2015-03

Offense-defense theory analysis of Russian cyber capability

Medvedev, Sergei A.

Monterey, California: Naval Postgraduate School

NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

OFFENSE-DEFENSE THEORY ANALYSIS OF RUSSIAN CYBER CAPABILITY

by

Sergei A. Medvedev

March 2015

Thesis Advisor: Wade L. Huntley
Co-Advisor: Mikhail Tsypkin

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE

Form Approved OMB No. 0704–0188

1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** March 2015	**3. REPORT TYPE AND DATES COVERED** Master's Thesis

4. TITLE AND SUBTITLE
OFFENSE-DEFENSE THEORY ANALYSIS OF RUSSIAN CYBER CAPABILITY

5. FUNDING NUMBERS

6. AUTHOR(S) Sergei A. Medvedev

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. IRB Protocol number ____N/A____.

12a. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for public release; distribution is unlimited

12b. DISTRIBUTION CODE

13. ABSTRACT (maximum 200 words)

The Russian Federation is a key state actor in cyberspace; cyber events associated with Russian state and non-state actors have threatened Russia's neighbors, shaped international cyber norms, as well as influenced strategists' understanding of cyber power. This thesis seeks to understand Russian cyber capability through the lens of Robert Jervis's offense-defense theory in order to answer the thesis's central question: Do Russian cyber capabilities reflect an investment in offensive or defensive cyber weapons, and do Russia's cyber technology, doctrine, and policy differentiate its posture as offensive or defensive? To evaluate Russian cyber capability, this thesis considers two factors—technology and geography—concluding that, although the Russian government is modifying its cyber terrain to improve defensiveness, Russia's brandished cyber weapons suggest that it pursues offensive capability. To evaluate Russia's posture differentiation, the thesis examines Russians' understanding of cyber power, Russian information warfare and hybrid warfare doctrines, and the country's international engagements, concluding that, although Russia has historically presented its posture as defensive, it is increasingly difficult to make that distinction. Finally, the thesis evaluates this state-level analysis in the broader context of the international system; Russia's historical aggression and current behavior in cyberspace likely reflects Stephen van Evera's explanatory hypothesis for the causes of war—defensive expansion.

14. SUBJECT TERMS
Russia, cyber, cyberspace, offense-defense theory, information warfare, hybrid warfare.

15. NUMBER OF PAGES
109

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	**18. SECURITY CLASSIFICATION OF THIS PAGE**	**19. SECURITY CLASSIFICATION OF ABSTRACT**	**20. LIMITATION OF ABSTRACT**
Unclassified	Unclassified	Unclassified	UU

NSN 7540–01-280-5500

Standard Form 298 (Rev. 2–89)
Prescribed by ANSI Std. 239–18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

OFFENSE-DEFENSE THEORY ANALYSIS OF RUSSIAN CYBER CAPABILITY

Sergei A. Medvedev
Major, United States Air Force
B.S., University of Illinois at Urbana-Champaign, 2003
M.H.R., University of Oklahoma, 2012

Submitted in partial fulfillment of the
requirements for the degree of

**MASTER OF ARTS IN SECURITY STUDIES
(EUROPE AND EURASIA)**

from the

**NAVAL POSTGRADUATE SCHOOL
March 2015**

Author: Sergei A. Medvedev

Approved by: Wade L. Huntley, Ph.D.
Thesis Advisor

Mikhail Tsypkin, Ph.D.
Co-Advisor

Mohammed M. Hafez, Ph.D.
Chair, Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

The Russian Federation is a key state actor in cyberspace; cyber events associated with Russian state and non-state actors have threatened Russia's neighbors, shaped international cyber norms, as well as influenced strategists' understanding of cyber power. This thesis seeks to understand Russian cyber capability through the lens of Robert Jervis's offense-defense theory in order to answer the thesis's central question: Do Russian cyber capabilities reflect an investment in offensive or defensive cyber weapons, and do Russia's cyber technology, doctrine, and policy differentiate its posture as offensive or defensive? To evaluate Russian cyber capability, this thesis considers two factors—technology and geography—concluding that, although the Russian government is modifying its cyber terrain to improve defensiveness, Russia's brandished cyber weapons suggest that it pursues offensive capability. To evaluate Russia's posture differentiation, the thesis examines Russians' understanding of cyber power, Russian information warfare and hybrid warfare doctrines, and the country's international engagements, concluding that, although Russia has historically presented its posture as defensive, it is increasingly difficult to make that distinction. Finally, the thesis evaluates this state-level analysis in the broader context of the international system; Russia's historical aggression and current behavior in cyberspace likely reflects Stephen van Evera's explanatory hypothesis for the causes of war—defensive expansion.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

APT28	Advanced Persistent Threat 28
CERT	computer emergency response team
DDoS	distributed denial of service attack
DoS	denial of service attack
FSB	Federal Security Service
GGE	group of governmental experts
GRU	Main Intelligence Directorate of the General Staff of the Armed Forces
ICT	Internet and communications technologies
IR	international relations
ISP	Internet service provider
RBN	Russian Business Network
Roskomnadzor	Federal Service for Supervision of Communications, Information Technology and Mass Media
SCO	Shanghai Cooperation Organization
SORM	System for Operative Investigative Activities
SVR	Foreign Intelligence Service of the Russian Federation
TDS	traffic direction system
Tor	The Onion Router

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

This thesis represents just a portion of the engaging and enriching academic experience I enjoyed at the Naval Postgraduate School. I am grateful to the school's faculty and staff for their world-class dedication, expertise, and professionalism—thank you!

I especially would like to thank my thesis co-advisors, Dr. Wade L. Huntley and Dr. Mikhail Tsypkin. They taught fascinating classes about Russia and cyberspace strategy that motivated me to pursue this topic. Throughout my research and writing process, they offered intriguing advice and thoughtful feedback that led to a very fulfilling learning experience. Your support and guidance were superb; I could not have hoped for better.

I would also like to thank my friends and family for their support and encouragement. In particular, I would like to thank my parents. Not only have they encouraged a lifetime of learning, but they also weathered the brunt of my rough drafts.

Finally, I want to acknowledge and thank my peers and colleagues—fellow cybernauts—alongside whom I have spent the last ten years building, defending, and operating the Department of Defense's cyberspace. Our operational experiences, debates about cyber power, and sometimes just simple mutual support continue to inspire me to think critically about our military's and nation's role in cyberspace.

THIS PAGE INTENTIONALLY LEFT BLANK

I. ASSESSING CYBER POWER

The development and proliferation of cyber technologies over the last thirty years has added a new dimension to international strategy, creating new threats and opportunities for cyberspace-based crime, espionage, and warfare.[1] A key actor in the cyber domain is the Russian Federation; cyber events associated with Russian state and non-state actors have shaped the international environment, created security challenges, and influenced strategists' understanding of cyber power. The relative novelty and rapid pace of cyber development, however, have also resulted in gaps in the understanding of cyber power as both an instrument of power and an element of national strategy.

This thesis evaluates the role and posture of the Russian Federation in cyberspace. In doing so, the author considers the extensive existing literature of cyber events associated with Russia, the scholarly works that have examined Russian information warfare doctrine, and the record of Russian engagement through international institutions. Though, individually, these subject areas provide a wealth of analysis and policy recommendations, the author's goal is to offer a holistic perspective on Russia's behavior in cyberspace through the lens of existing international relations theory. The value of understanding Russia's actions according to a theoretical framework is that policy makers may more effectively engage Russia, focusing not just on immediate crises or initiatives, but instead, on crafting a strategic approach that targets underlying causes of behavior.

A. PERSPECTIVES ON RUSSIAN CYBER CAPABILITY

Assessments of Russia's cyber power, as articulated by key U.S. officials, categorize the Russian Federation as one of the leading powers in cyberspace; this suggests that capability parity with the United States presents a potential threat to American national security, and that intent demonstrated through conflicts with its

[1] Lucas Kello, "The Meaning of the Cyber Revolution: Perils to Theory and Statecraft," *International Security* 38, no. 2 (Fall, 2013): 7-40. doi: 1.1162/ISEC_a_00138.

neighbors necessitates a continued cyber arms race.[2] Congressional reports highlight that Russia is a highly capable actor, recognizing that its cyber power can be applied for both espionage and attack.[3] Open-source U.S. military analysis suggests that Russian cyber power is integral to the country's military strategy for achieving its political international objectives and recommends a broad deterrence policy for the United States.[4] In addition to this primarily offensive conception of Russia's cyber capability, academic sources recognize Russia's own strategic security concerns in cyberspace, focusing on information warfare threats perceived by Russian political elites.[5] Collectively, the existing body of literature provides excellent insights into specific facets of Russia's cyber capability, but falls short of achieving a comprehensive analysis of Russia's cyber capabilities and linking these capabilities to Russia's offensive and defensive security strategy objectives.

International and U.S. evaluation of Russian cyber strategy and capabilities is mostly based on four sets of Russian-associated cyber activities: the 2007 Estonia Bronze Soldier crisis, the 2008 Russo-Georgian War, criminal activity associated with the Russian Business Network (RBN), and presumed capabilities of Russia's spy agencies. The cyber crisis in Estonia gained international prominence because of the large-scale disruption by cyber attacks directed at Estonia's cyber infrastructure and online services. In the aftermath of the month-long crisis, the attacks were attributed to Russian activists,

---

[2] Keith Alexander, "House Armed Services Subcommittee, Cyberspace Operations Testimony," The Cyber Domain, U.S. Department of Defense, September 23, 2010, http://www.defense.gov/home/features/2011/0411_cyberstrategy/docs/House%20Armed%20Services%20Subcommittee%20Cyberspace%20Operations%20Testimony%2020100923.pdf.

[3] "Cyber Threats from China, Russia, and Iran: Protecting American Critical Infrastructure," Committee on Homeland Security, 113th Congress (March 2013), http://www.gpo.gov/fdsys/pkg/CHRG-113hhrg82583/html/CHRG-113hhrg82583.htm.

[4] Richard G. Zoller, "Russian Cyberspace Strategy and a Proposed United States Response," Strategy Research Project, U.S. Army War College, 2010, http://handle.dtic.mil/100.2/ADA522027.

[5] Stephen Blank, "Threats to and from Russia: An Assessment," *The Journal of Slavic Military Studies* 21, no. 3 (2008): 491–526. doi:10.1080/13518040802313746.

but not to the government.[6] Similarly, despite compelling circumstantial evidence, cyber attacks concurrent with Russia's official military campaign against Georgia in August 2008 were conclusively linked solely to Russian activists and criminal organizations.[7] Both of the cyber events seemed to align with Russian government interests and suggested a permissive environment for non-state cyber actors.[8] Additionally, the Russian-Ukrainian conflict that began in 2014 offers an on-going demonstration of Russia's current cyber capabilities and tactics.

Whereas the cyber attacks on Estonia and Georgia occurred within well-defined operational windows, criminal cyber activity linked to Russia has spanned the last decade and is exemplified by the RBN. Malicious activities associated with Russian criminal organizations represent significant cyber capacity; Russia's criminals possess moderately sophisticated technology, but control vast online resources.[9] Additionally, most sources that assess Russia's cyber capability share an assumption that is inherently difficult to substantiate: Russia's intelligence and security agencies charged with cyber missions—Federal Security Service (FSB), Foreign Intelligence Service (SVR), and the military's Main Intelligence Directorate (GRU)—possess cyber exploitation ability on par with leading powers.[10]

---

[6] Eneken Tikk, Kadri Kaska, and Liis Vihul, *International Cyber Incidents: Legal Considerations*, (Tallinn: Cooperative Cyber Defense Centre of Excellence, 2010); Rain Ottis, "Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective," presented at the 7th European Conference on Information Warfare and Security, Plymouth. (Reading: Academic Publishing Limited, 2008), 163-8.

[7] "Russia/Georgia Cyber War – Findings and Analysis," Project Grey Goose: Phase I Report, last modified October 17, 2008, 9, http://blog.refractal.org/wp-content/uploads/2008/10/2i7t2qyiwv0g63e7l3g.pdf; "Overview by the US-CCU of the Cyber Campaign Against Georgia in August of 2008," U.S. Cyber Consequences Unit (2009), http://www.registan.net/wp-content/uploads/2009/08/US-CCU-Georgia-Cyber-Campaign-Overview.pdf; Carolina Vendil Pallin, and Fredrik Westerlund, "Russia's War in Georgia: Lessons and Consequences," *Small Wars & Insurgencies* 20, no. 2 (2009): 400-24. doi: 10.1080/09592310902975539

[8] Scott J. Shackelford, "State Responsibility for Cyber Attacks: Competing Standards for a Growing Problem," presented at the Conference on Cyber Conflict Proceedings 2010, (Tallinn, Estonia: CCD COE Publications, 2010): 197-208; Timothy L. Thomas, "Russia's Information Warfare Strategy: Can the Nation Cope in Future Conflicts?," *The Journal of Slavic Military Studies* 27, no. 1 (2014): 107-8, doi:10.1080/13518046.2014.874845.

[9] Alexander Klimburg, "Mobilizing Cyber Power," *Survival: Global Politics and Strategy* 53, no. 1 (2011): 41-60. doi: 10.1080/00396338.2011.555595.

[10] "Cyber Threats From China, Russia, and Iran."

The limitations of analysis based on these events are that they typically solely represent the cyber power of Russia's non-state actors, demonstrate only a portion of the broader spectrum of cyber capabilities, and focus exclusively on offensive capability. Despite these shortcomings, cyber events associated with Russia have stimulated the development of international norms and laws and have shaped defensive strategies of states that perceive themselves vulnerable to similar attacks.

In contrast to this offense-focused analysis, Russian and select international analysts seek to understand the information warfare ramifications of cyber power. Russian doctrine explicitly recognizes an information-psychological aspect of cyber confrontation, and the Russian government believes that it is already engaged in a defensive action in a global information war.[11] This perception is shaped by the role of social media and what Russia perceives as hostile propaganda during the Color Revolutions, the Arab Spring, and recently in its own domestic politics.[12] In response to this perceived security concern, Russia has continuously advocated for international treaty restrictions on cyber warfare.[13] Domestically, it has structured its information warfare doctrine to address this threat, and has regulated its information technology sector to increase resilience to hostile information operations, propaganda, and political dissent.[14] While American and other international experts categorize Russia as an

[11] "Conceptual Views Regarding the Activities of the Armed Forces of the Russian Federation in the Information Space," Unofficial NATO Translation, accessed March 24, 2014 (Tallinn: Cooperative Cyber Defense Centre of Excellence): 3, http://www.ccdcoe.org/strategies/Russian_Federation_unofficial_translation.pdf.

[12] Keir Giles, "'Information Troops' – a Russian Cyber Command?," presented at the 3rd International Conference on Cyber Conflict, Tallinn: Cooperative Cyber Defense Centre of Excellence (2011): 45-57, http://www.ccdcoe.org/publications/2011proceedings/InformationTroopsARussianCyberCommand-Giles.pdf.

[13] Keir Giles, "Russia's Public Stance on Cyberspace Issues," presented at the 4th International Conference on Cyber Conflict, Tallinn: Cooperative Cyber Defense Centre of Excellence (2012): 63-74, http://www.ccdcoe.org/publications/2012proceedings/2_1_Giles_RussiasPublicStanceOnCyberInformation Warfare.pdf; "Convention on International Information Security," Ministry of Foreign Affairs of the Russian Federation, last modified September 22, 2011, http://www.mid.ru/bdomp/ns-osndoc.nsf/1e5f0de28fe77fdcc32575d900298676/7b17ead7244e2064c3257925003bcbcc!OpenDocument.

[14] Stephen Blank, "Russian Information Warfare as Domestic Counterinsurgency," *American Foreign Policy Interests: The Journal of the National Committee on American Foreign Policy* 35, no. 1 (January 2013): 31–44. doi:10.1080/10803920.2013.757946.

aggressor based on the actions of Russian non-state actors, overt Russian state efforts and cyber developments appear to be more defensive.[15]

B. OFFENSE-DEFENSE THEORY

The international relations theoretic paradigm for analyzing Russian cyber capability that the author adopts throughout this thesis is Robert Jervis's offense-defense theory. The following sections describe the theory's fundamental explanatory argument, recapitulate critiques of the theory, and argue why this analytic paradigm is suitable for studying Russian cyber power.

1. Idealized Definition

In his 1978 study of problems in international politics, "Cooperation Under the Security Dilemma," Robert Jervis identifies the security dilemma as a problematic process that escalates international tension—security-seeking states appear to increase the insecurity of other states simply through defensive actions that should otherwise be nonthreatening. The intensity of this security dilemma, or whether or not the international systems manifests it in the first place, depends on two variables—"whether defensive weapons and policies can be distinguished from offensive ones, and whether the defense or the offense has the advantage."[16] Jervis further elaborates on factors that underlie these variables and under what conditions they affect the security dilemma.

The first variable, offense-defense differentiation, addresses states' perceptions of others—whether other states threaten them or not. States base these perceptions on whether other states' armaments can be used strictly for offense or defense (or both), and on the military and political strategies states pursue.[17] If it is possible to differentiate states' postures, then security-seeking states can cooperate with likeminded states, but revisionist states may still act aggressively. Such a situation, however, is stable—the

---

[15] Oleg Demidov, "Cyberwarfare and Russian Style of Cyberdefense," *Security Index: A Russian Journal on International Security* 19, no. 3 (September 2013): 70–71, doi:10.1080/19934270.2013.814955.

[16] Robert Jervis, "Cooperation Under the Security Dilemma," *World Politics* 30, no. 2 (January 1978): 186-7, http://www.jstor.org/stable/2009958.

[17] Ibid., 203.

transparency of intentions precludes the security dilemma and aggressive states signal hostile behavior. The second variable, the offense-defense balance, strives to ascertain whether weapons favor the attacker or the defender. At times when it is possible to differentiate whether offensive or defensive weapons dominate, Jervis predicts various security dilemma outcomes: if dollar-for-dollar offensive weapons are a better investment, states are more inclined to attack first; but when defensive weapons dominate, wars tend toward stalemates and status-quo powers prefer to cooperate.[18] According to Jervis, two factors determine this balance: military technology and geography.[19]

Based on the possible combinations of these two variables, Jervis proposes a "Four Worlds" model, according to which one can generalize the stability of the international system (see Figure 1).[20] This model depicts the world from the perspective of a status-quo power—an unstable world is a dangerous world, but revisionist states might instead see it as a world of opportunity. Although this idealized model eloquently distills international anarchy into four quadrants, Jervis explains that reality conforms to a continuum of possible magnitudes of the variables. Although reality is more nuanced than Jervis's basic model, the Four Worlds model nonetheless provides a succinct and coherent realist perspective for evaluating the conditions of the international system.

[18] Jervis, "Cooperation Under the Security Dilemma, " 188.

[19] Ibid., 194.

[20] Ibid., 211.

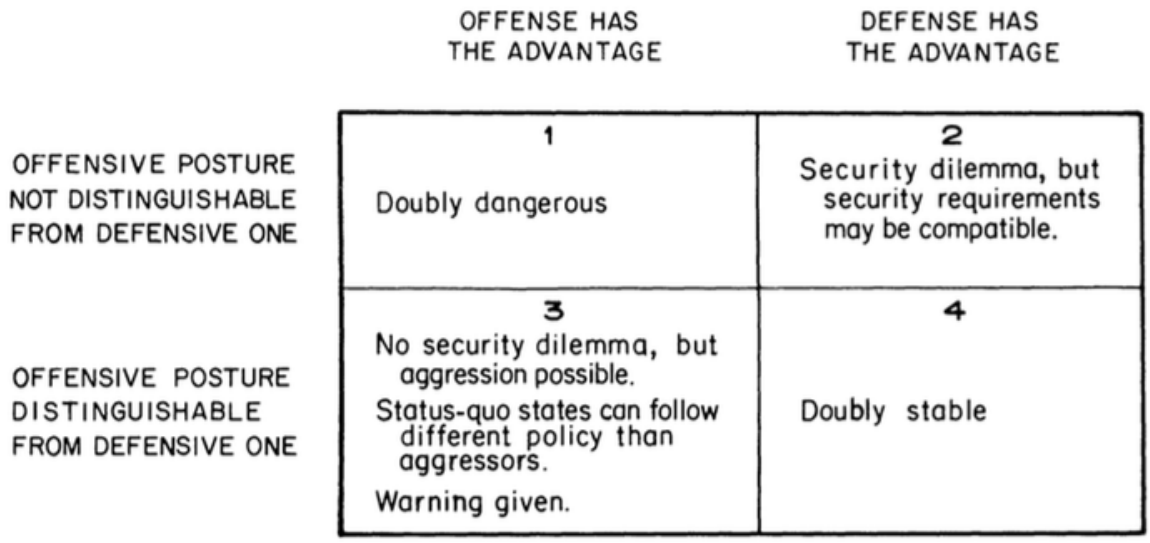

Figure 1. International Stability Outcomes Based on Jervis's Offense-Defense Theory.[21]

2. Critiques and Theoretical Variations

Since its publication over thirty-five years ago, Jervis's offense-defense theory has withstood critiques from some scholars, while other scholars have enriched its analytic, descriptive, and predictive depth. Sean M. Lynn-Jones summarizes the main criticisms of offense-defense theory and the corresponding rebuttals. Jervis's theory shares the underlying assumptions of realist international theory: a state of anarchy envelops the international system, states are self-reliant for security, and, although states may make mistakes, they act out of rational self-interest.[22] These fundamental assumptions and how they govern neorealist and neoliberal theory remain the subject of contemporary debate.[23]

In addition to these general criticisms, Lynn-Jones lists five specific objections. The first objection is that it is impossible to distinguish weapons as offensive or

[21] Jervis, "Cooperation Under the Security Dilemma, " 211.

[22] Sean M. Lynn-Jones, "Offense-Defense Theory and Its Critics," *Security Studies* 4, no. 4 (Summer 1995): 664-5. doi:10.1080/09636419509347600.

[23] Robert Powell, "Anarchy in International Relations Theory: The Neorealist-Neoliberal Debate Neorealism and its Critics. by Robert O. Keohane; Neorealism and Neoliberalism: The Contemporary Debate. by David A. Baldwin," *International Organization* 48, no. 2 (Spring 1994): 331-44, http://www.jstor.org/stable/2706934.

defensive.[24] Although this concern recognizes that most weapons systems contain offensive and defensive qualities, it overstates the resulting problem; despite the dual use of weapons, in practice, states still typically recognize which types of weapons are more cost advantageous for offensive operations, and which for defensive.[25] The second objection is that states fail to correctly perceive the offense-defense balance.[26] This concern, however, does not invalidate the theory—factors that cause states to incorrectly assess the situation are unit-level variables, and even if states miscalculate, offense-defense theory acknowledges that states base their actions on their individual perceptions, and not on universal objectivity.[27] Another critique suggests that Jervis misinterpreted the causal direction of international conflict—states create offensive and defensive advantages according to their strategic goals.[28] Though this criticism may have merit, concedes Lynn-Jones, it oversimplifies reality. In only rare cases does a single state shape the direction of military development to create its own singular advantage; even when a state obtains unique military technology, the diffusion of knowledge allows other states to emulate and achieve parity.[29]

Another set of criticisms contends that other variables and processes have a more dominant role in governing international conflict. Some claim that the offense-defense balance always favors defense—it is therefore a constant factor, not a variable one.[30] This criticism fails to recognize that the offense-defense balance is a continuum, with the relative advantage shrinking or growing at different historical periods, affording states the opportunity to concentrate resources to overcome the relative advantage of defensive weapons at that moment.[31] More importantly, even if the balance objectively favors defense at a given point in time, as famously illustrated by the offense-defense theory

[24] Lynn-Jones, "Offense-Defense Theory and Its Critics," 672-3.

[25] Ibid., 674-7.

[26] Ibid., 677-9.

[27] Ibid., 679-82.

[28] Ibid., 689.

[29] Ibid., 690.

[30] Ibid., 688.

[31] Ibid., 688-9.

analysis of World War I, states may still misinterpret the balance.[32] Another line of critique emphasizes the role of political intentions, distributions of power, and domestic dynamics as the driving forces of international instability.[33] The answer to these challenges, according to Lynn-Jones, is that these may be valid complementary explanations—such factors may bias states to act as either status-quo or revisionist actors, but the outcome of their foreign policy choices set by state-level dynamics will develop according to the international-level offense-defense balance.[34] In summary, although scholars have challenged Jervis, his work has withstood these criticisms, especially thanks to one of offense-defense theory's most powerful qualities—it incorporates subjectivity and uncertainty.

Subsequent scholarly work on offense-defense theory has strived to elucidate the challenges of subjectivity and uncertainty, allowing for greater accuracy and precision in measuring Jervis's critical variables. Charles Glaser and Chaim Kaufmann offer approaches for measuring the offense-defense balance. They propose a simple formula: a cost ratio of the forces an attacker must use to capture territory versus the cost of defensive forces to hold that territory. Based on this computation, "all else being equal, the larger this quotient, the greater the attacker's prospects for success."[35] They further nuance the offense-defense balance calculation as dependent on war objectives—modest territorial goals may be more tempting for aggressive states.[36] Glaser and Kaufman make another important observation: because of the complexity of contributing factors, it may be more meaningful to calculate dyadic, rather than systemic offense-defense balance, and it is valuable to consider the directional balance of a given dyad.[37] Because of this added measuring complexity, unlike Jervis's generalized offense-defense model that depends on technology and geography, Glaser and Kaufmann's measurement

[32] Lynn-Jones, "Offense-Defense Theory and Its Critics," 689.

[33] Ibid., 683.

[34] Ibid., 686-7.

[35] Charles L. Glaser and Chaim Kaufmann, "What Is the Offense-Defense Balance and Can We Measure It?," *International Security* 22, no. 4 (Spring 1998): 51, http://www.jstor.org/stable/2539240.

[36] Ibid., 53.

[37] Ibid., 57-9.

methodology also includes force size, nationalism, and cumulatively of resources, but excludes first-move advantage and alliance behavior. Despite these modifications, the authors conclude that ballpark estimates provide sufficient insight to accurately satisfy the offense-defense model.[38] Karen Ruth Adams's work confirms this conclusion. Her empirical study of armed conflict among great powers from 1800 to 1997 shows the statistical significance of what she describes as the offense-defense-deterrence balance: attacks on other states are less frequent and less successful in defense- and deterrence-dominant eras.[39]

Lastly, Stephen van Evera makes an important contribution to offense-defense theory by describing the mechanisms which may explain aggression in an offense-dominant world and evaluating these mechanisms' roles in historical conflicts. Like Adams, he finds that conflicts occurred as the theory predicts: in the last two centuries of European wars, conflicts occurred due to perceptions of offense dominance, the decline of international order throughout medieval China correlated with a shift toward offense dominance, and America's geographic security seems to have contributed to the United States' lower aggression.[40] Upon validating offense-defense theory's analytic power and analyzing in greater depth the mechanisms that influence aggression, van Evera also argues that the theory is especially valuable because of its wide real-world applicability.[41]

3. Applicability to Cyberspace

Due to its explanatory power and theoretical prominence alone, offense-defense theory is a worthy lens for evaluating the effect of cyber power on the international system. Many of the popular and scholarly discussions about cyber power often use offense-defense terminology without explicitly contextualizing it as such—commentators

---

[38] Glaser and Kaufmann, "What is the Offense-Defense Balance, " 78-9.

[39] Karen Ruth Adams, "Attack and Conquer? International Anarchy and the Offense-Defense-Deterrence Balance," *International Security* 28, no. 3 (Winter 2003/2004): 79-81, http://www.jstor.org/stable/4137477.

[40] Stephen van Evera, "Offense, Defense, and the Causes of War," *International Security* 22, no. 4 (Spring 1998): 36-9, http://www.jstor.org/stable/3539239.

[41] Ibid., 41.

refer to offense dominance, arms races, and power balance diffusion. These and other assertions about cyber power would benefit from analysis within an overarching theoretical framework.[42] As Dr. Wade L. Huntley suggests, a more systematic analysis of cyber power is necessary to validate what may be assumptions or false analogies about the relevance of cyber power in shaping the international system.[43]

Some scholars have begun to undertake this effort. Ilai Saltzman's 2013 article, "Cyber Posturing and the Offense-Defense Balance," reflects on the role of cyber power at the international level with an examination of activities by the United States, China, Russia, and NATO. His analysis shows that although it is necessary to modify some terminology to accommodate the nature of cyber weapons, an offense-defense theory analysis of cyber power yields insight into its distinct contributions to the overall balance of military power.[44] Whereas Saltzman considered the cyber offense-defense balance among three great powers, Patrick Malone proposes a model for calculating offense-defense cost ratios for various cyber attacks, showing that we can gain empirical insight into the balance of cyber weapons.[45] Both approaches show that a practical application of offense-defense theory to cyber power is meaningful and valuable.

The offense-defense theory approach to cyber power is not without its critics as well. Keir Lieber argues that in addition to offense-defense theory's conventional explanatory challenges, its utility in assessing cyber power is even more suspect because of cyber weapons' dubious effectiveness in achieving political ends.[46] Cyber weapons' secrecy, he argues, makes an arms race unlikely—states cannot respond to a secret weapons buildup.[47] According to his critique, although by analogy cyber weapons appear

---

[42] Wade L. Huntley, "Offense, Defense, and Cyber War" presented at the International Studies Association, Toronto, Canada (March 2014): 10.

[43] Ibid., 22-3.

[44] Ilai Saltzman, "Cyber Posturing and the Offense-Defense Balance," *Contemporary Security Policy* 34, no. 1 (2013): 40-63. doi: 10.1080/1352360/2013/771031.

[45] Patrick J. Malone, "Offense-Defense Balance in Cyberspace: A Proposed Model" (Naval Postgraduate School, 2012), http://hdl.handle.net/10945/27863.

[46] Keir Lieber, " The Offense-Defense Balance and Cyber Warfare," in *Cyber Analogies*. ed. Emily O. Goldman and John Arquilla (Monterey, California: Naval Postgraduate School, 2014): 103, http://hdl.handle.net/10945/40037.

[47] Ibid., 104.

to have offensive dominance, the qualitative nature of cyber power does not contribute to the security dilemma in the same fashion as conventional arms.

This thesis, however, assumes that offense-defense theory has sufficient explanatory capacity to incorporate cyber power as a facet of the overall balance of power among states. Furthermore, the theory's flexibility in incorporating secrecy, intentions, and ambiguity may be exactly the mechanisms strategists need to articulate the strategic effect of some of cyber weapons' problematic properties—attribution, secrecy, and perishability.

C. RESEARCH DESIGN

The role and nature of cyberspace in international relations (IR) is a subject of ongoing debate among policy makers, military planners, and subject matter experts. Although this theoretical debate is still inconclusive, this thesis forgoes the debate and assumes that defensive realism's concept of security dilemma applies to cyberspace. The value of this approach is that it provides a cyber power analysis that follows an existing IR paradigm and combines multiple facets of cyberspace development into a strategic assessment. Also, because the security dilemma applies to the international system, this approach affords an opportunity to compare and contrast Russia's behavior with expected state behavior.

Additionally, the quality and relevance of this thesis in assessing Russian cyber posture offers insight into the merits of offense-defense theory and validates the underlying assumption that existing IR concepts, specifically offense-defense balance, apply to cyberspace. This thesis is a practical application of IR concepts to cyber power. The quality of the author's efforts notwithstanding, this application of theory to an existing problem set may help gauge the applicability and relevance of offense-defense theory to cyberspace and help facilitate the theoretical debate about the nature of cyber power.

Robert Jervis defines two variables responsible for shaping the security dilemma: "whether defensive weapons and policies can be differentiated from offensive ones" and

"whether the offense or the defense has the advantage."[48] Jervis conceived this formula for an international level of analysis, but for clarity and applicability at the state level of analysis, the author adopts a modified definition. In this thesis, the author modifies the first variable, offense-defense differentiation, as Russia's cyber posture differentiation: can Russia's intentions be differentiated as either favoring offensive or defensive action? If a system level of analysis reveals that weapons and policies can be differentiated, then it is doubtful that a state-level analysis that merely narrows the scope of the question to that state's capability will provide additional insight—a state cannot change the fundamental property of weapons. Instead, at the state level it is more valuable to consider a state's posture and intentions. This differentiation among states, Jervis suggests, is beneficial for identifying status-quo and aggressor states, facilitating cooperation, or providing advanced warning.[49] By studying Russia's posture and intentions, one may be able to infer its role in the international system—whether it is exacerbating or abating the security dilemma.

The author also redefines Jervis's second variable, offense-defense advantage, as Russia's cyber force composition: does Russia invest in offensive or defensive capability? This definition results from extending Jervis's reasoning to the state level. At the international level of analysis, a world where offense dominates suggests that dollar for dollar, a state would rationally invest in offensive capability.[50] A state-level consequence of an offense-dominated world would be an international system in which states are armed with predominantly offensive weapons. To perform the same analysis bottom-up, at the state level, one would examine what category of weapons a state has chosen to invest in—offensive or defensive. The existing body of literature serves as the basis of Russia-related cyber weapons use. A consolidated analysis of this brandished, employed, and implied Russian cyber capability allows subsequent comparison of Russia against the international level, offering insight as to whether Russia is a status quo or a revisionist state. The same assessment of Russian capability may also serve as basis for

[48] Jervis, "Cooperation Under the Security Dilemma, " 186-7.

[49] Ibid,. 199-200.

[50] Ibid., 188.

dyadic comparison, perhaps forecasting if an arms race between Russia and a specific state is likely.

Based on these modified variables, this thesis makes the following four mutually exclusive hypotheses, according to Jervis's Four Worlds model:[51]

> H1. *Russia's cyber capability is offensive and the posture is indistinguishable as either offensive or defensive.*
>
> H2. *Russia's cyber capability is defensive and the posture is indistinguishable as either offensive or defensive.*
>
> H3. *Russia's cyber capability is offensive and the posture is distinguishable as either offensive or defensive.*
>
> H4. *Russia's cyber capability is defensive and the posture is distinguishable as either offensive or defensive.*

Another outcome of the research—the failure to produce substantive analysis—is possible:

> H5. *The unique properties of cyberspace preclude meaningful offense-defense theory analysis.*

Although this hypothesis would fail to provide insight into Russia's cyber capability, this failure may nonetheless provide useful insight about cyber power—if neither the analysis, evidence, nor method are faulty, then perhaps cyber power introduces unique challenges and factors that confound existing theoretical understanding of the security dilemma.

In addition to altering Jervis's variables to permit a state-level analysis, this thesis also proposes a different definition of geography. "Technology and geography," according to Jervis, "are the two main factors that determine whether the offense or the defense has the advantage."[52] Unlike technology, evaluating geography in cyberspace is inherently problematic—most definitions of cyberspace not only consider it a manmade domain, but also a virtual domain. This thesis adopts the Department of Defense's

[51] Jervis, "Cooperation Under the Security Dilemma, " 211-4.

[52] Ibid., 194.

definition of cyberspace: it is a global domain within the information environment that consists of three layers—physical, logical, and cyber persona.[53] Only the physical network layer has a geographic component, but the other layers also have their own relational topologies among and within other layers that may be more relevant to the efficacy of offense and defense than the topography of physical nodes and links that enable operations in cyberspace. Future technological developments in information technology will likely make it even more difficult to conceive of cyber geography. One such development, cloud computing, will further abstract cyberspace apart from physical geography by creating a distributed, dynamic, and ubiquitous resource pool for scalable, on-demand computing.[54] This evolution of computing will increasingly obfuscate the relationship between the physical, logical, and persona layers of cyberspace, necessitating a broad definition.

Because cyber geography is so different from physical geography, one may choose to modify Jervis's theory as applied to cyberspace by discarding geography as an analytic factor, or it may be possible to consider a metaphor for geography in cyberspace.[55] This thesis adopts the notion of a cyber geography that considers all three layers of cyberspace as cyber terrain, with differentiable security boundaries, mobility factors, attribution, and perishability. Thus, cyber terrain may be mapped out with metaphorical mobility corridors, high ground, key objectives, and barriers at the tactical and strategic levels. For the purpose of offense-defense analysis, however, only the strategic view of cyber terrain is useful. That is, this thesis's analysis only concerns with attributes of cyberspace within the jurisdiction of a state that are differentiable from cyberspace within the jurisdiction of other states. A trivial illustration of such differentiation is the unique Internet Protocol address scheme assigned to states by the Internet Corporation for Assigned Names and Numbers that maps national sovereignty to

---

[53] Joint Publication 3-12, "Cyberspace Operations," (Washington D.C.: Joint Chiefs of Staff, 2013), v, http://www.dtic.mil/doctrine/new_pubs/jp3_12R.pdf.

[54] Peter Mell and Timothy Grance, "NIST Special Publication 800-145: The NIST Definition of Cloud Computing," National Institute of Standards and Technology, U.S. Department of Commerce (2011): 2-3, http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf.

[55] Huntley, "Offense, Defense, and Cyber War," 16-7.

cyber coordinates. A more sophisticated international-level example of cyber terrain may be a state-managed firewall that regulates Internet traffic exchanged between its cyber resources and other states' cyber resources. An encryption protocol used by a sizable portion of Internet users across the world may be an example of a distinctive cyber mobility corridor that affects international cyber power. Just based on these three examples, it is apparent that an innumerable multitude of technical implementations may shape cyber geography, but the subjective task of this thesis is to identify cyber terrain features that both differentiate the totality of Russian cyberspace from the global cyberspace and influence whether offense or defense has the advantage.

II. RUSSIAN CYBER CAPABILITY

This chapter seeks to determine whether Russian cyber capability favors offense or defense. Following Robert Jervis' offense-defense theory formulation, this analysis considers two factors: cyber technology and cyber geography.[56]

First, this analysis of cyber technology is broader than strictly an evaluation of the Russian military's cyber capabilities—the militaries of states are latecomers to an international system that perhaps resembles the anarchic pre-Westphalian dispersal of power. The current state of cyber power, as Joseph S. Nye, Jr. argues, predisposes a diffusion of power within the cyber domain; non-state actors have very low barriers for obtaining and using offensive weapons.[57] The Russian government, therefore, may not strictly monopolize Russian cyber power, but may rely on other sources of domestic cyber power, exercising varying degrees of control over its proxies' methods, objectives, and actions. The author's underlying assumption throughout this thesis, therefore, is that as long as cyber power is exercised in a manner that supports the Russian Federation's objectives, it is unimportant whether the actors are uniformed military, security agents, mercenaries, coerced businesses, or other proxies. After all, other states, according to offense-defense theory logic, react based on their subjective, inherently pessimistic perceptions of these Russian-associated applications of cyber power. Furthermore, recent demonstrations of Russia's hybrid warfare military strategy in Ukraine illustrate the link between state and proxy actors, providing a practical validation to suspicions of surrogate actors. Therefore, when considering technology, this paper takes a broad view of the types of offensive cyber operations and the actors that undertake them that constitute Russia's cyber capability.

Second, this chapter places an emphasis on analyzing Russia's cyber geography (as defined in the introduction); since cyberspace is a manmade domain its geography is malleable. How Russia shapes its cyber terrain may as telling of its offensive or defensive

---

[56] Jervis, "Cooperation Under the Security Dilemma, " 194.

[57] Joseph S. Nye, Jr., "Cyber Power," Harvard Kennedy School, (Cambridge, MA: Harvard, 2010), http://belfercenter.ksg.harvard.edu/files/cyber-power.pdf.

capability as is its technological capability. Robert Jervis describes various manmade barriers as imitations of geographic obstacles and this logic has a very pronounced effect in cyberspace.[58] Despite the often-touted ubiquity of the Internet, the topology of long-haul communications links, access aggregation by Internet service providers, and country-specific IP space allocation schemes provide states with a technical means to circumscribe their national cyberspace. The People's Republic of China's notorious Great Firewall of China, for example, controls ingress and egress to Chinese cyberspace according to both, traffic origin and destination, and traffic content.[59] Additionally, various communications standards within a segment of cyberspace, such as encryption layers or authentication protocols, can affect user and data attribution. A state's choices in developing its cyber geography, much like its decisions to invest in minefields, demilitarized buffer zones, or off-gauge railroad tracks, affect its offensive or defensive capability.

A. CASE STUDIES

Following a broad definition of technological capability, this section examines a variety of cyber events perpetrated by or attributed to Russian actors and argues that although secrecy, according to Martin Libicki, constrains a state's ability to brandish cyber weapons, these attacks nonetheless suggest a pattern of state sponsorship and therefore exemplify Russian cyber capability.[60] The first section of this chapter evaluates the 2007 cyber attacks on Estonia, the cyber campaign that paralleled the 2008 Russo-Georgian War, and the 2014 Ukraine crisis. Additionally, this case study analysis considers the technological capacity of Russian cyber criminals and intelligence services.

---

[58] Jervis, "Cooperation Under the Security Dilemma, " 195.

[59] Ben Elgin and Bruce Einhorn, "The Great Firewall of China," *Bloomberg Business*, January 22, 2006, http://www.bloomberg.com/bw/stories/2006-01-22/the-great-firewall-of-china.

[60] Martin C. Libicki, "Brandishing Cyberattack Capabilities," RAND National Defense Institute, (Santa Monica, CA: RAND, 2013), http://www.rand.org/content/dam/rand/pubs/research_reports/RR100/RR175/RAND_RR175.pdf.

1. 2007 Estonia Cyber Attacks

In April 2007, nationalist tensions between Estonians and the ethnic Russian minority in Tallinn, Estonia culminated in what many observers and commentators have since considered a historic cyber event. These nationalist tensions initially centered on a World War II memorial honoring Soviet troops—to Estonians the memorial represented a vestige of Soviet occupation, whereas to the Russian minority it commemorated the sacrifice and heroism of the Great Patriotic War. Frustrated with their perceived marginalization in Estonian society, local Russians embraced the statue as a symbol of their plight. Throughout the spring of 2007, the situation in Tallinn deteriorated; displays of Russian nationalist pride at the Bronze Soldier memorial escalated into provocations, hooliganism, and eventually led to street violence and riots. Pro-Russian cyber attackers conducted a three-week campaign attacking Estonia's cyber infrastructure concurrently with the physical riots in Estonia.[61]

The technical characterization of the cyber attacks varied from low to moderate levels of sophistication. The first wave of attacks used basic Denial of Service (DoS) tactics and showed little coordination and target selection. NATO's Cooperative Cyber Defense Center of Excellence synopsis of the attacks in *International Cyber Incidents: Legal Considerations* bluntly describes the initial attacks as "simple, ineptly coordinated, and easily mitigated."[62] In contrast, the attacks that followed beginning on April 30 used more sophisticated Distributed DoS (DDoS) tools and demonstrated centralized command and control that effectively shifted among targets and concentrated attacker firepower. Throughout the initial DoS and the later DDoS phase of the cyber campaign, pro-Russian attackers also conducted website defacements and spamming, phishing, and personal harassment of Estonian victims.[63]

The variety of cyber attacks resulted in a corresponding variety of effects. Many of the low sophistication attacks were little more than a nuisance to their targets and to

---

[61] Ottis, "Analysis of the 2007 Cyber Attacks,"163.

[62] Tikk et al., *International Cyber Incidents*, 19.

[63] Ibid., 23.

Estonia's Computer Emergency Response Team (CERT).[64] The DDoS attacks on the media and financial organizations, however, resulted in a disruption of online financial services and strategic communication isolation from the rest of the world.[65] Despite accomplishing these technical effects, it is unclear that the campaign achieved a strategic objective.

One potential strategic objective may have been to compel the Estonian government to reverse its decision to return the Bronze Soldier statue to its previous place, which it did not do. If the attackers' objective was instead to cause economic harm to Estonia, this effect is difficult to measure outright—the losses from the disruptions had a notable effect on Estonia economy, but no businesses declared or claimed financial loses.[66] Although the net effect of the attacks may be difficult to ascertain, the attacks nonetheless offer an opportunity to calculate the relative cost ratio of the offensive and defensive actions, in order to better determine whether offensive or defensive weapons dominate. In his proposed model for calculating the offense-defense cost ratio in cyberspace, Patrick Malone estimates that for every dollar expended by attackers, Estonian defenders spent $424.[67] This degree of cost disparity suggests that cyber attacks such as the one against Estonia, despite dubious strategic effectiveness, may entice Russia and other states to act aggressively.

Although the cyber attacks against Estonia have not been attributed to the Russian government, circumstantially, they reflected Russian state interests. As the Bronze Soldier crisis developed within Estonia, the Russian Federation signaled its stake in a pro-Russian resolution of Estonia's domestic conflict. Prior to the eruption of violence, the Russian foreign ministry expressed Russia's position by issuing a protest about the Estonian government's plan to relocate the Bronze Soldier Memorial to a less prominent location. Once physical violence and cyber attacks commenced, the Russian Federation Council advocated freezing diplomatic ties with Estonia and wanted to impose economic

64 Tikk et al., *International Cyber Incidents*, 21.

65 Ibid., 20, 22, 25.

66 Ibid., 22, 25.

67 Malone, "Offense-Defense Balance in Cyberspace, " 53.

sanctions. Within the Russian Federation, police failed to protect the Estonian embassy when Russian youth groups physically attacked the compound and Estonian staff. An unofficial blockade disrupted trade on the Russian-Estonian border. Russian involvement in the conflict eventually prompted German Chancellor Angela Merkel to engage Russian President Vladimir Putin, discouraging official and unofficial Russian involvement.[68] This level of political commitment to the event on part of the Russian state, as well as the use of various soft instruments of power to coerce the Estonian government, are suggestive of a scenario in which Russia and other states may employ non-attributable cyber weapons to attempt to coerce, punish, or at least disorient another state.

The cyber attacks against Estonia serve as a valuable illustration within the context of offense-defense theory. Once the attacks reached moderate technical sophistication and coordination, they had a detrimental effect that the defenders struggled to counter. Perhaps more importantly, the attacks also adversely affected the Estonian government's ability to provide public services, disrupted civil society, and complicated the government's response to the underlying ethnic conflict. The attacks had another notable characteristic; the disruptions caused by the attacks lasted only as long as the attacks themselves. Unlike physical weapons, the cyber weapons used in this conflict resulted in little tangible or lasting damage; the attacks temporarily denied access to cyber resources, but did not destroy physical property or data. Though tactically successful, the attacks did not lead to a pro-Russian outcome; the Estonian government did not reverse its decision to move the Bronze Soldier statue to its new location. Although these attacks demonstrated that offense had the advantage at a tactical level, aggressive action, even when successful, resulted in limited pay-off.

The attacks also illustrated the importance of cyber geography. As an early and enthusiastic implementer of online commerce and civil society, Estonia was an inviting target for cyber attacks. After the incident, Estonia's cyber dependency became a cautionary example to the international community and hastened many states' efforts to

---

[68] Mathias Roth, *Bilateral Disputes between EU Member States and Russia*, CEPS Working Document (Centre for European Policy Studies, August 2009): 13-5, http://www.ceps.eu/files/book/2009/09/1900.pdf.

implement security countermeasures, especially in critical infrastructure. The attacks also demonstrated the discontinuity between physical and cyber borders; potential avenues of attack in cyberspace may be innumerable. The DDoS attacks against Estonia harnessed cyber resources from across the globe—to effectively defend against such attacks, defensive countermeasures needed to be not merely a national, but an international endeavor.[69]

2. 2008 Russo–Georgian War

The 2008 Russo–Georgian War was an important milestone in the use of cyber power; cyber attacks contributed to, and in several instances complemented, Russia's military campaign in an unprecedented fashion.[70] The interstate conflict was a continuation of nationalist ambitions of two Georgian regions, Abkhazia and South Ossetia. After a brief independence struggle subsequent to the dissolution of the USSR, these regions enjoyed de facto autonomy. Since then, joint Georgian and Russian peacekeeping forces maintained stability in South Ossetia. In August of 2008, however, after a series of cross-demilitarized zone provocations, the Georgian army invaded South Ossetia, capturing its capital. Russian forces that were regionally prepositioned thanks to exercises earlier that summer counterattacked, and within five days forced a cease-fire. Throughout the brief military engagement, a formally unacknowledged cyber campaign showed "Moscow's readiness to use asymmetric, as well as conventional means to achieve its goals."[71]

The cyber weapons and tactics employed against Georgia during the Russo-Georgian War were similar to, but more sophisticated than those used against Estonia in 2007. Botnet-perpetrated distributed denials of service attacks, along with targeted website defacements, comprised the mainstay of the offensive cyber weapons. Though the use of botnets to conduct DDoS attacks is increasingly a less sophisticated

---

[69] Tikk et al., *International Cyber Incidents*, 17-8, 25.

[70] David Hollis, "Cyberwar Case Study: Georgia 2008," *Small Wars Journal*. January 6, (2011): 2, http://smallwarsjournal.com/blog/journal/docs-temp/639-hollis.pdf.

[71] "Russia's Rapid Reaction," *Strategic Comments* 14, no. 7 (2008): 1. doi: 10.1080/13567880802482243.

endeavor—a black market exists for botnets for hire—the way DDoS attacks were conducted against Georgia showed an uncharacteristic level of sophistication. On July 19, a potential rehearsal attack using a thereto unknown botnet targeted the Georgian President's website—an attack profile atypical of common cybercrime.[72] Throughout the cyber campaign, attackers showed a high degree of command and control; they conducted training for participants, prioritized targets, distributed tools, and de-conflicted and synchronized attacks.[73] Unlike in Estonia, however, pro-Georgian actors retaliated with similar, but lower volume cyber attacks.[74] Overall, though the cyber attacks against Georgia showed higher sophistication than those used against Estonia, the technological sophistication of the tactics and tools was nonetheless at a low or moderate level.

The Russian Federation attained its limited strategic goals during the Russo-Georgian War, but it is unclear whether cyber attacks effectively contributed to Russia's strategic ends. As in Estonia, the attacks had the ephemeral effect of disrupting target government, media, and financial websites.[75] Efforts to digitally isolate Georgia led some analysts to compare the strategic effect to a cyber blockade, but in practice such a blockade only affected few—less than 10% of Georgians had access to the Internet, much less relied on it for government services and strategic communication.[76] Additionally, with international support, Georgians reacted rapidly to relocate their effected cyber resources to third-party states, overcoming Russian efforts to isolate them.[77] Following the war, influential Russian analysts like Igor Panarin assessed that, despite the disruption

---

[72] Eneken Tikk, Kadri Kaska, Kristel Rünnimeri, Mari Kert, Anna-Maria Talihärm, and Liis Vihul, *Cyber Attacks Against Georgia: Legal Lessons Identified,* (Tallinn: Cooperative Cyber Defense Centre of Excellence, 2008), accessed March 25, 2014, 46, http://www.carlisle.army.mil/DIME/documents/Georgia%201%200.pdf.

[73] Ibid., 9, 38.

[74] Hollis, "Cyberwar Case Study," 2.

[75] Tikk et al., *Cyber Attacks Against Georgia*, 37-8.

[76] Tikk et al., *Cyber Attacks Against Georgia*, 11; Hollis, "Cyberwar," 5; Tikk, *International Cyber Incidents, 68.*

[77] Paul A. Goble, "Defining Victory and Defeat: The Information War Between Russia and Georgia," in *The Guns of August 2008: Russia War in Georgia*, edited by Svantee E. Cornell and S. Frederick Starr (Armonk, N.Y.: M.E. Sharpe, 2009), 191.

of Georgian strategic communication with cyber attacks, Russia lost the broader information campaign during the Russo-Georgian War.[78]

Although the 2008 cyber attacks against Georgia seemingly supported the Russian Federation's military and political objectives, the Russian government has not acknowledged or claimed responsibility for the attacks. Despite the Georgian government's accusation that the Russian government sponsored the cyber campaign, analyst consensus maintains that no positive attacker linkage to the Russian government can be made, but "the historical record shows clear support of the Russian government and implied consent in its refusal to intervene or stop the hacker attacks."[79] Similar to the Estonia case, although the cyber attacks seemingly aligned with state interests, if the Russian state sponsored the attacks, it did so clandestinely.

Just like the distributed denial of services attacks against Estonia, the DDoS attacks against Georgia overwhelmed the targets' defensive capacity and the Georgian cyber security experts' technical ability to mitigate the attacks. At the tactical level, when employed as a first strike, the technology appeared to favor the offense. After the initial shock of the attacks dissipated, Georgians found that the simpler online services—government websites, but not electronic banking centers—could be easily re-provisioned on more robust third party servers. Although the attacks against Georgia demonstrated that offensive use of DDoS cyber weapons dominated defensive countermeasures, the attacks also revealed their limited value: defenders' resilience showed that attackers can expect disruption and denial effects of cyber-attacks to have a limited duration.

Unlike Estonian cyber infrastructure, Georgia's Internet presence and reliance on online services at the time of the Russo–Georgian War was very limited. Importantly, this limited domestic infrastructure connected to the Internet via either Russian or Turkish Internet service providers.[80] This limited path diversity further skewed the offense-defense balance in favor of the attackers who were accused of using this path bottleneck

---

[78] Goble, "Defining Victory and Defeat," 193-4.

[79] Tikk et al., *Cyber Attacks Against Georgia*, 45; "Russia/Georgia Cyber War," 9.

[80] Tikk et al., *Cyber Attacks Against Georgia*, 5-6.

to manipulate Georgian Internet traffic, enabling a cyber blockade not only logically through DDoS, but also by logically restricting or redirecting the physical flow of data. Although Georgian defenders found themselves overwhelmed by the offensive cyber weapons, they showed defensive resilience by exploiting a defining property of cyberspace, its manmade nature. Once pro-Russian hackers disabled Georgia's government sites, Georgians simply restored those sites on more defensible third-party cyber terrain.

Despite the offensive dominance of the cyber weapons employed during the conflicts, defenders also demonstrated that maneuver and resilience in cyberspace might be a more effective countermeasure than the direct defensive methods attempted a year earlier by Estonia's CERT. This observation does not imply that defense ultimately dominates offense in cyberspace, but instead that offensive cyber operations have ephemeral effects—they do not take and hold ground. The lesson for strategists, therefore, may be that cyber attacks produce a narrow effect window and require precise timing; if used indiscriminately, cyber attacks lose their value as defenders will likely mitigate the attack vector and reconstitute their services in a more defensible configuration. Alternately, low sophistication cyber attacks may simply be used to disrupt the adversary's military decision making process by adding another line of operations that defenders must react to. Five and a half years after the Russo-Georgian conflict, some of these lessons about effective application of cyber power appeared in the 2014 Russian-Ukrainian Conflict.

3. 2014 Russian–Ukrainian Conflict

The conflict between Russia and Ukraine that began in earnest after former Ukrainian President Viktor Yanukovich fled from office in February 2014 has been considered by many observers as typifying Russia's recently articulated hybrid warfare concept. Hybrid, or non-linear war, relies on operations across the full spectrum of instruments of power applied by regular and irregular forces, and cyber and information

operations are an integral element of this multifaceted strategy.[81] The Ukrainian conflict may be seen as the most contemporary refinement of the cyber power lessons from the Estonian and Georgian conflicts: offensive cyber operations conducted by Russian surrogates have undermined Ukrainian state legitimacy, embarrassed NATO allies, and intimidated opposition forces.

A wide variety of cyber operations have been conducted throughout the Russian-Ukrainian conflict, demonstrating a high degree of operational and tactical flexibility at the low, moderate, and high levels of technological sophistication. The pro-Russian, Ukrainian-based CyberBerkut hacker group claims many such accomplishments: the disruption of German government websites, intercept of U.S. –Ukrainian military cooperation documents, interference in the Ukrainian elections, DDoS attacks against NATO websites, blocking of Ukrainian government and media websites, and various negative messaging campaigns slandering pro-Ukrainian targets.[82] Other pro-Russian cyber actors leaked embarrassing telephone call transcripts, physically disrupted telecommunications infrastructure, blocked mobile phone communications of political leaders, and exfiltrated sensitive data from Ukrainian government computers.[83] Despite this variety of attack types, security experts speculate that the full arsenal of Russian cyber capability was not demonstrated, and that attack sophistication remained proportional to Russia's limited political objectives and concurrent military operations.[84]

The net effect of the cyber campaign appears to have positively contributed to the Russian strategy in Ukraine. The Russian formulation of hybrid war, according to the unofficial Gerasimov doctrine, relies on the information space—the Russian

---

[81] Mark Galeotti, "The 'Gerasimov Doctrine' and Russian Non-Linear War," *In Moscow's Shadows*, July 6, 2014, https://inmoscowsshadows.wordpress.com/2014/07/06/the-gerasimov-doctrine-and-russian-non-linear-war/.

[82] CyberBerkut, accessed February 12, 2014, http://cyber-berkut.org/en/.

[83] Daisy Sindelar, "Brussels, Kyiv, Moscow React to Leaked Nuland Phone Call," *Radio Free Europe/Radio Liberty*, February 7, 2014, sec. Ukraine, http://www.rferl.org/content/nuland-russia-eu-ukraine-reaction/25256828.html; Tim Maurer and Scott Janz, "The Russia-Ukraine Conflict: Cyber and Information Warfare in a Regional Context," October 17, 2014, http://www.isn.ethz.ch/Digital-Library/Articles/Detail/?id=184345.

[84] David Lee, "Russia and Ukraine in Cyber 'Stand-Off,'" *BBC News*, March 5, 2014, sec. Technology, http://www.bbc.com/news/technology-26447200.

terminological analogue to cyberspace—for "reducing the fighting potential of the enemy…influencing state structures and the population."[85] For example, efforts to influence Ukrainian parliamentary elections with DDoS attacks and a successful hack of Ukraine's Central Election Commission network prior to the Presidential election did not lead to a pro-Russian outcome, but likely undermined electoral legitimacy as perceived by Ukrainians and Russians.[86] Similarly, the intrusion into Ukraine's telecommunication system and release of U.S. Assistant Secretary of State Victoria Nuland's controversial telephone conversation with the U.S. Ambassador to Ukraine, Geoffrey Pyatt, created diplomatic embarrassment for the United States and possibly served to intimidate Ukraine's other international supporters. Unlike such targeted, sophisticated cyber attacks, lower sophistication attacks like DDoS and site defacements, seem to have had little effect and instead led to retaliatory DDoS and defacement strikes by pro-Ukrainian actors.[87] Through early 2015, Russia appears to have succeeded in its objectives in Crimea, and the cyber campaign contributed to this achievement, establishing Russian information dominance that limited Ukrainian command and control and facilitated pro-Russian messaging.

During the Estonia and Georgia cyber conflicts, direct attribution of pro-Russian cyber attacks to the Russian state proved impossible, and this aspect of cyber warfare was also true of the Ukrainian conflict. As before, Kremlin has denied involvement or sponsorship of the cyber attackers despite the obvious alignment with state interests. Additionally, Russians' reliance on irregular and covert ground troops during the conflict in order to establish plausible deniability and thwart retaliation mirrors the attribution

---

[85] Galeotti, "'Gerasimov Doctrine.'"

[86] "Hackers Target Ukraine's Election Website," *Agence France-Presse*, October 25, 2014, sec. Network Security, http://www.securityweek.com/hackers-target-ukraines-election-website; Anna Mihalenko, "Rigged Presidential Elections in Ukraine? Cyber Attack on the Central Election Commission," *Glboal Research*, May 26, 2014, http://www.globalresearch.ca/rigged-presidential-elections-in-ukraine-cyber-attack-on-the-central-election-commission/5383843.

[87] Jen Weedon and Laura Galante, "Intelligence Analysts Dissect the Headlines: Russia, Hackers, Cyberwar! Not So Fast," *FireEye Executive Perspectives*, March 12, 2014, https://www.fireeye.com/blog/executive-perspective/2014/03/intel-analysts-dissect-the-headlines-russia-hackers-cyberwar-not-so-fast.html.

difficulty in cyberspace. According to both its doctrine and actual force employment, Russian military capability should be understood as intentionally obfuscating the military means used to achieve political ends. Because during the Ukraine conflict Russia demonstrated that it sought to benefit from attribution uncertainty throughout the spectrum of its instruments of power, by relying on covert and perhaps perfidious tactics Russia will likely cause other states to view potential pro-Russian actions with greater suspicion. Russian plausible deniability has lost credibility, and, therefore, despite difficulty in positive attribution, future cyber attacks matching pro-Russian attack profiles may become de facto attributed to Russia.

The reporting of cyber operations during the ongoing Ukrainian conflict has been a narrative of successful offensive cyber operations. In March 2014, prior to the annexation of Crimea, security experts from FireEye predicted that Russian cyber strategy will be more subtle and sophisticated than the Russian-affiliated previous attacks against Estonia and Georgia, and that "Moscow is more likely to use narrowly focused, limited operations in support of strategic state objectives."[88] Though this prediction insightfully anticipated the use of more sophisticated attacks types, they may have overestimated the Russian government's ability to control its proxies; CyberBerkut, for example, has relied on seemingly senseless DDoS attacks against non-strategic targets. As the result, the use of low sophistication DDoS and defacements precipitated a pro-Ukrainian response in kind.[89] In contrast, sophisticated attacks against Ukrainian targets, such as a Snake/Uroboros malware exploits of government computers and jamming of Ukrainian parliamentarians' cell phones, appear to have succeeded without triggering analogous retaliation. Unfortunately, thus far, little has been reported about failed cyber attacks by each side, so it is difficult to identify instances in which defenders triumphed. As in previous cyber conflicts, the conflict in Ukraine demonstrated the dominance of offensive cyber weapons, but it has also shown a vulnerability to retaliation once widely available cyber weapons are launched. If the Russian government intentionally refrained from cyber escalation, as predicted by FireEye security experts, this may imply a Russian

[88] Weedon and Galante, "Intelligence Analysts Dissect the Headlines. "

[89] Ibid.

perception that cyber weapons may provide a punitive deterrent. Such perceptions may contribute to explaining Russian investments in hardening its cyber terrain and passing reforms that limit diffusion of cyber power to Russian non-state actors over whom the state may not exercise sufficient control.[90]

Lastly, according to the Freedom House assessment of Internet Freedom Status, though Internet use in Ukraine was not universal, and despite some efforts by the government to restrict Internet access, Ukrainians enjoyed a robust and open Internet prior to the conflict.[91] Unlike Georgians, who could only access the Internet by traversing Russian and Turkish infrastructure, Ukraine's ISPs were decentralized and had both terrestrial and satellite path diversity to the rest of the world.[92] This relative openness of Ukraine's cyberspace likely encouraged the continuous, broad range of cyber attacks within the country, including attacks by pro-Russian groups like CyberBerkut that claim to operate from within Ukraine. Unlike in Georgia in 2008, no attempts to isolate Ukraine in cyberspace have been reported. Instead, pro-Russian forces targeted key cyber terrain, such as the election system and the Crimean telecom infrastructure, at operationally decisive points. Most notably, as the Crimean invasion culminated, Russian Special Forces and Russian Military Intelligence contributed to the cyber campaign with physical operations designed to produce cyber effects; they installed data intercept devices and physically isolated Crimean Internet and telecommunications infrastructure, demonstrating the synergistic potential of operations synchronize among the cyber and other warfighting domains.[93] To date, the cyber campaigns against Ukraine demonstrated the vulnerability of an open national cyberspace and the value of cyber operations synchronized with ground objectives.

---

[90] [Evidence of these developments, such as investments such as content filtering systems and anti-cybercrime law enforcement efforts, is addressed at greater length in subsequent sections and in Chapter 3.]

[91] Sanja Kelly et al., *Freedom on the Net 2014*, Freedom on the Net (Freedom House, 2014): 820-1, https://freedomhouse.org/sites/default/files/FOTN_2014_Full_Report_compressedv2_0.pdf.

[92] Ibid., 830-2.

[93] "The Ukrainian Crisis – a Cyber Warfare Battlefield," *Defense Update*, April 5, 2014, http://defense-update.com/20140405_ukrainian-crisis-cyber-warfare-battlefield.html.

4. Other Sources of Cyber Capability

The cyber attacks against Estonia, Georgia, and Ukraine, assumed by the author to have been applications of Russian cyber power to achieve state interests, serve as examples of capability brandished by Russia. In addition to these overt cases, insight into Russian cyber capability can be gained from considering the capability of Russian cyber criminals and by making reasonable estimates about the capabilities of Russian intelligence services.

a. Cybercrime

After the 2008 Russo-Georgian Cyber War, security analysts concluded that the botnets used in the attack mimicked, or more likely, belonged to the Russian Business Network (RBN), a cybercriminal organization that gained notoriety in 2007 and 2008.[94] During the conflict, the RBN also likely performed hacks against Georgia's routing infrastructure in an effort to complement the attempted cyber blockade.[95] Additionally, RBN hosted the Internet forums that were so essential to the command and control of the cyber attacks, providing a so-called bulletproof hosting that gave attacker anonymity from security investigators and CERT responders.[96] Although it is unclear under what conditions RBN's resources were mobilized against Georgia, their resources played a key role in the cyber portion of the conflict.

Since 2008, the Russian Business Network faded from prominence, but Russia remains a hotspot of cybercrime. Cybercrime is a term that encompasses a broad range of illegal activities such as media piracy, child pornography distribution, and identity theft. Certain types of cybercrime tools and tactics can also double as offensive cyber

---

[94] *Project Grey Goose Phase II Report: The Evolving State of Cyber Warfare* (GreyLogic, March 20, 2009): 4, http://fserror.com/pdf/GreyGoose2.pdf.

[95] John Markoff, "Before the Gunfire, Cyberattacks," *New York Times*, August 12, 2008, New York edition, sec. Technology, http://www.nytimes.com/2008/08/13/technology/13cyber.html?_r=1&; "RBN (Russian Business Network) Now Nationalized, Invades Georgia Cyber Space," *Russian Business Network*, August 9, 2008, RBN (Russian Business Network) now nationalized, invades Georgia Cyber Space, http://rbnexploit.blogspot.com/2008/08/rbn-georgia-cyberwarfare.html.

[96] *Project Grey Goose Phase II Report*, 15-7; "RBN - Georgia Cyberwarfare - Status and Attribution," *Russian Business Network*, August 9, 2008, http://rbnexploit.blogspot.com/2008/08/rbn-georgia-cyberwarfare-status-and.html; "RBN - Russian Cyberwar on Georgia: Report," *Russian Business Network*, October 2, 2008, http://rbnexploit.blogspot.com/2008/10/rbn-russian-cyberwar-on-georgia.html.

operations. Botnets for rent, for example, can be used for conducting DDoS attacks, and malware droppers might also be used to gain remote access to a system in order to deliver a malicious payload or induce destructive system behavior. According to a Trend Micro analysis of the Russian cybercrime economy, today's Russian cyber criminals specialize in for-purchase traffic direction systems (TDS)—tools that steer legitimate Internet traffic toward sites that conduct specific follow-on attacks.[97] Though TDS is their current specialty, Russian cybercriminals also develop and sell other services that can be used for conducting a cyber attack: malware, exploit kits, bulletproof hosting, anonymizer services, hacking services, and DDoS attacks-by-the-hour.[98]

Although other countries, including the United States, also suffer from cybercrime, the Russian government stands out as a potential consumer of its cybercriminal underground. As the Georgian conflict illustrated, pro-Russian non-state actors like the Nashi Youth organization likely served as proxies who either purchased or coopted criminal-developed cyber weapons.[99] The Russian government has been criticized for its semi-permissive approach toward cybercrime, and this lax stance may reflect a deliberate intent to cultivate "an ecosystem of cybercrime" that may be mobilized to serve state interests during conflicts, avoiding direct attribution to the state.[100]

b. State Capabilities

Analysis of Russian cyber capability often alludes to presumed advanced technology and tradecraft of the Federal Security Services, Foreign Intelligence Service, and the Main Intelligence Directorate of the General Staff of the Armed Forces. Because these organizations operate with a high degree of secrecy, very little information on their

---

[97] Max Goncharov, *Russian Underground Revisited*, CyberCriminal Underground Economy Series (Trend Micro, 2014): 4, 7-8, http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-russian-underground-revisited.pdf.

[98] Ibid., 16-8.

[99] *Project Grey Goose Phase II Report*, 5.

[100] Ronald Deibert, "Tracking the Emerging Arms Race in Cyberspace." Interview, *Bulletin of the Atomic Scientists* 67, no. 1 (January/February 2011): 4.

capability is available, and capability analysis requires assumptions about capabilities that these organizations can be reasonably expected to possess.

Unlike the highly publicized, persistent cyber espionage against America by Chinese state actors, Russian intelligence agencies have maintained a stealthy cyber profile. When describing the cyber threat to the nation, U.S. officials often refer to Russia as a potentially highly sophisticated cyber adversary capable, according to Director of National Intelligence James Clapper, of carrying out attacks against critical infrastructure.[101] Little evidence of this capability exists in the public record. For example, a serious cyber security breach of Department of Defense networks in 2008 by Agent.BTZ malware was only loosely linked to Russia intelligence services.[102] Due to the difficulty in attributing cyber attacks and because Russia's intelligence services are highly adept at maintaining secrecy, their cyber capabilities are assumed to be highly sophisticated as a reflection of those intelligence services' overall reputations. Fortunately, some evidence of this high-level capability has been detected in the recent years, allowing for more reliable capability estimates.

In 2014, security experts at FireEye published a special report, "APT28: A Window into Russia's Cyber Espionage Operations?" detailing what they argue is a state-sponsored advanced persistent threat that Russia has used in various forms to collect foreign intelligence over the last seven years.[103] This set of cyber operations, labeled APT28, has exploited Georgian, Eastern European government, NATO, and OSCE targets for defense-related information. The tools used by APT28 have evolved since 2007, showing a development commitment that FireEye believes implies Russian

---

[101] James R. Clapper, "Remarks as Delivered by DNI James R. Clapper on 'National Intelligence, North Korea, and the National Cyber Discussion' at the International Conference on Cyber Security" presented at the International Conference on Cyber Security, Fordham University, January 8, 2015, http://www.dni.gov/index.php/newsroom/speeches-and-interviews/208-speeches-interviews-2015/1156-remarks-as-delivered-by-dni-james-r-clapper-on-"national-intelligence,-north-korea,-and-the-national-cyber-discussion"-at-the-international-conference-on-cyber-security; Alexander, "House Armed Services Subcommittee."

[102] Phil Stewart and Jim Wolf, "Old Worm Won't Die after 2008 Attack on Military," *Reuters*, June 16, 2011, US edition, http://www.reuters.com/article/2011/06/17/us-usa-cybersecurity-worm-idUSTRE75F5TB20110617.

[103] *APT28 - A Window Into Russia's Cyber Espionage Operations?*, Special Report (FireEye, 2014): 3, https://www2.fireeye.com/apt28.html.

government sponsorship.[104] If the report's conclusions are correct, it illuminates Russia's ability not only to disrupt cyber systems, but also to gain access to secure systems, enabling a range of hostile cyber operations: intelligence collection, data manipulation, and remote system control. Due to the inherent perishability of high-end cyber payloads, unless they are used in a conflict that rises to jus ad bellum conditions, such payloads will likely remain merely hypothesized, but highly sophisticated delivery systems like those used by ATP28 may serve as a payload capability indicator. Because U.S. officials consistently categorize Russian intelligence services' cyber capabilities as on par with other leading states, and because the ability of the Russian state actors to gain access to secure foreign networks has been demonstrated, strategic analysis should assume that the Russian military and intelligence services possess highly sophisticated offensive cyber weapons.

B. CYBER GEOGRAPHY

The geography of cyberspace is an important factor for gauging a state's cyber capability. States' Internet topologies, infrastructure resources, and control over the salient features of their cyberspace vary greatly. These geographic differences likewise differentiate their utility for offensive and defensive. Martin Libicki argues that the defensive operations in cyberspace are in effect actions that "change the particular features of one's own portion of cyberspace itself so that it is less tolerant of attack."[105] The extent to which a state may have the technical means to modify this terrain may therefore translate to its defensive capacity. The following section will consider Russia's cyber geography according to two categories: the key features of Russian cyberspace and the Russian government's technological ability to manipulate its cyberspace.

---

[104] *APT28*, 19.

[105] Martin C. Libicki, "Cyberspace Is Not a Warfighting Domain," *I/S: A Journal of Law and Policy for the Information Society* 8, no. 2 (Fall 2012): 326.

1. Cyber Terrain Features

Among U.S. officials and security analysts, it is canon that national cyber security relies on a partnership between the government and the private sector; it is the private sector that owns and operates the vast majority of American critical infrastructure and is exposed to the preponderance of cyber attacks.[106] Although the nature of the government-private relationship in Putin's Russia is a mixture of state and crony capitalism, Russian industry likewise plays an important role in Russian cyber security. The key features of Russian cyber terrain are its telecommunications infrastructure, hardware supply chain, and information security technology sector.

The backbone of the Internet is the telecommunication sector—the organizations that provide broadband, cellular, and satellite transport for data. Russia's broadband and mobile communications sectors are highly consolidated; just six companies dominate 77.1% of the broadband market, while 92% of the mobile market is controlled by four operators.[107] Although most of these companies are privately owned, the largest operator that controls one third of all Russian broadband access, Rostelecom, is state-owned.[108] Importantly, these companies operate, if not in collusion with, then under the coercion of the Russian government through its onerous telecommunication regulations. Additionally, because some of these companies also operate abroad, those countries effectively rely on Russian cyber terrain to access their own cyber resources.[109]

Although the Russian government exercises some control over the telecommunications infrastructure operators, the physical infrastructure of Russia's cyberspace, the hardware and software components that transmit, process, and store data, is almost exclusively of foreign design and manufacture. In an interview with Radio Echo Moscow, Major-General Igor Sheremet, the Chairman of the Russian Federation's

---

[106] James P. Farwell, "Industry's Vital Role in National Cyber Security," *Strategic Studies Quarterly*, (Winter 2012): 10, 34-35, http://www.au.af.mil/au/ssq/digital/pdf/winter_12/farwell.pdf.

[107] Sanja Kelly et al., *Freedom on the Net 2014: Russia*, Freedom on the Net (Freedom House, 2014): 3, https://freedomhouse.org/sites/default/files/resources/Russia.pdf.

[108] Kelly, *Freedom on the Net 2014: Russia*, 3.

[109] Patrick Tucker, "Why Ukraine Has Already Lost the Cyberwar, Too," *Defense One*, April 28, 2014, http://www.defenseone.com/technology/2014/04/why-ukraine-has-already-lost-cyberwar-too/83350/.

General Staff's Military-Science Committee, acknowledged that Russia relies on Cisco routers and other foreign technology for its cyber infrastructure.[110] He argues, however, that the Russian government minimizes this risk through a rigorous component certification program, and through state projects to create domestically-manufactured electronic components for military and other critical uses. Although he acknowledges that it is unrealistic to expect Russian technology companies to outcompete foreign manufacturers in the domestic market, Sheremet claims that Russia already has the domestic capacity to supply 30% of its military requirements, and expects this number to grow to 95% by 2020.[111]

In a 2014 article that he authored, Major-General Sheremet further asserts that Russia's technological dependence is only temporary. According to him, the Russian government is making a serious academic investment to leapfrog current technology leaders by investing in quantum and optical computing.[112] While such technological leaps may be more hopeful than practical, the Russian government has taken concrete steps to stimulate domestic technology development. The most prominent initiative, the Skolkovo Innovation Center, aspires to create a Russian Silicon Valley.[113] Despite continued financial commitment from the Russian government, this project faces an uncertain future, however. Early international enthusiasm and support for Skolkovo has declined due to Ukraine conflict-related economic sanctions, while corruption-ridden construction projects missed deadlines and exceeded cost estimates.[114] Whether this attempt to grow Russia's own technology base succeeds increasingly seems unlikely.

---

[110] Sergei Buntman, Aleksandr Kurennoy, and Anatoliy Ermolin, "Informatsionnaya i Kiberbezopasnost' [Information and Cybersecurity]," transcript, *Radio Echo Moscow* (Moscow, December 2, 2013), http://echo.msk.ru/programs/arsenal/1208183-echo/.

[111] Buntman, Kurennoy, and Ermolin, "Informatsionnaya i Kiberbezopasnost' [Information and Cybersecurity];" Igor Sheremet, "Kiberugrozy Rossii Rastut —Chast' I [Cyberthreats to Russia Grow - Part I," *Voyenno-promyshlennyy Kur'yer*, February 12, 2014, http://vpk-news.ru/articles/19092.

[112] Sheremet, "Kiberugrozy Rossii Rastut —Chast' I. "

[113] Elena Zinovyeva, "U.S. Digital Diplomacy: Impact on International Security and Opportunities for Russia," *Security Index: A Russian Journal on International Security* 19, no. 2 (April 2013): 39. doi:10.1080/19934270.2013.779430.

[114] Yuliya Chernova, "Russia's Startup Scene Fades," *Wall Street Journal,* September 10, 2014, Europe, http://search.proquest.com/docview/1560926461.

The highlight of the Russian information security technology sector is the privately owned security company Kaspersky Lab. This cyber security company named after its cofounder, Eugene Kaspersky, has continued to play a leading role in international cyber security, rivaling its competitors: McAfee, Norton, and Symantec. According to its website, Kaspersky Lab products protect over 400 million users worldwide, and the company has established a renowned reputation by being the first to identify and analyze Stuxnet, as well as its derivative variants.[115] The company's security analysis extends beyond conventional cyber threats; according to Kaspersky, his company's research and developments also includes secure operating systems to defend SCADA-reliant critical infrastructure—a vital area of cyber security.[116]

In addition to the Kaspersky Lab's impressive technical prowess, the company has an intriguing relationship with the Russian state. Although in an interview with the Russian newspaper, "Kommersant," Kaspersky casually laughs off the interviewer's suggestion that he coordinates with the Putin administration, the company's relationship with the Russian state is potentially suspect.[117] Eugene Kaspersky began his education at a KGB-backed science academy and applied this training as a Soviet army intelligence officer.[118] A decade later, after the collapse of the U.S.S.R., he started Kaspersky Lab. According to Wired Magazine's profile of Kaspersky labs, although the FSB does not tamper with Kaspersky Lab software, the company and the state security agency maintain a close working relationship.[119] Russia's Foreign Ministry likewise relies on Kaspersky Lab services, while Kaspersky often echoes the Russian government's cyber rhetoric at international forums.[120] The extent of this relationship is a matter of speculation, but

---

115 "About Kaspersky Lab," Kaspersky Lab, accessed January 19, 2014, http://www.kaspersky.com/about.

116 "Yesli Budut 'Valit'" Region, Gorod Ili Stranu Tselikom — Do Svidan'ya [If They Attack a Region, City, or the Whole Country - Goodbye]," *Kommersant*, March 28, 2013, http://www.kommersant.ru/doc/2155845.

117 Ibid.

118 Noah Shachtman, "Russia's Top Cyber Sleuth Foils US Spies, Helps Kremlin Pals," *Wired Magazine*, July 23, 2012, http://www.wired.com/2012/07/ff_kaspersky/.

119 Ibid.

120 Oleg Demidov and Maxim Simonenko, "Flame in Cyberspace," *Security Index: A Russian Journal on International Security* 19, no. 1 (February 2013): 71-2. doi:10.1080/19934270.2013.757131.

Kaspersky Lab's technology prominence is not. The company is a key actor in international cyber security, and it is cloud-based threat network may also double as a powerful sensor and defensive mechanism that operates from within Russian cyberspace.

2. Cyberspace Control

The Russian government's position on the role of the Internet in society has varied over the past decade. According to the Freedom House report, "Freedom on the Net 2014: Russia," 61% of Russia's population had access to the Internet in 2013.[121] Though this Internet penetration rate lags behind France's 82%, United States' 84%, and United Kingdom's 90% Internet penetration rate for 2013, it nonetheless represents a sizable segment of the worlds' Internet users.[122] Aforementioned cyber capability case studies demonstrated the Russian state's reliance on its patriotic Internet users, hackers, and cyber criminals as a militia to be mobilized in support of state interests. While the hacktivists enjoyed a semi-permissive Internet environment at the time of the Estonia and Georgia cyber attacks, the rest of Russia's population enjoyed a liberal Internet experience. This attitude of the Russian government's toward Russia's own Internet users has been changing since 2012, however. During the 2011 parliamentary election, opposition groups rallied on Internet social media sites to protest the Putin regime.[123] Since then, the Russian government has made changes to Russian Internet architecture and domestic policy. Freedom House calculates that these changes were the most severe decline of Internet freedom of any state in 2013.[124] This curtailment of Russians' Internet freedom has resulted in an improved defensiveness of Russia's cyber terrain, and coincidentally also made attacking from Russia's cyberspace more difficult.

Russia's battle against the Tor network technology epitomized these technological changes. In July of 2014, Russian President Vladimir Putin made headlines when the

---

[121] Kelly, *Freedom on the Net 2014: Russia*, 2.

[122] Kelly, *Freedom on the Net 2104*, 300, 877, 858,

[123] Natalie Duffy, *Internet Freedom in Vladimir Putin's Russia: The Noose Tightens* (American Enterprise Institute, January 2015): 1-2, http://www.aei.org/wp-content/uploads/2015/01/Internet-freedom-in-Putins-Russia.pdf.

[124] Kelly, *Freedom on the Net 2104*, 3.

Russian Interior Ministry offered a 3.9 million-ruble bounty for a technical solution for identifying Tor (The Onion Router) users.[125] This solicitation was just Russia's latest effort at curbing Tor use; the Russian government had previously considered legislation to ban the technology and related software products.[126] The government's rationale for targeting Tor and its users is to curb certain types of cybercrime—Tor is the premier technology for masking online identity. For the same reason, it has also become the tool of choice for critics of the Putin regime, who use the network to circumvent Russia's other increasingly draconian Internet censorship measures.[127] Though the Russian government has yet to succeed in developing a Tor countermeasure, when it does, it will be capable not only of thwarting child pornographers and political dissidents, but it will also improve its defense against many variants of cyber attacks. Because Tor functions as an anonymous network overlaid on top of existing networks, it is commonly used as an unattributable mechanism for attacks command and control and for establishing a secure pathway for cyber attacks.[128] If successful, Russia's efforts to prevent Tor use will strip a layer of non-attribution from cyber attacks. Unlike its permissive attitude toward cybercrime at the time of the Russo-Georgian War, more recently, the Russian government appears willing to sacrifice the offensive capability of its criminal proxies in favor of improved defensiveness.

Restrictions on Tor use would deny users secure and anonymous access to online resources, but the Russian government has also attempted to limit anonymity through less sophisticated measures. User attribution begins with access to the Internet Service Provider (ISP). According to TNS Russia, a research firm cited by Freedom House, half

---

125 "Russia Offers $110,000 to Crack Tor Anonymous Network," *BBC News*, July 28, 2014, sec. Technology, http://www.bbc.com/news/technology-28526021.

126 "Russia's FSB Mulls Ban on 'Tor' Online Anonymity Network," *RT*, August 16, 2013, sec. Russian Politics, http://rt.com/politics/russia-tor-anonymizer-ban-571/.

127 Alexey Eremenko, "Anonymous Browser Mass Hit as Russians Seek to Escape Internet Censorship," *Moscow Times*, June 18, 2014, http://www.themoscowtimes.com/news/article/anonymous-browser-mass-hit-as-russians-seek-to-escape-internet-censorship/502169.html.

128 Daniel Gonzalez, "Preventing Cyber Attacks: Sharing Information About Tor," *The RAND Blog*, December 17, 2014, http://www.rand.org/blog/2014/12/preventing-cyber-attacks-sharing-information-about.html; Alastair Stevenson, "Hackers Turning to Tor Network to Hide Evolved Malware, Warns Kaspersky Lab," *V3*, March 20, 2014, sec. Security, http://www.v3.co.uk/v3-uk/news/2335401/hackers-turning-to-tor-network-to-hide-evolved-malware-warns-kaspersky-lab.

of Russia's Internet users access the web via their mobile devices.[129] This mobile access is tracked to individuals through SIM cards; which in Russia must be registered to a person's passport. The same passport-based registration also applies to terrestrial, paid Internet service.[130] A law passed in August 2014 further restricts Internet access by likewise requiring passport information to connect to state-funded public, and possibly, to commercially-provided public Wi-Fi Internet access points.[131] The sum effect of these rules is that within Russian cyberspace, one's cyber persona is strongly attributed to the physical persona upon connecting to the Internet.

In addition to restricting anonymous access and anonymous transport, Russian authorities have attempted to limit anonymous content. A law passed in May of 2014 has established a standard for content attribution; blogging sites that attract a daily audience of more than 3,000 visitors must register with the Federal Service for Supervision of Communications, Information Technology and Mass Media, or Roskomnadzor. This law requires bloggers meeting this threshold to provide personally identifiable information and assume financial liability for the accuracy of the contents on their blogs.[132] To support the technical ability of the state to enforce this policy, the Russian government also introduced law that mandates data localization. By 2016, companies that collect and store data belonging to Russian citizens will be required to physically store that data on Russian territory.[133] When implemented, this requirement will enable easier data intercept, data retrieval, and possibly data protection by moving Russian citizens' data within the state's legal and physical jurisdiction.

---

[129] Kelly, *Freedom on the Net 2014: Russia*, 3.

[130] "Russian Security Services Seek Control Over Wireless Connectivity - Website," *BBC Monitoring Former Soviet Union,* September 26, 2009, http://search.proquest.com/docview/460251841.

[131] Alexey Eremenko, "Russia Bans Anonymous Public Wi-Fi," *Moscow Times*, August 10, 2014, http://www.themoscowtimes.com/news/article/russia-bans-anonymous-public-wi-fi/504855.html.

[132] Michael Birnbaum, "Russian Blogger Law Puts New Restrictions on Internet Freedoms," *Washington Post,* August 1, 2014. http://search.proquest.com/docview/1550033701.

[133] Paul Sonne and Olga Razumovskaya, "Russia Steps Up New Law to Control Foreign Internet Companies," *Wall Street Journal*, September 24, 2014, http://www.wsj.com/articles/russia-steps-up-new-law-to-control-foreign-internet-companies-1411574920.

Along with the changes to Russian cyberspace to restrict anonymity, the Russian government has also implemented technology that restricts—based on content—information flow within Russian cyberspace. Beginning with Putin's election to the presidency in 2012, his government has passed legislation has enables the Russian government to filter website content. These restrictions began under the pretense of protecting children on the Internet: on November 1, 2012, the Russian government passed a law enabling Roskomnadzor to blacklist offender websites without trial.[134] On December 2013, the government expanded these powers to authorize, without due process, the shutdown of websites "for participation in unsanctioned public actions."[135] Though the Russian government's ability and willingness to silence free speech on the Internet is disconcerting from a human rights perspective, from an offense-defense analysis perspective this ability also reflects changes to the defensiveness of Russia's cyber terrain. The creation and access of content within Russian cyberspace is now controlled through technical measures implemented by Russian ISPs at the behest of the Russian government. These content blacklists are a form of allow-by-default deny-by-exception security posture, and though this posture is not as restrictive as a deny-by-default allow-by-exception security stance, it represents a shift away from a fully open allow-all Internet environment to a nationally censored, individually attributable Internet.[136]

In addition to the Roskomnadzor's control of data flow, within Russian cyberspace, the government dominates the analogue to the physical high ground with FSB sensors: its System for Operative Investigative Activities (SORM) allows the state to intercept and monitor Russian Internet traffic and analog telecommunications. SORM is a descendent of Soviet-era KGB research and development efforts; over three generations of SORM device refinements, the FSB has developed the capability to completely track, monitor, and store all of Russians' electronic communications. The initial 1990s SORM

---

134 "Russia Internet Blacklist Law Takes Effect," *BBC News*, October 13, 2012, sec. Technology, http://www.bbc.com/news/technology-20096274.

135 Kelly, *Freedom on the Net 2014: Russia*, 4.

136 Harold F. Tipton, ed., *Official (ISC)^2 Guide to the CISSP CBK*, 2nd Ed., (New York: CRC Press, 2010), 119.

variant, SORM-1 intercepted and recorded land and mobile telephone conversations. Versions 2 and 3 expanded that capability to include Internet traffic—including bitwise capture and storage of all transmitted data and metadata.[137] Russian law requires all Russian ISPs to install this surveillance hardware and configure their data routing to pass through SORM devices, which in turn forward that data to FSB and other Russian intelligence services for additional exploitation.[138]

Although SORM is a powerful sensor technology, its reach is limited by its physical placement. The devices can only be placed within Russian jurisdiction—intercept of data transmissions to and from internationally hosted content is more problematic.[139] Some of this limitation may be overcome by SORM's speculated ability to perform deep packet inspection, or the ability to view the content of the data packets encapsulated with TCP/IP and UDP communications protocols used for much of the Internet data transmission. The devices, therefore, may be able to capture and reconstruct a portion of the unencrypted communication between Russian users and non-Russian resources.[140] However, encrypted communication by popular social media and other Internet service sites is increasingly becoming the norm, and this trend will be a growing challenge for FSB. The Russian government may have a strategy to overcome these encryption barriers. When Russian data localization legislation takes effect in 2016 and Russian user data has to be hosted at Russian locations, SORM boxes at the data centers will likely be placed on the unencrypted side of the communication path, preempting many data-in-transport encryption safeguards. There is a technology race between methods to intercept data and techniques to hide it, but at the movement, Russia's SORM appears to have the upper hand within Russian cyberspace.

---

[137] Andrei Soldatov and Irina Borogan, "Russia's Surveillance State," *World Policy Journal* 30, no. 3 (Fall 2013): 24-5. doi: 10.1177/0740277513506378.

[138] Giles, "'Information Troops,'" 8-9.

[139] Soldatov and Borogan, "Russia's Surveillance State," 27-8.

[140] Thor Benson, "Russia's Wiretapping 'SORM' Boxes in Sochi Make the NSA Look Like Saints," *Digital Trends*, February 5, 2014, http://www.digitaltrends.com/cool-tech/sochis-wiretapping-black-boxes-make-nsa-look-like-saints/.

C. HYPOTHESIS ASSESSMENT

The historical case studies of Russian-affiliated cyber attacks clearly demonstrate that the offensive cyber weapons in the Russian government's arsenal have the advantage—cyber attacks consistently succeeded at disrupting or compromising their targets. The available evidence, therefore, best supports hypotheses H1. *Russia's cyber capability is offensive and the posture is indistinguishable as either offensive or defensive* and H3. *Russia's cyber capability is offensive and the posture is distinguishable as either offensive or defensive*. This delineation, however, acknowledges that Russia has access to cyber weapons along the spectrum of offensive-defense cyber capability, and not in strictly offensive weapons. Although it is infamous for widely perceived complicity in the Estonian and Georgian cyber attacks, the Russian government is also increasingly investing in defensive capability, and this may suggest a future shift in its capability balance. Alternately, and more likely, Russia may be investing in both offensive and defensive capabilities, but the defensive investments are less secretive.

Because this chapter's case studies are instances cyber weapons use, the analytic difficulty caused by the inherent secrecy of cyber weapons capability is not as challenging in practice as it is in theory. Russia has notoriously been at the forefront of cyber weapon use, so there is less uncertainty about the capability and performance of its cyber weapons. Although, as illustrated by the discovery of APT28, Russia may reasonably be presumed to possess and continuously develop high sophistication offensive cyber weapons, the historic record of its cyber weapon use is that of low to moderate technical sophistication weapons employed with increasingly improving tradecraft. This weapon selection and use has two important implications on the degree to which Russia's offensive cyber weapons are dominant over the defense. The cyber attacks, as in the case of the Russo-Georgian conflict, though skillfully coordinated and executed, either targeted known vulnerabilities or used publicly available attack tools. Thus, although analysis of the international system predicts some weapons use restraint due to the desire for states to maintain their perishable cyber capabilities secret, Russia's reliance on publically available tools and published exploits does not suffer from this restraint. Additionally, as Patrick Malone estimates in his offense-defense cost ratio

comparison between the brute force Estonian cyber attacks and the highly sophisticated Stuxnet attack that used unpublished exploits and a custom payload, low sophistication attacks are several orders of magnitude less costly for attackers.[141] Lastly, Russian law enforcement's semi-permissive attitude toward cybercrime further lowers the state's cost for maintaining its low-end capabilities. By using high cost ratio cyber weapons whose technology is already public, Russia pays a lower cost for weapon use. Though the disadvantage of Russians' cheaper cyber weapon selection is lower likelihood of success, the disappointingly long timeframe for securing systems against published exploits presents Russians with a target-rich environment.[142]

Russian cyber weapons also escalate instability because their weapon type and tactics increase the incentive for cyber retaliation. The DDoS and defacement attacks used in Georgia and Ukraine did not destroy their victims' capacity to respond in kind, leading to retaliatory strikes. Importantly, because proxy actors conducted pro-Russian attacks, the Russian government was less able to restrain their proxies' weapons selection and targeting than if state actors conducted the attacks. Unfortunately, it is difficult to establish the exact nature of this relationship, and the degree of control or direction that the Russian government can exercise over its proxies. Additionally, both Georgia and Ukraine followed the Russian model for cyber attacks and relied on their own non-state proxies for retaliation. Consequently, the Russian cyber capability dramatically raises the international instability in cyberspace—its low-end cyber weapon use encourages retaliation without the institutional restraint mechanisms that apply to conventional conflict and it encourages the diffusion of cyber power to non-state actors. While FireEye security experts suspected that the prospect of retaliation along with the weapons' relative crudeness might deter Russia from using low-end cyber weapons in Ukraine, because the Russian government relies on surrogates, such restraint is difficult to achieve.

Russian cyber weapon capability encourages aggression, but Russia is also changing its cyber geography to increase its defensiveness under the pretext of

---

[141] Malone, "Offense-Defense Balance in Cyberspace, " i.

[142] *Internet Security Threat Report 2014* (Symantec Corporation, 2014): 6, http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v19_21291018.en-us.pdf.

safeguarding against internal cyber threats, but this technology is also applicable to external threats. Professor Wade Huntley observes that one explanation for why cyberspace has not been designed to increase its defensiveness is that states may believe that the cost of rebuilding it to be more defensive exceeds the cumulative costs of potential attacks.[143] This notional challenge of cost sharing and return on investment appears to be recognized in practice by U.S. critical infrastructure security guidance and policy documents.[144] Russian willingness to invest in restructuring its cyber terrain suggests that the Russian government increasingly views its cyberspace as an existential threat to the regime due to potential political opponents' ability to organize and mobilize online. Thus, the Russian Federation's cost analysis for hardening cyberspace differs from the Western cost analysis that puts a positive value on the Internet's openness and freedom from heavy-handed government regulation; to the Russian government the openness of the Internet incurs an additional security cost.

The technological changes that the Russian government has implemented in its cyberspace increasingly shift weapon capability in favor of defenders. The Russian government can monitor, intercept, and block various types of Internet traffic. It can also reduce actor anonymity. In the most extreme case, the Russian government may possess the capability to create a fractured cyberspace, isolating itself from external threats—the pinnacle of geographical defensiveness.[145] At the present, however, these capabilities appear to be internally facing, intended to suppress domestic cyber threats. If in the future these defensive features are reoriented externally, though this change would improve Russian defenders' advantage, this change might nonetheless increase the security dilemma. If Russia's cyber defensiveness exceeds the average defensiveness of other states, it may be even more enticed to act aggressively, knowing that others' ability to retaliate is reduced.

---

[143] Huntley, "Offense, Defense, and Cyber War," 16.

[144] *Blueprint for a Secure Cyber Future: The Cybersecurity Strategy for the Homeland Security Enterprise* (Department of Homeland Security, November 2011): 24, http://www.dhs.gov/xlibrary/assets/nppd/blueprint-for-a-secure-cyber-future.pdf.

[145] Soldatov and Borogan, "Russia's Surveillance State," 24.

Finally, Russia's changes to its cyber geography potentially undermine its offensive weapons' capability. Its terrain's defensive features such as content filtering and reduced anonymity negate their weapons and tactics effectiveness. If the Russian government implements security backdoors in their sensors and defense tools to allow proxy actors to continue to operate, in doing so they negate their plausible deniability and potentially signal early warnings and indicators. The alternative is that Russian proxies move their operations outside of Russian cyberspace, but in doing so they expose themselves to foreign jurisdictions where they might be detected and thwarted with greater ease. Though this may be a promising consequence of Russian cyber terrain hardening, it is likely only to decrease the security instability caused by Russia's least sophisticated weapons and actors.

This chapter considered Robert Jervis's key security dilemma variable as applied to Russia—whether Russia has invested in offensive or defense cyber capability, as reflected by Russia's brandished cyber weapons and by the properties of Russian cyber terrain. The author's conclusion is that Russian cyber capability shows an existing investment in offensive cyber weapons, as well as efforts to improve the defensiveness of its cyber terrain. Alarmingly, the weapon capability of Russia and the diffusion of cyber power to non-state actors appears to create security dilemma pressures that may be more acute than the security dilemma expected at the international system level of analysis. The following chapter will consider Jervis's second variable—whether Russian cyber posture can be distinguished as offensive or defensive by evaluating Russian cyber policy and doctrine.

THIS PAGE INTENTIONALLY LEFT BLANK

III. RUSSIAN CYBER POSTURE

This chapter seeks to determine whether Russia's cyber posture is distinguishable as either offensive or defensive. The following sections examine Russians' official and unofficial conception of cyber power, the cyber doctrine of the Russian Federation's Armed Forces, and Russia's efforts to shape the international cyber environment thru international institutions. If Russia's cyber posture is distinguishable as either offensive or defensive, these three lanes of inquiry may provide insight into its orientation.

A. RUSSIAN UNDERSTANDING OF CYBER POWER

The Russian view on cyber power and on Russia's own cyber capabilities differs in significant ways from the American perspective. Most importantly, Russian academics and military experts conceive of cyber warfare more broadly than Western strategists and view Russia not as an aggressor, but as a vulnerable state defending itself from a hostile global cyber campaign. Though Russian cyber terminology differs in key ways, Russian cyber experts recognize many of the same challenges of cyber power—offense dominance, secrecy, non-attribution, escalation, etc.—that are also widely discussed by Western academics.

Understanding the terminological difference between U.S. and Russian cyber discourse is essential for contextualizing how Russian thinking about cyber power shapes Russia's doctrine and international position on cyber security. Keir Giles summarizes the Russian view of cyber war as *informatsionnaya voyna*—a "holistic concept" of information war that includes computer network operations, electronic warfare, psychological operations, and information operations.[146] Russians subdivide this broad concept of information war into two components: information-technological and the information-psychological.[147] Major-General Sheremet describes information-technical

[146] Giles, "'Information Troops,'" 46.

[147] Timothy L. Thomas, "Russian Information Warfare Theory: The Consequences of August 2008," in *The Russian Military Today and Tomorrow: Essays in Memory of Mary Fitzgerald*, ed. Stephen J. Blank and Richard Weitz (U.S. Army War College, Carlisle, PA: Strategic Studies Institute, 2010), 266, http://www.strategicstudiesinstitute.army.mil/pdffiles/pub997.pdf.

attacks as cyberattacks ranging from influence operations via website defacements to physical damage resulting from altered rocket trajectories.[148] Information-psychological operations, in contrast, include operations that attack the morale and the perceptions of the population, as exemplified by the Arab Spring, Orange Revolution, and even the dissolution of the Soviet Union.[149]

This understanding of cyber power is not limited to just a handful of Russian scholars. In an extensive literature review of Russian academic and official writing, Stephen Blank demonstrates that this is mainstream Russian thinking about cyber power, with important consequences. By incorporating the struggle of ideologies into cyber power, Russian analysts continue "the Leninist tradition of a constant state of siege within and between states, societies, and blocs."[150] As a consequence, the Russian state and its cyber analysts discuss cyberspace issues—to Russians "information space"—as a lens for "viewing the domestic and international situation."[151] This inclusion of hostile content as a source of cyber threat differs from the West's more narrow focus on strictly hostile code and leads to Russians' particular perception of peacetime and wartime cyber threats and vulnerabilities.[152] In the following discussion, the author uses Russian information war terminology—cyber power is an implied component of that definition but cannot be extricated from the Russian conception of information warfare for standalone assessment.

1. Hostile Content

Russians' understanding of hostile content as an information security issue is illustrated in an article in the journal *Security Index: A Russian Journal on International Security* by Elena Zinovyeva, who describes the role of information-psychological aspects of cyber power in shaping the security dilemma at the international level. This

---

[148] Sheremet, "Kiberugrozy Rossii Rastut —Chast' I. "

[149] Igor Sheremet, "Kiberugrozy Rossii Rastut —Chast' II [Cyberthreats to Russia Grow - Part II," *Voyenno-promyshlennyy Kur'yer*, February 19, 2014, http://vpk-news.ru/articles/19194.

[150] Blank, "Russian Information Warfare," 32.

[151] Thomas, "Russia's Information Warfare Strategy, "102.

[152] Giles, "'Information Troops,'" 48.

analysis cites and builds on the work of Martin Libicki and Joseph Nye to conclude that the balance of power among nations has been disturbed by "the very nature of international politics in the information sphere."[153] The source of this instability, she argues, is U.S. digital diplomacy. Zinovyeva describes the policy of digital diplomacy as a series of programs enabled by "technological instrument[s]" with which American diplomats engage foreign populaces through organizations such as the Department of State, Department of Defense, Central Intelligence Agency, and U.S. Agency for International Development.[154] The notable goals and priorities of these programs are:

- "discredit the ideological enemies of the United States"
- "limit Russia's media presence in the former Soviet Republics"
- "creat[e] information services aimed at supporting the opposition in authoritarian countries"
- "creat[e] shadow Internet systems and independent mobile networks which...can help the opponents of authoritarian regimes to exchange information online, circumventing the government's restrictions."[155]

According to Zinovyeva, this digital diplomacy is enabled by structural changes in the international system brought about by advances in cyberspace, and although the United States is currently at the forefront of capitalizing on the power potential of these technologies, the Russian Federation should develop its own offensive information-psychological cyber weapons to be used in the information confrontation with the West. Importantly, Russia must make this investment urgently—"it is quickly running out of time."[156]

U.S. Army War College Professor Stephen Blank's assessment of the Russian perspective on information-psychological operations in cyberspace is starker: Russia is fighting a domestic counterinsurgency.[157] Russian politicians, heads of state agencies, and academics believe that the United States is actively engaged in a network war against

[153] Zinovyeva, "U.S. Digital Diplomacy, " 38.

[154] Ibid., 32-4.

[155] Ibid., 34-5.

[156] Ibid., 39-41.

[157] Blank, "Russian Information Warfare," 32.

Russia, facilitating a domestic insurgency.[158] Zinovyeva's argument described previously is typical of Russian academic literature, and in Blank's opinion, this view reflects an attempt to externalize the causes of the domestic instability of an illiberal democracy.[159] Whereas a Western perspective on the Arab Spring, the color revolutions, and the civil disturbances following the 2011 Russian parliamentary election focuses on issues prominent at the state level of analysis, Russians see the same international events as caused by the international security dilemma stemming from offensive application of information technology. This divergence in analytic perspectives is important for contextualizing Russian doctrine development and stance on international cyber issues.

In addition to the lessons drawn from the role of Internet technologies in fostering worldwide anti-authoritarian political movements, Russian military experience in recent armed conflicts—the Chechen Wars and especially the 2008 Russo-Georgian War—has also shaped Russians' understanding of the relevance of cyber power in conducting IW and IO as part of a military campaign. While the military phase of the Russo-Georgian War was swift and decisively in favor of the Russian Federation, in the Russian government's view the perception of the conflict and the perception of its legitimacy by the international community was more important than what occurred on the battlefield.[160]

To the Kremlin and to Russian critics alike, the Russo-Georgian conflict demonstrated Russian shortcomings in strategic communications strategies and faulty technical performance of their information-enabled weapons systems.[161] Subsequent calls for reform focused on the Russian Federation's ability to shape and influence international perceptions of future conflicts.[162] Information security analyses were less common than strategic communications criticism, however. Among such analyses, Colonel-General Anatoliy Nogovitsyn's notable cyber security-focused critique, while

---

[158] Blank, "Russian Information Warfare," 34, 40-2.

[159] Ibid., 32.

[160] Goble, "Defining Victory and Defeat,"181-2.

[161] Goble, "Defining Victory and Defeat," 192-4; Ronald J. Deibert, Rafal Rohozinski, and Masashi Crete-Nishihata, "Cyclones in Cyberspace: Information Shaping and Denial in the 2008 Russia-Georgia War," *Security Dialogue* 43, no. 1 (February 2012): 9-10. doi: 10.1177/0967010611431079.

[162] Thomas, "Russian Information Warfare Theory, " 279-82.

recognizing the low cost of cyber weapons and heightened international vulnerability of states due to new technologies, emphasized the new capacity of information weapons to target population morale, provoke social and ethnic conflicts, and undermine government legitimacy.[163] In contrast, Western observers and analysts focused much more on the technical details of the cyber attacks during the Russo-Georgian War, and on those weapons' implications to collective security arrangements, law of armed conflict, and technical characteristics of cyber conflicts. This difference in lessons learned from the Russo-Georgian War illustrates the analytics lens with which Russians approach cyber power—hostile content is central to Russian understanding of information confrontation.

2. Hostile Code

Although Russian cyber power scholarship emphasizes the importance of hostile content, or the information-psychological aspect of information warfare, Russian thinkers also recognize value of information-technical weapons—hostile code. This technical and strategic discussion of cyber power is evident in the Russian press, academic publications, and military journals. A frequent commentator in public forums on Russian Security issues, Major-General Sheremet explains that potential cyber attacks on its critical infrastructure are a vital information-technical threat to the Russian Federation.[164] His position is particularly interesting: although he explains the varied approaches the Russian government is undertaking to reduce these risks, he also notes that because of the difficulty of positively attributing cyber attacks, the Russian response to such attacks would be simply to do nothing and "uchit'sya na oshibkakh"—learn from mistakes.[165]

Eugene Kaspersky takes a similar view; Russia must make security investments in its critical infrastructure, information technology infrastructure, and telecommunications sectors. Although such defensive measures may reduce Russia's vulnerability to cybercrime and cyber terrorism, in the case of a true cyber warfare threat, he argues that no defensive measures will be sufficient to absorb through resilience or deter through

---

[163] Thomas, "Russian Information Warfare Theory, "290-1.

[164] Sheremet, "Kiberugrozy Rossii Rastut —Chast' I. "

[165] Buntman et al., "Informatsionnaya i Kiberbezopasnost."

denial the attacks. Russia would have to retaliate.[166] Though both Sheremet's and Kaspersky's responses to cyber attack are not nearly as drastic as V. I. Tsymbal's 1996 assertion that "Russia retains the right to use nuclear weapons first against the means and forces of information warfare, and then against the aggressor state itself," all three positions stem from a recognition of information-technical attacks' offensive dominance and Russia's vulnerability to such attacks.[167]

Russian academic publications also increasingly publish analyses of strategic implications of informational-technical aspects of cyber weapons. The Russian Institute for Policy Studies Center's journal, *Security Index*, for example, published eight articles dedicated to cyber security topics in 2013. In comparison, it dedicated five articles to cyber issues in 2012, and only two articles in the four years prior to then.[168] The analysis that is published is both technically competent and insightful. In describing "Cyberwarfare and Russian Style of Cyberdefense," Oleg Demidov's analysis of DDoS attacks and the Stuxnet family of malicious code identifies important issues: non-attribution, asymmetric response, power diffusion, offensive retaliation, and a zero-sum arms race.[169] The Russian reaction to the international system shaped by such weapons, argues Demidov, is an increased militarization of Russian cybersecurity functions—a mirror imaging of U.S. CYBERCOM.[170]

Dmitry I. Grigoriev presents another viewpoint on Russian cybersecurity measures at the EastWest Institute. "Some nations," he writes, "set up special units to conduct cyber warfare," and this militarization creates an inherently offensive, covert,

---

166 "Yesli Budut 'Valit' Region, Gorod Ili Stranu Tselikom. " [The translation of the Kaspersky's phrase "Возможен только реактивный ответ." is ambiguous. It may mean immediate retaliation, or it may mean retaliate with ballistic weapons, implying escalation to conventional arms.]

167 Timothy L. Thomas, "Russian Views on Information-Based Warfare," *Airpower Journal,* special edition (1996): 26, http://www.airpower.maxwell.af.mil/airchronicles/apj/apj96/spec96/thomas.pdf.

168 "Security Index Journal," *PIR Center*, accessed February 17, 2015, http://pircenter.org/security-index.

169 Demidov, "Cyberwarfare," 67-9.

170 Ibid., 70-1.

and indefensible cross-border threat.[171] The Russian government's approach to countering this threat to international stability, he explains, is to create a series of bilateral and multilateral arrangements that ban the use of cyber weapons for military-political purposes. Such international arrangements should also create technical mechanisms for establishing attack attribution and adopting Internet protocols that secure the Internet.[172] Though Demidov's and Grigoriev's positions differ in their proposed solutions, their analysis is representative of a defensive tone to Russian cyber analysis—Russia is responding defensively to a perceived security arms race led by the United States.

Finally, the Russian Armed Forces demonstrate some understanding of cyber weapons and of American doctrinal and technical developments in cyberspace. In the *Military Thought* article "Operations in Cyberspace: Theory, Politics, and Law," the authors summarize unclassified U.S. Department of Defense publications pertaining to cyber operations. In addition to summarizing American cyber doctrine, the authors criticize it for, in their view, failing to integrate international law into the concept of cyber operations, for increasing international tension with an ambiguous retaliatory policy in light of the difficulty of cyber attribution, and for approaching the security dilemma caused by the nature of cyber weapons through a NATO and not an international framework.[173] A similar analysis of cyber power emphasizes that the United States, China, United Kingdom, and many other countries are forming cyber attack units, and that the United States, specifically, views cyber war as inevitable and as serious as a confrontation in any other military theater.[174] Both analyses, while introducing their readers to cyber definitions, terms, and concepts, also point out that the cyber domain is characterized by an already in-progress offensive arms race.

---

[171] Dmitry I. Grigoriev, "Russian Priorities and Steps Towards Cybersecurity," in *Global Cyber Deterrence: Views From China, the U.S., Russia, India, and Norway*, ed. Andrew Nagorski (New York: EastWest Institute, 2010), 5–6, http://www.ewi.info/sites/default/files/ideas-files/CyberDeterrenceWeb.pdf.

[172] Ibid., 6.

[173] I.N. Dylevsky, S.A. Komov, S.V. Korotkov, and A.N. Petruinn, "Operations in Cyberspace: Theory, Politics, Law," *Military Thought* 20, no. 3 (2011): 158-60. ProQuest 923221882.

[174] P.I. Antonovich, "Cyberwarfare: Nature and Content," *Military Thought* 20*,* no. 3 (2011): 41. ProQuest 923219578.

It is notable that cyber power analysis by Russian military officers focuses much less on operational art and force development than it does on the role of international institutions. The *Military Thought* article "Potential Approaches to Implementing the Russian Federation's Military Policies on International Information Security in the Present Situation" only vaguely references the military's role in the "creation of a Eurasian system for joint response to threats."[175] Instead, the authors criticize the Euro-Atlantic approach to cyber security as militarizing cyberspace, violating national sovereignty under the pretense of law enforcement, and ultimately fostering an arms race.[176] The alternative they suggest is to support the Shanghai Cooperation Organization approach that strives to restrict new information weapon development, limits existing weapons use, and provides a mechanism for collective response to cyber aggression.[177] In what may well be a complementary article, I.N. Dylevsky suggests that based on U.N. precedent in defining aggression, the Stuxnet, Estonian, and Georgian cyber attacks meet the spirit of the U.N. definition of aggression.[178] The authors suggest that states may be dis-incentivized from cyber aggression if the U.N. modifies the Article 3 definition of aggression by including:

- "use of information weapons by the armed forces of a state against the information resources of another state's critically important facilities;"
- "propaganda of war and use of force by a state and spreading seditious information, which helps destabilize the internal and international situation, unleash and escalate armed conflicts."[179]

The popular, academic, and military perspectives on informational-technological aspects of information warfare share several themes. The authors recognize cyber weapons' offensive dominance and point to a cyber arms race. Their perceived primary culprit and apparent aggressor in this arms race is the United States. Although much of

---

[175] S.M. Boyko et al., "Potential Approaches to Implementing the Russian Federation's Military Policies on International Information Security in the Present Situation," *Military Thought* 18, no. 2 (2009): 13. ProQuest 211447654.

[176] Ibid., 11-2.

[177] Ibid., 12.

[178] I.N. Dylevsky, S.A. Komov, and A.N. Petruinn, "Informational Aspects of the Concept of Aggression in International Law," *Military Thought* 22, no. 4 (2013): 4-5. ProQuest 1537889195.

[179] Ibid., 9-10.

Russian analysis acknowledges a cyber security dilemma and points out many of cyber weapons' strategic and tactical characteristics, the proposed solutions seem divorced from these factors. Russians advocate for an international institutional solution, but do not explain how these mechanisms would mitigate the properties of cyber weapons that necessitate nations to establish offensive cyber units. This likely reflects a perception that Russia cannot compete in a cyber arms race and its vulnerability is so great that only international regimes can guarantee its security. Because international institutions are unlikely to address the challenge of weapon secrecy in cyberspace and covert acquisition, Russians likely hope that if other nations voluntarily halt their offensive cyber weapons programs in accordance with international agreements, Russian cyber development can secretly attain parity.

B. OFFICIAL RUSSIAN VIEW OF CYBER POWER

In addition to the discussion of cyber power by Russian academia, military, and media, the government of the Russian Federation has also mentioned the role of cyberspace in its national planning guidance and military doctrine. This official mention of cyber power gives insight into what Russian leaders believe are their nation's security challenges and priorities, and, importantly, it illustrates how the Russian government wishes others to perceive its posture on cyberspace issues.

1. National Security Perspective

At the foundation of the official Russian Federation's view of cyber power is its *Information Security Doctrine*, published on September 9, 2000. The document is the "totality of official views, objectives, principles, and basic guidelines for ensuring information security of the Russian Federation" and is the basis for "shaping government policy" and "devising targeted national information security programs."[180] It lists four key areas of Russian national interest in the information sphere, threats and sources of threats to these national interests, and methods for ensuring information security. Though

180 "Information Security Doctrine of the Russian Federation," *Ministry of Foreign Affairs of the Russian Federation*, last modified December 29, 2008, http://www.mid.ru/bdomp/ns-osndoc.nsf/1e5f0de28fe77fdcc32575d900298676/2deaa9ee15ddd24bc32575d9002c442b!OpenDocument.

much of the doctrine focuses on supporting Russia's then fragile economy, civil society, and political system, the document also identifies potential information warfare threats from other states. Two such key sources of threat are detailed in Article 1, Section 3:

- "activities of foreign political, economic, military, intelligence and information entities, directed against the interests of the Russian Federation in the information sphere;"
- "development by a number of states of information war concepts that provide for creating means for dangerous attack on the information spheres of other countries of the world, disturbing the normal functioning of their information and telecommunication systems, breaching the security of their information resources and gaining unsanctioned access to them."[181]

These two sources of threats mirror Russian information warfare concepts of information-psychological and information-technological weapons, although, as Timothy Thomas points out, the terms themselves are not used.[182] In addition to identifying threats and vulnerabilities, the *Information Security Doctrine* articulates various legal, organizational-technical, and economic approaches to combating these sources of threat. Finally, in summarizing the international system, the doctrine recognizes leading world powers' efforts to develop information weapons, warns of an impending arms race, and emphasizes the need for an international approach for safeguarding Russia's information space.[183]

The tone of the *Information Security Doctrine of the Russian Federation*, according to Keir Giles, is entirely defensive—there is no mention of offensive operations.[184] Although the document appears to take a holistic approach to information security, it lists several concepts that differ from Western approaches to security. The most important divergence is an illiberal attitude toward the media. Regardless whether a media entity is private or state-owned, the doctrine states that it is acceptable and essential that the government ensures pro-Russian messaging. The Russian government

---

[181] "Information Security Doctrine of the Russian Federation."

[182] Thomas, "Russian Information Warfare Theory, " 275-6.

[183] "Information Security Doctrine of the Russian Federation."

[184] Giles, "'Information Troops,'" 47-8.

clarified that this position intended only to provide state oversight and not censorship, but Giles argues that historical evidence suggests the latter outcome.[185]

Surprisingly, despite the depth of information security guidance in the *Information Security Doctrine*, the *Russian Federation National Security Strategy Through 2020*, approved on 12 May 2009, barely addresses this security area. This key official guidance and planning document for Russian security services, while describing in-depth a multitude of criminal, economic, and healthcare threats and security strategies, approaches information security challenges only indirectly. In describing the international environment, the strategy recognizes that global information confrontations exist and will escalate, and that illegal activity using cybernetic and other technological weapons will threaten Russian interests.[186] Consequent strategic guidance, however, is sparse and vague:

> ensuring...the availability of information technologies and also information on the various issues of society's sociopolitical, economic, and spiritual life…
>
> developing information and telecommunications technology, computer hardware, electronics, telecommunications equipment, and software industries…
>
> overcome the technological lag in the most important spheres of information science, telecommunications, and communications that determine the condition of national security...and also provide conditions for the harmonization of the national information infrastructure with global information networks and systems…
>
> threats to information security are to be prevented by improving the security of the functioning of the information and telecommunications systems of critically important infrastructure facilities...and by creating a single information-telecommunications support system for the needs of the national security system.[187]

---

[185] Giles, "'Information Troops,'" 70-1.

[186] "Russia's National Security Strategy to 2020," *Rustrans Useful Translations*, last modified September 17, 2012, http://rustrans.wikidot.com/russia-s-national-security-strategy-to-2020.

[187] Ibid.

Though these tasks address threats to Russia's cyber civil society, supply chain, and critical infrastructure, the *National Security Strategy* fails to address Russians' perceived global information confrontation or the disruptive effect of cyber weapons.

It is possible that this paucity of guidance reflects the Russian government's lack of information security concerns in 2009, but considering the high degree of reflection on the information warfare campaign during the previous year's Russo-Georgian conflict, this seems unlikely. Keir Giles offers one explanation—President Medvedev intended the document to focus on economics and to convey a positive, aspirational tone of a newly confident and cooperative Russia.[188] Yet another possibility is that the Russian government restricted in-depth strategic consideration of information war to classified documents. Whatever the explanation, the lack of substantive discussion of information and cyber security in the *Russian Federation's National Security Strategy Until 2020*, especially relative to the more overt defensive posture described in the *Information Security Doctrine*, confounds a clear interpretation of Russia's cyber posture.

2. Military Doctrine

Historically, Russia's cyber capabilities were concentrated in the nation's security services. The FSB maintains and operates SORM; Roskomnadzor controls information blacklists; and the MVD's Directorate K focuses on information crime issues. The Federal Agency for Government Communications and Information was briefly tasked with information security, but the agency was disbanded in the 1990s and its capabilities redistributed among larger security organizations. In comparison to these agencies' various level of cyber capability, the Russian military has only maintained an electronic warfare force.[189] Following the criticism of the Russo-Georgian War, however, President Medvedev undertook military reform that included a directive to "develop forces and resources for information warfare."[190]

---

[188] Keir Giles, *Russia's National Security Strategy to 2020* (NATO Defense College, June 2009): 4-5, 11, http://www.conflictstudies.org.uk/files/rusnatsecstrategyto2020.pdf.

[189] Giles, "'Information Troops,'" 51-3.

[190] "The Military Doctrine of the Russian Federation," *The School of Russian and Asian Studies*, last modified February 2, 2010, http://www.sras.org/military_doctrine_russian_federation_2010.

The *Military Doctrine of the Russian Federation*, approved on 5 February 2010, responded to the national defense tasks in the *Russian Federation's National Security Strategy Through 2020* and codified President Medvedev and Defense Minister Serdykov's reform initiatives. Because the document's intent was to support reform measures, the doctrine focuses mainly on Russia's efforts to transition from a mass-mobilization Soviet-era military to a highly mobile permanently ready professional force. Nonetheless, it contains several interesting observations about the international system and the nature of modern warfare.

The foremost assertion is that future military conflicts will include a cyber or informational component. According to the doctrine, the role of information warfare will intensify while new weapons systems "based on new physical principles" will be "comparable to nuclear weapons in terms of effectiveness."[191] Additionally, military conflicts will combine military and nonmilitary forces and resources—a possible reference to irregular combatants or surrogate forces such as the ones typical of Russian-affiliated cyber attacks.[192] During future conflicts, information warfare will be essential for pre-conflict shaping of the political space and for "shaping a favorable response from the world community to the utilization of military force."[193] Clearly, the information troops that the doctrine establishes will have a role in Russian military art.

Whether this role will be offensive or defensive is not clear from the doctrine. The sections on external dangers and threat analysis only vaguely refer to information threats: efforts to destabilize states and regions on Russia's periphery and interference in the internal affairs of the Russian Federation.[194] Likewise, the doctrine does not outline any specific deterrence tasks or wartime tasks of a cyber or information warfare nature. At most, the doctrine describes the need for information systems support for its military modernization plans.[195] It may be the case that such tasks and analysis may be too

---

[191] "Military Doctrine of the Russian Federation. "

[192] Ibid.

[193] Ibid.

[194] Ibid.

[195] Thomas, "Russia's Information Warfare Strategy, "114-5.

ambitious for a doctrinal document that first seeks to establish information warfare troops. It is also possible that the Russian Federation does not consider these threats as sufficiently serious to define in doctrine. As with the *National Security Strategy*, the Russian Federation's military doctrine takes an ambiguous position; though it recognizes the importance of information warfare to Russian security and in military conflicts in general, it does not describe the Russian approach to cyber warfare.

Shortly after the release of the *2010 Military Doctrine*, the Russian Ministry of Defense published the *Conceptual Views Regarding the Activities of the Armed Forces of the Russian Federation in Information Space*. Keir Giles describes the *Conceptual Views* as "a Russian military cyber proto-doctrine" and "the first explicit public statement of the Russian military's role in cyberspace."[196] Though the document is a relatively succinct fifteen pages of terms and definitions, principles, rules, and confidence building measures, it provides new insight into the Russian military's development in cyberspace doctrine.

Like previous Russian literature about information operations and war, the *Conceptual Views* defines the operational terms from an information-centric perspective. It defines information war as actions that may damage information systems and resources; undermine political, economic, and social systems; brainwash the population; or coerce the victim government. The information space within which information war may take place is the "area of activity related to the formation, creation, transformation, transmission, use, and storage of information."[197] These definitions reflect a broader perspective than the U.S. definition, which considers cyberspace as a domain within the information environment.[198] As defined in the *Conceptual Views*, the Russian concept of an information war is an amalgam of U.S. cyber operations and information operations doctrines. Unlike the American doctrine that categorizes cyber operations as offensive,

196 Giles, "Russia's Public Stance," 67.

197 "Conceptual Views," 5.

198 Joint Publication 3-12, "Cyberspace Operations," (Washington, DC: Joint Chiefs of Staff, 2013), v, http://www.dtic.mil/doctrine/new_pubs/jp3_12R.pdf.

defensive, or sustainment, however, the *Conceptual Views* only specifies defensive cyber operations.[199]

In addition to outlining strictly defensive operations, the *Conceptual Views* also delineates a narrow scope of military responsibilities. It tasks the Armed Forces of the Russian Federation with solely their own information security. Although a secondary task of the Armed Forces is to provide broader information security, the military's priority is on the defense of the Armed Forces—identifying threats and avoiding disorganization of command and control, disruption to military logistics, and demoralization of the military.[200] The task of broader national defense against military-political information threats is less apparent. These implementation measures consist of interagency coordination, early threat detection, and international cooperation and norm-setting.[201]

Though the *Conceptual Views* emphasize the centrality of international institutions for maintaining information security, it emphasizes the need for international norms, regulations, and non-military conflict resolution under the U.N. aegis, rather than through regional collective security arrangements. This focus, argues Giles, also distinguishes the Russian military's approach to information warfare from the West's.[202] As he points out, the Russian military's task to promote international institutions is atypical for Western militaries. The reason for this focus may be that the Russian government genuinely considers its Armed Forces as champions of its non-military foreign policy initiatives, but the more likely explanation is that the Russian government lacks confidence in the Army's ability to provide for its own information security.

The latest iteration of Russian military doctrine on cyber operations may be the so-called Gerasimov doctrine. This unofficial doctrine, published in *Voyenno-Promyshlennyy Kuryer* in 2013 by Russian Armed Forces Chief of General Staff Army-General Valery Gerasimov, represents a potential future development of the Russian

---

[199] Giles, "Russia's Public Stance," 67-8.

[200] "Conceptual Views," 7-10.

[201] Ibid., 8, 10-1.

[202] Giles, "Russia's Public Stance," 69.

military art.[203] Giving credence to speculation that this article represents official views, Russian operations in Crimea and Eastern Ukraine, called hybrid war or non-linear war by commentators, demonstrate many facets of Gerasimov's ideas—the conflict in Ukraine consists of "simultaneously occurring guerrilla and conventional fighting, economic, cyber, and information war."[204] Unlike in Russia's official military doctrine, cyber operations play an essential and prominent offensive role in the Gerasimov doctrine.

The underlying postulate of the new doctrine, as Mark Galeotti highlights in his review of Gerasimov's article, is that the rules of war have changed—non-military means may be more effective than conventional ones.[205] This realization about 21st Century conflicts requires a new approach to war, and the main purpose of the article is a call for action for Russian military academics to address Gerasimov's observations about the international system and the nature of warfare. His key points in relation to cyber and information warfare are:

- Conflict increasingly consists of information and other non-military means
- Covert actions and irregular forces are increasingly important in information confrontation
- The distinctions between strategic, operational, and tactical levels and offensive and defensive operations are disappearing
- Information weapons enable asymmetric operations that counteract adversary advantages and allow the formation of a resistance front throughout the entirety of enemy territory
- Information confrontation creates opportunities to lower the adversary's combat potential.[206]

---

[203] Roger McDermott, "Myth and Reality—A Net Assessment of Russia's 'Hybrid Warfare' Strategy Since the Start of 2014 (Part One)," *Eurasia Daily Monitor* 11, no. 184 (October 17, 2014), http://www.jamestown.org/programs/edm/single/?tx_ttnews%5Btt_news%5D=42966&cHash=6807c1930eae4cbece171314536d557c#.VMwHucbn3GA.

[204] Margarita Šešelgytė, "Can Hybrid War Become the Main Security Challenge for Eastern Europe?," *European Leadership Network*, last modified October 17, 2014, http://www.europeanleadershipnetwork.org/can-hybrid-war-become-the-main-security-challenge-for-eastern-europe_2025.html.

[205] Galeotti, "'Gerasimov Doctrine.'"

[206] Valery Gerasimov, "Tsennost' Nauki v Vredvidenii [Value of Applied Science]," *Voyenno-Promyshlennyy Kuryer*, last modified February 27, 2013, http://www.vpk-news.ru/articles/14632.

The nature of modern conflict necessitates that information warfare spans all phases of conflict and includes military and non-military forces (see Figure 2).

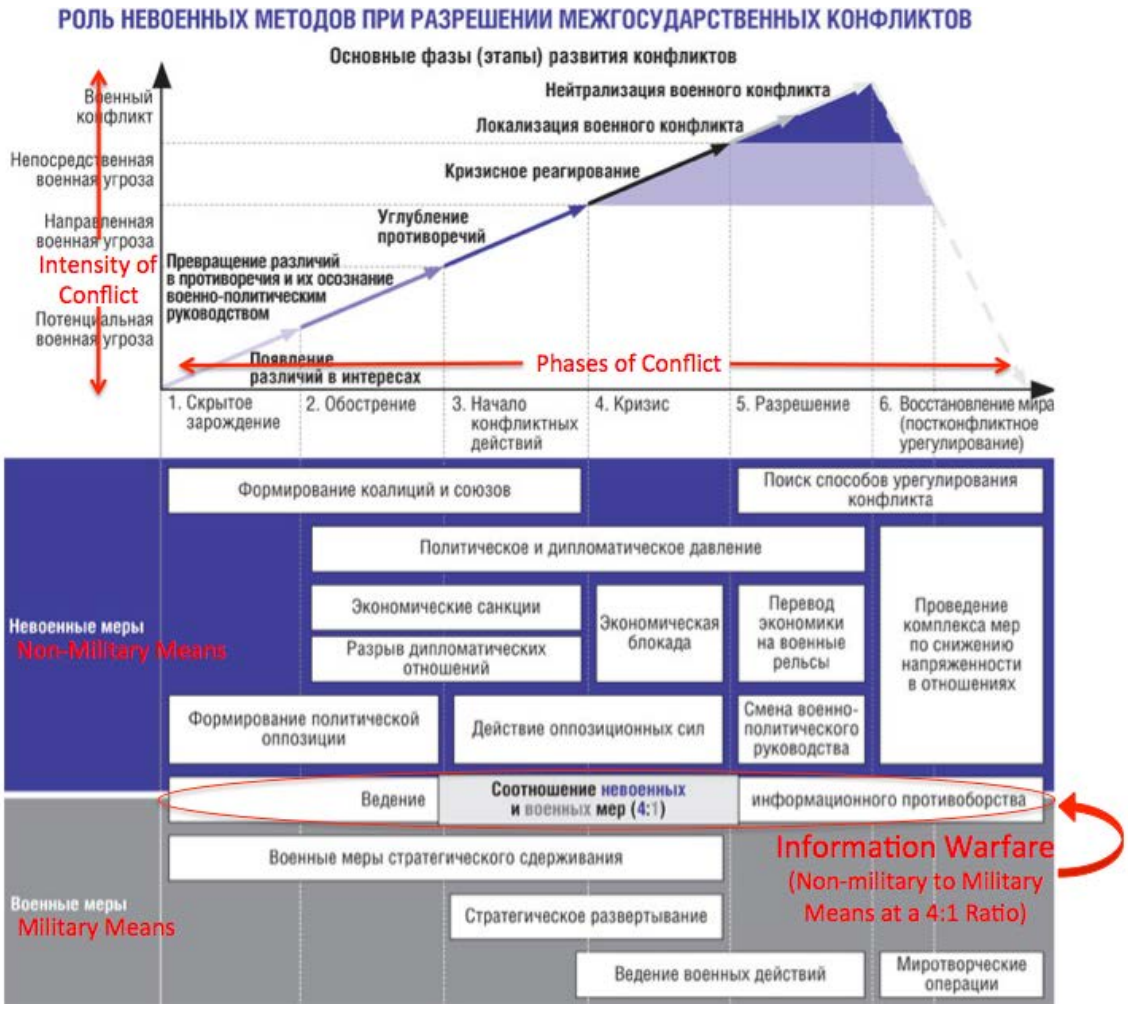

Figure 2. Role of Non-military Means for Resolving Interstate Conflicts According to the Gerasimov doctrine.[207]

Gerasimov's article, if it eventually translates into Russian military doctrine, establishes an aggressive, offensive cyber posture. Information activities against another state may begin ahead of overt political and military crises, and if executed according to doctrine, will employ means and methods that will be difficult to attribute to the military and to the Russian Federation. Disconcertingly, the doctrine does not discuss the use of

[207] Gerasimov, "Tsennost' Nauki v Vredvidenii." [The author's translations are in red font.]

information weapons for deterrence or de-escalation during the initial phases of conflicts—instead, information weapons will have only an offensive role.

This doctrinal formulation of the role of information weapons is potentially highly disruptive to international security. By doctrinal implication, all pro-Russian activity in the information environment is potentially threatening to other states. A Russian company's investment into another nation's telecommunications infrastructure may be a covert Phase 1 attempt to gain access to critical infrastructure. Similarly, a DDoS attack or a website defacement of a particular political group may signal an attempt to influence political opinions or morale. A significant security problem stemming from the Gerasimov Doctrine is that countries that consider Russia as a potential security threat may now see neutral Russian actions or hostile non-Russian actions in cyberspace as covert hostile acts in preparation for a wider conflict. Although according to the realist worldview, states are naturally distrustful of other states, the Gerasimov Doctrine exacerbates mistrust toward Russia.

C. INTERNATIONAL POSITION

It is apparent from unofficial and official Russian information warfare discussion that international engagement in cyberspace is an essential element of their cyber posture—Timothy Thomas considers international efforts to be one prong of Russians' strategic approach to security.[208] These efforts at international engagement have not always been successful at creating international consensus, but they have outlined a clear vision for a potential Internet structure. More so, this Russian proposition for international cyber norms is already being implemented through regional Eurasian blocs: Russia's vision for information security is not just rhetorical.

1. United Nations

The Russian Federation's substantive efforts to shape the international cyber discussion began in 1998, with Russia's modest proposal at the United Nations General Assembly's Fifty-third session to solicit information security views and assessments from

[208] Thomas, "Russian Information Warfare Theory, " 267-8.

member states. Specifically, Resolution 53/70, "Developments in the Field of Information and Telecommunications in the Context of International Security," called on U.N. members to promote international consideration of information threats and invited members to provide their views on information security in general, on definitions, and on the advisability of developing international principles to address information terrorism and criminality.[209] Though it recognized information technology's potential military applications, the resolution did not address information security as a military issue, however.

The resolution achieved its intent of opening an international dialogue on information security. For example, in the 2010 "Report of the Secretary General," in response to A/RES/53/70, Cuba took the opportunity to express its concerns with "radio-electric aggression against Cuba from United States," accusing the United States of violating Cuba's sovereignty through provocative and subversive radio and television broadcasts.[210] A similar report from Georgia in A/RES/69/112 voiced the state's concerns about the use of cyber weapons during the 2008 Russo-Georgian conflict.[211] This forum has also allowed NATO and OSCE member states to articulate their perspectives on international information security strategies.

More importantly, Russia's 1998 resolution also initiated a parallel U.N. process for studying cyber threats. Again thanks to Moscow's advocacy, the U.N. assembled a fifteen-member Group of Governmental Experts (GGE) with a mission to evaluate cyber threats and to propose cooperative solutions. The Group's first effort in 2004 failed; according to the GGE's report to the Secretary-General, "given the complexity of the issues involved, no consensus was reached on the preparation of the final report."[212] The main stumbling block, according to a member of the Russian delegation, was the

---

[209] Developments in the Field of Information and Telecommunications in the Context of International Security, A/RES/53/70, United Nations, 53rd sess. (1999).

[210] Report of the Secretary-General, A/RES/65/154, United Nations, 65th sess. (2010): 2-5.

[211] Report of the Secretary-General, A/RES/69/112, United Nations, 69th sess. (2014): 9-10.

[212] Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, A/60/202, United Nations, 60th sess.(2005): 2.

applicability of international humanitarian law.[213] The U.N. Office for Disarmament Affairs clarifies the issues faced by the first GGE:

> The first issue was the question of the impact of developments in information and communications technologies (ICTs) on national security and military affairs. While there was general agreement regarding the importance of such developments, consensus could not be found on the amount of emphasis to be placed on this concern, and whether or not to include language that stressed the new threats posed by State exploitation of ICTs for military and national security purposes.
>
> The second issue was the question of whether the discussion should address issues of information content or should focus only on information infrastructures. There was particular disagreement regarding the claim that trans-border information content should be controlled as a matter of national security.[214]

In short, the GGE was divided on whether information security considered only hostile code or also recognized hostile content.

Despite the initial impasse, the GGE succeeded in publishing its first report in November 2005. Of the 164 nations voting, the United States was the sole country to vote against the draft information security resolution in that report.[215] The cause of the resolution's contentiousness was the U.S. concern that information technologies "may adversely affect the integrity of the infrastructure of States to the detriment of their security in both civil and military fields."[216] What the United States considered implicit in the resolution was an attempt to establish the groundwork for measures that would allow states to restrict perceived malicious information flow across state boundaries. The United States also stated that the Russian proposal failed to focus on cybercrime and

---

[213] Tim Maurer, "Cyber Norm Emergence at the United Nations—An Analysis of the UN's Activities Regarding Cyber-security, " Discussion Paper 2011-12, Science, Technology, and Public Policy Program, Belfer Center for Science and International Affairs, Harvard Kennedy School, (September 2011): 22.

[214] "Fact Sheet: Developments in the Field of Information and Telecommunications in the Context of International Security," U.N. Office for Disarmament Affairs, last modified June 2013, http://www.un.org/disarmament/HomePage/factsheet/iob/Information_Security_Fact_Sheet.pdf.

[215] Developments in the Field of Information and Telecommunications in the Context of International Security, A/60/452, United Nations, 60th sess. (2005): 2.

[216] Developments in the Field of Information and Telecommunications, 3.

unnecessarily emphasized military concerns, which the United States considered to be already addressed under existing international humanitarian law.[217]

The 2005 resolution included provisions for subsequent GGEs, which produced reports in 2009 and 2013. The second and third GGE's reports and resolutions have advanced the discussion on information security. The 2013 report, A/68/98, recognized the dual-use nature of Information and Communications Technologies (ICT) as either legitimate or malicious, the security challenge posed by global interconnectedness and anonymity, and the hostile potential of state and non-state actors. It also emphasized responsible state behavior, particularly state sovereignty and jurisdiction over ICT infrastructure, as well as states' responsibilities for proxies and operation of non-State actors within national jurisdiction.[218] This formulation seems to be a Russian concession to accusations of its permissive attitude toward the pro-Russian cyber attacks against Estonia and Georgia; by condemning and disavowing as illegitimate the sort of hostile acts that were previously associated with Russia, Russia's diplomats have in return gained acceptance of broader definitions of threats and inserted references to domestic cyber sovereignty and hostile content. The potential significance of the current stage of U.N. discussion might, therefore, be a mutual recognition of subjective cyber threats perceived by the Western and Russian governments.

Perhaps just as important as its success in shaping the cyber terminology via U.N. resolutions, Russia has managed to increase international support for its initiatives and perspective. Through 2005, Russia was the sole sponsor of its resolutions on information security. From 2006 to 2009, Russia attracted 29 cosponsors, including the People's Republic of China. In 2010, The United States also joined as a co-sponsor—a notable change of position for a state that had voted against the resolutions from 2005–2008 (the United States neither co-sponsored nor vetoed the resolution in 2013).[219] This trend,

---

[217] Developments in the field of Information and Telecommunications in the Context of International Security, Addendum, A/59/116/Add.1, United Nations, 59th sess. (2004): 3-4.

[218] Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, A/68/98, United Nations, 68th sess. (2013): 6-7.

[219] Maurer, "Cyber Norm Emergence," 26-7.

however, does not necessarily imply that the Russian position has shifted closer to the U.S.'s. Among the 43 cosponsors of the 2013 Resolution were Belarus, China, Cuba, the Democratic People's Republic of Korea, Myanmar, the Syrian Arab Republic, Sierra Leone, Turkmenistan, and the Sudan—not a single E.U. member state cosponsored it.[220] It appears that Russian advocacy of cyber norms favoring its cyber threat perception is gaining increasing support in the U.N.; the Russian Federation's vision of an international information security regime seems to have attracted a following of like-minded states.

The Shanghai Cooperation Organization (SCO) is the core of the international bloc through which the Russian Federation is attempting to influence the global international system. Following Russia's successful sponsorship in 2005 of A/RES/60/45, "Developments in the Field of Information and Telecommunications in the Context of International Security," the heads of SCO member states released a statement on information security, endorsing the U.N.'s approach. Several Russian information security concerns are evident in the statement: ICT threats to internal affairs of sovereign states, military and political ICT uses that threaten international stability, and the ongoing use of ICTs by some countries that adversely affect the whole world.[221] Unlike the U.N. resolutions' wording that leaves room for multiple interpretations, Russia's position expressed via the SCO is unambiguous: Russia believes that the United States is using information weapons, or hostile content, to destabilize other states, interfering in their internal affairs.

In 2011, four members of the SCO, China; Russia; Tajikistan; and Uzbekistan, appealed to the U.N. for an *International Code of Conduct* for information security. Though the preamble to the *Code of Conduct* echoed the wording of U.N. resolutions, its recommendations more closely resembled SCO statement on information security. Foremost in the *Code of Conduct* is a pledge to neither carry out hostile acts nor

---

220 Developments in the Field of Information and Telecommunications in the Context of International Security, A/68/406, United Nations, 68th sess. (2013): 2.

221 "Zayavleniye Glav Gosudarstv-Chlenov SHOS po Mezhdunarodnoy Informatsionnoy Bezopasnosti [Statement of Heads of SCO Member States on International Information Security]," The Shanghai Cooperation Organization, last modified June 15, 2006, http://www.sectsco.org/RU123/show.asp?id=107.

proliferate information weapons. The *Code of Conduct* pledge repeatedly stresses mutual respect of state sovereignty—states may defend their information space against various threats according to their own definitions of such threats, and according to their own definitions of rights and freedoms in the information space. In addition, states that accept the *Code of Conduct* must also cooperate with other states in "curbing the dissemination of information that...undermines other countries' political, economic, and social stability."[222] Russia's proposed *Code of Conduct* not only codifies content as hostile, but also obligates other states to assist Russia in removing hostile content, even within their own cyberspace.

Though Russian efforts at the United Nations have not resulted in a predominantly pro-Russian international consensus, they are indicative of Russia's posture and intentions. The Russian Federation continues to work toward an international framework that establishes cyber assurances and reduces the cyber arms race as Russia sees that race to be unfolding. Its defensive tone is slowly gaining international acceptance and support as other illiberal democracies and authoritarian regimes that share Russian security concerns align themselves with Russia's position.

2. Draft Convention on International Information Security

Within ten days of proposing the *Code of Conduct* to the U.N., Russia presented a conceptual *Convention on International Information Security* at the 2nd International Meeting of High-Ranking Officials Responsible for Security Matters—an effort to shape international discourse concurrently with similar U.N. efforts. This document is a lucid articulation of Russian perceptions of information threats, and Russia's international agenda. Keir Giles succinctly summarizes the draft *Convention*: the Russian vision of Internet governance espouses "important caveats on the flow of information and an insistence on national sovereignty in cyberspace."[223]

---

[222] Letter Dated 12 September 2011 From the Permanent Representatives of China, the Russian Federation, Tajikistan, and Uzbekistan to the United Nations Addressed to the Secretary-General, A/66/359, United Nations, 66th sess. (2011): 4.

[223] Giles, "Russia's Public Stance," 67.

From the outset, Russia proposes a trade-off between freedom of information flow and openness, in Article 1, Subject and Aim of the *Convention*. The *Convention* defines the rights of government in the information spaces as "compatible with the right of each individual to seek, receive, and distribute information and ideas, as is affirmed in UN documents, while keeping in mind that this right may be restricted through legislation to protect the national and social security of each State" and "guaranteeing the free exchange of technology and information, while maintaining respect for the sovereignty of States."[224] In order to promote international peace and security, including non-interference in domestic issues, the *Convention* proposes a version of the Internet subject to the domestic politics of participating states.

These aims follow from Russia's definition of information threats to international security. Of the eleven stated threats, three derive from the Russian understanding of the information-psychological aspect of information warfare:

> 4) actions in the information space aimed at undermining the political, economic, and social system of another government, and psychological campaigns carried out against the population of a State with the intent of destabilizing society…
>
> 6) the dissemination of information across national borders, in a manner counter to the principles and norms of international law, as well as the national legislation of the government involved…
>
> 8) the manipulation of the flow of information in the information space of other governments, disinformation or the concealment of information with the goal of adversely affecting the psychological or spiritual state of society, or eroding traditional cultural, moral, ethical, and aesthetic values[225]

These threats are also captured in the *Convention's* definition of information warfare, which, in addition to information-technical attacks, includes psychological campaigns intended to destabilize society and government.

In its principles for ensuring international information security, the *Convention* reiterates the observance of non-use of force, illegality of information warfare, non-

[224] "Convention on International Information Security."

[225] Ibid.

interference in foreign information spaces, necessity for balancing human rights and information security, and primacy of national sovereignty with respect to Internet governance. It also introduces appeals to the notion of indivisibility of security, prohibiting states from strengthening "their security at the expense of the security of other states."[226] This appeal, as Keir Giles argues, is based on loaded term that masks different understandings of "indivisibility of security" by Russia and the West.[227] What the *Convention* implies behind the concept is unclear, but based on the subsequent principle addressing the need for bridging a digital divide among various states, Russia may be alluding to U.S. investment in military cyber forces. If so, the *Convention* echoes Jervis's definition of the security dilemma; a situation in which purely defensive investments increase the insecurity of other states. For this to occur, however, postures must be indistinguishable as offensive or defensive. Therefore, Russia's claim that other states' information security investments violate the principle of indivisibility of security implies that Russians view the international environment as one in which cyber postures cannot be easily distinguished.

Chapters 2, 3, and 4 of the draft *Convention* propose measures for averting military conflict, preventing terrorist use, and counteracting illegal activities. Among these proposed measures several stand out. To prevent military conflict, states adopting the *Convention*, must agree not only to refrain from undertaking or threatening with hostile actions, but must also "refrain from developing and adopting plans or doctrines capable of increasing threats...straining relations."[228] States must also take measures to prevent "untruthful or distorted messages" originating within their own information space that other states might consider hostile.[229] Effectively, the *Convention* seeks not just a freeze on military development in cyberspace, but mandates that states take action to assuage the security concerns of other states, according to those states' threat perceptions. This framework for international security extends the responsibility for states to respond

---

[226] "Convention on International Information Security."

[227] Giles, "Russia's Public Stance," 65.

[228] "Convention on International Information Security."

[229] Ibid.

to the actions of domestic non-state actors, upon the request of aggrieved states, suggesting that not all states have the domestic capacity to defend themselves.

Though Russia has not advocated for this conceptual convention to be proposed at the United Nations, it has presented an alternative to Western approaches, particularly to the *Council of Europe Convention on Cybercrime* that Russia has not signed.[230] The *Convention* articulates a vision for the Internet that may appeal to states that are not able to safeguard their information space. Its emphasis on military restrictions along with criminal countermeasures likely reflects its own insecurity and defensive orientation. Russia appears willing to cooperate internationally, preventing events like the 2007 Estonia cyber attacks or curbing its cybercriminal underground, to gain broader security guarantees and to halt the development of America's military cyber power. This may imply that Russia places more strategic value on defending against its perceived global information threat than on the offensive capability used during the Estonia attacks.

D. HYPOTHESIS ASSESSMENT

The dominant theme throughout Russian scholarly discourse, official documents, military doctrine, and international efforts is that Russia feels vulnerable in cyberspace relative to other great powers, and takes a defensive posture on cyberspace issues.[231] Cyber power, according to David Betz and Tim Stevens, can be subdivided as compulsory, institutional, structural, or productive.[232] The Russian position seems to recognize a capability gap in its compulsory, structural, and productive cyber power; consequently, Russia appears to focus its efforts on developing and exercising its institutional cyber power. The intent of these efforts is either to eliminate Russia's cyber vulnerabilities through an international prohibition on the types of weapons that they perceive as threatening, or to buy time to develop its own offensive capability by stalling leading cyber powers. This interpretation supports H3. *Russia's cyber capability is*

230 Giles, "Russia's Public Stance," 66-67.

231 [This analysis assumes that Russian sources genuinely convey Russian security concerns, and that they are not deliberately misleading. Because Russia places high value on information operations, this may be an incorrect assumption, but the author did not find sources that suggest a misinformation campaign.]

232 David J. Betz and Tim Stevens, "Chapter One: Power and Cyberspace," *Adelphi Series* 51, no. 424 (2011): 42-53. doi: 10.1080/19445571.2011.636954.

offensive and the posture is distinguishable as either offensive or defensive and H4. *Russia's cyber capability is defensive and the posture is distinguishable as either offensive or defensive*. There are several nuances to Russia's position that potentially weaken this interpretation, however.

First, because the Russian concept of cyber capability is inextricably linked to the notion of information confrontation, its posture reflects Russia's unique understanding of the international system. That is, Russia's defensive posture reflects a different set of threats and a different understanding of a security dilemma. The West's understanding of the cyber security dilemma does not consider, for example, non-governmental organizations that promote democratic reforms as a potential means of hostile confrontation—Russia's understanding does. Because of this divergent understanding, Russia sees its own vulnerabilities and hostile enemy capabilities where others might not. Thus, in considering Russia's posture and intentions, it is important to recognize that if its state-level intentions or posture seems inconsistent with an international-level understanding of the security dilemma, this may be the consequence not of Russian deliberate misalignment or misunderstanding or the international system, but instead the result of a fundamentally different understanding of cyber power.

Another confounding factor is the longitudinal aspect of this chapter's analysis—Russia's posture has changed over time. Though the documents differ in scope and focus, the shallow consideration of information security issues in the *Russian Federation National Security Strategy Through 2020* may suggest that Russian insecurity is decreasing relative to the security assessment at the publication of the *Information Security Doctrine*. At the very least, the sparse references to information security in *National Security Strategy* make assessment of Russia's posture more difficult than the clearly expressed concerns of the much earlier *Information Security Doctrine*. This Chapter's cross-sectional methodology that also considered international efforts and scholarly opinions may mitigate some of these concerns, however. The contemporaneous stance of Russian scholars and military officers, as well as Russian international efforts, compensate for the *National Security Strategy's* ambiguity.

Developments in the Russian military doctrine also complicate posture analysis. The *Military Doctrine of the Russian Federation* appears to be defensive, but vague; the *Conceptual Views Regarding the Activities of the Armed Forces of the Russian Federation in Information Space* was defensively-minded; and the Gerasimov doctrine appears highly aggressive. This apparent contradiction of doctrinal views reduces the level of certainty in Russia's cyber posture. It may be possible to reconcile these contradictory views somewhat. Russia's defensive posture seems oriented toward Russia's perceived global information confrontation with America. Russia's offensive posture, on the other hand, is oriented toward its near abroad. Depending on the relative balance of cyber power, Russia acts defensively or aggressively. Alternatively, it may be the case that Russia's aggression on its periphery stems from its defensive insecurity. As John Mearsheimer argues more broadly about the conflict in Ukraine, Russia's aggressive actions toward its neighbors may be seen as a defensive a reaction to encroachment on a great power's periphery.[233]

In summary, this chapter evaluated whether Russia's cyber posture is distinguishable—Robert Jervis's second critical variable that determines the security dilemma. The author's conclusion based on Russian public and official sources suggests that the posture is most accurately distinguished as defensive. Like Russia's changing cyber weapons investments, this posture is also dynamic. In addition to the inherent difficulty in ascertaining whether the publically-perceived posture genuinely reflects the Russian government's actual intentions, inconsistencies among Russian sources might suggest that the Russian cyber posture is changing. Nonetheless, the preponderance of evidence points to a predominantly defensive posture.

[233] John Mearsheimer, "Why the Ukraine Crisis Is the West's Fault," *Foreign Affairs* 93, no. 5 (September 2014): 77-89. Business Source Complete, EBSCOhost (accessed February 1, 2015).

IV. CONCLUSION

This final chapter uses the evidence, findings, and warrants from the previous evidentiary chapters that evaluated Russia's cyber power according to Robert Jervis's offense-defense variables. The first section determines the dominant hypothesis that answers the author's research question: what are Russia's capabilities and intentions in cyberspace? Based on the dominant hypothesis, the following section addresses the study's implications and significance for both the international relations understanding of Russian cyber power and the efficacy of using offense-defense theory to study this issue. The final section of the chapter acknowledges the limitations of this study and proposes topics for subsequent research.

A. HYPOTHESIS ASSESSMENT

Chapters II and III ascertained that Russia's cyber capability is offensive and that its posture is distinguishable, specifically that it is defensive. These conclusions support hypothesis three:

> H3. *Russia's cyber capability is offensive and the posture is distinguishable as either offensive or defensive.*

According to Robert Jervis's Four Worlds model, an international system that reflects this hypothesis does not inherently lead to a security dilemma, but it does allow for circumstances under which revisionist or even status-quo states might war.[234] If the postures of all major states were like Russia's, according to Jervis, "states will have to watch each other carefully, and there is room for false suspicions"; it is a world in which stability depends on early warnings.[235] In cyberspace, surveillance and detection of aggressive intentions is especially difficult; and Russia's bellicose behavior, aggressive Gerasimov doctrine, and overt efforts at manipulating international perceptions suggest that other states should be especially wary of the Russian Federation.

---

[234] Jervis, "Cooperation Under the Security Dilemma, " 213-4.

[235] Ibid., 213.

Recent Russian efforts seek to harden its cyber terrain as well as improving domestic Internet governance, perhaps signaling that it is attempting to dampen security dilemma pressures. This may not necessarily be the case, however, since even defensive investments might make other states feel more insecure. For example, Russian restrictions on anonymous domestic Internet use may limit Russia's own offensive capability since it will be more difficult to conduct unattributed attacks from within Russia's cyber terrain, but such changes also increase the cost for others to conduct attacks on Russian targets. Similarly, although Russian law enforcement authorities dismantled the Russian Business Network cybercrime organization, a sophisticated and decentralized cyber underground has emerged in its place. Russian investments in domestically focused firewalls, content filters, and SORM devices appear to defend against domestic hostile content, but the underlying technology can be reoriented externally as well. Russia's goal appears to be to create a fractured Internet and to have the ability to exert control over the content and logic within its cyberspace. The following section outlines some possible consequences of a "fractured Internet."

Although Russian documents cite purely defensive security concerns for these developments, they may in reality be a defensive buildup to deny preemptive or counter attacks. It may be more likely that Russia is on a trajectory that would move it closer to Jervis's unstable first world case; a world in which offense dominates, and the posture is indistinguishable as offensive or defensive. Specifically, Russia has muddled the degree to which states can clearly distinguish its posture as defensive. Whereas Russian academic and military discussions of cyber power increasingly discuss its offensive applications as both hostile code and content, Russian official doctrine and government policy makes less mention of cyber security considerations. This may suggest a shift in Russian posture toward a more aggressive and secretive stance; the Gerasimov Doctrine may have provided an unofficial insight into this new, more aggressive view on employing cyber power. As with Russia's initiatives to harden its cyber terrain, this change in posture similarly increases uncertainty about Russia's intentions; this increased uncertainty and reliance on perceptions is likely to increase security dilemma pressures on the international system, or at least among Russia's neighbors.

Additionally, although this paper applied Jervis's offense-defense theory at the state level, the resulting hypothesis should also be interpreted in the context of the international system. Russia's security concerns appear to be based on perceived vulnerability relative to the aggressive behavior of other great powers—responding to their content-as-a-weapon offensive intended to destabilize Russia's domestic environment, according to Russian leaders. Despite this publically-articulated security concern, Russians, or pro-Russian proxies, have also used its offensive cyber capabilities against their neighbors. Russia's capabilities, perceptions, and posture in cyberspace, therefore, differ depending on one's perspective; it acts defensively relative to other great powers, but offensively as a would-be regional hegemon.

Although this net assessment appears nuanced, it fits a theoretical pattern that Stephen van Evera hypothesized as a consequence of the offense-defense theory paradigm for the causes of war. He described ten explanations for why some states may choose to go to war in a world in which offense dominates, and two of these complimentary hypotheses appear to match Russia's behavior: defensive expansionism and fierce resistance to expansion.[236] According to van Evera, when conquest is easy, states compete more aggressively for resources on their periphery, creating buffer zones, expanding their own resources, and, importantly, preempting adversaries' expansion into the same space.[237] Applying this concept to the cyber domain, using the Russian concept of both hostile code and hostile content, Russian cyber aggression towards its neighbors is an attempt to preempt or thwart what current Russian leaders perceive—evidenced according to them by color revolutions and the Arab Spring—as adversarial expansion by hostile powers into the same information space. Russia's global defensive posture, but local aggressiveness, therefore, suggests that Russia's role in cyberspace may be categorized as motivated by defensive expansion.

Finally, the author anticipated that a potential research outcome could be an inapplicability of offense-defense theory to the subject of Russian cyber capability—hypothesis five. With modifications to suit a state-level analysis and the distinctive

[236] van Evera, "Offense, Defense, and the Causes of War," 7.

[237] Ibid., 7-9

properties of cyber power, this theoretical framework appears applicable and effective. More so, because the offense-defense paradigm assessment of Russian behavior comports with Stephen van Evera's theoretical pattern of state behavior, this approach also demonstrates internal theoretical consistency and parsimony for applying Robert Jervis's offense-defense theory to the study of cyber power.

B. LIMITATIONS AND FUTURE RESEARCH

The secrecy necessary to develop and preserve sophisticated cyber weapons and to establish and maintain persistent access to potential adversaries' cyber assets, as well as the difficulty in attributing offensive cyber operations, complicate cyber capability assessments. In the relatively short history of cyber conflict many of the key international cyber events have been associated with Russia, and this study benefits from having a historical record of what might otherwise be a silent arms race.[238] Despite the public knowledge and scholarly examination of Russia-affiliated cyber events, the evidence still presents analytic challenges. Most importantly, the challenge of positive attribution and the difficulty in assessing the degree of control that the Russian government has over its proxy cyber actors means that it is possible that the author incorrectly attributed these capabilities. Similarly, the secrecy of high-end Russian cyber weapons requires relying on other states' speculations about such capabilities. Official Russian documents also demand skepticism; it is almost certain that Russian doctrine and strategy in cyberspace is more thoroughly addressed in classified forums. These challenges are not as troubling as they appear, however. Russian-affiliated cyber attacks have typically relied on low-sophistication cyber weapons that were widely known and available; Russia's main cyber capability is not secret. States that perceive Russia as a cyber threat may, therefore, protect against most of Russian offensive cyber capability by investing in defenses against known vulnerabilities and exploits.

A merit of offense-defense theory is that it can incorporate and reflect the weapons capability uncertainty stemming from secrecy and attribution difficulties; the theory's virtue is that its variables fundamentally acknowledge states' perceptions and

[238] Huntley, "Offense, Defense, and Cyber War," 5.

partial information. Unfortunately, because perceptions, according to realist international relations theory, tend to reflect pessimistic expectations about others' intentions, states' assessments of an international system that relies on perceptions more than on facts, may lead to suboptimal foreign policy decisions and create more volatility than the actual situation warrants.

Another challenge is reconciling Russia's state-level assessment with the international-level view of the cyberspace security dilemma; Russia's understanding of cyber power that includes hostile content differs from the Western definition that does not. This difference in definitions complicates the understanding of the forces underlying the security dilemma. In describing the international environment, Jervis describes states' security demands as subjective; the vulnerability that states feel is situationally subjective.[239] Russia's feeling of insecurity in cyberspace is an extreme case of this phenomenon. Their belief that content can be hostile leads Russian leaders to feel threatened in situations in which other states might not perceive, or feel responsible for causing, a security threat. Aside from emphasizing offense-defense theory's acknowledgement of the subjectivity of security perceptions, the author does not see an elegant solution for reconciling security perceptions in an international system in which two different sets of states categorize different types of cyber operations as security threats. Additional research may resolve this challenge by comparatively examining U.S. doctrine for cyber-enabled information and psychological operations and the Russian doctrine for information warfare.

Finally, the author does not strive to recommend or comment on specific U.S. cyber policy, but instead proposes an offense-defense theory interpretation of divergent Western and Shanghai Cooperation Organization approaches to international Internet governance. The SCO bloc of countries consistently proposes internationally, and implements domestically, a policy that may lead to a fractured Internet, or at least a more nationalized implementation of their cyber terrain. This impulse appears to stem from these states' concerns that the open, indefensible current structure of the Internet presents

[239] Jervis, "Cooperation Under the Security Dilemma, " 174-6.

a security threat, due mainly to their perception that hostile content may destabilize their autocratic regimes. The U.S. and European Union bloc of countries, in contrast, recognize a threat based on malicious logic, but not content.

Russian emphasis on increasing cyber terrain defensiveness only reflects Russia's investment choices. The difference in Russian and Western perspectives of the cyber threat, and the resulting divergent defensive approaches, exacerbate the offense-dominance security dilemma pressures in cyberspace. However, further study is necessary to ascertain if a fractured Internet would fundamentally change the offense dominance of cyber weapons at the international level. For example, a potential approach to decreasing security dilemma pressures may be to support, or at least tolerate, a fracturing of cyberspace. If states divide the Internet into national zones, new defensive Internet terrain features will emerge—a fractured Internet will be an Internet that raises the cost of aggression for all parties, reducing the security dilemma. Alternately, if Western bloc countries perceive themselves as the current and future victors of a cyber arms race, then it may instead be in their interest to uphold an open Internet structure that gives them a position of greater relative power, denying others an Internet re-architecture that would make them relatively less weak.

As Kenneth N. Waltz eloquently summarizes the value of realist international relations theory in *Man, the State, and War: A Theoretical Analysis*, "Each state pursues its own interests, however defined, in ways it judges best… a foreign policy based on [the international system level of analysis] of international relations is neither moral nor immoral, but embodies merely a reasoned response to the world about us."[240] This study concludes that Robert Jervis's offense-defense theory is an excellent tool for conducting this reasoned, dispassionate analysis to better understand state behavior in cyberspace and to craft foreign policy accordingly.

[240] Kenneth N. Waltz, *Man, the State, and War: A Theoretical Analysis* (New York: Columbia University, 1969), 238. [Waltz's original text is "A foreign policy based on this image of international relations." The image that he references is his proposed third image of analysis—the anarchic international system.]

APPENDIX. ADDITIONAL ANALYTIC CONSIDERATIONS

This appendix presents additional research findings amplifying, corroborating, and refuting, as appropriate and applicable, the open source material referenced in this thesis. The appendix is classified TOP SECRET. To obtain a copy of this classified appendix, please contact the Naval Postgraduate School's Dudley Knox Library.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

Adams, Karen Ruth. "Attack and Conquer? International Anarchy and the Offense-Defense-Deterrence Balance." *International Security* 28, no. 3 (Winter 2004/2003): 45–83. http://www.jstor.org/stable/4137477.

Alexander, Keith. "House Armed Services Subcommittee, Cyberspace Operations Testimony." The Cyber Domain. U.S. Department of Defense. September 23, 2010. http://www.defense.gov/home/features/2011/0411_cyberstrategy/docs/House%20Armed%20Services%20Subcommittee%20Cyberspace%20Operations%20Testimony%2020100923.pdf.

Antonovich, P.I. "Cyberwarfare: Nature and Content." *Military Thought* 20*,* no. 3 (2011): 35–43. ProQuest 923219578.

APT28—A Window Into Russia's Cyber Espionage Operations?. Special Report. FireEye, 2014. https://www2.fireeye.com/apt28.html.

Benson, Thor. "Russia's Wiretapping 'SORM' Boxes in Sochi Make the NSA Look Like Saints." *Digital Trends*, February 5, 2014. http://www.digitaltrends.com/cool-tech/sochis-wiretapping-black-boxes-make-nsa-look-like-saints/.

Betz, David J. and Tim Stevens. "Chapter One: Power and Cyberspace." *Adelphi Series* 51, no. 424 (2011): 35–54. doi: 10.1080/19445571.2011.636954.

Birnbaum, Michael. "Russian Blogger Law Puts New Restrictions on Internet Freedoms." *Washington Post,* August 1, 2014. http://search.proquest.com/docview/1550033701.

Blank, Stephen. "Russian Information Warfare as Domestic Counterinsurgency." *American Foreign Policy Interests: The Journal of the National Committee on American Foreign Policy* 35, no. 1 (January 2013): 31–44. doi:10.1080/10803920.2013.757946.

———. "Threats to and from Russia: An Assessment." *The Journal of Slavic Military Studies* 21, no. 3 (2008): 491–526. doi:10.1080/13518040802313746.

Blueprint for a Secure Cyber Future: The Cybersecurity Strategy for the Homeland Security Enterprise. Department of Homeland Security, November 2011. http://www.dhs.gov/xlibrary/assets/nppd/blueprint-for-a-secure-cyber-future.pdf.

Boyko, S.M., I.N. Dylevsky, S.A. Komov, S.V. Korotkov, S.N. Rodionov, and A.V. Fedorov. "Potential Approaches to Implementing the Russian Federation's

Military Policies on International Information Security in the Present Situation," *Military Thought* 18, no. 2 (2009): 10–16. ProQuest 211447654.

Buntman, Sergei, Aleksandr Kurennoy, and Anatoliy Ermolin. "Informatsionnaya i Kiberbezopasnost' [Information and Cybersecurity]." Transcript. *Radio Echo Moscow*. Moscow, December 2, 2013. http://echo.msk.ru/programs/arsenal/1208183-echo/.

Chernova, Yuliya. "Russia's Startup Scene Fades." *Wall Street Journal,* September 10, 2014, Europe. http://search.proquest.com/docview/1560926461.

Clapper, James R. "Remarks as Delivered by DNI James R. Clapper on 'National Intelligence, North Korea, and the National Cyber Discussion' at the International Conference on Cyber Security." Presented at the International Conference on Cyber Security, Fordham University, January 2015. http://www.dni.gov/index.php/newsroom/speeches-and-interviews/208-speeches-interviews-2015/1156-remarks-as-delivered-by-dni-james-r-clapper-on-"national-intelligence,-north-korea,-and-the-national-cyber-discussion"-at-the-international-conference-on-cyber-security.

"Conceptual Views Regarding the Activities of the Armed Forces of the Russian Federation in the Information Space." Unofficial NATO Translation. Tallinn: Cooperative Cyber Defense Centre of Excellence. Accessed March 24, 2014. http://www.ccdcoe.org/strategies/Russian_Federation_unofficial_translation.pdf.

CyberBerkut. Accessed February 12, 2014. http://cyber-berkut.org/en/.

"Cyber Threats from China, Russia, and Iran: Protecting American Critical Infrastructure." Committee on Homeland Security. 113th Congress. March 20, 2013. http://www.gpo.gov/fdsys/pkg/CHRG-113hhrg82583/html/CHRG-113hhrg82583.htm.

Deibert, Ronald J. "Tracking the Emerging Arms Race in Cyberspace." Interview. *Bulletin of the Atomic Scientists* 67, no. 1 (January/February 2011): 1–8.

Deibert, Ronald J., Rafal Rohozinski, and Masashi Crete-Nishihata. "Cyclones in Cyberspace: Information Shaping and Denial in the 2008 Russia–Georgia War." *Security Dialogue* 43, no. 1 (February 2012): 3–24. doi: 10.1177/0967010611431079.

Demidov, Oleg. "Cyberwarfare and Russian Style of Cyberdefense." *Security Index: A Russian Journal on International Security* 19, no. 3 (September 2013): 70–71. doi:10.1080/19934270.2013.814955.

Demidov, Oleg and Maxim Simonenko. "Flame in Cyberspace." *Security Index: A Russian Journal on International Security* 19, no. 1 (February 2013): 71–72. doi:10.1080/19934270.2013.757131.

Duffy, Natalie. *Internet Freedom in Vladimir Putin's Russia: The Noose Tightens*. American Enterprise Institute. January 2015. http://www.aei.org/wp-content/uploads/2015/01/Internet-freedom-in-Putins-Russia.pdf.

Dylevsky, I.N., S.A. Komov, S.V. Korotkov, and A.N. Petruinn. "Operations in Cyberspace: Theory, Politics, Law." *Military Thought* 20, no. 3 (2011): 154–61. ProQuest 923221882.

Dylevsky, I.N., S.A. Komov, and A.N. Petruinn. "Informational Aspects of the Concept of Aggression in International Law." *Military Thought* 22, no. 4 (2013). ProQuest: 1537889195.

Elgin, Ben and Bruce Einhorn. "The Great Firewall of China." *Bloomberg Business*, January 22, 2006. http://www.bloomberg.com/bw/stories/2006-01-22/the-great-firewall-of-china.

Eremenko, Alexey. "Anonymous Browser Mass Hit as Russians Seek to Escape Internet Censorship." *Moscow Times*, June 18, 2014. http://www.themoscowtimes.com/news/article/anonymous-browser-mass-hit-as-russians-seek-to-escape-Internet-censorship/502169.html.

———. "Russia Bans Anonymous Public Wi-Fi." *Moscow Times*, August 10, 2014. http://www.themoscowtimes.com/news/article/russia-bans-anonymous-public-wi-fi/504855.html.

Farwell, James P. "Industry's Vital Role in National Cyber Security." *Strategic Studies Quarterly*, (Winter 2012): 10–41. http://www.au.af.mil/au/ssq/digital/pdf/winter_12/farwell.pdf.

Galeotti, Mark. "The 'Gerasimov Doctrine' and Russian Non-Linear War." *In Moscow's Shadows*, July 6, 2014. https://inmoscowsshadows.wordpress.com/2014/07/06/the-gerasimov-doctrine-and-russian-non-linear-war/.

Gerasimov, Valery. "Tsennost' Nauki v Vredvidenii [Value of Applied Science]." *Voyenno-Promyshlennyy Kuryer*, February 27, 2013. http://www.vpk-news.ru/articles/14632.

Giles, Keir. "'Information Troops' – a Russian Cyber Command?." Paper presented at the 3rd International Conference on Cyber Conflict. Tallinn: Cooperative Cyber Defense Centre of Excellence, 2011. http://www.ccdcoe.org/publications/2011proceedings/InformationTroopsARussianCyberCommand-Giles.pdf

———. "Russia's Public Stance on Cyberspace Issues." Paper presented at the 4th International Conference on Cyber Conflict. Tallinn: Cooperative Cyber Defense Centre of Excellence, 2012.

http://www.ccdcoe.org/publications/2012proceedings/2_1_Giles_RussiasPublicStanceOnCyberInformationWarfare.pdf.

———. *Russia's National Security Strategy to 2020*. NATO Defense College, June 2009. http://www.conflictstudies.org.uk/files/rusnatsecstrategyto2020.pdf.

Glaser, Charles L., and Chaim Kaufmann. "What Is the Offense-Defense Balance and Can We Measure It?" *International Security* 22, no. 4 (Spring 1998): 44–82. http://www.jstor.org/stable/2539240.

Goble, Paul A. "Defining Victory and Defeat: The Information War Between Russia and Georgia." In *The Guns of August 2008: Russia War in Georgia*, edited by Svantee E. Cornell and S. Frederick Starr, 181–195. Armonk, NY: M.E. Sharpe, 2009.

Goncharov, Max. *Russian Underground Revisited*. CyberCriminal Underground Economy Series. Trend Micro, 2014. http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-russian-underground-revisited.pdf.

Gonzalez, Daniel. "Preventing Cyber Attacks: Sharing Information About Tor." *The RAND Blog*, December 17, 2014. http://www.rand.org/blog/2014/12/preventing-cyber-attacks-sharing-information-about.html.

Grigoriev, Dmitry I. "Russian Priorities and Steps Towards Cybersecurity." In *Global Cyber Deterrence: Views From China, the U.S., Russia, India, and Norway*, edited by Andrew Nagorski, 5–7. New York: EastWest Institute, 2010. http://www.ewi.info/sites/default/files/ideas-files/CyberDeterrenceWeb.pdf.

"Hackers Target Ukraine's Election Website." *Agence France-Presse*, October 25, 2014, sec. Network Security. http://www.securityweek.com/hackers-target-ukraines-election-website.

Hollis, David. "Cyberwar Case Study: Georgia 2008." *Small Wars Journal*. January 6, 2011. http://smallwarsjournal.com/blog/journal/docs-temp/639-hollis.pdf.

Huntley, Wade L. "Offense, Defense, and Cyber War." Paper presented at the International Studies Association, Toronto, Canada, March 2014.

"Information Security Doctrine of the Russian Federation." *Ministry of Foreign Affairs of the Russian Federation*. Last modified December 29, 2008. http://www.mid.ru/bdomp/ns-osndoc.nsf/1e5f0de28fe77fdcc32575d900298676/2deaa9ee15ddd24bc32575d9002c442b!OpenDocument.

Internet Security Threat Report 2014. Symantec Corporation, 2014. http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v19_21291018.en-us.pdf.

Jervis, Robert. “Cooperation under the Security Dilemma.” *World Politics* 30, no. 2 (January 1978): 167–214. http://www.jstor.org/stable/2009958.

Joint Publication 3-12. “Cyberspace Operations.” Washington, DC: Joint Chiefs of Staff, 2013. http://www.dtic.mil/doctrine/new_pubs/jp3_12R.pdf.

Kaspersky Lab. “About Kaspersky Lab.” Accessed January 19, 2014. http://www.kaspersky.com/about.

Kello, Lucas. “The Meaning of the Cyber Revolution: Perils to Theory and Statecraft.” *International Security* 38, no. 2 (Fall 2013): 7–40. doi: 1.1162/ISEC_a_00138.

Kelly, Sanja, Madeline Earp, Laura Reed, Adrian Shahbaz, and Mai Truong. *Freedom on the Net 2014*. Freedom on the Net. Freedom House, 2014. https://freedomhouse.org/sites/default/files/FOTN_2014_Full_Report_compressedv2_0.pdf.

———. *Freedom on the Net 2014: Russia*. Freedom on the Net. Freedom House, 2014. https://freedomhouse.org/sites/default/files/resources/Russia.pdf.

Klimburg, Alexander. “Mobilizing Cyber Power.” *Survival: Global Politics and Strategy* 53, no. 1 (2011): 41–60. doi: 10.1080/00396338.2011.555595.

Lee, David. “Russia and Ukraine in Cyber ‘Stand-Off.’” *BBC News*, March 5, 2014, sec. Technology. http://www.bbc.com/news/technology-26447200.

Libicki, Martin C. “Brandishing Cyberattack Capabilities.” RAND National Defense Institute, Santa Monica, CA: RAND, 2013. http://www.rand.org/content/dam/rand/pubs/research_reports/RR100/RR175/RAND_RR175.pdf.

———. “Cyberspace Is Not a Warfighting Domain.” *I/S: A Journal of Law and Policy for the Information Society* 8, no. 2 (Fall 2012): 325–40.

Lieber, Keir. “The Offense-Defense Balance and Cyber Warfare.” In *Cyber Analogies*, edited by Emily O. Goldman and John Arquilla, 96–107. Monterey, CA: Naval Postgraduate School, 2014. http://hdl.handle.net/10945/40037.

Lynn-Jones, Sean M. “Offense-Defense Theory and Its Critics.” *Security Studies* 4, no. 4 (Summer 1995): 660–91. doi:10.1080/09636419509347600.

Malone, Patrick J. “Offense-Defense Balance in Cyberspace: A Proposed Model.” Monterey, CA: Naval Postgraduate School, 2012. http://hdl.handle.net/10945/27863.

Markoff, John. “Before the Gunfire, Cyberattacks.” *New York Times*, August 12, 2008, New York edition, sec. Technology. http://www.nytimes.com/2008/08/13/technology/13cyber.html?_r=1&.

Maurer, Tim. “Cyber Norm Emergence at the United Nations—An Analysis of the UN's Activities Regarding Cyber-security.” Discussion Paper 2011-12. Science, Technology, and Public Policy Program. Belfer Center for Science and International Affairs. Harvard Kennedy School. September 2011.

Maurer, Tim, and Scott Janz. “The Russia–Ukraine Conflict: Cyber and Information Warfare in a Regional Context.” October 17, 2014. http://www.isn.ethz.ch/Digital-Library/Articles/Detail/?id=184345.

McDermott, Roger. “Myth and Reality—A Net Assessment of Russia’s ‘Hybrid Warfare’ Strategy Since the Start of 2014 (Part One).” *Eurasia Daily Monitor* 11, no. 184 (October 2014). http://www.jamestown.org/programs/edm/single/?tx_ttnews%5Btt_news%5D=42966&cHash=6807c1930eae4cbece171314536d557c#.VMwHucbn3GA.

Mearsheimer, John. “Why the Ukraine Crisis Is the West’s Fault.” *Foreign Affairs* 93, no. 5 (September 2014). EBSCOhost.

Mell, Peter and Timothy Grance. “NIST Special Publication 800–145: The NIST Definition of Cloud Computing.” National Institute of Standards and Technology. U.S. Department of Commerce (2011). http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf.

Mihalenko, Anna. “Rigged Presidential Elections in Ukraine? Cyber Attack on the Central Election Commission.” *Global Research*, May 26, 2014. http://www.globalresearch.ca/rigged-presidential-elections-in-ukraine-cyber-attack-on-the-central-election-commission/5383843.

Ministry of Foreign Affairs of the Russian Federation. “Convention on International Information Security.” Last modified September 22, 2011. http://www.mid.ru/bdomp/ns-osndoc.nsf/1e5f0de28fe77fdcc32575d900298676/7b17ead7244e2064c3257925003bcbcc!OpenDocument.

Nye, Joseph S. Jr. “Cyber Power.” Cambridge, MA: Harvard, 2010. http://belfercenter.ksg.harvard.edu/files/cyber-power.pdf.

Ottis, Rain. “Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective.” In Proceedings of the 7th European Conference on Information Warfare and Security, Plymouth. Reading: Academic Publishing Limited, 2008: 163–8.

Pallin, Carolina Vendil, and Fredrik Westerlund. “Russia’s War in Georgia: Lessons and Consequences.” *Small Wars & Insurgencies* 20, no. 2 (2009): 400–424. doi: 10.1080/09592310902975539.

Powell, Robert. “Anarchy in International Relations Theory: The Neorealist-Neoliberal Debate Neorealism and its Critics. by Robert O. Keohane; Neorealism and Neoliberalism: The Contemporary Debate. by David A. Baldwin*.” International Organization* 48, no. 2 (Spring 1994): 331–344. http://www.jstor.org/stable/2706934.

Project Grey Goose Phase II Report: The Evolving State of Cyber Warfare. GreyLogic, March 20, 2009. http://fserror.com/pdf/GreyGoose2.pdf.

“RBN - Georgia Cyberwarfare - Status and Attribution.” *Russian Business Network*, August 9, 2008. http://rbnexploit.blogspot.com/2008/08/rbn-georgia-cyberwarfare-status-and.html.

“RBN (Russian Business Network) Now Nationalized, Invades Georgia Cyber Space.” *Russian Business Network*, August 9, 2008. http://rbnexploit.blogspot.com/2008/08/rbn-georgia-cyberwarfare.html.

“RBN - Russian Cyberwar on Georgia: Report.” *Russian Business Network*, October 2, 2008. http://rbnexploit.blogspot.com/2008/10/rbn-russian-cyberwar-on-georgia.html.

Roth, Mathias. *Bilateral Disputes between EU Member States and Russia*. CEPS Working Document. Centre for European Policy Studies, August 2009. http://www.ceps.eu/files/book/2009/09/1900.pdf.

“Russia Internet Blacklist Law Takes Effect.” *BBC News*, October 13, 2012, sec. Technology. http://www.bbc.com/news/technology-20096274.

“Russia Offers $110,000 to Crack Tor Anonymous Network.” *BBC News*, July 28, 2014, sec. Technology. http://www.bbc.com/news/technology-28526021.

“Russian Security Services Seek Control Over Wireless Connectivity - website.” *BBC Monitoring Former Soviet Union,* Sep 26, 2009. http://search.proquest.com/docview/460251841.

“Russia’s FSB Mulls Ban on ‘Tor’ Online Anonymity Network.” *RT*, August 16, 2013, sec. Russian Politics. http://rt.com/politics/russia-tor-anonymizer-ban-571/.

“Russia’s National Security Strategy to 2020.” *Rustrans Useful Translations*, Last modified September 17, 2012. http://rustrans.wikidot.com/russia-s-national-security-strategy-to-2020.

"Russia's Rapid Reaction." *Strategic Comments* 14, no. 7 (2008): 1–2. doi: 10.1080/13567880802482243.

"Russia/Georgia Cyber War – Findings and Analysis." Project Grey Goose: Phase I Report. October 17, 2008. http://blog.refractal.org/wp-content/uploads/2008/10/2i7t2qyiwv0g63e7l3g.pdf.

Shackelford, Scott J. "State Responsibility for Cyber Attacks: Competing Standards for a Growing Problem." In Conference on Cyber Conflict Proceedings 2010. Tallinn, Estonia: CCD COE Publications, 2010: 197–208.

Saltzman, Ilai. "Cyber Posturing and the Offense-Defense Balance." *Contemporary Security Policy* 34, no. 1 (2013): 40–63. doi: 10.1080/1352360/2013/771031.

"Security Index Journal." *PIR Center*. Accessed February 17, 2015. http://pircenter.org/security-index.

Šešelgytė, Margarita. "Can Hybrid War Become the Main Security Challenge for Eastern Europe?." *European Leadership Network*, Last modified October 17, 2014. http://www.europeanleadershipnetwork.org/can-hybrid-war-become-the-main-security-challenge-for-eastern-europe_2025.html.

Shachtman, Noah. "Russia's Top Cyber Sleuth Foils U.S. Spies, Helps Kremlin Pals." *Wired Magazine*, July 23, 2012. http://www.wired.com/2012/07/ff_kaspersky/.

Sheremet, Igor. "Kiberugrozy Rossii Rastut—Chast' I [Cyberthreats to Russia Grow - Part I." *Voyenno-Promyshlennyy Kur'yer*, February 12, 2014. http://vpk-news.ru/articles/19092.

———. "Kiberugrozy Rossii Rastut—Chast' II [Cyberthreats to Russia Grow - Part II." *Voyenno-Promyshlennyy Kur'yer*, February 19, 2014. http://vpk-news.ru/articles/19194.

Sindelar, Daisy. "Brussels, Kyiv, Moscow React to Leaked Nuland Phone Call." *Radio Free Europe/Radio Liberty*, February 7, 2014, sec. Ukraine. http://www.rferl.org/content/nuland-russia-eu-ukraine-reaction/25256828.html.

Soldatov, Andrei and Irina Borogan. "Russia's Surveillance State." *World Policy Journal* 30, no. 3 (Fall 2013): 23–30. doi: 10.1177/0740277513506378.

Sonne, Paul, and Olga Razumovskaya. "Russia Steps Up New Law to Control Foreign Internet Companies." *Wall Street Journal*, September 24, 2014. http://www.wsj.com/articles/russia-steps-up-new-law-to-control-foreign-Internet-companies-1411574920.

Stevenson, Alastair. "Hackers Turning to Tor Network to Hide Evolved Malware, Warns Kaspersky Lab." *V3*, March 20, 2014, sec. Security. http://www.v3.co.uk/v3-

uk/news/2335401/hackers-turning-to-tor-network-to-hide-evolved-malware-warns-kaspersky-lab.

Stewart, Phil, and Jim Wolf. "Old Worm Won't Die after 2008 Attack on Military." *Reuters*. June 16, 2011, U.S. edition. http://www.reuters.com/article/2011/06/17/us-usa-cybersecurity-worm-idUSTRE75F5TB20110617.

Tikk, Eneken, Kadri Kaska, Kristel Rünnimeri, Mari Kert, Anna-Maria Talihärm, and Liis Vihul. *Cyber Attacks Against Georgia: Legal Lessons Identified.* Tallinn: Cooperative Cyber Defense Centre of Excellence, 2008. Accessed March 25, 2014. http://www.carlisle.army.mil/DIME/documents/Georgia%201%200.pdf.

Tikk, Eneken, Kadri Kaska, and Liis Vihul. *International Cyber Incidents: Legal Considerations*. Tallinn: Cooperative Cyber Defense Centre of Excellence, 2010.

Tipton, Harold F., ed. *Official (ISC)^2 Guide to the CISSP CBK*. 2nd Ed. New York: CRC Press, 2010.

"The Military Doctrine of the Russian Federation." *The School of Russian and Asian Studies*, Last modified February 2, 2010. http://www.sras.org/military_doctrine_russian_federation_2010.

"The Ukrainian Crisis – a Cyber Warfare Battlefield." *Defense Update*, April 5, 2014. http://defense-update.com/20140405_ukrainian-crisis-cyber-warfare-battlefield.html.

Thomas, Timothy L. "Russia's Information Warfare Strategy: Can the Nation Cope in Future Conflicts?" *The Journal of Slavic Military Studies* 27, no. 1 (2014): 101–30. doi:10.1080/13518046.2014.874845.

———. "Russian Information Warfare Theory: The Consequences of August 2008." In *The Russian Military Today and Tomorrow: Essays in Memory of Mary Fitzgerald*, edited by Stephen J. Blank and Richard Weitz, 265–300. U.S. Army War College, Carlisle, PA: Strategic Studies Institute, 2010. http://www.strategicstudiesinstitute.army.mil/pdffiles/pub997.pdf.

———. "Russian Views on Information-Based Warfare." *Airpower Journal.* Special edition (1996): 26–35. http://www.airpower.maxwell.af.mil/airchronicles/apj/apj96/spec96/thomas.pdf.

Tucker, Patrick. "Why Ukraine Has Already Lost the Cyberwar, Too." *Defense One*, April 28, 2014. http://www.defenseone.com/technology/2014/04/why-ukraine-has-already-lost-cyberwar-too/83350/.

U.N. Office for Disarmament Affairs. "Fact Sheet: Developments in the Field of Information and Telecommunications in the Context of International Security."

Last modified June 2013. http://www.un.org/disarmament/HomePage/factsheet/iob/Information_Security_Fact_Sheet.pdf.

U.S. Cyber Consequences Unit. "Overview by the US-CCU of the Cyber Campaign Against Georgia in August of 2008." August 2009. http://www.registan.net/wp-content/uploads/2009/08/US-CCU-Georgia-Cyber-Campaign-Overview.pdf.

Van Evera, Stephen. "Offense, Defense, and the Causes of War." *International Security* 22, no. 4 (Spring 1998): 5–43. http://www.jstor.org/stable/3539239.

Waltz, Kenneth N. *Man, the State, and War: A Theoretical Analysis.* New York: Columbia University, 1969.

Weedon, Jen, and Laura Galante. "Intelligence Analysts Dissect the Headlines: Russia, Hackers, Cyberwar! Not So Fast." *FireEye Executive Perspectives*, March 12, 2014. https://www.fireeye.com/blog/executive-perspective/2014/03/intel-analysts-dissect-the-headlines-russia-hackers-cyberwar-not-so-fast.html.

"Yesli Budut 'Valit'' Region, Gorod Ili Stranu Tselikom—Do Svidan'ya [If They Attack a Region, City, or the Whole Country—Goodbye]." *Kommersant*, March 28, 2013. http://www.kommersant.ru/doc/2155845.

"Zayavleniye Glav Gosudarstv-Chlenov SHOS po Mezhdunarodnoy Informatsionnoy Bezopasnosti [Statement of Heads of SCO Member States on International Information Security]." The Shanghai Cooperation Organization. Last modified June 15, 2006. http://www.sectsco.org/RU123/show.asp?id=107.

Zinovyeva, Elena. "U.S. Digital Diplomacy: Impact on International Security and Opportunities for Russia." *Security Index: A Russian Journal on International Security* 19, no. 2 (April 2013): 33–43. doi:10.1080/19934270.2013.779430.

Zoller, Richard G. "Russian Cyberspace Strategy and a Proposed United States Response." Strategy Research Project. U.S. Army War College, 2010. http://handle.dtic.mil/100.2/ADA522027.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California