APT29 “used legitimate domains, to include domains associated with U.S. organizations and educational institutions, to host malware and send spearphishing emails.”¹⁹⁷ Once APT29 gained access to the system, it was able to steal credentials, hide its presence, analyze and gather intelligence information, and establish command and control.¹⁹⁸ APT29 continued to exfiltrate emails and other documents until its discovery in April of 2016.

On April 18, 2016, Fancy Bear (APT28) gained access to the DNC’s systems.¹⁹⁹ The JAR states that APT28 gained access using targeted spearphishing campaigns that “tricked recipients into changing their passwords through a fake webmail domain hosted on APT28 operational infrastructure.”²⁰⁰ CrowdStrike reports that Fancy Bear is a Russian actor that typically targets organizations of strategic interest to Russia and is believed to have ties to the Main Intelligence Department or GRU.²⁰¹ The JAR states that “APT28 was able to gain access and steal content, likely leading to the exfiltration of information from multiple senior party members,” information which was “leaked to the press and publicly disclosed.”²⁰² The DNC discovered the presence of unusual cyber activity on April 28, 2016, which led to the DNC calling in cybersecurity firm CrowdStrike to investigate.²⁰³ In a DNC lawsuit, it is revealed that the Russian hackers had access “not only to email systems, but also to backup servers, VOIP calls, and chats.”²⁰⁴ The damage cost the DNC over a million dollars and it “had to ‘decommission more than 140 servers,

¹⁹⁶ P. W. Singer, *Cybersecurity and Cyberwar: What Everyone Needs to Know* (Oxford ; New York: Oxford University Press, 2014), 298.

¹⁹⁷ Department of Homeland Security, GRIZZLY STEPPE—Russian Malicious Cyber Activity, 2–3.

¹⁹⁸ Ibid.

¹⁹⁹ Barrett, “DNC Lawsuit Against Russia Reveals New Details About 2016 Hack.”

²⁰⁰ Department of Homeland Security, GRIZZLY STEPPE—Russian Malicious Cyber Activity, 3.

²⁰¹ Alperovitch, “Bears in the Midst.”

²⁰² Department of Homeland Security, GRIZZLY STEPPE—Russian Malicious Cyber Activity, 3.

²⁰³ Barrett, “DNC Lawsuit Against Russia Reveals New Details About 2016 Hack.”

²⁰⁴ Ibid.

remove and reinstall all software, including the operating systems, for more than 180 computers, and rebuild at least 11 servers.’”²⁰⁵

Barret reports that on June 14, 2016, the DNC publically disclosed that it had been hacked and “the following day, persona going by Guccifer 2.0 ... claimed responsibility, leaking a 237-page opposition research report on Donald Trump in the process.”²⁰⁶ Starting in June, “Guccifer 2.0” gave 20,000 emails and reports to WikiLeaks as a way of interfering with the election.²⁰⁷ It was believed that Guccifer 2.0 was actually a Russian agent, and on October 7, 2016, the Department of Homeland Security (DHS) released a statement that “the U.S. Intelligence Community (USIC) is confident that the Russian Government directed the recent compromise of e-mails from U.S. persons and institutions, including from U.S. political organizations [DNC].”²⁰⁸ Mai Schotz reports that Guccifer 2.0 was eventually traced to a Moscow IP address; U.S. investigators “traced it [the IP address] directly to the GRU headquarters.”²⁰⁹

While APT28 and APT29 were hacking the DNC to undermine the presidential election, the IRA was stepping up its social media presence to spread disinformation and sow discord.²¹⁰ The ICA reports that in March 2016, RT and Sputnik, which are Russia funded media outlets, began to express support for candidate Donald Trump.²¹¹ The ICA also finds that Russia, through the IRA, utilized trolls to “influence efforts to denigrate Secretary Clinton. This effort amplified stories on scandals about Secretary Clinton and the

²⁰⁵ Ibid.

²⁰⁶ Ibid.

²⁰⁷ Ibid.

²⁰⁸ “Joint Statement from the Department of Homeland Security and Office of the Director of National Intelligence on Election Security,” Department of Homeland Security, October 7, 2016, <https://www.dhs.gov/news/2016/10/07/joint-statement-department-homeland-security-and-office-director-national>.

²⁰⁹ Lily Hay Newman, “Guccifer 2.0’s Slip-Up Shows That Even Elite Hackers Make Mistakes,” *Wired*, March 25, 2018, <https://www.wired.com/story/guccifer-elite-hackers-mistakes/>.

²¹⁰ Director of National Intelligence, Background to “Assessing Russian Activities and Intentions in Recent U.S. Elections”: The Analytic Process and Cyber Incident Attribution.

²¹¹ Ibid., 3–4.

role of WikiLeaks in the election campaign.”²¹² The Senate Report found that, “often within the context of the election or in reference to a candidate, most IRA content discreetly messaged narratives of disunity, discontent, hopelessness, and contempt of others, all aimed at sowing societal division.”²¹³ The USIC estimates that over 100 million Americans were reached through Russian social media influence campaigns.²¹⁴

4. Findings and Implications

Russia’s strategic attempt to disrupt U.S. Democratic processes poses serious concern for foreign influence within Western states and domestic affairs. Russian actions to directly interfere in the democratic election process via cyber intrusions as well as influencing the population through social media demonstrated the antithesis of the defined stance on “non-interference in domestic affairs of States” as stated in its Foreign Policy Concept.²¹⁵ The ICA concludes that “President Putin ordered an influence campaign in 2016 aimed at the U.S. presidential election.”²¹⁶ Additionally, “Moscow’s influence campaign followed a Russian messaging strategy that blends covert intelligence operations—such as cyber activity—with overt efforts by Russian Government agencies, state-funded media, third-party intermediaries, and paid social media users or ‘trolls.’”²¹⁷ Although President Putin continues to deny that Russia had any involvement in election interference, evidence affirms that Russia intentionally meddled in the Democratic electoral process on an unprecedented scale.²¹⁸ Central to this case, CrowdStrike revealed

²¹² Ibid.

²¹³ Select Committee on Intelligence, Russian Active Measures Campaigns and Interference in the 2016 U.S. Election Volume 2: Russia’s Use of Social Media with Additional Views, 32.

²¹⁴ “Exposing Russia’s Effort to Sow Discord Online: The Internet Research Agency and Advertisements | Permanent Select Committee on Intelligence,” accessed October 28, 2019, <https://intelligence.house.gov/social-media-content/>.

²¹⁵ Ibid.

²¹⁶ Director of National Intelligence, Background to “Assessing Russian Activities and Intentions in Recent U.S. Elections”: The Analytic Process and Cyber Incident Attribution, ii.

²¹⁷ Ibid., ii.

²¹⁸ Gary Pruitt, “Putin Claims Russia Hasn’t Meddled in U.S. Elections, despite Evidence of Influence Campaign,” PBS NewsHour, June 6, 2019, <https://www.pbs.org/newshour/world/putin-claims-russia-hasnt-meddled-in-u-s-elections-despite-evidence-of-influence-campaign>.

that APT28 and APT29, respectively, had ties to the GRU and SVR but were operating independently of each other to achieve the same goal of stealing election information for public release, actions which potentially lead to their intrusion being discovered.²¹⁹

Widespread use of social media by Americans made it easier for Russia to target the general population. This expansive approach made it easier for Russia to spread propaganda directed at different populations in order to target societal division and weaken the United States domestically. Russia's ability to sow discord through the 2016 presidential election and beyond has led to a more divisive U.S. population. The ICA report concludes that Russia will take the lessons learned from the United States and apply them "to future influence efforts worldwide, including against U.S. allies and their election processes."²²⁰ Specifically, the findings indicate that social media information has the potential to impact voter's decision making processes. As a result, it is plausible that misinformation campaigns, as an emerging warfare tactic, should be considered with countermeasures to minimize potential threats to democratic processes.

Political cohesion is critical for the security and strength of NATO and each state needs to be able to respond to a crisis with effectiveness and speed. Russia's ability to divide individual states of NATO affirms the potential for current and future negative impacts on the Alliance. Past actions demonstrate Russia's intentional use of grand strategy to weaken individual states with the potential to weaken the organization itself. Domestic issues could potentially divert states from recognizing an impending threat to the NATO Alliance from Russia, and this places Russia in a strategically advantageous position. Russian interference in the U.S. presidential election was directed specifically at the United States and through this disruption had the potential to affect the NATO Alliance by weakening a member state domestically. This interference allowed Russia to test the limits

²¹⁹ Alperovitch, "Bears in the Midst."

²²⁰ Director of National Intelligence, Background to "Assessing Russian Activities and Intentions in Recent U.S. Elections": The Analytic Process and Cyber Incident Attribution, iii.

of accepted behavior by a state within the cyberspace domain in order to determine the response level from an adversary state.²²¹

B. 2017 FRENCH PRESIDENTIAL ELECTION

1. Overview

Due to reported Russian interference in the 2016 U.S. presidential election, the National Cybersecurity Agency of France (ANSSI) took proactive actions in preparation to protect France's presidential candidates and deter against possible cyber intrusions aiming to disrupt their campaigns.²²² In spite of measures implemented by French authorities, the candidates contend that cyber actors immediately initiated attacks on presidential candidates' systems in October 2016. The purpose of the attacks focused on finding and stealing information to strengthen and guide disinformation campaigns.²²³ This information was circulated in the media as well as through social media.²²⁴ Cyberattacks persisted through the winter of 2017, leading to presidential candidate Emmanuel Macron's campaign being plagued with leaked emails and other information prior to the election in May 2017.²²⁵ Despite the continued Russian interference into Emmanuel Macron's campaign he was elected president.²²⁶

²²¹ NATO CCDCOE, "DNC Hack: An Escalation That Cannot Be Ignored," Defence IQ, August 11, 2016, <https://www.defenceiq.com/cyber-defence-and-security/articles/dnc-hack-an-escalation-that-cannot-be-ignored>.

²²² Erik Brattberg and Tim Maurer, "Russian Election Interference: Europe's Counter to Fake News and Cyber Attacks," Carnegie Endowment for International Peace, May 2018, 8, <https://carnegieendowment.org/2018/05/23/russian-election-interference-europe-s-counter-to-fake-news-and-cyber-attacks-pub-76435>.

²²³ Brattberg and Maurer, 9; Jean-Baptiste Jeangène Vilmer, "The 'Macron Leaks' Operation: A Post-Mortem" (Washington, DC: Atlantic Council, June 20, 2019), 10, https://www.atlanticcouncil.org/wp-content/uploads/2019/06/The_Macron_Leaks_Operation-A_Post-Mortem.pdf.

²²⁴ Vilmer, "The 'Macron Leaks' Operation: A Post-Mortem," 4–7.

²²⁵ Brattberg and Maurer, "Russian Election Interference."

²²⁶ Heather Conley, "Successfully Countering Russian Electoral Interference," Center for Strategic & International Studies, June 21, 2018, <https://www.csis.org/analysis/successfully-countering-russian-electoral-interference>.

2. Contextual Analysis

An essential element of the 2017 French presidential election is the level of preparation that France developed and implemented to defend against anticipated undue foreign influence. French officials analyzed the lessons learned from the 2016 U.S. presidential election to create a plan to mitigate any influence in France's election.²²⁷ The lessons learned from the U.S. presidential election provided preemptive strategies which the French authorities utilized to minimize potential cyber threats to the campaigns by a foreign entity.

Christopher Chivvis represented the RAND Corporation and gave testimony to the U.S. House of Representatives on March 22, 2017, in regard to Russian hybrid warfare, and gray zone tactics to influence foreign states.²²⁸ Chivvis highlighted Russia's ability to use gray zone tactics through information operations as well as cyber operations in order to "ensure that political outcomes in targeted countries serve Russia's national interests."²²⁹ Chivvis predicted that, due to Emmanuel Macron's stance against Russia and his opponents' pro-Russian stances, that Russia may very well attempt to undermine his election campaign.²³⁰

Jean-Baptiste Jeangène Vilmer argues that "Moscow considers its actions to be defensive" due to the view that Russia is "the victim of an information war waged by the West."²³¹ Vilmer continues, arguing that even though Russian actors are believed to be behind this interference, it is important to note that strategically it was an operational failure because "the result of the election did not coincide with the aim of the attackers."²³²

²²⁷ Conley.

²²⁸ Christopher Chivvis, *Understanding Russian "Hybrid Warfare": And What Can Be Done About It* (RAND Corporation, 2017), 1, <https://doi.org/10.7249/CT468>.

²²⁹ Chivvis, 3.

²³⁰ Chivvis, 5.

²³¹ Vilmer, "The 'Macron Leaks' Operation: A Post-Mortem," 1.

²³² *Ibid.*, 2.

3. Event Timeline

Emmanuel Macron's cybersecurity team reported that they began to experience phishing attacks as early as December 2016.²³³ Vilmer reported that the campaign experienced email spoofing. This type of attack introduces an email address looks identical to a sender's but in this case was missing one letter, containing documents that would steal credentials from campaign staff to gain access to the systems.²³⁴ Erik Brattberg and Tim Maurer report that in February 2017, Jean-Marc Ayrault, who was the French Foreign Minister at the time, told Moscow that Paris would not tolerate any interference in the election.²³⁵ This statement was made due to the repeated cyberattacks that Macron's campaign was experiencing.

While Macron's staff was focused on combating cyber intrusions, they were also fighting off a disinformation campaign lead by Russian media. Vilmer reports that from January 2017 until the election date, Macron faced media rumors and lies meant to degrade him as a candidate.²³⁶ He also notes that around January is when Macron began to become a front runner in the election cycle. Vilmer highlights RT and Sputnik as the leading media outlets publishing false information against Macron and his campaign.²³⁷ Sputnik would cleverly manipulate information to provide a false idea about Macron in order to discredit him, but would report it in a way that allowed the organization to avoid punishment for reporting "fake news."²³⁸ On April 27, 2017, the Macron campaign banned Sputnik and RT from attending any more of its events due to the disinformation and continued lies the two organizations perpetuated.²³⁹

²³³ Christopher Dickey, "Fighting Back Against Putin's Hackers," *The Daily Beast*, April 25, 2017, <https://www.thedailybeast.com/articles/2017/04/25/fighting-back-against-putin-s-hackers>.

²³⁴ Vilmer, "The 'Macron Leaks' Operation: A Post-Mortem," 11.

²³⁵ Brattberg and Maurer, "Russian Election Interference," 9.

²³⁶ Vilmer, "The 'Macron Leaks' Operation: A Post-Mortem," 4.

²³⁷ Ibid.

²³⁸ Vilmer, "The 'Macron Leaks' Operation: A Post-Mortem," 5.

²³⁹ Conley, "Successfully Countering Russian Electoral Interference."

Trend Micro released a report examining the cyber actions of Pawn Storm or APT28 which was one of the hacker groups responsible for the DNC hack in 2016.²⁴⁰ Within this report is a list of organizations targeted by APT28, and on March 15, 2017, Macron's campaign was a target of a phishing campaign.²⁴¹ Following this report, Macron's campaign reported that several thousand attempts had been made to hack and disrupt the campaign.²⁴² Russia is known to favor pro-Russian candidates such as Marine Le Pen, Macron's opposition for election, and Russia, in 2014, loaned €9.4 million to her political party.²⁴³ French officials have not directly attributed blame to Russia for the APT28 phishing campaigns but they do believe the attacks were in line with Russian interests.²⁴⁴ The United States has been more outspoken with the NSA attributing blame to Russia for interfering in the French election.²⁴⁵

Emmanuel Macron's strategic responses continued to combat the misinformation campaign against him routinely until election day on May 7, 2017. Erik Brattberg and Tim Mauer reported that on May 5, 2017, the hackers dumped over "9 gigabytes of stolen files and 21,000 emails were uploaded to the platform Pastebin."²⁴⁶ The leak had a mix of real and forged email documents meant to discredit Macron.²⁴⁷ French law delineates that no campaign communications will be allowed 44 hours before French presidential election voting and that the media also cannot comment on the poll during this time.²⁴⁸ This law is the reason the hackers, who had gained the materials in March, waited until just before the

²⁴⁰ Hacquebord, "Two Years of Pawn Storm Examining an Increasingly Relevant Threat."

²⁴¹ Ibid., 13.

²⁴² Vilmer, "The 'Macron Leaks' Operation: A Post-Mortem," 20.

²⁴³ Brattberg and Maurer, "Russian Election Interference," 11; Vilmer, "The 'Macron Leaks' Operation: A Post-Mortem," 24.

²⁴⁴ Vilmer, "The 'Macron Leaks' Operation: A Post-Mortem," 23.

²⁴⁵ Andy Greenberg, "NSA Director Confirms That Russia Really Did Hack the French Election," *Wired*, May 9, 2017, <https://www.wired.com/2017/05/nsa-director-confirms-russia-hacked-french-election-infrastructure/>.

²⁴⁶ Brattberg and Maurer, "Russian Election Interference," 10.

²⁴⁷ Conley, "Successfully Countering Russian Electoral Interference."

²⁴⁸ "French Media Rules Prohibit Election Coverage over Weekend," *France 24*, May 6, 2017, <https://www.france24.com/en/20170506-france-media-rules-prohibit-election-coverage-over-weekend-presidential-poll>.

voting began so as to prevent Macron from refuting any allegations.²⁴⁹ This leak circulated on Twitter under “#MacronLeaks” where certain political groups and bot accounts helped it spread first in the United States and then internationally, but the French people reported a stronger trust of conventional media outlets rather than social media, especially English speaking, and therefore the leak struggled to gain traction within France.²⁵⁰

4. Findings and Implications

The Macron campaign quickly responded to both media disinformation campaigns and cyberattacks and, as a result, was able to minimize potential negative outcomes to the election. Macron’s team was transparent about the attacks and raised awareness to the issue while working diligently to respond to disinformation in the media.²⁵¹ Russia ran into several issues in its attempts to interfere in the election. Vilmer states that Macron was not expected to become a front runner in the election and he ended up winning the presidential race even which left the hackers unprepared to prevent him from gaining success.²⁵² He continues, stating that, because of this, it left hackers little time to dig up information meant to harm Macron’s electability. This led to them forging documents to be released in May in a futile effort to hurt Macron’s position.²⁵³ Macron’s campaign addressed the leaks stating that there were, “numerous false documents intended to sow doubt and disinformation.”²⁵⁴

France took an active role to mitigate any interference in the election, and this made it more difficult for Russian actors to carry out a successful operation. France had the opportunity to learn from the mistakes made during the U.S. election interference which

²⁴⁹ Conley, “Successfully Countering Russian Electoral Interference.”

²⁵⁰ Vilmer, “The ‘Macron Leaks’ Operation: A Post-Mortem,” 12–14; Conley, “Successfully Countering Russian Electoral Interference.”

²⁵¹ Conley, “Successfully Countering Russian Electoral Interference.”

²⁵² Vilmer, “The ‘Macron Leaks’ Operation: A Post-Mortem,” 28.

²⁵³ Ibid.

²⁵⁴ Andy Greenberg, “Hackers Hit Macron with Huge Email Leak Ahead of French Election,” *Wired*, May 5, 2017, <https://www.wired.com/2017/05/macron-email-hack-french-election/>.

allowed the French government to prepare differently.²⁵⁵ Russian interference attempted a “hack and leak” disinformation campaign to undermine Macron but it was not successful because the hackers did not understand the French culture and attempted to spread rumors about Macron’s sexuality and private life which is not scandalous to the French.²⁵⁶ NATO member states worked together to prevent interference in the election, with the United States warning French officials about Russian threat actors attempting to access their election infrastructure as well as German officials sharing data information with France.²⁵⁷ The French government used the ANSSI to maintain the integrity of the election as well as for coordination with individual campaigns to alert them of potential security risks and measures to mitigate those risks.²⁵⁸ Close cooperation as well as French anticipation of interference helped prepare the candidates to defend against Russian influence in the election cycle.²⁵⁹ This cooperation demonstrates the importance of NATO states working together to defend against Russian threats, and against Russian influence meant to divide a state to create a domestic political position favorable to Russia. Additionally, the proactive cyber deception plans, such as creating fake documents to delegitimize the hackers when they get released, created and implemented by campaign specialists demonstrated cyberattacks could be minimized and transparent communications strengthened the democratic processes in the presidential election.²⁶⁰

C. DRAGONFLY CAMPAIGNS

1. Overview

Cybersecurity firm Symantec discovered that Dragonfly, also known as Energetic Bear, in February 2013 began conducting cyber operations within the energy sector in

²⁵⁵ Vilmer, “The ‘Macron Leaks’ Operation: A Post-Mortem,” 29–30.

²⁵⁶ Ibid., 29.

²⁵⁷ “Cyber Command Chief Says U.S. Warned France About Russia-Backed Hackers During Election,” RadioFreeEurope/RadioLiberty, May 9, 2017, <https://www.rferl.org/a/us-warned-france-russian-hacking/28476837.html>.

²⁵⁸ Vilmer, “The ‘Macron Leaks’ Operation: A Post-Mortem,” 31–32.

²⁵⁹ Conley, “Successfully Countering Russian Electoral Interference.”

²⁶⁰ Vlmer, “The ‘Macron Leaks’ Operation: A Post-Mortem,” 34.

several NATO states as well as industrial control systems (ICS) equipment providers.²⁶¹ This operation continued into 2014, which is when Symantec discovered the cyber intrusions and published the initial report. Symantec states that during this operation, Dragonfly “managed to compromise a number of strategically important organizations for spying purposes.”²⁶² In December 2015, “Dragonfly 2.0” began using similar tactics as seen in the first Dragonfly operation.²⁶³ However, this time the group focused on learning and gaining control of systems, for reconnaissance purposes, to disrupt or sabotage the energy sector if necessary.²⁶⁴ This cyber activity, within the critical infrastructure of the energy sector, continued into 2017, specifically targeting a small group of NATO members and partner states.²⁶⁵ On March 15, 2018, the Cybersecurity and Infrastructure Security Agency (CISA) released an alert attributing blame on Russian government cyber actors for hacking into the energy sector networks of the United States as a part of the Dragonfly 2.0 campaign.²⁶⁶

2. Contextual Analysis

Disruption of the energy sector could be classified as an imminent threat to reduce NATO’s resiliency and civil preparedness and potentially hinder the Alliance’s response in a crisis. Reliance and technology depend heavily on power provided from the energy sector. NATO resiliency is crucial for the Alliance and partner states for “strengthening the

²⁶¹ A Johnson, “Endpoint Protection—Symantec Enterprise,” June 30, 2014, <https://community.broadcom.com/symantecenterprise/communities/community-home/librarydocuments/viewdocument?DocumentKey=7382dce7-0260-4782-84cc-890971ed3f17&CommunityKey=1ecf5f55-9545-44d6-b0f4-4e4a7f5f5e68&tab=librarydocuments>.

²⁶² Ibid.

²⁶³ Security Response Attack Investigation Team, “Dragonfly: Western Energy Sector Targeted by Sophisticated Attack Group,” Symantec Blogs, October 20, 2017, <https://www.symantec.com/blogs/threat-intelligence/dragonfly-energy-sector-cyber-attacks>.

²⁶⁴ Ibid.

²⁶⁵ Ibid.

²⁶⁶ CISA, “Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors,” March 16, 2018, <https://www.us-cert.gov/ncas/alerts/TA18-074A>.

Alliance's deterrence and defence posture.”²⁶⁷ NATO's ability to swiftly respond to a crisis hinges on individual states' ability to be able to defend against or mitigate the effects of a cyberattack against critical infrastructure. Jens Stoltenberg, the Secretary General of NATO stated: “A serious cyberattack could trigger Article 5, where an attack against one ally is treated as an attack against all.”²⁶⁸ NATO's stance on cyberattacks demonstrates the importance of understanding the effect a large scale attack against a state's critical infrastructure has on the Alliance.

3. Event Timeline

Symantec reports that the Dragonfly operation began in February 2013 via a spear phishing campaign that targeted senior employees within energy sector companies.²⁶⁹ Symantec continues, stating that Dragonfly targeted seven different organizations from February to June 2013 with this spear phishing campaign. Symantec states that Spain, U.S., France, Italy, Germany, Turkey, Poland, Romania, Greece, and Serbia, ordered from most malicious activities to least, were the countries with active malicious infections, meaning they were the most likely targets of the campaign.²⁷⁰ Dragonfly managed to infect other systems through compromising three ICS equipment providers.²⁷¹ This compromise allowed Dragonfly to insert malware into software packages that were available for download directly from these ICS providers' websites for customers.

Cybersecurity experts believe that Dragonfly was “interested in both learning how energy facilities operate and also gaining access to operational systems themselves.”²⁷²

²⁶⁷ Wolf-Diether Roepke and Hasit Thankey, “Resilience: The First Line of Defence,” NATO Review, February 27, 2019, <https://www.nato.int/docu/review/articles/2019/02/27/resilience-the-first-line-of-defence/index.html>.

²⁶⁸ Jens Stoltenberg, “NATO Will Defend Itself (Article by NATO Secretary General Jens Stoltenberg Published in Prospect),” NATO, August 29, 2019, http://www.nato.int/cps/en/natohq/news_168435.htm.

²⁶⁹ Johnson, “Endpoint Protection—Symantec Enterprise.”

²⁷⁰ Ibid.; Symantec Security Response, “Dragonfly: Cyberespionage Attacks Against Energy Suppliers,” Security Response (Symantec, July 7, 2014).

²⁷¹ Johnson, “Endpoint Protection—Symantec Enterprise.”

²⁷² Security Response Attack Investigation Team, “Dragonfly: Western Energy Sector Targeted by Sophisticated Attack Group.”

Symantec’s report further endorses this view by gathering data on targeted companies from September 2013 until June 2014.²⁷³ This data indicates that “fifty percent of identified targets were energy industry related and thirty percent were energy control system,” with a shift to prioritizing targeting energy control systems in March 2014. When Dragonfly was discovered, experts did not know whom to attribute blame to; however, upon examining the time stamps associated to the hacker’s malware, it was discovered that they worked Monday-Friday from 9am to 6pm in the UTC +4 time zone.²⁷⁴ During the dates that the Dragonfly operation took place, Moscow was in the UTC +4 time zone before it permanently switched to UTC +3 in October 2014.²⁷⁵

Dragonfly focused on gathering data and intelligence about how these energy companies operated in order to potentially plan for future attacks. Dragonfly reportedly refrained from operations again until the Dragonfly 2.0 campaign, which emerged in December 2015 and targeted the energy sectors within Turkey, the United States, and Switzerland.²⁷⁶ Dragonfly 2.0 used phishing emails, similar to the first operation, from December 2015 into 2017, targeting energy sectors. Rebecca Smith reports that Jonathan Homer, chief of ICS analysis for DHS, explained that the hackers exploited vendors to gain access into utility networks.²⁷⁷ Homer stated that the hackers studied network configuration, equipment use and control, and became familiar with facility operations in order to cause disruptions if necessary. He noted that the goal of these hackers was “to disguise themselves as ‘the people who touch these systems on a daily basis’” in order to avoid detection.²⁷⁸ Experts at Symantec concur with this belief and conclude that “the Dragonfly 2.0 campaigns show how the attackers may be entering into a new phase, with

²⁷³ Symantec Security Response, “Dragonfly: Cyberespionage Attacks Against Energy Suppliers,” 7.

²⁷⁴ Ibid.

²⁷⁵ “Time Zone & Clock Changes 2010–2019 in Moscow, Russia,” accessed April 16, 2020, <https://www.timeanddate.com/time/zone/russia/moscow?year=2014>.

²⁷⁶ Security Response Attack Investigation Team, “Dragonfly: Western Energy Sector Targeted by Sophisticated Attack Group.”

²⁷⁷ Rebecca Smith, “Russian Hackers Reach U.S. Utility Control Rooms, Homeland Security Officials Say—WSJ,” July 23, 2018, <https://www.wsj.com/articles/russian-hackers-reach-u-s-utility-control-rooms-homeland-security-officials-say-1532388110?redirect=amp>.

²⁷⁸ Ibid.

recent campaigns potentially providing them with access to operational systems, access that could be used for more disruptive purposes in future.”²⁷⁹

In March 2018, the United States formally blamed Russia for what DHS and FBI called, a “multi-stage intrusion campaign” targeting ICS and critical energy sectors.²⁸⁰ In the JAR published after the 2016 U.S. presidential election Dragonfly and Energetic Bear were both listed as “Reported Russian Military and Civilian Intelligence Services.”²⁸¹ Experts surmised that Dragonfly 2.0 may have had a destructive intent but they affirm the hackers did not disrupt any energy operations.²⁸² Homer stated, “‘they [Dragonfly 2.0] got to the point where they could have thrown switches’ and disrupted power flows.”²⁸³

4. Findings and Implications

This case affirms that Russian cyber actors accessed systems, conducted reconnaissance, and demonstrated the potential to disrupt the flow of energy and electrical power while avoiding detection for an extended period of time. Private sector security companies were the first to report on the cyber intrusions into the victim organizations systems. The scope and technical ability of Russian cyber hackers to target weaker links as well as software vendors in order to gain further access into victims’ systems displays the high level of skill of the Dragonfly threat actors. In this case, the hackers did not disrupt the flow of power, but they did have the ability to disrupt the power flows, thus potentially causing chaos within the target states. These hackers are versatile and well-sourced, a scenario which affirms NATO’s shift toward better cyber defense and deterrence measures.

²⁷⁹ Security Response Attack Investigation Team, “Dragonfly: Western Energy Sector Targeted by Sophisticated Attack Group.”

²⁸⁰ CISA, “Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors.”

²⁸¹ Department of Homeland Security, GRIZZLY STEPPE—Russian Malicious Cyber Activity, 4.

²⁸² Pierluigi Paganini, “Dragonfly 2.0: The Sophisticated Attack Group Is Back with Destructive Purposes,” Security Affairs, September 7, 2017, <https://securityaffairs.co/wordpress/62782/hacking/dragonfly-2-0-campaigns.html>.

²⁸³ Smith, “Russian Hackers Reach U.S. Utility Control Rooms, Homeland Security Officials Say—WSJ.”

Additionally, the case reveals the direct correlation to the increase in technological capabilities of NATO states and subsequent increase in potential technological weaknesses that can be exploited by an adversary in cyberspace. With this in mind, NATO, since 2016, has steadily increased its focus and deterrence capabilities in the cyber domain. In July 2016, NATO published the “Cyber Defence Pledge” which prioritized enhancing national infrastructures and networks to create a strong and resilient cyber system.²⁸⁴ The Brussels Summit in 2018 reaffirmed this pledge, stating the continual efforts to increase cyber resilience are crucial to increasing the strength of the Alliance and member states.²⁸⁵ Cyber deterrence is a fundamental shift within NATO to include the cyber domain into the collective defense domain. The full effects of a cyberattack against energy and critical infrastructure operations have not been demonstrated against a NATO member but experts fear it could have detrimental consequences if NATO is not prepared to defend against such an attack.²⁸⁶

D. NOTPETYA

1. Overview

On June 27, 2017, state cyber actors targeted systems within Ukraine in order to destroy critical infrastructure areas with the NotPetya cyberattack.²⁸⁷ Banks, airports, and energy firms were central in the conflict of the Ukrainian target industries.²⁸⁸ The cyberattack used malware that had a rapid and destructive impact while spreading from system to system indiscriminately.²⁸⁹ Less than eight months after the attack, blame was

²⁸⁴ NATO, “Cyber Defence Pledge,” NATO, July 8, 2016, http://www.nato.int/cps/en/natohq/official_texts_133177.htm.

²⁸⁵ NATO, “Brussels Summit Declaration Issued by the Heads of State and Government Participating in the Meeting of the North Atlantic Council in Brussels, 11–12 July 2018,” NATO, July 11, 2018, http://www.nato.int/cps/en/natohq/official_texts_156624.htm.

²⁸⁶ John Allen et al., “Future War NATO? From Hybrid War to Hyper War via Cyber War,” GLOBSEC, November 2017, <https://www.globsec.org/publications/future-war-nato-hybrid-war-hyper-war-via-cyber-war/>.

²⁸⁷ Greenberg, “The Untold Story of NotPetya, the Most Devastating Cyberattack in History.”

²⁸⁸ Andy Greenberg, “Ukrainians Say Petya Ransomware Hides State-Sponsored Attacks,” *Wired*, June 28, 2017, <https://www.wired.com/story/petya-ransomware-ukraine/>.

²⁸⁹ Greenberg, “The Untold Story of NotPetya, the Most Devastating Cyberattack in History.”

attributed to the Russian military for the devastating and most costly cyberattack in history.²⁹⁰ NotPetya spread rapidly within Ukraine and then indiscriminately outside of Ukraine, initially targeting companies that held an office inside Ukrainian borders.²⁹¹ This attack slowed the global operations of companies inside and outside of Ukraine for months and placed increased strain and concern on critical infrastructure within NATO states while creating an estimated \$10 billion in damage.²⁹²

2. Contextual Analysis

NotPetya is an unprecedented case with global implications due to its relevance to the critical infrastructure security of NATO states. While NotPetya was a result of the undeclared war between Ukraine and Russia, neither of which is a NATO member, the attack did widespread collateral damage to NATO member states.²⁹³ This case study reveals the major threat that cyberattacks pose to a globalized and interconnected world. The effects of the attack were evidenced for months after the initial strike and reinforced to NATO the need for increased strength and resiliency in the face of a cyberattack. Russian cyber actors have been undertaking critical infrastructure cyberattacks in Ukraine for years, and the processes used by the hackers are becoming more efficient and stealthy.²⁹⁴ Experts contend that Russia's expansion of its grand strategy included focused and purposeful cyberattacks on Ukraine to implement enhanced tactics and test retaliation strategies.²⁹⁵

3. Event Timeline

Cisco's Talos intelligence group investigated the Ukrainian attack and reported that the cyber actor behind NotPetya was able to gain access to victim companies' servers through a "watering hole" attack using M.E.Doc, which is identified as a Ukrainian tax

²⁹⁰ White House, "Statement from the Press Secretary," February 15, 2018, <https://www.whitehouse.gov/briefings-statements/statement-press-secretary-25/>.

²⁹¹ Greenberg, "The Untold Story of NotPetya, the Most Devastating Cyberattack in History."

²⁹² Ibid.

²⁹³ Ibid.

²⁹⁴ Andy Greenberg, "How an Entire Nation Became Russia's Test Lab for Cyberwar," *Wired*, June 20, 2017, <https://www.wired.com/story/russian-hackers-attack-ukraine/>.

²⁹⁵ Ibid.

accounting software provider.²⁹⁶ Talos revealed that the attack introduced malware with the intent to destroy systems and the malware was camouflaged to look like a ransomware attack. Talos uncovered that over 2,000 companies were affected in Ukraine. The specific timeline establishes that the attackers began uploading a backdoor containing the malware to the victims on April 14, 2017, via M.E.Doc software updates. The upload was made possible due to the early access into M.E.Doc's software and the software updates were released with backdoors built into the code again on May 15 and June 22; this lead up to the June 27 attack.

The cyber actors gained access to the target systems months before they unleashed the malware on them which was one day before Ukraine's constitution day, June 28.²⁹⁷ Ukrainian officials believed the attack was "more likely state-sponsored" due to the timing coupled with the ongoing conflict with Russia.²⁹⁸ Within hours of NotPetya's release, the malware spread all around Ukraine and then struck global companies such as Maersk, Merck Pharmaceuticals, and TNT Express (which had just been bought by FedEx).²⁹⁹ The malware was able to spread to these companies because they each had at least one computer with M.E.Doc software on it, and this enabled the malware to then target each company's systems in a rapid and destructive manner.³⁰⁰ The damage incurred by NotPetya was an estimated cost of \$10 billion, making it the most costly cyberattack in history.³⁰¹

Andy Greenberg reported on the effects different companies and government entities experienced as a result of the NotPetya malware attack.³⁰² He notes that at least four hospitals, two airports, six power companies, 22 banks, credit card systems, transportation systems, and almost every federal agency were crucially impacted by the

²⁹⁶ David Maynor et al., "The MeDoc Connection," July 5, 2017, <http://blog.talosintelligence.com/2017/07/the-medoc-connection.html>.

²⁹⁷ Greenberg, "Ukrainians Say Petya Ransomware Hides State-Sponsored Attacks."

²⁹⁸ Ibid.

²⁹⁹ Greenberg, "The Untold Story of NotPetya, the Most Devastating Cyberattack in History."

³⁰⁰ Ibid.

³⁰¹ Ibid.

³⁰² Ibid.

attack. Greenberg quotes Volodymyr Omelyan, Ukrainian minister of infrastructure, who said “the government was dead” and that NotPetya “was a massive bombing of all our systems.”³⁰³ This was not the first time that the Ukrainian power grid had been compromised by hackers; Greenberg reports that Sandworm, a Russian GRU cyber hacking group, had done so in 2015 and 2016.³⁰⁴ For companies based outside of Ukraine this sentiment echoed true as well. Greenberg reports that Denmark-based Maersk shipping had 17 shipping terminals located all around the world and ceased operations for days due to the collapse of its systems.³⁰⁵ Further, he states that globalized transportation experienced a significant loss, noting how Maersk had to rebuild 4,000 servers and 45,000 computers and lost \$300 million due to the attack. NotPetya resulted in Merck pharmaceutical operational closures, specific to vaccine manufacturing, for several months after the attack.³⁰⁶ European package shipping company TNT Express did not fully recover from the cyberattack until September 2017.³⁰⁷ This attack required the implementation of an antiquated package system to organize orders and deliveries via pen and paper. The loss of online systems to manage distribution resulted in lost or delayed packages being sent all around Europe.³⁰⁸

Greenberg reports that one week after NotPetya Ukrainian officials seized all of M.E.Doc’s servers in order to prevent any further malware spread and to allow experts to examine them in order to analyze how the hackers carried out the attack.³⁰⁹ On June 30, 2017, NATO’s Cooperative Cyber Defense Center of Excellence (CCDCOE) released a

³⁰³ Greenberg, “The Untold Story of NotPetya, the Most Devastating Cyberattack in History.”

³⁰⁴ Andy Greenberg, “A Brief Tour of Russia’s Infrastructure Hacking Teams,” *Wired*, July 12, 2017, <https://www.wired.com/story/russian-hacking-teams-infrastructure/>.

³⁰⁵ *Ibid.*

³⁰⁶ Paul Roberts, “NotPetya Infection Left Merck Short of Key HPV Vaccine,” *The Security Ledger*, October 27, 2017, <https://securityledger.com/2017/10/notpetya-infection-left-merck-short-key-vaccine-gardasil/>.

³⁰⁷ “Cyber-Attack Cost TNT at Least \$300m,” *BBC News*, September 20, 2017, <https://www.bbc.com/news/technology-41336086>.

³⁰⁸ Miles Brignall, “TNT Parcels ‘backed up to Ceiling’ in Wake of Massive Cyberattack,” *The Guardian*, July 25, 2017, <https://www.theguardian.com/money/2017/jul/25/tnt-parcels-cyber-attack-courier-fedex-notpetya>.

³⁰⁹ Greenberg, “The Untold Story of NotPetya, the Most Devastating Cyberattack in History.”

statement stating that NotPetya “can most likely be attributed to a state actor.”³¹⁰ In February 2018, the United States officially blamed Russia for NotPetya stating, “it was part of the Kremlin’s ongoing effort to destabilize Ukraine and demonstrates ever more clearly Russia’s involvement in the ongoing conflict. This was also a reckless and indiscriminate cyberattack that will be met with international consequences.”³¹¹

4. Findings and Implications

The NotPetya cyberattack had a cascading global effect. The malware impacted healthcare, logistics, energy, banking, and several other critical infrastructure sectors. This attack displayed the drawback of globalized and interconnected systems. The attack was meant to target Ukraine but rapidly spread, affecting 65 countries, including several NATO member states as well as partner states.³¹² NotPetya allowed Russia to implement new cyber tactics against a real-time adversary without real repercussions due to its ongoing conflict with Ukraine. Although all impacted states were not identified as direct targets, the affected states are considered “collateral damage” which establishes the expansive reach of a targeted cyberattack. NotPetya was reckless and displayed a state actor that disregards the established norms of cyberspace.

NotPetya disrupted critical infrastructure operations such as healthcare, logistics, and energy within NATO states. The relative ease in which the malware infected so many different sectors revealed a weakness within state’s cybersecurity. NATO Allies should require organizations and companies to adequately prepare security and defense measures to prevent damage. Russia’s attack demonstrated the ability to shut down technology through cyber channels; NATO has a responsibility to prepare a collective defense to deter

³¹⁰ “CCDCOE,” accessed April 17, 2020, <https://ccdcoe.org/news/2017/notpetya-and-wannacry-call-for-a-joint-response-from-international-community/>; Luke Graham, “NATO Think-Tank Says a ‘state Actor’ Was behind the Massive Ransomware Attack and Could Trigger Military Response,” CNBC, June 30, 2017, <https://www.cnbc.com/2017/06/30/petya-ransomware-attack-nato-says-state-actor-to-blame.html>.

³¹¹ White House, “Statement from the Press Secretary.”

³¹² Graham, “NATO Think-Tank Says a ‘state Actor’ Was behind the Massive Ransomware Attack and Could Trigger Military Response.”

malware attacks from taking place within the borders of a member state.³¹³ NATO released statements concerning an Article 5 retaliation to a cyberattack but has yet to determine where the threshold for such an attack exists.³¹⁴ Russia has effectively carried out critical infrastructure cyber operations against Ukraine with relative ease. This case affirms that cyberattacks, within Russia's grand strategy, are purposeful to test, refine, and implement global attacks. Central to this finding is the need for NATO leaders to collaborate to identify potential threats, analyze previous malware, develop countermeasures for future attacks and establish training protocols for cyber specialists. Communication is essential to the ability of the Alliance to limit malware attacks and refine cyber systems to minimize attacks and maximize effectiveness.

E. CONCLUSION

Russian cyber operations, within these four case studies, demonstrate the evolution and scope of Russian grand strategy in the cyber domain. These studies affirmed Russia utilized information gained from previous operations and applied evolving tactics during subsequent operations. The Dragonfly operations demonstrated the ability for Russia to gather intelligence to develop an understanding for how the energy sector operates. Dragonfly presented a proof of concept, that critical infrastructure can be hacked via a cyber operation. The NotPetya cyberattack against Ukraine demonstrated the scope and damage that can be done to critical infrastructure via cyberattacks. NotPetya created \$10 billion in damage due to a cyberattack targeting one state.³¹⁵ The potential scope of damage caused by a cyberattack is not fully understood, but NotPetya demonstrated that there is a possibility for a stronger and more damaging cyberattack in the future.

In order to recognize the power of the gray zone, it is valuable to note the lessons that Russia learned through each case in regard to grand strategic goals. Influence operations have a high potential to create instability within a target state when executed

³¹³ NATO, "Warsaw Summit Communiqué—Issued by the Heads of State and Government Participating in the Meeting of the North Atlantic Council in Warsaw, 8–9 July 2016."

³¹⁴ Stoltenberg, "NATO Will Defend Itself (Article by NATO Secretary General Jens Stoltenberg Published in Prospect)."

³¹⁵ Greenberg, "The Untold Story of NotPetya, the Most Devastating Cyberattack in History."

effectively. Russia's attempts to influence American and French election outcomes were not as effective due to culture and language barriers.³¹⁶ Russia had the opportunity to carry out disinformation operations within two NATO members. While neither of these operations swayed the outcome of the election, Russia can build upon the failures in these cases to create more effective influence campaigns.

Russia's multiple election interference operations demonstrate the ability to destabilize specific NATO members in order to affect the Alliance as a whole. Destabilizing strong NATO members, domestically, has the ability to display a weakened NATO Alliance to the world. If member states are distracted by handling divisive domestic issues, as generated by election interference, the Alliance is left in a weakened position. The Alliance requires a cohesive response from all members and a unified posture is essential to display strength. If NATO appears weak to the international community, it creates an opportunity for Russia to gain a strategic position of power.

³¹⁶ Vilmer, "The 'Macron Leaks' Operation: A Post-Mortem," 29–30.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. COUNTERING RUSSIAN CYBER OPERATIONS

A. RESEARCH SUMMARY

The thesis evaluated four case studies to examine Russia's grand strategy and consequent impacts on the NATO Alliance. Specifically, the research investigated the question: what is the intersection between Russian cyber operations and grand strategy to weaken the NATO Alliance? The research conducted found that Russia's cyber operations within information operations and against critical infrastructure domains provided evidence of Russian grand strategy objectives. The findings of this thesis contend that analysis of the functional, fiscal, and political effects of cyber operations are essential to policy recommendations to minimize Russia's grand strategy outcomes. Russian grand strategy demonstrates strategic and long-term goals to weaken the Alliance. In contrast to date, the Alliance has, since 2016, begun to recognize cyber as a military domain and develop strategic plans to recognize and combat cyberattacks.³¹⁷ Additionally, the case studies require policy makers to compare and contrast defensive and offensive warfare tactics. The studies indicate that Russia did not seek to respond to NATO expansion through defensive actions but rather developed their grand strategy as an offensive warfare tactic to destabilize NATO and establish Russia as a formidable actor in cyber operations.

As this thesis established in Chapter II, Russia has demonstrated the ability to effectively use cyber operations to achieve grand strategy goals through political destabilization and critical infrastructure attacks in order to weaken a response from the NATO Alliance or member states. Russian operations to interfere in multiple presidential elections were carried out to destabilize NATO states and strengthen Russian influence. Attempts to get state leaders elected that Russia viewed as beneficial had the predetermined purpose to divide the NATO Alliance. Wirtz argues that, "Russia, more than any other nascent actor on the cyber stage, seems to have devised a way to integrate cyber warfare

³¹⁷ Laura Brent, "NATO's Role in Cyberspace," NATO Review, February 12, 2019, <https://www.nato.int/docu/review/articles/2019/02/12/natos-role-in-cyberspace/index.html>.

into a grand strategy capable of achieving political objectives.”³¹⁸ Geir Karlsen contends that Russia’s focus on creating instability within adversary states plays into its long term plan of weakening adversaries from within in order to project its own strength and rise to global power.³¹⁹ Russia has effectively operated within the gray zone by using asymmetric cyber operations that remained below the threshold for conflict. Russian strategy focuses on creating instability in order to weaken a state from within. Russian cyber operations implemented an array of cyber actors such as bots, trolls, and hacktivists in coordination with social media and news organizations to disseminate disinformation to large populations within targeted states. These interference operations are short-term focused with more immediate effects; however, they also work toward Russia’s long-term goal of disrupting the NATO Alliance in order to weaken it.

The scope of NotPetya displayed the capabilities that cyberattacks on critical infrastructure have and the widespread damage that can be inflicted with such an operation. After NotPetya, UN Secretary-General Antonio Guterres said, “The next war will begin with a massive cyberattack to destroy military capacity ... and paralyze basic infrastructure such as the electric networks.”³²⁰ The possibilities for cyber are still not fully developed and Russia is continually adapting its cyber operations, with experts Maness, Jensen, and Valeriano stating that, “Russia still has not unleashed the full potential of cyber operations against critical energy targets.”³²¹ NotPetya demonstrated the detrimental effects that cyberattacks on critical infrastructure create, effects such as widespread power outages, global logistical delays, healthcare shortages, and electronic banking collapses. Dragonfly also demonstrated the ability to infiltrate a power grid in order to gather intelligence about how it operates with the possibility to later carry out an attack that disables or destroys the energy and power sector. If cyber operations have not been utilized to their fullest potential

³¹⁸ Wirtz, “Cyber War and Strategic Culture: The Russian Integration of Cyber Power into Grand Strategy,” 31.

³¹⁹ Karlsen, “Divide and Rule,” February 8, 2019.

³²⁰ “UN Chief Calls for Regulatory Scheme for Cyberwarfare,” RadioFreeEurope/RadioLiberty, February 19, 2018, <https://www.rferl.org/a/un-guterres-calls-for-cyberwarfare-rules/29049069.html>.

³²¹ Brandon Valeriano, Benjamin M. Jensen, and Ryan C. Maness, *Cyber Strategy: The Evolving Character of Cyber Power and Strategy* (New York, NY: Oxford University Press, 2018), 142.

as of yet, then understanding previous operational capabilities is important for NATO when preparing for future operations.

Russia has the capability through cyber operations to destabilize NATO by creating weaknesses within Alliance members that threatens state security and stability. Arguably, one of the most important drivers of the NATO Alliance is Article 5 and collective defense.³²² Collective defense requires a cohesive response from every member of the Alliance, a response which can be hampered due to internal domestic issues or through critical infrastructure failures. Cyber operations have the potential to destabilize a region politically as well as physically, and this could leave NATO members distracted, unable to quickly and effectively respond to an impending threat from Russia.

B. POLICY CONSIDERATIONS

1. Evaluate NATO Attribution for Cyber Operations

Russia's apparent interest in destabilizing NATO at the strategic level likely entails degrading relationships not only within the Alliance but also within individual states of the Alliance. Karlsen notes that promoting division within the Alliance is what Western security institutions believe to be a key goal of Russian cyber operations.³²³ Due to this, cyber attribution is a critical aspect of responding to a cyber operation and NATO needs to denounce and openly attribute blame to the provocateur of a cyber operation. Open attribution places the aggressor state in the international spotlight which works to deter that state from future operations. It is the recommendation of this author that NATO adjust its posture and demonstrate a willingness to denounce any cyber activity that experts believe is from Russia. The case studies demonstrate the significant challenge to investigate and accurately attribute responsibility for cyberattacks. It is the recommendation for policy makers to conduct ongoing research and analyze findings to guide countermeasures and training.

³²² NATO, "Collective Defence—Article 5," NATO, November 25, 2019, http://www.nato.int/cps/en/natohq/topics_110496.htm.

³²³ Karlsen, "Divide and Rule," February 8, 2019.

Currently, not all NATO states are as willing as the United States to attribute blame for a cyber operation. The French presidential election provided documented evidence that resulted in the U.S. government's willingness to blame Russia; in contrast, the French government refrained from directly attributing the cyber operation to Russia.³²⁴ In order to strengthen the Alliance and its position as a leading institution, NATO leaders are encouraged to evaluate future events and require collective recognition and responses to Russian cyber operations. A collective response and agreement from all of the NATO states, in response to a cyber operation against one member, displays a unity within the Alliance that further strengthens NATO. A unified NATO response demonstrates a strong Alliance that will minimize Russia's ability to create division within the states and an Alliance that is prepared to respond to any threat.

2. Determine NATO Threshold for Response and Retaliation

The NATO Alliance is centered around the Article 5 commitment to collective defense from a conventional attack. In 2019, NATO Secretary General Jens Stoltenberg affirmed that "a serious cyberattack could trigger Article 5."³²⁵ This is an evolving stance on cyberattacks that the Alliance did not demonstrate during previous incidents of Russian cyber operations analyzed in this thesis. Russia was able to carry out those cyber operations with minimal repercussions due to the issue of attribution. Following a systematic intelligence gathering and review, the NATO Alliance will be better equipped to determine the threshold for an Article 5 response. Creating and implementing NATO guidelines and strategies to evaluate, identify, and respond to cyber threats, allows NATO the ability to compare and contrast previous attacks against present threats to determine thresholds in each case. NATO should then publish a statement that all NATO member states have come together to determine the threshold for a cyber Article 5 response and are committed as an Alliance to respond to such an attack. Determining a threshold and then reaffirming

³²⁴ Vilmer, "The 'Macron Leaks' Operation: A Post-Mortem."

³²⁵ Stoltenberg, "NATO Will Defend Itself (Article by NATO Secretary General Jens Stoltenberg Published in Prospect)."

commitment to retaliating to an Article 5 attack extends the longstanding strength of the Alliance, which in turns solidifies its legitimacy as an institution.

Not every cyber threat or cyberattack will warrant an Article 5 response, but in order to display the strength and commitment of the Alliance, a measured response is a critical tactic from the Alliance. For Russian attempts to interfere with the domestic electoral proceedings of a NATO member the Alliance could invoke Article 4 which states “The Parties will consult together whenever, in the opinion of any of them, the territorial integrity, political independence or security of any of the Parties is threatened.”³²⁶ This allows the Alliance to come up with a unified response to a threat to a member state. Cyber operations involving influence operations or critical infrastructure threats warrant individual evaluation. NATO needs to develop guidelines for responding to cyber operations against member states that handle operations on a case by case basis. Not all operations are undertaken for the same purpose and therefore require strategic responses. NATO has exercised responses to issues below the threshold of Article 5 for conventional matters; implementing guidelines and strategies in response to a cyber threat below this threshold would strengthen the legitimacy of NATO in cyber while deterring future adversaries.

3. Strengthen Intelligence Sharing Cooperation

Intelligence sharing is a key element of any alliance, and NATO member states are obligated to continually improve and strengthen intelligence cooperation. Greater cooperation between NATO states strengthens the Alliance as well as prepares states to defend against cyber operations while creating a deterrent. Greater intelligence cooperation will lead to further strengthening NATO resiliency and defense as specified in Article 3 which states “In order more effectively to achieve the objectives of this Treaty, the Parties, separately and jointly, by means of continuous and effective self-help and mutual aid, will maintain and develop their individual and collective capacity to resist armed attack.”³²⁷

³²⁶ NATO, “The Consultation Process and Article 4,” NATO, February 28, 2020, http://www.nato.int/cps/en/natohq/topics_49187.htm.

³²⁷ NATO, “Resilience and Article 3.”

Cooperation and collaboration between partner states makes it more difficult for an adversary, such as Russia, to carry out a cyber operation against a NATO state. In the French presidential election, the U.S. government was able to communicate with the French government to alert it to Russian cyber activity meant to interfere in the election.³²⁸ Continual intelligence sharing between NATO members enables them to design and implement cyber defenses resulting in a stronger Alliance.

Cooperation between NATO states is crucial to strengthening cyber defenses; additionally, it is critical that policies identify cooperation between state and private entities. Private cybersecurity firms as well as areas of critical infrastructure of a state need to work closely with government agencies to create a stronger defense network. Dragonfly was first discovered by cybersecurity firm Symantec, a discovery which led to governments being able to track the cyber operation back to the Russian government.³²⁹ Private entities may discover suspicious cyber activity and through close cooperation with government agencies could deter, defend, and even attribute cyber operations before an attack or effective information operation could take place. Intelligence sharing and cooperation within a NATO state can then be taken to the Alliance to be shared with other states and private entities. Close collaboration and intelligence sharing benefits the Alliance and further strengthens its commitment to the defense of NATO states.

4. Develop NATO Cybersecurity Tactics, Training, and Procedures

NATO conducts exercises to strengthen military cooperation and demonstrate the capabilities of the Alliance as a deterrent to adversaries. The findings of the case studies highlight the lack of essential security procedures and training to minimize future attacks and the need for NATO leaders to rapidly advance tactics and training to respond appropriately. In contrast, Russia identified and executed a long-term strategy to weaken the Alliance. Recognizing the changing battlefield, it is imperative to develop cyber training tactics and procedures that increase member states' abilities to collaborate in order

³²⁸ "Cyber Command Chief Says U.S. Warned France About Russia-Backed Hackers During Election."

³²⁹ Paganini, "Dragonfly 2.0: The Sophisticated Attack Group Is Back with Destructive Purposes."

to strengthen, deter, and defeat a cyber adversary. The evolving battlefield and consequent adjustments to policy and procedures will demonstrate the adaptability of the Alliance to recognize imminent threats to the Alliance. Cyber training allows the Alliance to identify strengths and weaknesses of Allied members while increasing the effectiveness of the Alliance to operate in the cyber domain. Training at the Alliance level can then be taken to the individual state level to increase the state's cyber abilities. This training invites the Alliance members to observe and adjust effective warfare tactics in the cyber domain while simultaneously enhancing strategies with Allies. Attention to continual training ensures the NATO Alliance is responding to potential and imminent threats from Russia and other adversary states.

Cyberattacks have the potential to disrupt critical infrastructure but they also have the potential to be a detriment financially to the global economy. NotPetya accrued over \$10 billion in damages and it started as a cyberattack against one state, Ukraine, that then had a global impact affecting a multitude of industries.³³⁰ The fiscal damage inflicted by cyberattacks demonstrates the reality of an evolving battlefield and immediate responsibility for states to take a proactive stance on identifying cyberattacks and targets. Collaboration with the private sector can strengthen an organization and minimize physical as well as fiscal damage due to a cyberattack. Proactive and updated systems strengthen a state's response capabilities but also works to deter a cyber operation through hardening the intended targets systems. Creating guidelines and procedures for training and testing systems allows Allied states to prepare for a cyberattack while strengthening its own cyber position, thus further deterring an adversary.

³³⁰ Greenberg, "The Untold Story of NotPetya, the Most Devastating Cyberattack in History."

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

- Allen, John, Philip Breedlove, Julian Lindley-French, and George Zambellas. "Future War NATO? From Hybrid War to Hyper War via Cyber War." GLOBSEC, November 2017. <https://www.globsec.org/publications/future-war-nato-hybrid-war-hyper-war-via-cyber-war/>.
- Alperovitch, Dmitri. "Bears in the Midst: Intrusion into the Democratic National Committee," June 14, 2016. <https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/>.
- Applebaum, Anne. "Putin's Grand Strategy." *South Central Review* 35, no. 1 (April 17, 2018): 22–34. <https://doi.org/10.1353/scr.2018.0001>.
- Associated Press. "Putin: Soviet Collapse a 'Genuine Tragedy.'" NBCNEWS, April 25, 2005. http://www.nbcnews.com/id/7632057/ns/world_news/t/putin-soviet-collapse-genuine-tragedy/.
- Barrett, Brian. "DNC Lawsuit Against Russia Reveals New Details About 2016 Hack." *Wired*, April 20, 2018. <https://www.wired.com/story/dnc-lawsuit-reveals-key-details-2016-hack/>.
- Bodine-Baron, Elizabeth, Todd Helmus, Andrew Radin, and Elina Treyger. *Countering Russian Social Media Influence*. RAND Corporation, 2018. <https://doi.org/10.7249/RR2740>.
- Brands, Hal. "Paradoxes of the Gray Zone." *Foreign Policy Research Institute*, February 5, 2016. <https://www.fpri.org/article/2016/02/paradoxes-gray-zone/>.
- Brattberg, Erik, and Tim Maurer. "Russian Election Interference: Europe's Counter to Fake News and Cyber Attacks." Carnegie Endowment for International Peace, May 2018. <https://carnegieendowment.org/2018/05/23/russian-election-interference-europe-s-counter-to-fake-news-and-cyber-attacks-pub-76435>.
- Brent, Laura. "NATO's Role in Cyberspace." NATO Review, February 12, 2019. <https://www.nato.int/docu/review/articles/2019/02/12/natos-role-in-cyberspace/index.html>.
- Brignall, Miles. "TNT Parcels 'backed up to Ceiling' in Wake of Massive Cyberattack." *The Guardian*, July 25, 2017. <https://www.theguardian.com/money/2017/jul/25/tnt-parcels-cyber-attack-courier-fedex-notpetya>.
- CCDCOE, NATO. "DNC Hack: An Escalation That Cannot Be Ignored." Defence IQ, August 11, 2016. <https://www.defenceiq.com/cyber-defence-and-security/articles/dnc-hack-an-escalation-that-cannot-be-ignored>.

- “CCDCOE.” Accessed April 17, 2020. <https://ccdcoe.org/news/2017/notpetya-and-wannacry-call-for-a-joint-response-from-international-community/>.
- Chivvis, Christopher. *Understanding Russian “Hybrid Warfare”: And What Can Be Done About It*. RAND Corporation, 2017. <https://doi.org/10.7249/CT468>.
- CISA. “Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors,” March 16, 2018. <https://www.us-cert.gov/ncas/alerts/TA18-074A>.
- “Competing in the Gray Zone.” Accessed February 6, 2020. <https://www.csis.org/features/competing-gray-zone>.
- Conley, Heather. “Successfully Countering Russian Electoral Interference.” Center for Strategic & International Studies, June 21, 2018. <https://www.csis.org/analysis/successfully-countering-russian-electoral-interference>.
- Connell, Michael, and Sarah Vogler. “Russia’s Approach to Cyber Warfare.” Final. Arlington, VA: Center for Naval Analyses, September 2016. https://www.cna.org/CNA_files/PDF/DOP-2016-U-014231-1Rev.pdf.
- “Cyber-Attack Cost TNT at Least \$300m.” *BBC News*, September 20, 2017. <https://www.bbc.com/news/technology-41336086>.
- Defense Intelligence Agency. *Russia Military Power Building a Military to Support Great Power Aspirations*. Washington, DC: Defense Intelligence Agency, 2017. <https://www.dia.mil/Portals/27/Documents/News/Military%20Power%20Publications/Russia%20Military%20Power%20Report%202017.pdf>.
- Department of Homeland Security. *GRIZZLY STEPPE – Russian Malicious Cyber Activity*. Washington, DC: Department of Homeland Security, 2016. https://www.us-cert.gov/sites/default/files/publications/JAR_16-20296A_GRIZZLY%20STEPPE-2016-1229.pdf.
- Department of Homeland Security. “Joint Statement from the Department Of Homeland
- Dickey, Christopher. “Fighting Back Against Putin’s Hackers.” *The Daily Beast*, April 25, 2017. <https://www.thedailybeast.com/articles/2017/04/25/fighting-back-against-putin-s-hackers>.
- Director of National Intelligence. *Background to “Assessing Russian Activities and Intentions in Recent U.S. Elections”: The Analytic Process and Cyber Incident Attribution*. Washington, DC: Director of National Intelligence, 2017. https://www.dni.gov/files/documents/ICA_2017_01.pdf.

- Duffield, John S. "NATO's Functions after the Cold War." *Political Science Quarterly* 109, no. 5 (1994): 763–87. <https://doi.org/10.2307/2152531>.
- "Exposing Russia's Effort to Sow Discord Online: The Internet Research Agency and Advertisements | Permanent Select Committee on Intelligence." Accessed October 28, 2019. <https://intelligence.house.gov/social-media-content/>.
- Feaver, Peter. "What Is Grand Strategy and Why Do We Need It?" *Foreign Policy*, April 8, 2019. <https://foreignpolicy.com/2009/04/08/what-is-grand-strategy-and-why-do-we-need-it/>.
- France 24. "French Media Rules Prohibit Election Coverage over Weekend," May 6, 2017. <https://www.france24.com/en/20170506-france-media-rules-prohibit-election-coverage-over-weekend-presidential-poll>.
- Geers, Kenneth, and NATO Cooperative Cyber Defence Centre of Excellence. *Cyber War in Perspective: Russian Aggression against Ukraine*, 2015. <https://www.ccdcoe.org/library/publications/cyber-war-in-perspective-russian-aggression-against-ukraine/>.
- Gerasimov, Valery. "The Value of Science Is in the Foresight New Challenges Demand Rethinking the Forms and Methods of Carrying out Combat Operations." *Military Review*, February 2016. https://www.armyupress.army.mil/Portals/7/military-review/Archives/English/MilitaryReview_20160228_art008.pdf.
- Giles, Keir. "Handbook of Russian Information Warfare." *Fellowship Monograph* 9, 11/16, 90.
- . "Information Troops"—A Russian Cyber Command?, 2011.
- Giles, Keir, James Sherr, and Anthony Seaboyer. "Russian Reflexive Control." Kingston, ON, Canada: Royal Military College of Canada, 2018.
- Glaser, April. "Here's What We Know About Russia and the DNC Hack." *Wired*, July 27, 2016. <https://www.wired.com/2016/07/heres-know-russia-dnc-hack/>.
- Graham, Luke. "NATO Think-Tank Says a 'State Actor' Was behind the Massive Ransomware Attack and Could Trigger Military Response." CNBC, June 30, 2017. <https://www.cnbc.com/2017/06/30/petya-ransomware-attack-nato-says-state-actor-to-blame.html>.
- Graham, Thomas. "The Sources of Russia's Insecurity." *Survival* 52, no. 1 (March 2010): 55–74. <https://doi.org/10.1080/00396331003612471>.
- Gray, Colin S. *Modern Strategy*. New York: Oxford University Press, 1999.

- Greenberg, Andy. "A Brief Tour of Russia's Infrastructure Hacking Teams." *Wired*, July 12, 2017. <https://www.wired.com/story/russian-hacking-teams-infrastructure/>.
- . "Hackers Hit Macron with Huge Email Leak Ahead of French Election." *Wired*, May 5, 2017. <https://www.wired.com/2017/05/macron-email-hack-french-election/>.
- . "How an Entire Nation Became Russia's Test Lab for Cyberwar." *Wired*, June 20, 2017. <https://www.wired.com/story/russian-hackers-attack-ukraine/>.
- . "NSA Director Confirms That Russia Really Did Hack the French Election." *Wired*, May 9, 2017. <https://www.wired.com/2017/05/nsa-director-confirms-russia-hacked-french-election-infrastructure/>.
- . "Russia's Cozy Bear Hackers Resurface with Clever New Tricks." *Wired*, October 17, 2019. <https://www.wired.com/story/cozy-bear-dukes-russian-hackers-new-tricks/>.
- . "The Untold Story of NotPetya, the Most Devastating Cyberattack in History." *Wired*, August 22, 2018. <https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/>.
- . "Ukrainians Say Petya Ransomware Hides State-Sponsored Attacks." *Wired*, June 28, 2017. <https://www.wired.com/story/petya-ransomware-ukraine/>.
- Hacquebord, Feike. "Two Years of Pawn Storm Examining an Increasingly Relevant Threat." Manilla: TrendLabs, 2017.
- Hay Newman, Lily. "Guccifer 2.0's Slip-Up Shows That Even Elite Hackers Make Mistakes." *Wired*, March 25, 2018. <https://www.wired.com/story/guccifer-elite-hackers-mistakes/>.
- Hill, Fiona. "Putin: The One-Man Show the West Doesn't Understand." *Bulletin of the Atomic Scientists* 72, no. 3 (May 3, 2016): 140–44. <https://doi.org/10.1080/00963402.2016.1170361>.
- House of Commons Defence Committee. "Russia: Implications for UK Defence and Security." London, England: House of Commons Defence Committee, June 28, 2016. <https://publications.parliament.uk/pa/cm201617/cmselect/cmdfence/107/107.pdf>.
- Ilyushina, Mary, and Euan McKirdy. "Putin: 'Patriotic' Russian Hackers May Have Targeted U.S. Election," June 2, 2017. <https://www.cnn.com/2017/06/01/politics/russia-putin-hackers-election/index.html>.

- Johnson, A. "Endpoint Protection—Symantec Enterprise," June 30, 2014.
<https://community.broadcom.com/symantecenterprise/communities/community-home/librarydocuments/viewdocument?DocumentKey=7382dce7-0260-4782-84cc-890971ed3f17&CommunityKey=1ecf5f55-9545-44d6-b0f4-4e4a7f5f5e68&tab=librarydocuments>.
- Joint Chiefs of Staff. *Cyberspace Operations*. JP 3-12. Washington, DC: Joint Chiefs of Staff, 2018. https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf.
- Karlsen, Geir Hågen. "Divide and Rule: Ten Lessons about Russian Political Influence Activities in Europe." *Palgrave Communications* 5, no. 1 (February 8, 2019): 1–14. <https://doi.org/10.1057/s41599-019-0227-8>.
- Kofman, Michael. "Drivers of Russian Grand Strategy." Stockholm: Frivärld, April 23, 2019. <https://frivarld.se/rapporter/drivers-of-russian-grand-strategy-2/>.
- Kramer, Mark. "TWQ: The Myth of a No-NATO-Enlargement Pledge to Russia—Spring 2009." *Center for Strategic & International Studies*, April 1, 2009. <https://www.csis.org/analysis/twq-myth-no-nato-enlargement-pledge-russia-spring-2009>.
- Kremlin. *Doctrine of Information Security of the Russian Federation*. Moscow, Russia: Kremlin, 2016. https://www.mid.ru/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/2563163.
- . *Foreign Policy Concept of the Russian Federation*. Moscow, Russia: Kremlin, 2016. https://www.mid.ru/en/foreign_policy/official_documents//asset_publisher/CptICkB6BZ29/content/id/2542248.
- . *Russian National Security Strategy*. Moscow, Russia: The Kremlin, 2015. <http://www.ieee.es/Galerias/fichero/OtrasPublicaciones/Internacional/2016/Russian-National-Security-Strategy-31Dec2015.pdf>.
- . *The Military Doctrine of the Russian Federation*. Moscow, Russia: Russian Federation, 2010. https://carnegieendowment.org/files/2010russia_military_doctrine.pdf.
- . *The Military Doctrine of the Russian Federation*. Moscow, Russia: Russian Federation, 2014. <http://rusemb.org.uk/press/2029>.
- Kucharski, Lesley. "Russian Multi-Domain Strategy against NATO: Information Confrontation and U.S. Forward-Deployed Nuclear Weapons in Europe." The Center for Global Security Research: Lawrence Livermore National Laboratory, 2018. https://cgsl.llnl.gov/content/assets/docs/4Feb_IPb_against_NATO_nuclear_posture.pdf.

- Masters, Jonathan. "An Unsettled Alliance." Council on Foreign Relations, December 3, 2019. <https://www.cfr.org/background/north-atlantic-treaty-organization-nato>.
- Maynor, David, Aleksandar Nikolic, Matt Olney, and Yves Younan. "The MeDoc Connection," July 5, 2017. <http://blog.talosintelligence.com/2017/07/the-medoc-connection.html>.
- Mazarr, Michael J. "Struggle in the Gray Zone and World Order." *War on the Rocks*, December 22, 2015. <https://warontherocks.com/2015/12/struggle-in-the-gray-zone-and-world-order/>.
- McFaul, Michael. Russia's Transition to Democracy and U.S.-Russia Relations: Unfinished Business, § U.S. Congress (2003). <https://carnegieendowment.org/2003/09/30/russia-s-transition-to-democracy-and-u.s.-russia-relations-unfinished-business-pub-1363>.
- Monaghan, Andrew. "Putin's Russia: Shaping a 'Grand Strategy'?" *International Affairs (Royal Institute of International Affairs 1944-)* 89, no. 5 (2013): 1221–36.
- Morris, Lyle, Michael Mazarr, Jeffrey Hornung, Stephanie Pezard, Anika Binnendijk, and Marta Kepe. *Gaining Competitive Advantage in the Gray Zone: Response Options for Coercive Aggression Below the Threshold of Major War*. RAND Corporation, 2019. <https://doi.org/10.7249/RR2942>.
- Mshvidobadze, Khatuna. "The Battlefield on Your Laptop." RadioFreeEurope/RadioLiberty, March 21, 2011. https://www.rferl.org/a/commentary_battlefield_on_your_desktop/2345202.html.
- Mueller, Robert. *Report On The Investigation Into Russian Interference In The 2016 Presidential Election, Volume I of II*. Washington, DC: U.S. Department of Justice, 2019. <https://www.justice.gov/storage/report.pdf>.
- NATO. "A Short History of NATO." NATO. Accessed January 28, 2020. http://www.nato.int/cps/en/natohq/declassified_139339.htm.
- . "Brussels Summit Declaration Issued by the Heads of State and Government Participating in the Meeting of the North Atlantic Council in Brussels, 11–12 July 2018." NATO, July 11, 2018. http://www.nato.int/cps/en/natohq/official_texts_156624.htm.
- . "Civil Preparedness." NATO, March 31, 2020. http://www.nato.int/cps/en/natohq/topics_49158.htm.
- . "Collective Defence—Article 5." NATO, November 25, 2019. http://www.nato.int/cps/en/natohq/topics_110496.htm.

- . “Cyber Defence Pledge.” NATO, July 8, 2016. http://www.nato.int/cps/en/natohq/official_texts_133177.htm.
- . “NATO Enlargement & Open Door,” 2017. https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2017_11/20171130_1711-factsheet-enlargement-eng.pdf.
- . “Resilience and Article 3.” NATO, March 31, 2020. http://www.nato.int/cps/en/natohq/topics_132722.htm.
- . “The Consultation Process and Article 4.” NATO, February 28, 2020. http://www.nato.int/cps/en/natohq/topics_49187.htm.
- . “The North Atlantic Treaty.” NATO. Accessed January 28, 2020. http://www.nato.int/cps/en/natohq/official_texts_17120.htm.
- . “Wales Summit Declaration Issued by the Heads of State and Government Participating in the Meeting of the North Atlantic Council in Wales.” NATO, September 5, 2014. http://www.nato.int/cps/en/natohq/official_texts_112964.htm.
- . “Warsaw Summit Communiqué—Issued by the Heads of State and Government Participating in the Meeting of the North Atlantic Council in Warsaw, 8–9 July 2016.” NATO, July 9, 2016. http://www.nato.int/cps/en/natohq/official_texts_133169.htm.
- Nye, Joseph S. *Power in the Global Information Age: From Realism to Globalization*. London ; New York: Routledge, 2005.
- . *Soft Power: The Means to Success in World Politics*. 1st ed. New York: Public Affairs, 2004.
- Ottis, Rain. “Analysis of the 2007 Cyber Attacks against Estonia from the Information Warfare Perspective.” *Cooperative Cyber Defence Centre of Excellence*, 2008, 6.
- Paganini, Pierluigi. “Dragonfly 2.0: The Sophisticated Attack Group Is Back with Destructive Purposes.” *Security Affairs*, September 7, 2017. <https://securityaffairs.co/wordpress/62782/hacking/dragonfly-2-0-campaigns.html>.
- . “FBI-DHS JAR Report Links Russian Hackers to Presidential Election Hacks.” *Security Affairs*, December 31, 2016. <https://securityaffairs.co/wordpress/54900/cyber-warfare-2/fbi-dhs-jar-report.html>.
- Pape, Robert A. “Soft Balancing against the United States.” *International Security* 30, no. 1 (July 2005): 7–45. <https://doi.org/10.1162/0162288054894607>.

- Patrushev, Nikolay, and Ivan Yegorov. Cold War II: Interview with Nikolay Patrushev, Secretary of the Russian Security Council, October 15, 2014. <https://mideastshuffle.com/2014/10/22/cold-war-ii-interview-with-nikolay-patrushev-secretary-of-the-russian-security-council/>.
- Person, Robert. "Russian Grand Strategy in the 21st Century." Presentation, NSI SMA Speaker Series, Boston, MA, May 3, 2019. <https://nsiteam.com/russian-grand-strategy-in-the-21st-century/>.
- . *Russian Grand Strategy in the 21st Century*. Lecture. Future of Global Competition & Conflict. NSI SMA Speaker Series, Boston, MA, 2019. <https://nsiteam.com/russian-grand-strategy-in-the-21st-century/>.
- Pettyjohn, Stacie, and Becca Wasser. *Competing in the Gray Zone: Russian Tactics and Western Responses*. RAND Corporation, 2019. <https://doi.org/10.7249/RR2791>.
- Prior, Tim. "NATO: Pushing Boundaries for Resilience." *CSS Analyses in Security Policy*, no. 213 (September 2017): 4.
- Pruitt, Gary. "Putin Claims Russia Hasn't Meddled in U.S. Elections, despite Evidence of Influence Campaign." PBS NewsHour, June 6, 2019. <https://www.pbs.org/newshour/world/putin-claims-russia-hasnt-meddled-in-u-s-elections-despite-evidence-of-influence-campaign>.
- Putin, Vladimir. "Putin's Prepared Remarks at 43rd Munich Conference on Security Policy," February 12, 2007. <http://www.washingtonpost.com/wp-dyn/content/article/2007/02/12/AR2007021200555.html>.
- RadioFreeEurope/RadioLiberty. "Cyber Command Chief Says U.S. Warned France About Russia-Backed Hackers During Election," May 9, 2017. <https://www.rferl.org/a/us-warned-france-russian-hacking/28476837.html>.
- Renz, Bettina, and Hanna Smith. "Russia and Hybrid Warfare—Going Beyond the Label." *Aleksanteri Papers*, January 2016, 65.
- Reuters. "Putin Criticizes NATO Expansion." The Moscow Times, December 3, 2019. <https://www.themoscowtimes.com/2019/12/03/putin-criticizes-nato-expansion-as-alliance-holds-london-summit-a68457>.
- Roberts, Paul. "NotPetya Infection Left Merck Short of Key HPV Vaccine." The Security Ledger, October 27, 2017. <https://securityledger.com/2017/10/notpetya-infection-left-merck-short-key-vaccine-gardasil/>.
- Roepke, Wolf-Diether, and Hasit Thankey. "Resilience: The First Line of Defence." NATO Review, February 27, 2019. <https://www.nato.int/docu/review/articles/2019/02/27/resilience-the-first-line-of-defence/index.html>.

- Rühle, Michael. "NATO Enlargement and Russia: Die-Hard Myths and Real Dilemmas." NDC Research Report. Italy: NATO Defense College, May 15, 2014.
- Ruiz Palmer, Diego. "A Strategic Odyssey: Constancy of Purpose and Strategy-Making in NATO, 1949–2019." NDC Research Paper. Italy: NATO Defense College, June 2019. <http://www.ndc.nato.int/news/news.php?icode=1330>.
- Polskie Radio dla Zagranicy. "Russia Seeking to Sow Discord, NATO Must React: Polish President." Accessed November 21, 2019. <http://archiwum.thenews.pl/1/10/Artykul/410646,Russia-seeking-to-sow-discord-NATO-must-react-Polish-president>.
- RadioFreeEurope/RadioLiberty. "UN Chief Calls for Regulatory Scheme For Cyberwarfare," February 19, 2018. <https://www.rferl.org/a/un-guterres-calls-for-cyberwarfare-rules/29049069.html>.
- Russia, Team of the Official website of the President of. "Address by President of the Russian Federation." President of Russia, March 18, 2014. <http://en.kremlin.ru/events/president/news/20603>.
- Security and Office of the Director of National Intelligence on Election Security," October 7, 2016. <https://www.dhs.gov/news/2016/10/07/joint-statement-department-homeland-security-and-office-director-national>.
- Security Response Attack Investigation Team. "Dragonfly: Western Energy Sector Targeted by Sophisticated Attack Group." Symantec Blogs, October 20, 2017. <https://www.symantec.com/blogs/threat-intelligence/dragonfly-energy-sector-cyber-attacks>.
- Select Committee on Intelligence. *Russian Active Measures Campaigns and Interference in the 2016 U.S. Election Volume 2: Russia's Use of Social Media with Additional Views*. Washington, DC: United States Senate, 2019. https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume2.pdf.
- Singer, P. W. *Cybersecurity and Cyberwar: What Everyone Needs to Know*. Oxford ; New York: Oxford University Press, 2014.
- Smith, Rebecca. "Russian Hackers Reach U.S. Utility Control Rooms, Homeland Security Officials Say—WSJ," July 23, 2018. <https://www.wsj.com/articles/russian-hackers-reach-u-s-utility-control-rooms-homeland-security-officials-say-1532388110?redirect=amp>.
- Stoltenberg, Jens. "NATO Will Defend Itself (Article by NATO Secretary General Jens Stoltenberg Published in Prospect)." NATO, August 29, 2019. http://www.nato.int/cps/en/natohq/news_168435.htm.

- Symantec Security Response. "Dragonfly: Cyberespionage Attacks Against Energy Suppliers." Security Response. Symantec, July 7, 2014.
- Tertrais, Bruno. "Article 5 of the Washington Treaty: Its Origins, Meaning and Future," no. 130 (2016): 8.
- Theohary, Catherine A. "Defense Primer: Information Operations." CRS In Focus. Washington, DC: Congressional Research Service, December 18, 2018.
- Thomas, Timothy. "Russian Information Warfare Theory: The Consequences of August 2008." In *The Russian Military Today and Tomorrow: Essays in Memory of Mary Fitzgerald* /. Carlisle, PA, 2010. <http://hdl.handle.net/2027/mdp.39015085911041>.
- "Time Zone & Clock Changes 2010–2019 in Moscow, Russia." Accessed April 16, 2020. <https://www.timeanddate.com/time/zone/russia/moscow?year=2014>.
- Tsygankov, Andrei P. "Preserving Influence in a Changing World: Russia's Grand Strategy." *Problems of Post-Communism* 58, no. 2 (March 2011): 28–44. <https://doi.org/10.2753/PPC1075-8216580203>.
- , ed. *Routledge Handbook of Russian Foreign Policy*. London ; New York: Routledge, Taylor & Francis Group, 2018.
- Valeriano, Brandon, Benjamin M. Jensen, and Ryan C. Maness. *Cyber Strategy: The Evolving Character of Cyber Power and Strategy*. New York, NY: Oxford University Press, 2018.
- Vilmer, Jean-Baptiste Jeangène. "The 'Macron Leaks' Operation: A Post-Mortem." Washington, DC: Atlantic Council, June 20, 2019. https://www.atlanticcouncil.org/wp-content/uploads/2019/06/The_Macron_Leaks_Operation-A_Post-Mortem.pdf.
- Waltz, Kenneth Neal. *Theory of International Politics*. Reissued. Long Grove, Ill: Waveland Press, 2010.
- White House. "Statement from the Press Secretary," February 15, 2018. <https://www.whitehouse.gov/briefings-statements/statement-press-secretary-25/>.
- Wirtz, James J. "Cyber War and Strategic Culture: The Russian Integration of Cyber Power into Grand Strategy." In *Cyber War in Perspective: Russian Aggression Against Ukraine*, 11. Estonia: CCDCOE, 2015.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
Ft. Belvoir, Virginia
2. Dudley Knox Library
Naval Postgraduate School
Monterey, California