CYBERWAR IN THE SEAMS: RUSSIAN EXPLOITATION OF INTERNATIONAL AND HUMANITARIAN LAW IN OFFENSIVE CYBER OPERATIONS

A thesis presented to the Faculty of the U.S. Army Command and General Staff College in partial fulfillment of the requirements for the degree

MASTER OF MILITARY ART AND SCIENCE
Information Advantage Scholars

by

SID B. MARU, MAJOR, UNITED STATES AIR FORCE
M.S., Creighton University, Omaha, Nebraska, 2015

Fort Leavenworth, Kansas
2022

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE (DD-MM-YYYY)	2. REPORT TYPE	3. DATES COVERED *(From - To)*
10-06-2022	Master's Thesis	AUG 2021 – JUN 2022

4. TITLE AND SUBTITLE

Cyberwar in the Seams: Russian Exploitation of International and Humanitarian Law in Offensive Cyber Operations

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Sid B. Maru

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

U.S. Army Command and General Staff College
ATTN: ATZL-SWD-GD
Fort Leavenworth, KS 66027-2301

8. PERFORMING ORG REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT

Approved for Public Release; Distribution is Unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

Russia is able to conduct offensive cyber operations that impact civilians, while maintaining the illusion of compliance with international law. This study analyzed Russian offensive cyber operations case studies to assess the scope and impact of the attack as well as determine the loopholes, ambiguities, or gaps in international law that Russia may exploit. The results of the case studies were analyzed with factors established from research on Russian military thought to establish likely political and military strategic objectives. The common objectives present in the case studies provided a baseline for Russian offensive cyber operations, and inform the document analysis of the various sources of international law. The mechanism exploited by Russia is textualism, an overemphasis on the definition of international law terms without consideration of the intent of the law. This can be mitigated by an effects-based approach to determining violations of international laws, specifically use of force and breach of sovereignty. Furthermore, the research indicated that Russia follows a deliberate course of action when conducting offensive cyber operations that gradually enables significant cyberattacks without triggering protections under international law or international humanitarian law.

15. SUBJECT TERMS

Offensive Cyber Operations; International Law; International Humanitarian Law; United Nations; Geneva Conventions; Cyber Attacks; Russia; Georgia; Ukraine

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			19b. PHONE NUMBER *(include area code)*
(U)	(U)	(U)	(U)	94	

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std. Z39.18

MASTER OF MILITARY ART AND SCIENCE

THESIS APPROVAL PAGE

Name of Candidate: Sid Maru

Thesis Title: Cyberwar in the Seams: Russian Exploitation of International and Humanitarian Law in Offensive Cyber Operations

Approved by:

_____, Thesis Committee Chair
LTC Mark B. McCool, M.A.

_____, Member
Michelle M. Garcia, MSA, MMAS

_____, Member
Mark R. Wilcox, Ph.D.

Accepted this 10th day of June 2022 by:

_____, Assistant Dean of Academics for
Dale F. Spurlin, Ph.D. Degree Programs and Research

The opinions and conclusions expressed herein are those of the student author and do not necessarily represent the views of the U.S. Army Command and General Staff College or any other governmental agency. (References to this study should include the foregoing statement.)

ABSTRACT

CYBERWAR IN THE SEAMS: RUSSIAN EXPLOITATION OF INTERNATIONAL AND HUMANITARIAN LAW IN OFFENSIVE CYBER OPERATIONS, by Sid B. Maru, 94 pages.

Russia is able to conduct offensive cyber operations that impact civilians, while maintaining the illusion of compliance with international law. This study analyzed Russian offensive cyber operations case studies to assess the scope and impact of the attack as well as determine the loopholes, ambiguities, or gaps in international law that Russia may exploit. The results of the case studies were analyzed with factors established from research on Russian military thought to establish likely political and military strategic objectives. The common objectives present in the case studies provided a baseline for Russian offensive cyber operations, and inform the document analysis of the various sources of international law. The mechanism exploited by Russia is textualism, an overemphasis on the definition of international law terms without consideration of the intent of the law. This can be mitigated by an effects-based approach to determining violations of international laws, specifically use of force and breach of sovereignty. Furthermore, the research indicated that Russia follows a deliberate course of action when conducting offensive cyber operations that gradually enables significant cyberattacks without triggering protections under international law or international humanitarian law.

ACKNOWLEDGMENTS

A short paragraph is hardly a fitting acknowledgement to recognize the mountains of support provided to me by my wife, Emily, during the research and completion of this thesis. Sometimes a sheer prodigy of effort, sometimes delegating proofreading to the nearest loved-one, she consistently provides investments into my interests for which I am truly grateful. Her ability to manage our energetic and lovely daughter, a full-time job, and my long hours at the library, all the while being pregnant with our son will never cease to amaze me.

Likewise, the hours of scholarly discourse offered by my fellow inaugural Information Advantage Scholars, and the leadership of the program's Director, Mr. Pete Im, were invaluable for refining my thoughts into what I hope becomes a worthwhile discussion for future researchers. Despite being towered by your experiences and intellect, I've enjoyed every minute, meme, aside, and tweet.

TABLE OF CONTENTS

Page

ACRONYMS

ICRC	International Committee of the Red Cross
OCO	Offensive Cyber Operations
NATO	North Atlantic Treaty Organization
RCT	Reflexive Control Theory
UN	United Nations

ILLUSTRATIONS

Page

TABLES

Page

CHAPTER 1

INTRODUCTION

Background

> I cannot forecast to you the action of Russia. It is a riddle wrapped in a mystery inside an enigma.
>
> —Sir Winston Churchill, radio broadcast, 1 October 1939

The digital age is a cornucopia of opportunities made possible by technology, data, communications, and their integration into our daily lives. Individuals utilize connected technologies for everything from relationships to livelihood via the digitally-enabled gig economy. Academic institutions utilize cyberspace to collaborate on research and analyze vast amounts of data, model systems and theories, and expand the reach of education. Governments use the cyber domain to facilitate transparency and governance, coordinate social programs and emergency response, and modern identity services. Industry, too, has integrated connected information technology into remote work, storefronts, teleworking, and through technologies such as blockchains for asset management, authentication, smart contracts, and payments. Modern militaries use cyber-enabled capabilities to facilitate dispersed communications, conduct research and development, expedite virtual testing and evaluation of new weapons systems, and conduct daily operations such as intelligence, reconnaissance, and logistics.[1]

[1] *Hearing to Review Testimony on United States Special Operations Command and United States Cyber Command in Review of the Defense Authorization Request for Fiscal Year 2020 and the Future Years Defense Program* (Washington, DC: Committee on Armed Services, February 14, 2019), 3, https://www.armed-services.senate.gov/hearings/19-02-14-united-states-special-operations-command-and-united-states-cyber-command. Hereafter referred to as Nakasone Testimony.

The digital age is also a cornucopia of risk made possible by technology, data, communications, and their integration into our daily lives. Individuals, academic institutions, government, industry, and militaries have never been more accessible and vulnerable to cyberattacks by malicious actors across the globe. Many malicious actors have been State-sponsored, State-directed or State-run, and many of the victims have been civilians. Academics, industry leaders, non-governmental organizations, and international agencies such as the International Committee of the Red Cross (ICRC) have been advocates for recognizing the high potential for tangible harm to civilians in future cyberspace conflicts. They also recognize the absence of codified protections of civilians, similar to the Geneva Conventions, and seek a purpose-built solution for the unique environment that is cyberspace.[2] Regrettably, these advocates lack enforcement mechanisms and authority. Nations and international organizations with such authority have been slow to react to the issue meaningfully.

Unfortunately, adversaries can leverage the general population and their reliance on connected technology as potential targets for supportive measures or even decisive attacks. General Paul Nakasone, Commander of USCYBERCOMMAND, highlighted the strategic impacts of these decisive adversary actions to the Senate Armed Services Committee in 2019 and specifically defined "malicious cyber actors [who] weaponize personal information, steal intellectual property, and mount influence campaigns" as

[2] International Committee of the Red Cross (ICRC), "Special Series: Avoiding Civilian Harm During Military Cyber Operations," *Law and Policy* (blog), *International Committee of the Red Cross*, June 15, 2021, https://blogs.icrc.org/law-and-policy/category/special-themes/avoiding-civilian-harm-during-military-cyber-operations.

corrosive threats.[3] The implications of these corrosive threats are well recognized by the Department of Defense (DoD); the current DoD Cyber Strategy aptly summarizes recognized actors and the risks they present:

> China is eroding U.S. military overmatch and the Nation's economic vitality by persistently exfiltrating sensitive information from U.S. public and private sector institutions. Russia has used cyber-enabled information operations to influence our population and challenge our democratic processes. Other actors, such as North Korea and Iran, have similarly employed malicious cyber activities to harm U.S. citizens and threaten U.S. interests. Globally, the scope and pace of malicious cyber activity continue to rise. The United States' growing dependence on the cyberspace domain for nearly every essential civilian and military function makes this an urgent and unacceptable risk to the Nation.[4]

The essential services in the cyberspace domain that serve both military and civilian functions are known as dual-use. The Geneva Conventions does not prohibit attacks on dual-use objects[5] Article 52 of the 1977 Additional Protocols makes clear the protection of solely-civilian objects by explicitly stating, "[c]ivilian objects shall not be the object of attack or reprisals."[6] The same Article further defines military targets as "objects which by their nature, location, purpose or use make an effective contribution to military action and whose total or partial destruction … offers a definite military advantage."[7] The space

---

[3] Nakasone Testimony, 3–5.

[4] Department of Defense (DoD), *Summary: Department of Defense Cyber Strategy* (Washington, DC: DoD, 2018), 3, https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/cyber_strategy_final.pdf.

[5] International Committee of the Red Cross (ICRC), *Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I)* (Geneva, Switzerland: ICRC Headquarters, June 8, 1977), 265, https://www.refworld.org/docid/3ae6b36b4.html.

[6] Ibid., 266.

[7] Ibid., 266.

between exclusively civilian and military objects is either presumed civilian or a legal dual-use target. Carrying this set of rules designed for a distinctly physical environment into the digital age creates a unique set of problems. In cyberspace, these lines blur when one considers that military data may transit over physical hardware across routers throughout the world or be processed in cloud computing services alongside civilian data.

Whether the hardware across the globe hosting the malicious network traffic is facilitating the attack or should be considered neutral, or even a victim, is challenging to answer. International organizations, such as NATO's Cooperative Cyber Defence Center of Excellence, have expended significant efforts to identify how existing international law applies to cyberspace. These studies, known as the Tallinn Manuals, are insightful and detailed, but purely academic. Despite years of research and peer review, the non-legally binding nature of these studies leaves civilians as vulnerable as ever to cyberattacks from State actors. In fact, various State-supported actors have utilized cyber operations against individuals in support of strategic economic, military, and political goals, such as during the Russo-Georgian War and the Russo-Ukrainian War.

The corrosive threat actors, as identified by General Nakasone, recognize cyber operations as a part of a system of systems, where the cyber component is complementary to kinetic operations, accelerating the path towards a strategic goal. Adversaries, such as Russia, take a step further and integrate cyber operations on civilians during peacetime, adapting gray-zone conflict to the 21st century faster than treaties can be amended or written to prevent it. Russia, in particular, has integrated cyber operations deeply within its warfighting theories while still projecting an image of compliance with international law by avoiding the designation of armed conflict. These

gaps, a result of applying laws written for physical conflict to a digital world, enable adversaries to unduly influence U.S. and allied government and military decision-making by leveraging the well-being of the civilian population.

Problem Statement

Over the past two decades, the broad reach, difficulty in attribution, and dual-use nature of cyberspace have made the domain a valuable target for attack by corrosive threats, with the potential for significant direct and collateral harm to civilians.[8] In order to further their objectives, adversaries are willing and capable of conducting cyber operations, risking harm to civilians, while maintaining an image of compliance with international law. Gray-zone tactics and loopholes, ambiguities, and gaps in international law keep cyber operations below the threshold of armed conflict, minimizing risk to adversary forces while significantly complicating the legal recourse or potential responses available to the victim State or their allies. Unless the international community addresses the loopholes, ambiguities, and gaps in international law's application to cyberspace, Russia will continue to leverage the well-being of the civilian population to achieve its strategic goals. Furthermore, other adversaries are likely to mimic Russia's belligerent impunity in cyberspace, establishing the act of digitally harming civilians as an acceptable practice in a future conflict.

[8] Attribution, as discussed throughout this thesis, relies on technical and legal attribution. Technical analysis by experts in cybersecurity, and investigation by authorities such as the Department of Justice, offer a less biased attribution than a political statement asserting blame without having accomplished analysis.

Purpose of the Study

The study aimed to identify how Russia can perform OCO that impacts civilians, while maintaining the illusion of compliance with international law. This required researching historical examples of adversary cyber operations, and a reasonable understanding of international law and its constraints. The result offers insight into the baseline of cyber operations that an adversary may consider suitable towards the ends of achieving their strategic goals while minimizing risk to force, limiting the response to below the threshold of armed conflict, and feigning compliance with international law and international humanitarian law, in order to maintain a permissive cyberspace environment for future conflict.

Research Questions

Within the frame of the problem statement and purpose of the study, three research questions arose that provided structure to the study. The primary research question was:

1. How does Russia project an image of compliance with international law in the conduct of offensive cyber operations (OCO)?

The intent behind the primary research question was to offer historical examples of feigned compliance with international law and compare key elements of the examples with one another. The result would then provide the opportunity to look forward and determine how Russia might act in the future.

The secondary research questions look to the future, informing the discussion with Russian methodology rather than western insights. The secondary research questions are:

2. What loopholes or gaps exist in international law and its protections of civilians as it applies to OCO?
3. How does Reflexive Control Theory (RCT) apply to the use of cyberspace operations?

Assumptions

In order to facilitate the study, the researcher made several assumptions that materially impact the validity of the result. If these assumptions are proven to be incorrect, then the cross-case synthesis will need to be amended to remove the implications of the false assumption. The riskiest of these assumptions were generalizations made about Russia's tactics and techniques. First, Russia will continue its political and military belligerence, supported by OCO. The 2021 *Interim National Security Strategic Guidance* supports this assumption of continued belligerence, stating, "Russia remains determined to enhance its global influence and play a disruptive role on the world stage."[9]

Additionally, the author assumed that Russia would continue to employ gray-zone conflict tactics in cyberspace. Gray-zone conflict generally includes both State and non-State actors and is intended to pursue strategic goals while remaining short of the threshold of armed conflict. Another assumption is that the Russian government and military's use of RCT measures in OCO will be evident through evidence or inference. Some risk is associated with this assumption, though it was partially mitigated by

[9] U.S. President, *Interim National Security Strategy of the United States of America* (Washington, DC: Executive Office of the President, March 2021), 8, https://www.whitehouse.gov/wp-content/uploads/2021/03/NSC-1v2.pdf.

research conducted to support the analysis, which showed that while Russia may utilize multiple warfighting theories, a majority of their actions in cyberspace are supported under the concepts of RCT.[10]

Assumptions that shift away from Russia include postulations on international law. The first of these assumptions is that existing international law is insufficient to protect individuals in cyberspace. This assumption relies heavily on the lack of application of existing international law to cyber-attacks recognized as performed by or sponsored by a State actor. Article 52 of Additional Protocol I of the Geneva Conventions restricts lawful targets to solely military targets, offering some protection to civilian objects. However, dual-use objects such as telecommunications infrastructure used by both military and civilians are not protected under Article 52, and therefore are at risk of attack. This could easily manifest as an attack on civilian networks or remotely-controlled utilities simply because the military or its members rely on some part of that resource. Within the ethical framework of Just War Theory, *jus in bello* requires warfighters to exercise the principle of discrimination. Relying on ethics would provide for more stringent delineations between military and civilian targets, however recent events such as Russia's foreign intelligence service-linked attacks on civilian information

[10] Marek Posard, Marta Kepe, Hilary Reininger, James Marrone, Todd Helmus, and Jordan Reimer, *From Consensus to Conflict: Understanding Foreign Measures Targeting U.S. Elections* (Santa Monica, CA: RAND Corporation, 2020), 12, https://www.rand.org/pubs/research_reports/RRA704-1.html.

technology systems easily fall short of discrimination without feeling the burden of international legal repercussions.[11]

A final assumption is that cyber warfare will be at least a significant supporting effort, if not the main effort, of conflicts in the future. Conflicts that exist purely in the physical domain do not rely on the conclusions presented in this work. Considering the significant investments and efforts adversaries are taking to bolster offensive and defensive cyber capabilities, cyber warfare will likely have a part to play in future conflicts. In the last decade, adversaries such as China prioritized building offensive cyber capabilities, with efforts such as PLA Unit 61398. Similarly, Russia enacted Sovereign Internet legislation that allows the government to disconnect itself from external networks, isolating the Russian internet from vulnerabilities associated with persistent global connectivity.

Definition of Terms

Cyberspace – Defined by Joint Publication (JP) 3-12, *Cyberspace Operations*, cyberspace is the "domain within the information environment that consists of the interdependent network of information technology (IT) infrastructures and resident data. It includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers."[12] Russian doctrine does not refer to this concept as

[11] Tom Burt, "New Activity from Russian Actor Nobelium," *On the Issues* (blog), November 13, 2021, https://blogs.microsoft.com/on-the-issues/2021/10/24/new-activity-from-russian-actor-nobelium.

[12] Chairman of the Joint Chiefs of Staff (CJCS), Joint Publication (JP) 3-12, *Cyberspace Operations* (Washington, DC: Joint Chiefs of Staff, 2018), I-1.

cyberspace, but rather as an element of Information Space that is not considered separate from human information processing.[13]

Cyberspace Operations – Defined by JP 3-12, *Cyberspace Operations*, is the employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace.[14]

Cyber Warfare – Implied as an escalation of cyberspace attack, which JP 3-12, *Cyberspace Operations* defines as "actions taken in cyberspace that create noticeable denial effects … in cyberspace or manipulation that leads to denial that appears in a physical domain, and is considered a form of fires."[15]

Offensive Cyberspace Operation – Defined by JP 3-12, *Cyberspace Operations*, these are "missions intended to project power in and through cyberspace."[16]

Defensive Cyberspace Operations – Defined by JP 3-12, *Cyberspace Operations*, these are "missions to preserve the ability to utilize blue cyberspace capabilities and protect data, networks, cyberspace-enabled devices, and other designated systems by defeating on-going or imminent malicious cyberspace activity."[17]

---

[13] Timothy Thomas, "Information Security Thinking: A Comparison of U.S., Russian, and Chinese Concepts," (Foreign Military Studies Office, Fort Leavenworth, KS, July 2001), 2, https://community.apan.org/wg/tradoc-g2/fmso/m/fmso-monographs/240293.

[14] CJCS, JP 3-12, I–1.

[15] Ibid., II-7.

[16] Ibid., GL-5.

[17] Ibid., GL-4.

Gray Cyberspace – Implied by JP 3-12, *Cyberspace Operations*, gray cyberspace is the remaining cyberspace that is not considered blue or red.[18] Blue cyberspace is controlled or protected by the U.S. and its mission partners. Red cyberspace is controlled by the adversary. Red and blue cyberspace are mutually exclusive, as the control of the space delineates the owner. Gray cyberspace utilized by military forces may become vulnerable to attack, similar to dual-use areas in existing international humanitarian law.

Gray-Zone Conflict – generally defined as a form of conflict that "pursues political objectives, … employs mostly non-military or non-kinetic tools, … strives to remain under key escalatory or red line thresholds to avoid outright, conventional conflict and, … moves gradually toward its objectives rather than seeking conclusive results in a specific period of time."[19] Gray-zone conflict is separate and distinct from the similarly named gray cyberspace.

Information Warfare (Russian*: informatsionnaya voyna*) – Defined by many publications, but succinctly summarized by TRADOC Pamphlet 525-3-1, information warfare is "Employing information capabilities in a deliberate disinformation campaign supported by actions of the intelligence organizations designed to confuse the enemy and achieve strategic objectives at minimal cost."[20] Information warfare is considered a

[18] CJCS, JP 3-12, I–5.

[19] Michael Mazarr, "Mastering the Gray Zone, Understanding a Changing Era of Conflict" (Monograph, U.S. Army War College, 2015), 58, https://press.armywarcollege.edu/monographs/428.

[20] U.S. Army Training and Doctrine Command (TRADOC), TRADOC Pamphlet 525-3-1, *The U.S. Army in Multi-Domain Operations 2028* (Fort Eustis, VA: TRADOC, 2021), GL-6.

permissible ruse of war under the provisions of Protocol 1 of the Additional Protocols to the Geneva Conventions of 1949.[21] Russian doctrine refers to military deception (Russian: *maskirovka*) as an integral part of information warfare.[22]

Perfidy (Acts of Perfidy) – Defined by the Geneva Conventions as acts which "are those inviting the confidence of an adversary, thus leading that adversary to believe that there is an entitlement, or an obligation, to accord protection provided under the [Law of Armed Conflict], with an intent to betray that confidence."[23]

Reflexive Control Theory (RCT) – Defined by mathematician Vladimir Lefebvre to discuss influence techniques, RCT discusses a method by which one purposefully manipulates their opponent's decision-making.[24] The original premise was to provide only select prepared information to force an opponent towards a decision beneficial to the manipulator. RCT focuses on low-cost, semi-deniable information operations to predetermine and maneuver an opponent's decision in the adversary's favor.

Semi-deniability – In the context of OCO, semi-deniability is a step further from plausible deniability toward attribution. The intent of a semi-deniable offensive cyber

---

[21] ICRC, *Protocol I,* 258, Article 37-2.

[22] Keir Giles, *Handbook on Russian Information Warfare,* Fellowship Monograph (Rome: NATO Defense College, Research Division, November 2016), 6.

[23] International Committee of the Red Cross (ICRC), *Study on Customary International Humanitarian Law* (Geneva: ICRC Headquarters, August 15, 2005), part 65, https://www.icrc.org/en/doc/resources/documents/misc/customary-law-q-and-a-150805.htm.

[24] Timothy Thomas, "Russia's Reflexive Control Theory and the Military," *The Journal of Slavic Military Studies* 17, no. 2 (June 2004): 237-256, https://www.rit.edu/~w-cmmc/literature/Thomas_2004.pdf.

operation is for the perpetrator to embed enough information on the source of the attack to ensure the strategic messaging of the perpetrators is evident to the victims, without providing any concrete, legally-undeniable proof of the identity of the perpetrator.

Limitations and Delimitations

Several limitations exist in studying international law's applicability to individuals in cyberspace, but the most impactful to this thesis is scope. While several years can, and should, be dedicated to the study of preventing non-combatants harm in any future cyberspace conflict, the scope of this study is narrower than the topic deserves due to the time limitation of the degree for which this thesis is written. The inability to travel to research primary sources, due to degree requirements as well as the on-going global pandemic, present another limitation on this thesis.

Furthermore, the research is limited by two primary factors: the limited distribution of Russian doctrine, especially as it relates to information warfare, and the author's reliance on translated materials for Russian-language documents and research. The research relies on synthesis, analysis, and secondary sources about adversary strategic and operational frameworks. Fortunately, much attention has been paid to Russian OCO recently, mitigating some aspects of the limitation.

Moreover, Russia's overarching defensive perspective presents a limitation as well. Russian doctrine and military literature frame their military actions as a response to hypothetical aggression from Western countries. This defensive outlook enables Russian military action confined only by the hypothetical offending Western military action. NATO's *Handbook of Russian Information Warfare* emphasizes that:

> [i]t should be noted that the majority of these Russian sources present their research and findings as describing not Russia's own approaches, but the approaches which they say are adopted by foreign powers seeking to harm Russia. In some cases, the principles described reflect not home-grown theory, but Russian adoption of what it believes to be Western practice.[25]

Therefore, the author will seek to recognize this perspective when researching Russian doctrine and military thought.

In addition to limitations, this thesis is subject to self-imposed delimitations to facilitate one aspect or another of the study. While the most accurate and relevant information on adversary cyber warfare capabilities may be available in classified form, this thesis will include only public-domain documents in the research, and provide an unclassified analysis. Subjecting the thesis to classification would unnecessarily limit distribution and hamper the benefit it could provide, adding depth and data without significantly changing the resulting study.

Furthermore, the study is limited to a specific adversary. As identified in the DoD Cyber Strategy, several State actors and non-State actors are capable of some level of cyber warfare, such as China, Russia, North Korea, and Iran. This study is limited to solely Russia due to a combination of the researcher's interest in Russian information warfare and limitations on time due to degree requirements.

Finally, the chronological scope of the research ends in 2021 as a function of a rapidly redeveloping conflict in Ukraine with Russia as the principal aggressor. Apart from the stated difficulty in attribution for OCO, not enough time has passed to allow for establishing facts for the renewed Russo-Ukrainian Conflict in 2022. Additional study

[25] Giles, *Handbook on Russian Information Warfare*, 1–2.

should be accomplished to integrate this unfolding conflict into the framework of this thesis.

Significance of the Study

The study into adversary exploitation of the international law and international humanitarian law as it applies to cyberspace is most relevant to strategic parties, such as government and military leaders. The analysis provided by this study will help inform, or reinforce, what to expect and how to defend against this specific adversary. It can be applied to any adversary who desires to project the illusion of compliance with international law while conducting OCO against the general population in an opponent's country.

Summary

The benefits of today's connected society come hand-in-hand with significant concerns. Adversaries now enjoy instantaneous access to the entirety of an opponent's population and have a desire to use that vulnerability toward strategic political and military goals. While civilians are customarily protected from harm in a physical conflict between States by treaties and international humanitarian law, applying these same constructs to cyberspace is not a simple task. The gaps created when international law is applied to cyberspace implicitly create liberal boundaries, or maneuver space, for what OCO crosses into the threshold of armed conflict. This maneuver space allows adversaries to unduly leverage U.S. and allied civilian population's wellbeing to achieve their strategic political and military goals.

CHAPTER 2

LITERATURE REVIEW

Introduction

Attacking civilians during warfare is far from a new concept. Italian General Giulio Douhet discussed a concept known as Strategic Bombing in 1921, defined as inflicting an incredibly high cost on non-military targets to decimate civilian morale.[26] While OCO against civilians are not meant individually as decisive wartime efforts, as strategic bombing was intended, they share the tactic of employing harm to civilians to manipulate an opponent's government towards some strategic goal. This chapter provides a foundational understanding of international law, Russian military thought, and OCO against civilians. This literature provides context to recent historical examples, specifically the Russo-Georgian War and Russo-Ukrainian War. The specifics of how the conflicts were chosen will be explained in detail in the next chapter's discussion on research methodology. The literature reviewed for this work provided the basis for answering these primary and secondary research questions:

1. 1 How does Russia project an image of compliance with international law in the conduct of OCO?
2. What loopholes or gaps exist in international law and international humanitarian law and its protections of civilians as it applies to OCO?

[26] Giulio Douhet, *The Command of the Air* (Eastford, CT: Martino Fine Books, 1921), 248.

3. How does Reflexive Control Theory (RCT) apply to the use of cyberspace operations?

International Law and Cyberspace

A notable proponent in the space of modernizing international humanitarian law, specifically, has been the ICRC.[27] Henry Durant's observations of the horrific conditions endured by the 35,000 wounded soldiers after the Battle of Solferino inspired efforts to create a private impartial aid organization to support war wounded and non-combatants, regardless of allegiance.[28] This private agency formally became the ICRC as a result of the Geneva Conventions of 1949, and as a function of historical efforts towards protecting civilians, the ICRC has also been a vocal proponent for protections of civilians in cyberspace.[29] The agency recently renewed its focus on the implications of cyber warfare on the civilian population. It advocates for a variety of measures to include legal frameworks and strict separation of civilian and explicitly-military interests in cyberspace to limit damage to civilians if military systems are attacked. This is, of course, complicated by the recent push of governments and militaries to embrace Cloud services offered by providers such as Amazon Web Services, Microsoft AZURE, and the like. The

[27] The ICRC identifies as a private agency, rather than a non-governmental organization. They are charged as the custodians of the Geneva Conventions.

[28] International Committee of the Red Cross (ICRC), *Solferino and the International Committee of the Red Cross: Background, Facts and Figures* (Geneva, Switzerland: ICRC Headquarters, January 6, 2010), https://www.icrc.org/en/doc/resources/documents/feature/2010/solferino-feature-240609.htm.

[29] ICRC, "Avoiding Civilian Harm During Military Cyber Operations". As of the date of access, the ICRC has published 6 insightful articles under the special topic of Avoiding Civilian Harm During Military Cyber Operations.

essence of the ICRC's standpoint on this complex issue is summarized into six key points that can be juxtaposed with perspectives from other key multinational actors:

1. "States should address the concerns posed by the increasing integration of cyber operations with other military capabilities during armed conflicts."[30]

NATO and the UN independently concur with the prospect of addressing the stated concern.[31] NATO's efforts offer scholarly studies and non-legally binding works on how existing international law may be applied to various types of cyberspace conflict. The Secretary General of the United Nations recently remarked on the need for addressing these same concerns, doing so under two working groups, a U.S.-sponsored Group of Governmental Experts, and a Russian-sponsored Open Ended Working Group.[32] Notably, the Russian-sponsored Open Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security, the sixth

[30] International Committee of the Red Cross, "Special Series: Avoiding Civilian Harm During Military Cyber Operations," *International Committee of the Red Cross* (blog), June 15, 2021, 1, https://blogs.icrc.org/law-and-policy/category/special-themes/avoiding-civilian-harm-during-military-cyber-operations.

[31] North Atlantic Treaty Organization (NATO), *Bucharest Summit Declaration* (Bucharest, Romania: NATO, April 3, 2008), para. 47, accessed May 5, 2022, https://www.nato.int/cps/en/natolive/official_texts_8443.htm; Antonio Guterres, "Remarks to the General Assembly on the Secretary-General's Priorities for 2020 (As Delivered)" (Transcript, United Nations, January 22, 2020), https://www.un.org/sg/en/content/sg/speeches/2020-01-22/remarks-general-assembly-priorities-for-2020.

[32] Guterres, "Remarks to the General Assembly on the Secretary-General's Priorities for 2020 (As Delivered)."

of its kind to address the issue of protection in cyberspace, did not result in directive or prescriptive action.[33]

2. "Existing processes must be adapted to the cyber context to ensure compliance with international humanitarian law."[34]

The ICRC and NATO stand in direct contrast to one another regarding the adaptation of existing international humanitarian law. Historically, the ICRC's proposals follow the path of least resistance to garner consensus towards their goals. NATO's attempts to fit cyberspace into existing laws are the true path of least resistance, providing context for States to create their own legal precedent. Both the UN and NATO have also acknowledged the difficulty in gaining consensus on the path to codify these international norms, be it customary or treaty law.[35]

3. "States must put in place measures to mitigate the risk of civilian harm posed by the use of military cyber capabilities."[36]

---

[33] United Nations (UN) General Assembly, *Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security*, Final Substantive Report (New York, NY: UN, March 10, 2021), https://undocs.org/A/75/816.

[34] ICRC, "Special Series: Avoiding Civilian Harm During Military Cyber Operations," 15 June 2021, 2.

[35] UN General Assembly, *Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security*, 11; Guterres, "Remarks to the General Assembly on the Secretary-General's Priorities for 2020"; Michael N. Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, 2nd ed. (New York, NY: Cambridge University Press, 2017), 1–6.

[36] ICRC, "Special Series: Avoiding Civilian Harm During Military Cyber Operations," 15 June 2021, 3.

The UN working group independently came to a similar conclusion, acknowledging that these networks "may be owned, managed, or operated by the private sector, [and] may be shared or networked with another State or operated across different States. As a result, inter-State or public-private cooperation may be necessary to protect its integrity, functioning and availability."[37] This puts the onus on member States and industry rather than the purview of treaty or intergovernmental organizations. Some cybersecurity industry advocates recommend that international law be amended or developed, eliminating the voluntary application of norms that the UN, NATO, or the ICRC opt to support.[38] It is worth noting that the UN has two divergent views on how to apply this tenet to proceed. The Russian-sponsored Open Ended Working Group's final report offers solutions that require States to mitigate threats with measures that allow for national restrictions on cyberspace and onerous requirements on industry regarding data portability.[39] This perspective coincides with greater Russian initiatives to maintain a sovereign internet and direct control of the cyberspace within their national borders. The Open Ended Working Group also re-framed foundational elements of existing norms,

---

[37] UN General Assembly, *Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security*, 4.

[38] Brad Smith, "The Need for a Digital Geneva Convention at the RSA Conference (As Delivered)" (Transcript of Keynote Address at the RSA Conference, San Francisco, CA, February 14, 2017), 5–6, https://blogs.microsoft.com/wp-content/uploads/2017/03/Transcript-of-Brad-Smiths-Keynote-Address-at-the-RSA-Conference-2017.pdf.

[39] NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), "A Surprising Turn of Events: UN Creates Two Working Groups on Cyberspace," *INCYDER*, March 11, 2019, para. 8, https://ccdcoe.org/incyder-articles/a-surprising-turn-of-events-un-creates-two-working-groups-on-cyberspace.

seeking to "deliberately distort their meaning and undermine their status as the consensus normative basis which to move forward."[40] The U.S.-sponsored Group of Governmental Experts, in contrast, offers mitigating measures that promote an open, unrestricted internet.[41]

4. "States must put in place measures to protect the civilian population against the dangers resulting from military cyber operations."[42]

The ICRC, NATO, and both the Russian-sponsored and U.S.-sponsored UN groups agree that measures need to be taken to prevent harm to the civilian population during military cyber operations. The difference, however, is found in how each group defines harm. Considering the Russian disinformation campaign during the 2016 U.S. presidential elections, perpetrated predominantly in cyberspace and directed primarily at civilians, the Russian definition of harm via cyberspace is limited to actual physical violence. Conversely, the U.S. definition includes influence, obstruction, and tangible or intangible

[40] Marc-André Blanchard, "Explanation of Vote on Resolution L.27/Rev1: Developments in the Field of Information and Telecommunications in the Context of International Security" (Government of Canada, November 7, 2018), 1–2, https://www.international.gc.ca/world-monde/international_relations-relations_internationales/un-onu/statements-declarations/2018-11-07-telecommunications.aspx.

[41] United Nations (UN) General Assembly, *Advancing Responsible State Behaviour in Cyberspace in the Context of International Security* (New York, NY: UN, October 10, 2018), 1–3, https://undocs.org/A/C.1/73/L.37.

[42] ICRC, "Special Series: Avoiding Civilian Harm During Military Cyber Operations," 15 June 2021, 3.

harm.[43] Defining a breach of national sovereignty encounters the same ambiguity when discussing cyberspace instead of the physical domain.

5. "States should address the risk of civilian harm posed by information operations and gray-zone operations."[44]

The ICRC, NATO, and the UN agree that minimizing civilian harm caused by information operations and gray-zone operations is critical to continued peace. None of these organizations possess their own cyberweapons, though NATO may utilize its member-states' cyberweapons in support of an authorized operation. Individual states, in stark contrast, are wary of agreeing to any international norms that might restrict their ability to respond to cyberattacks from State or non-State actors.[45]

6. "States and other stakeholders should continue to develop their understanding of the risk of civilian harm posed by new technologies and work towards mitigating those risks."[46]

Reviewing the ICRC and UN General Assembly reports on historical and potential future military actions in gray-zones and civilian areas of cyberspace provides reputable

---

[43] Michael N. Schmitt, "'Virtual' Disenfranchisement: Cyber Election Meddling in the Grey Zones of International Law," *Chicago Journal of International Law* 19, no. 1 (August 16, 2018), https://chicagounbound.uchicago.edu/cjil/vol19/iss1/2.

[44] ICRC, "Special Series: Avoiding Civilian Harm During Military Cyber Operations," 15 June 2021, 3.

[45] Michael N. Schmitt, "Taming the Lawless Void: Tracking the Evolution of International Law Rules for Cyberspace," *Chicago Journal of International Law* 3, no. 3, (Summer 2020): 38, https://chicagounbound.uchicago.edu/cjil/vol19/iss1/2.

[46] Ewan Lawson and Kubo Macak, *Avoiding Civilian Harm From Military Cyber Operations During Armed Conflicts,* ICRC Expert Meeting (Geneva, Switzerland: ICRC, January 21-22, 2020), 6–7, https://shop.icrc.org/download/ebook?sku=4539/002-ebook.

information and context, and offers insight behind an otherwise covert area of adversary government and military cyberspace and information operations.[47]

In addition to multinational organizations and aid agencies, various commercial entities have expressed support for protections for civilian enterprises in cyberspace. Microsoft has been an advocate for protections in cyberspace, protections from nation-state information and influence operations, and more. Leaders at Microsoft regularly publish articles, including Digital Defense Reports, as well as speak on the matter.[48] Recently, Tom Burt, Corporate Vice President of Customer Security & Trust offered insight into a Russian State actor, Nobelium. Burt draws correlations between the SolarWinds hack and its fallout, and compares the pervasiveness of Nobelium's recent actions, noting that "Russia is trying to gain long term, systematic access to a variety of points in the technology supply chain and establish a mechanism for surveilling … targets of interest."[49] Several years before the Nobelium attacks, Brad Smith, President and Vice Chairman of Microsoft, advocated at a prominent security conference for a purpose-built digital Geneva Convention, explicitly hoping to form protections that

---

[47] Lawson and Macak, *Avoiding Civilian Harm From Military Cyber Operations During Armed Conflicts*; United Nations (UN) General Assembly, *Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security* (New York, NY: UN, July 14, 2021. https://undocs.org/A/76/135); United Nations (UN) General Assembly, *Developments in the Field of Information and Telecommunications in the Context of International Security*.

[48] Microsoft's archive of semi-annual Digital Defense Reports, from 2008 to 2018, is available at https://www.microsoft.com/en-us/security/business/security-intelligence-report. The report provides broad statistics on threats that were spreading globally, while the regional reports offer specifics based on victim State.

[49] Burt, "New Activity from Russian Actor Nobelium."

would prevent governments from targeting private sector and critical infrastructure with cyber-attacks. Smith echoed the Secretary General of the United Nations, stating that existing international law is insufficient in its protection of civilians in cyberspace, referencing nation-state actors attacking private sector infrastructure as advancing the premise that corrosive threats are already leveraging the gaps in international humanitarian law to their benefit.[50] Smith recognized the barriers to change in multinational organizations and offered that "just as… the protection of civilians required the active involvement of the Red Cross [*sic*], protection against nation-state cyberattacks requires the active assistance of technology companies."[51] He proposed a framework of six rules which expand beyond the scope of the Geneva Conventions and strive to limit cyberwar significantly, and have the distinct flavor of protecting the technology industry, almost above all. Notwithstanding the industry bias, Smith's framework is a useful lens to view the response from multinational organizations such as NATO and the UN.

As mentioned in the previous chapter, the Tallinn Manual was prepared for NATO's Cooperative Cyber Defence Center of Excellence in order research how to apply existing international law to the most severe OCO. *Tallinn Manual 2.0* expands the focus to examine how existing international law applies to cyber operations that fall below the threshold of armed conflict. *Tallinn Manual 2.0* is, again, a scholarly work that is non-legally binding yet proves informative due to its in-depth discussions on the genesis of the legal precedent. It offers 154 black-letter rules that its authors consider widely

[50] Smith, "The Need for a Digital Geneva Convention at the RSA Conference," 2–3.

[51] Ibid., 2.

accepted and free from doubt, pragmatically adapted from existing international law. The manual expends great effort on detailing the origination of the law and expands significantly on the definitions and justifications of each rule throughout the work. The Tallinn Manual and its 2.0 revision are substantial efforts towards establishing a common framework of applicability of international law to cyberspace.[52]

Considering one of Smith's aspirational Digital Geneva Convention rules of limiting targets to exclude tech companies or infrastructure, there is a stark contrast with the *Tallinn Manual 2.0* modification of Article 52 of the 1977 Additional Protocols of the Geneva Conventions.[53] Despite the potential for labeling some private companies or critical infrastructure as dual-use in the physical realm, the *Tallinn Manual 2.0* recognizes the greater likelihood of dual-use targets in cyberspace. Rule 99 offers that "[c]ivilian objects shall not be made the object of cyberattacks. Cyber infrastructure may only be made the object of attack if it qualifies as a military objective,"[54] followed by a detailed discussion on dual-use objects as legal targets.[55]

Smith offers an idealistic perspective that States should "exercise restraint in developing cyber weapons" and "limit offensive operation."[56] The *Tallinn Manual 2.0*

---

[52] NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), "The Tallinn Manual," Research, para. 8, accessed May 6, 2022, https://ccdcoe.org/research/tallinn-manual; Schmitt, *Tallinn Manual 2.0*, xxv–xxvii.

[53] Smith, "The Need for a Digital Geneva Convention at the RSA Conference," 2.

[54] Schmitt, *Tallinn Manual 2.0*, 434.

[55] ICRC, *Protocol I*, 264–268.

[56] Smith, "The Need for a Digital Geneva Convention at the RSA Conference," 2.

more pragmatically suggests in Rule 110 that all States must "ensure that the cyber means of warfare that they acquire or use comply with the rules of law of armed conflict that bind them."[57] It is evident that Smith's efforts are partially driven by the costs incurred by private corporations rather than the Tallinn Manual's objectivity in the laws of war. The ICRC seems to concur with the Tallinn Manual perspective of limited aims in preventing civilian harm in an impending cyberwar, explicitly stating, "existing processes must be adapted to the cyber context to ensure compliance with international humanitarian law."[58]

State actors leveraging existing gaps in international humanitarian law and laws of war have enabled the concept of gray-zone conflict in the latter half of the 20th century, where opponents utilize non-military and non-kinetic means to achieve political goals over an extended period.[59] The advent of cyberspace has dramatically expanded the area in which gray-zone conflict can occur, enabling opponents to target the other instantaneously and attack those targets across the globe. While the ICRC does not presume to be able to outlaw gray-zone conflict, they highlight the increasing trend of State actors using technology to "engage in operations that spread disinformation, undermine social cohesion, or even incite violence."[60] Furthermore, they encourage

---

[57] Schmitt, *Tallinn Manual 2.0*, 464.

[58] ICRC, "Special Series: Avoiding Civilian Harm During Military Cyber Operations," 15 June 2021, 6.

[59] Mazarr, "Mastering the Gray Zone," 58.

[60] ICRC, "Special Series: Avoiding Civilian Harm During Military Cyber Operations," 15 June 2021, 3.

States to recognize the risks associated with gray-zone operations and the applicability of international humanitarian law.[61] The *Tallinn Manual 2.0* expands on the applicability of international humanitarian law to perfidy operations, explicitly stating in Rule 123 that "Cyber operations that qualify as ruses of war are permitted."[62] The manual states explicitly that psychological warfare activities, such as disinformation activities, are permitted.[63] A complication that highlights the difficulty of overlaying aged rules over newer concepts is a subset of ruse generally known as camouflage. Camouflaging military data and networks on civilian infrastructure brings forth questions of ethics and legality on both sides of the conflict, and is a concern worthy of discussion, albeit outside the scope of this thesis.

Regardless of the preferred path, whether the reader supports the industry perspective of revolutionary change, the ICRC's perspective of evolutionary, iterative change, or the Tallinn Manual's adaptation of existing laws to cyberspace, the concept of adhering to international law and protecting civilians in cyberspace are foundational elements of all paths.

International law and international humanitarian law have a variety of sources. Customary international law consists of practices that have occurred throughout recent history to become a norm. International legal proceedings, such as those from the International Court of Justice, are another example of sources for customary international

---

[61] ICRC, "Special Series: Avoiding Civilian Harm During Military Cyber Operations," 15 June 2021, 3

[62] Schmitt, *Tallinn Manual 2.0*, 495.

[63] Ibid., 495–496.

law. The Geneva Conventions and the Charter of the United Nations are examples of international law or international humanitarian law that finds their source in treaties.

The International Court of Justice *Draft Articles on the Responsibility of States for Internationally Wrongful Acts*, the Charter of the United Nations, and the Geneva Conventions provide the context for exploring which international laws are potentially violated during OCO.

Russian Military Thought on Offensive Cyber Operations

The researcher's understanding of current Russian military thought relies heavily upon the commentaries of two Russian military authors who co-authored a series of articles between 2010 and 2017. The authors, Colonel S. G. Chekinov and Lieutenant General (ret.) S. A. Bogdanov penned 13 articles, collectively referred to as the Chekinov-Bogdanov commentaries, which offer insight into the state of Russian military thought on the heels of the Russo-Georgian War, as well as the evolution of those principles during the lead up to, and after the 2013-2019 timeframe of the Russo-Ukrainian War as the conflict escalated and cyberattacks increased in scope and complexity. While Chekinov-Bogdanov wrote only thrice on OCO, in 2013 with "Nature and Content of Wars of a New Generation War," and 2015 with "A Forecast for Future Wars: Meditations on What They Will Look Like," and 2017 with "The Evolution of the Essence and Content of 'War' in the 21st Century," much can be gleaned from the remaining commentaries when one is reminded that Russians view OCO in the same

breath as information operations and information warfare.[64] Timothy Thomas, a prolific author and retired Lieutenant Colonel in the U.S. Army, offers much insight in his literature on Russian military thought.

Before any in-depth discussion on Russian doctrine and military thought, it is important to recognize that the perspective they have regarding their tactics is generally framed as being defensive in nature, responding to the aggression of a belligerent West. Throughout the research on Russian sources, the Russian government and military view themselves as simply adopting tactics employed against Russia. On the other hand, Western nations would consider those same tactics as uniquely Russian, many of them objectively past the threshold of war crimes. NATO's *Handbook of Russian Information Warfare* introduces Russian sources with the preface that "the majority of these Russian sources present their research and findings as describing not Russia's own approaches, but the approaches which they say are adopted by foreign powers seeking to harm Russia."[65]

Russian military thought leading up to the Russo-Georgian war focused on adapting lessons learned from the U.S.'s experience during the Gulf War. Termed New Generation Warfare, Chekinov and Bogdanov inferred several points from their study: the U.S. technological superiority in defeating an Iraqi numerical advantage, the efficacy

[64] Timothy Thomas has selected and analyzed several of the Chekinov-Bogdanov commentaries, highlighting key elements from 9 of the published works. As the scope of this thesis is focused on offensive cyber operations, the researcher reviewed additional articles published by Chekinov and Bogdanov to gain a greater understanding of Russian perspectives on cyber operations as a subset of information warfare.

[65] Giles, *Handbook on Russian Information Warfare*, 1–2.

of aerial and sea-launched weapons, and the merits of electronic warfare. They presumed that in New Generation Warfare, Russia's adversaries would focus heavily on "an aerospace operation of several days" with "attacks from enemy military robots" as well as "efforts to involve all public institutions in the country it attacks, such as the mass media, religious organizations, public movements" while "decisive battles … will rage in the information environment."[66] Combining the efforts to involve public movements and decisive battles in the information environment become a concern when viewed together.

The implication is quite simply that OCO, referenced as information operations, on non-military targets is a core tenet of Russian New Generation Warfare.[67] Since then, particularly after Russian Chief of the General Staff Valery Gerasimov discussed a new concept of warfare in 2013, Russian military thought has galvanized around new-type warfare. New type warfare is heavily focused on non-military methods, and is allegedly how Western nations sought to control Russia after World War II. New-type warfare methods include "political pressure, information sabotage, the exploitation of humanitarian issues, secret service activity, and unfair and cunning diplomacy."[68]

Reflexive Control Theory

Another unique topic for Russian military thought is the socio-psychological theory of Reflexive Control. Developed in the 1960s by mathematical psychologist

---

[66] Thomas, *The Chekinov-Bogdanov Commentaries of 2010-2017*, 8.

[67] Colonel S. G. Chekinov and Lieutenant General S. A. Bogdanov, "Nature and Content of a New Generation War," *Military Thought*, no. 10 (2013): 18, 22.

[68] Thomas, *The Chekinov-Bogdanov Commentaries of 2010-2017*, 14.

Vladimir Lefebvre, Reflexive Control is the manipulation of an opponent's decision-making process. While discussing its merits as the foundation for understanding information warfare, the U.S. Army sources their definition of a "means of conveying to a partner or an opponent specifically prepared information to incline him to voluntarily make the predetermined decision desired by the initiator of the action" from Timothy Thomas' 2004 work on Reflexive Control.[69] Despite being a Soviet-era theory, continually developed after it earned a Top Secret classification by the Soviet General Staff, Reflexive Control is presumed to be employed across the whole-of-government in Russia.[70] As Reflexive Control continues to evolve and its scope expands, it becomes uniquely fitting for offensive operations in cyberspace.[71]

Lefebvre's basis for RCT was founded in mathematics, creating a construct that can measure one's own, or an opponent's, reflexion score. In Lefebvre's original mathematical psychology work, the reflexion score is an identifier, measured in

---

[69] Timothy Thomas, "Russia's Reflexive Control Theory and the Military," *The Journal of Slavic Military Studies* 17, no. 2 (June 2004): 237, https://www.rit.edu/~w-cmmc/literature/Thomas_2004.pdf. The U.S. Army has incorporated this definition into TRADOC Pamphlet 525-3-1, GL-6, Fn. 55.

[70] Diane Chotikul, "The Soviet Theory of Reflexive Control in Historical and Psychocultural Perspective," (Technical Report, Naval Postgraduate School, July 1986), 6, https://apps.dtic.mil/sti/citations/ADA170613; Antti Vasara, "Theory of Reflexive Control: Origins, Evolution and Application in the Framework of Contemporary Russian Military Strategy," (National Defence University, 2020), 6, 29, https://www.doria.fi/handle/10024/176978.

[71] It is important to note that Soviet Reflexive Control Theory also forms the foundation for Information Warfare as defined in the U.S. Army's TRADOC Pamphlet 525-3-1, though fundamental differences in methods of employment exist between Russian and American implementations of the base theory.

exponents, of one's ability to understand the cognitive map of another.[72] If one presumes Russian entity X is attempting to influence a foreign entity Y, then entity X must have a higher reflexion score to successfully reflexively control Y. That score is measured by elements that serve to control the opponent. If X is attempting to control Y, they must understand Y's decision-making process, which increases X's reflexion score. If Y recognizes this control effort, Y's score increases as well. X must then devise a new method of influencing or controlling Y's actions. As long as X maintains a higher reflexion score, some level of reflexive control is achieved.

The above description simplifies the theory considerably, as Lefebvre includes methods to integrate formal and informal leaders in an entity, and the power they have over an organization.[73] Mathematically, the leader sets the floor of reflexion score; the organization can surpass it but not move lower than the leader due to his influence in the decision-making process. The theory also recognizes the impact of dissonance between a leader's reflexion score and the organization and emphasizes the need to understand when the leader will choose his internal mental model rather than the organization's.

This thesis offers that OCO-enabled RCT operations can target mass populations, foreign and domestic, much more granularly that Soviet-era RCT. This could be

---

[72] Vladimir Lefebvre and Victorina Lefebvre, *Reflexive Control: The Soviet Concept of Influencing an Adversary's Decision Making Process* (Englewood, CO: Science Applications Inc., 1984), quoted in Erick D. McCroskey, "Decision Space Operations: Campaign Design Aimed at an Adversary's Decision Making" (Monograph, School of Advanced Military Studies, U.S. Army Command and General Staff College, 2003), 18–31.

[73] Lefebvre and Lefebvre, *Reflexive Control,* quoted in McCroskey, "Decision Space Operations," 24.

accomplished by practitioners (entity X) refining baselines for entire population groups (entity Y), simulating the general population's decision-making process to determine reflexive structure. Enacting RCT methods in cyberspace allows for a significant optimization in the process of Reflexive Control of any entity Y, even as their full cognitive map is not yet known. Offensive cyber-attacks can be utilized to manipulate or elucidate the psychology of the target, providing feedback to build a better baseline model.

Once entity Y's reflexion baseline is created, any attempt at influence can help categorize sub-groups of entity Y. This may manifest as a haphazard, broadly aimed cyber-attack or misinformation campaign that resounds with some part of the entity Y population. If that part of the population contains an informal leader in a social group or movement, Reflexive Control methods categorize the sub-group, bounding the groups reflexion score, further reflexively controlling entity Y's subgroup (hypothetically labelled Y-1). The general population is subject to reasonably well understood psychological principles, leaving only the reflexive structure of the sub-group Y-1 above the Y-baseline to be identified. Military targets, as an example, generally follow prescribed (often incredibly detailed and readily available) decision-making processes such as the Military Decision Making Process. This bypasses the need for expending repeated effort for reflexive control over multiple social organizations or military units, and enables predetermining the baseline reflexion score of entity Y-1 as a mathematical variable. As additional information becomes available to identify the rest of Y's decision-making process, it can be added to the Y-baseline or the Y-1 sub-group baseline.

Furthermore, repeating the process on the remainder of entity Y to create more sub-groups (Y-2, Y-3, and so on) allows for a system of Reflexive Control to be built that captures an entire population. While this was a task-intensive process with Soviet-era Reflexive Control, this becomes a mundane task when presented with the general public target, or even the military target set, enabled by the immediate feedback of cyber-attacks and misinformation campaigns. With the advent of cyberspace, RCT methods became the primary method of influencing enemy strategy at negligible risk to force, ephemeral consequence on the perpetrator, and minimal cost compared to physical operations.[74] As an example, the U.S. has twice fallen victim to recent Russian use of RCT to the adversary's strategic benefit, in Ukraine and in Syria.[75] General Nakasone, Commander of USCYBERCOMMAND, specifically acknowledged the strategic impact of an enemy subversively manipulating U.S. decision-making as a greater threat than an offensive cyberweapon.[76]

While Russian doctrine and warfighting theories are seldom publicly available, a few researchers have had success in studying the theory informed by its founding

[74] Thomas, "Russia's Reflexive Control Theory and the Military," 246–247; Keir Giles, James Sherr, and Anthony Seaboyer, "Russian Reflexive Control," (Royal Military College of Canada, Kingston, Ontario, October 2018), 28–40.

[75] Maria Snegovaya, *Putin's Information Warfare in Ukraine: Soviet Origins of Russia's Hybrid Warfare,* Russia Report 1 (Washington, DC: Institute for the Study of War, September 2015), 7.

[76] Mark Miles and Charles Miller, "Global Risks and Opportunities - The Great Power Competition Paradigm," *Joint Force Quarterly*, no. 94 (July 2019): 81, https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-94/jfq-94_86-91_Miles-Miller.pdf.

principles as well as through observed and implied adversary actions.[77] Notably, Thomas offers one of the earliest analyses of RCT in a 2004 paper and offers insight into the theory's evolution in his 2019 work "Russian Military Thought: Concepts and Elements." This technical paper dedicates a significant space to updates on Russia's use of Reflexive Control concepts, and forecasts on future Russian conflicts, including their focus on cyberspace. Taken together, Thomas' works build a framework for understanding how the warfighting theory has developed over the past two decades, as connected technology and corrosive threats have matured hand-in-hand. Thomas' perspectives facilitate building a foundation for an understanding of the modern Russian way of war, and the fallacies of projecting uniquely Western ideologies onto Russian cyber and information operations.[78]

Additional context on Russia's information warfare techniques is presented in the frame of the Russo-Ukrainian War in Maria Snegovaya's report, though some aspects of the report are dissonant with respect to Thomas' works. Specifically, she focuses on comparing Russian styles of warfare with Western styles of warfare. Snegovaya does, however, inform with a historical perspective, and describes discreet applications of

[77] Russian military doctrine was available at the commencement of research through the Security Council of Russia (http://www.scrf.gov.ru), however after sovereign internet measures were taken after the beginning of the 2022 invasion of Ukraine, many Russian government websites became unavailable.

[78] Timothy Thomas, "Russian Military Thought: Concepts and Elements," (Technical Paper, The MITRE Corporation, McLean, VA, August 2019), https://www.mitre.org/publications/technical-papers/russian-military-thought-concepts-and-elements.

Reflexive Control in military and non-military situations.[79] These examples offer a more modern context to the operationalization of RCT than Thomas' examples from the 1990s, and support Giles' examples from the Russo-Georgian and Russo-Ukrainian wars.[80]

Summary

This literature review sought to organize and summarize existing research in the fields on the primary and secondary research questions. States, industry stakeholders, and international organizations alike recognize the challenge of applying existing laws to cyberspace, but differ on paths forward. Despite sponsoring a UN working group towards establishing universal cyberspace norms, Russia has used offensive cyber operations, often impacting civilians, towards its strategic political and military goals.

The following chapters will utilize the research discussed here to answer how Russia is able to maintain an image of compliance with international humanitarian law as they conduct offensive cyberattacks against civilians, and whether Reflexive Control is utilized to support that effort.

[79] Snegovaya, *Putin's Information Warfare in Ukraine.*

[80] Giles, Sherr, and Seaboyer, "Russian Reflexive Control," 13–23; Thomas, "Russia's Reflexive Control Theory and the Military," 252–253.

CHAPTER 3

RESEARCH METHODOLOGY

Introduction

This study intends to determine the role of OCO against civilians, and civilian infrastructure, in Russia's application of RCT. Supporting the stated intent, the research sought to answer the primary and two secondary research questions:

1. How does Russia project an image of compliance with international law in the conduct of OCO?
2. What loopholes or gaps exist in international humanitarian law and its protections of civilians as it applies to OCO?
3. How does Reflexive Control Theory (RCT) apply to the use of cyberspace operations?

The researcher selected a qualitative analytical approach that identified key elements across historical examples to apply those elements to a framework that may provide insight into future incidents. While various individual methodologies might have been applicable, the researcher chose a mixed methods approach as it suitably addresses the primary and secondary research questions. This mixed-method approach consisted of two qualitative methods, a cross-case synthesis followed by structured document analysis. The combination of methodologies minimized the shortcomings of comparative case studies with small sample sizes.

Method

The selected method strove to empirically investigate Russia's image of compliance with international humanitarian law, substantiated by recent examples of uses of OCO on civilians that exploit gaps in international humanitarian law. Robert Yin's *Case Study Research and Applications* set the stage towards that goal adeptly, identifying that all research methodologies can be used for any of three distinct purposes: exploratory, descriptive, and explanatory.[81] Researching via process tracing, defined by Yin as "tracing of operational processes over time, rather than mere frequencies or incidence," lends itself to explanatory research methods, namely case studies.[82] Case study methodology is particularly applicable when the case deals with "a contemporary set of events…over which a researcher has little or no control."[83] These tenets are readily visible and present in the assessment of the primary and secondary research questions.

Following Yin's prescribed research design techniques, the next task was defining and selecting the cases. Russia, whether as a function of RCT or due to the clandestine nature of the OCO, regularly repudiates any allegations of Russian-influenced offensive cyberattacks. However, the U.S. asserts that Russia is a primary perpetrator of OCO against American individuals, companies, and infrastructure. Attribution in cyberspace is a challenging task; malicious actors can use code pilfered from a State actor, route network traffic through compromised routers, or remotely execute distributed attacks via

---

[81] Robert K. Yin, *Case Study Research and Applications: Design and Methods,* 6th ed. (Los Angeles: SAGE, 2018), 10.

[82] Ibid., 10.

[83] Ibid., 13.

botnets worldwide. Recognizing these complexities, the researcher deferred to trusted sources for determining attribution. This thesis relies on attributions as supported or determined by the U.S. Government and NATO. These attributions stem from evidence-based investigations, including those conducted by the Department of Justice and the Federal Bureau of Investigation, or attributed to Russia in Senate hearings, and are therefore considered trustworthy.

The list of possible conflicts, pared down to include only those with OCO, then again limited to those attributed to Russia, resulted in the selection of two viable cases. The researcher validated the cases as both recent enough to reflect newer Russian doctrine and old enough to have provided the opportunity for a large body of research. The selected cases are the Russo-Georgian War, and the Russo-Ukrainian War.

While the researcher was preparing this thesis, the Russo-Ukrainian War resumed after a six-year ceasefire, complicating the how future researchers can replicate these results. Various scholarly articles used in this thesis refer to the Annexation of Crimea, the War in Donbas, or the Russo-Ukrainian War, not knowing that the conflict would resume in 2022. This thesis will utilize the Russo-Ukrainian War to indicate the Russian aggression in the 2013-2017 period, as the tactics, military and political goals, and scope of the 2022 Russian invasion of Ukraine are fundamentally distinct from the earlier phase of conflict.

After selecting the Russo-Georgian and Russo-Ukrainian Wars as the cases, a specific methodology was required to determine valid inferences and apply them to future conflicts. Instead of analyzing the selected conflicts as a singular case, the researcher utilized cross-case synthesis, as identified in Figure 1. The goal of the cross-case

synthesis in this thesis was to bring forth key inferences within a framework that was common to Russian OCO; those key inferences are then used to provide structure to the document analysis.

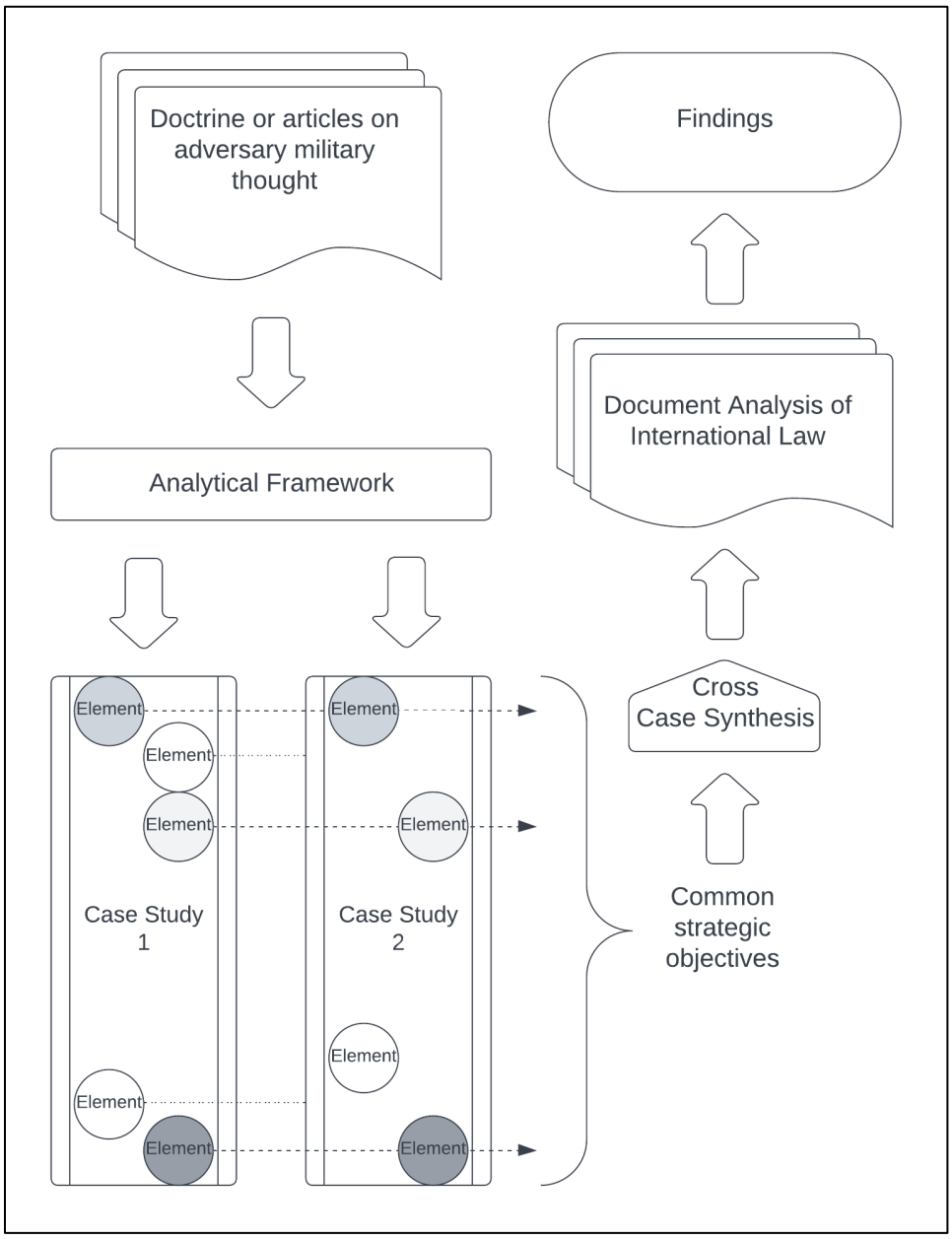

Figure 1. Mixed Methods Research Design Utilized in Support of Thesis

Source: Created by author.

The researcher used the Chekinov-Bogdanov commentaries to build a framework of analytical factors to apply to the case studies. The framework included ten factors identified in Table 1, including one not explicitly stated in the commentaries: Reflexive Control methods.

Table 1. Framework Drawn from Chekinov-Bogdanov Commentaries

Chekinov/Bogdanov Political and Military Strategic Goals	
Less costly methods of war	Socio-psychological impact
Complicate rules and customs of war	Support goals prior to use of ground force
Conceal operations	Destroy economy
Mislead opponents	Adjust public opinion
Destabilize social situations, induce riots	Reflexive Control methods

Source: Thomas, *The Chekinov-Bogdanov Commentaries of 2010-2017: What Did They Teach Us About Russia's New Way of War*; Chekinov and Bogdanov, "The Art of War in the Early 21st Century: Issues and Opinions"; Chekinov and Bogdanov, "Nature and Content of a New Generation War"; Chekinov and Bogdanov, "A Forecast for Future Wars: Meditations on What They Will Look Like"; Chekinov and Bogdanov, "The Evolution of the Essence and Content of 'War' in the 21st Century"; Chekinov and Bogdanov, "Military Strategy: A Look into the Future"; Chekinov and Bogdanov, "Predicting the Nature and Content of Future Wars: Problems and Opinions"; Chekinov and Bogdanov, "Initial Periods of War and their Influence on a Country's Preparations for Future War"; Chekinov and Bogdanov, "Strategic Deterrence and Russia's National Security Today"; Chekinov and Bogdanov, "The Influence of the Indirect Approach on the Nature of Modern Warfare."

As the framework was applied to the case studies and elements of the framework were found, they were labeled as key inferences and annotated to build a baseline for Russian OCO. This baseline then provided structure for the document analysis.

The document analysis focuses on international humanitarian law to identify loopholes or gaps that have been exploited. As a function of addressing the primary

research question of how Russia projects an image of compliance with international humanitarian law in the conduct of OCO, the document analysis also frames the answer to the secondary research questions of how RCT applies to the use of offensive cyberspace operations.

The case studies utilized in this mixed methodology research are not without criticisms. Cyber warfare is still novel, attribution is challenging, and the number of cyberattacks thus far limits the sample size. Considering the small sample size, countering bias plays an integral role in ensuring the analysis's validity. In an effort to mitigate bias concerns, the research relies on an expansive variety of authoritative authors when primary sources are unavailable. Yin describes case study evidence as coming from many sources, such as "documentation, archival records, interviews, direct observations, participant-observation, and physical artifacts."[84] Each of these six sources has strengths and weaknesses, particularly when considering the research topic, and "no single source has a complete advantage over all the others," according to Yin.[85]

Documentation provided a majority of the material for researching this thesis. Documentation, specifically scholarly articles, administrative documents, meeting minutes, proposals, internal records, and formal studies are readily available in a connected society. Yin describes the benefits of documentation as specificity and covering a broad range of times, topics, and settings, but highlights that documentation poses challenges in lacking ready accessibility and the potential for bias in selectivity and

[84] Yin, *Case Study Research and Applications*, 153.

[85] Ibid., 156.

reporting.[86] When available, the researcher directly reviewed reports from the UN and the NATO, recognizing the potential for bias based on the party sponsoring the report or working group.

Several other sources were explicitly ruled out for this thesis. While archival records improve upon documentation's strengths with precision and potentially offer quantitative data, quantitative data does not directly support the researcher's chosen methodology. Therefore, no archival records were utilized in support of this research. Additionally, while often insightful and targetable to provide focused information, interviews are also not utilized in this thesis. Limitations due to available time to complete degree requirements, travel restrictions, and readily available documentation are contributing factors to the omission of interviews and the researcher's desire not to cross the gap to human subject research. Moreover, physical artifacts are also omitted due to a lack of relevance to the topic. "Physical artifacts may have less potential relevance in the most typical kind of case study," especially considering the non-physical nature of the actions of the corrosive Russian cyber threat.[87]

As a function of the difficulty in attribution for offensive cyberattacks, the research utilized the principle of triangulation. Taken in the context of research, triangulation leverages a strength of the case study methodology, namely the "opportunity to use many different sources of evidence" to discern and validate adversary

[86] Yin, *Case Study Research and Applications*, Figure 4.1.

[87] Ibid., 169.

strategies reasonably reliably.[88] Utilizing multiple sources aids researchers in establishing facts when the biases of the source documentation are not explicitly known. Utilizing theory triangulation, defined by Yin as "of perspectives to the same data set," the researcher can maximize the advantage of converging lines of inquiry.[89] Converging lines of inquiry support coupling assessments on the identified key inferences in the cross-case synthesis, and applying that analytical lens to analysis of existing international humanitarian law, to determine Russia's likely courses of action in future conflict.

Summary

The mixed methodology chosen by the researcher discretely analyzed two historical incidents, identified key inferences between the two independently assessed cases, and utilized the results to identify answers to the research questions, via cross-case synthesis and document analysis. While case study methodology has viable critiques, as identified in this chapter, the combination of methods offers an opportunity for verification and repeatability. As future incidents occur, another researcher only need accomplish a single case study of that event and verify that the key inferences identified in this work are still present in future incidents.

[88] Yin, *Case Study Research and Applications*, 171.

[89] Ibid., 172.

CHAPTER 4

ANALYSIS

> Russia has never had anything to do with any types of cybercrimes.
> —Dmitry Peskov, Kremlin spokesperson, 13 February 2019

The analysis and findings presented in this chapter are categorized into three primary sections, beginning with a section discussing the analysis and findings from the case study of the Russo-Georgian War. Following the first section is an analysis and findings from the case study of the Russo-Ukrainian War, specifically during the 2013-2019 time period. The researcher uses a framework derived from the Chekinov-Bogdanov commentaries to identify elements of each case study and correlate existing features of Russian military thought. While Colonel Chekinov and Lieutenant General Bogdanov's perspectives in their series of commentaries apply broadly to military thought and recognizing that Russian doctrine does not view cyber operations as separate and distinct from the greater information operations function, applying the Chekinov-Bogdanov's perspectives provides Western militaries a framework to view research on Russian offensive cyber operations prior to extensive research on Russian military thought.

The Chekinov-Bogdanov framework establishes several possible overarching military and political objectives: reflexive control, concealment of operations, destruction of the opponent's economy, socio-psychological impact, adjustment of public opinion, destabilization of social situations, and re-anchoring or complicating the rules and customs of war. As the Chekinov-Bogdanov commentaries included forward-thinking articles that generally apply to military operations rather than solely OCO, several other

objectives were discussed in the Chekinov-Bogdanov commentaries were present in the framework but not evident in the case studies, and therefore were not included in the document analysis. The key inferences that were found in the case studies were then evaluated with respect to which international laws they sought to exploit, if any. Finally, the chapter concludes with a more robust analysis of the specific exploited articles of international law that were being exploited, as well as a summary.

Russo-Georgian War

In August 2008, over five days, Russia seized the Georgian territories of Abkhazia and South Ossetia. The tensions leading up to this find their roots in the aftermath of the fall of the Soviet Union, reignited by Georgia's Rose Revolution and aspirations to become a member of NATO, sustained by continued tensions in the South Ossetia region leading up to hostilities, until the situation was manipulated for Russian benefit. Russian tactics in this conflict were especially novel, as this appeared to be "the first case in history of a coordinated cyberspace domain attack synchronized with major combat actions in the other warfighting domains."[90] The cyberspace environment was prepared in the preceding month, as hackers tested their access and prepared materials and statements for the defaced websites. Once the Russian offensive military operation commenced, cyberattacks defaced and denied access to the cyber presence of Georgian government offices, as well as media, commercial, and finance industry websites.[91] The

[90] David Hollis, "Cyberwar Case Study: Georgia 2008," *Small Wars Journal* (January 6, 2011): 2, https://smallwarsjournal.com/jrnl/art/cyberwar-case-study-georgia-2008.

[91] Ibid.

networks that were attacked seemed deliberately selected to minimize physical harm and maximize psychological impact by preventing messaging to the civilian population and denying access to financial institutions. In contrast, power and other critical infrastructure networks were not obstructed despite being valuable military targets. Viewing the cyberattack on Georgia from a technical standpoint is critical in determining the overarching lack of complexity, small scope, and success of the attack.

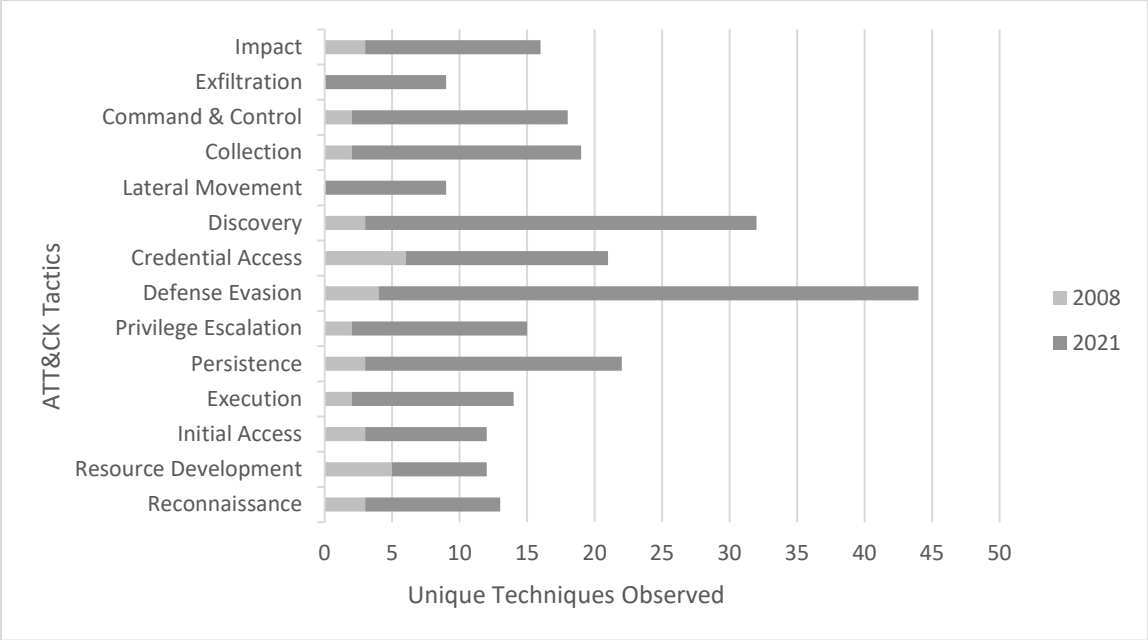

Figure 2. Graphical Comparison of OCO Techniques Observed during the 2008 Russo-Georgian War and by 2021

Source: Created by author. ATT&CK Tactics obtained from The MITRE Corporation. "Enterprise tactics." ATT&CK. Accessed April 1, 2022. https://attack.mitre.org/tactics/enterprise.

Utilizing the industry-standard MITRE ATT&CK matrix tactics as categories, and documenting any offensive cyber techniques that could result in the denial of service or defacement of Georgian websites, it becomes evident that the complexity of the attack

was relatively low, as depicted in Figure 2, compared to Russian offensive cyber capabilities demonstrated thereafter.[92] Bot-nets controlled via the original BlackEnergy trojan malware, email spamming coordinated through pro-Kremlin forums such as StopGeorgia.ru, and malicious SQL-payloads were the primary vectors for attacking the general population in cyberspace.[93] The scope of the cyberattacks against civilians was also relatively narrow; in 2008, less than 10 percent of Georgians had internet access. Determining the successfulness of the cyberattack is more challenging, as it varies based on the undisclosed objectives the operation had. Fortunately, the framework built from the Chekinov-Bogdanov commentaries enabled the researcher to analyze the offensive cyber operations, resulting in the discovery of several key inferences that proved helpful in the cross-case synthesis.

As an aspect of the framework, the concealment of operations stems from the 2012 Chekinov-Bogdanov commentary titled "Initial Periods of War and their Influence on a Country's Preparations for Future War." They note that in preparing for conflict, "the attacker will presumably make wide use of nonmilitary (indirect) moves and techniques, including targeted cyber-attacks against the communications systems" to

[92] The MITRE ATT&CK matrix is a threat intelligence database intended to explore known human, network, and systems exploits, as well as a database of malicious cyber actors. The MITRE ATT&CK matrix can be found online at https://attack.mitre.org, and is used industry-wide to understand a cyberattack's techniques, tactics and procedures.

[93] Nicu Popescu and Stanislav Secrieru, "Hacks, Leaks and Disruptions: Russian Cyber Strategies," (Chaillot Paper No. 148, European Union for Security Studies, Paris, France, October 2018), 59, https://www.iss.europa.eu/sites/default/files/EUISSFiles/CP_148.pdf.

prevail in information warfare.[94] Despite the lack of complexity and scope, the operation successfully served to conceal the preparation, nature, and execution of the operations by denying telecommunications, as well as disabling local media outlets and methods for the government to disperse messages and influence or control narratives leaving the country.[95] Harm to civilian data, websites and telecommunications was collateral to the main effort of concealing operations from the Georgian government and military, as well as the international audience, and controlling information in the area of military operations.

Chekinov and Bogdanov highlight, in "Nature and Content of a New-Generation War," that "new-generation war will be dominated by information and psychological warfare that will seek to … depress the opponent's armed forces personnel and population morally and psychologically."[96] This perspective on warfare is reminiscent of Giulio Douhet's thoughts on demoralizing civilians with strategic bombing in World War I. Taking the element of the framework of adjusting public opinion, and applying it to the Russo-Georgian War, the researcher found a handful of OCO that served to manipulate the opinion of civilians in the general population and "[reduce] the opposing sides'

---

[94] Colonel S. G. Chekinov and Lieutenant General S. A. Bogdanov, "Initial Periods of War and their Influence on a Country's Preparations for Future War," *Military Thought*, no. 11 (2012), 18.

[95] Timothy Thomas, *Recasting the Red Star: Russia Forges Tradition and Technology Through Toughness* (Fort Leavenworth, KS: Foreign Military Studies Office, 2011), 157, https://community.apan.org/wg/tradoc-g2/fmso/m/fmso-books/195632.

[96] Colonel S. G. Chekinov and Lieutenant General S. A. Bogdanov, "The Art of War in the Early 21st Century: Issues and Opinions," *Military Thought*, no. 1 (2015), 16.

determination to resist."[97] The disabling of Russian and Georgian news sites that provided a pro-Georgian view, redirecting civilian internet traffic to Russian-controlled websites, as well as defacing Russian news sites and implying Georgian culpability shifted public opinion by the omission of a narrative counter to that of the Russian government's narrative.[98] This early cyber-enabled information warfare was notably effective at adjusting public opinion and destabilizing social situations, as more than a decade later, over half the Georgian population believes the greatest failure of their government was human rights abuses and failure to prevent the 2008 war.[99] The cyber-enabled disinformation campaign supporting this narrative has continued to present day, as seen in news releases, social media, and online videos, dutifully cataloged and disproven by the European Union's counter-disinformation efforts.[100]

Finally, Chekinov and Bogdanov emphasize that "war will be fought by the rules and customs of the side that is best prepared to put the recent breakthroughs in warfare economics to a practical test."[101] OCO during the Russo-Georgian war has generally been

---

[97] Chekinov and Bogdanov, "The Art of War in the Early 21st Century," 42, quoted in Thomas, *The Chekinov-Bogdanov Commentaries of 2010-2017*, 19.

[98] Natia Chankyetadze and Ketevan Murusidze, "Re-Examining the Radicalizing Narratives of Georgia's Conflicts," (Carnegie Europe, Brussels, Belgium, May 12, 2021), https://carnegieeurope.eu/2021/05/12/re-examining-radicalizing-narratives-of-georgia-s-conflicts-pub-84508.

[99] Ibid.

[100] The European Union's East StratCom Task Force catalogs Russian disinformation campaigns on their website https://euvsdisinfo.eu.

[101] Chekinov and Bogdanov, "Nature and Content of a New Generation War," 22, quoted in Thomas, *The Chekinov-Bogdanov Commentaries of 2010-2017: What Did They Teach Us About Russia's New Way of War*, 7.

attributed to the Russian Business Network, a cybercrime gang directed by the Russian government.[102] The legal implications of State-directed criminal organizations significantly complicate the rules and customs of war due to attribution issues and plausible deniability. The re-anchoring and complicating of the rules and customs of war is another facet of the Chekinov-Bogdanov framework.

Overall, the analysis of the OCO in the Russo-Georgian War found several key inferences within the analytical framework built from the Chekinov-Bogdanov commentaries: concealment of operations, adjust public opinion, destabilization of social situations, complicate rules and customs of war. The researcher's labeling of objectives as key inferences does not indicate complexity, scope, or success. It is only intended to highlight that OCO supports these generalized objectives, even in a rudimentary and unsophisticated manner.

Russo-Ukrainian War (2013-2019)

Beginning in February 2014, shortly after Ukraine's Revolution of Dignity, Russian soldiers, without identifying insignia, began to seize the Ukrainian peninsula of Crimea under the pretext of protecting Russian speakers from the Ukrainian government. After annexing Crimea, Russian-backed separatists, and eventually Russian troops, began a conflict with Ukrainian troops in the Donbas region. Russian OCO are alleged to have begun as early as 2013, with malware such as RedOctober, MiniDuke, NetTraveler, and

[102] Putin's Asymmetric Assault on Democracy in Russia and Europe: Implications for U.S. National Security, A Minority Staff Report Prepared for the use of the Committee on Foreign Relations, 115th Cong., 2nd sess. January 10, 2018, S Prt. 115-21 (Washington, DC: U.S. Government Publishing Office, 2018), 73–76, 181–184, https://www.foreign.senate.gov/imo/media/doc/FinalRR.pdf.

Uroboros, though the attackers showed voluntary restraint in target selection and attack at the onset of the conflict. In lockstep with Russian military thought, OCO were predominantly integrated into reconnaissance support for military strikes, as well as information operations facilitated by cutting-edge malware, until the scope broadened and restraint withered as the conflict continued.[103]

The U.S. Department of Justice, in charges against six officers from the Main Directorate of the General Staff of the Armed Forces of the Russian Federation (often referred to by its former acronym, GRU, or former designation as the Main Intelligence Directorate) and Military Unit 74455, offered evidence of the deployment of various destructive malwares, including BlackEnergy, KillDisk, and Industroyer, specifically targeted against Ukraine's electrical grid, Ukrainian government offices, and private financial organizations. This BlackEnergy malware, updated since its use in Georgia in 2008, served to control massive bot-nets to facilitate distributed denial of service attacks on Ukrainian internet infrastructure. While the indictment covers a variety of incidents, perpetrators, and victims, the most prevalent actor during the Russo-Ukrainian War listed in the indictment was the SANDWORM team.[104] The indictment summarizes their OCO techniques as:

> (1) Communicate, research and probe victim computer networks; (2) register malicious websites and domains with names mimicking legitimate ones; (2) send spearphishing emails (4) store and distribute additional malware; (5) manage malware; (6) transfer stolen data; and (7) negatively influence the public

[103] Amos C. Fox, "Hybrid Warfare: The 21st Century Russian Way of Warfare," (Monograph, School of Advanced Military Studies, U.S. Army Command and General Staff College, 2017), 7, 23, https://apps.dtic.mil/sti/pdfs/AD1038987.pdf.

[104] The SANDWORM team is also known as Russian Military Unit 74455 or VOODOO BEAR, depending on the organization analyzing the threat.

> perception of some of the victims. The Conspirators reused some of the same infrastructure to target multiple victim organizations and individuals.[105]

These operations coincided well with military operations, offering evidence of normalizing this new tactic of hybrid warfare in Russian military thought. Analyzing Russian OCO in the Russo-Ukrainian War using the Chekinov-Bogdanov framework highlighted several possible political and military objectives: reflexive control, mislead opponents, conceal operations, destabilize social situations, destroy economy, socio-psychological impact, adjust public opinion, re-anchor and complicate the rules and customs of war.

As early as 2013, the Gamaredon Group targeted Ukrainians in order to obtain information on the Ukrainian government and military intentions.[106] The custom malware, known as Pteranodon, was delivered via forged but enticing documents purporting to be from the Ukrainian government, instead delivering a custom payload that installed malicious executables, captured screenshots, searched the infected drives for sensitive materials, and enabled remote access.[107]

Though the researcher did not find evidence of spillage into civilian cyberspace, Gamaredon Group's cyber operations are noteworthy because of how the stolen information was weaponized to enable kinetic and devastating military strikes. After

---

[105] Scott Brady, *United States v. Yuriy Sergeyevich Andrienko, et al.* (U.S. District Court, Western District of Pennsylvania, 2020), 7.

[106] The Gamaredon Group is also known as Armageddon or PRIMITIVE BEAR, depending on the organization analyzing the threat.

[107] Anthony Kasza and Dominik Reichel, "The Gamaredon Group Toolset Evolution," Unit 42, last updated February 27, 2017, https://unit42.paloaltonetworks.com/unit-42-title-gamaredon-group-toolset-evolution.

Gamaredon Group stole sensitive information, the Russian military followed through by kinetically destroying those identified Ukrainian positions or forces, highlighting the deep integration and precise nature of cyber-enabled targeting, as well as a causal linkage between the cyberattacker and the State.[108] In fact, in 2021, Congress was presented with a report identifying Gamaredon Group as associated with the Russian Federal Security Service (often referred to by their pseudo-acronym, FSB); this attribution reaffirms a 2021 report published by the Security Service of Ukraine which provides technical analysis and identifies 31 distinct techniques used by Gamaredon Group.[109] Though there is a specific linkage between some intelligence and subsequent military action, other stolen intelligence may have been used for less visible methods, specifically aiding Reflexive Control efforts.

From the onset of the armed conflict, Russia effectively utilized Reflexive Control techniques, and was greatly aided by the maneuverability offered by cyberspace. Defacing, manipulating, and denying news services' websites offered the opportunity for Russia to successfully "[obfuscate] its objectives and repeatedly deny its military presence in the country despite overwhelming evidence to the contrary," while OCO effectively facilitated the manipulation of Ukrainian decision-making through denial of

[108] Unit 42, "Russia's Gamaredon AKA Primitive Bear APT Group Actively Targeting Ukraine," PaloAltoNetworks, last updated February 16, 2022, https://unit42.paloaltonetworks.com/gamaredon-primitive-bear-ukraine-update-2021.

[109] Andrew S. Bowen, "Russian Cyber Units," (Congressional Research Service, Washington, DC, February 2, 2022), 2, https://crsreports.congress.gov/product/details?prodcode=IF11718; Cyber Security Situational Centre, The Security Service of Ukraine (SSU), *Gamaredon/Armageddon Group* (Kyiv, Ukraine: SSU, 2021), 34–35.

communication networks in conjunction with the initiation of the shooting war.[110] At the time, these actions were viewed as expected, but novel uses of cyberspace. The operations also met the Chekinov-Bogdanov framework objectives of misleading opponents and concealing operations, as would be expected of a country that views cyber operations as an integral facet of military information operations.

The scope of the OCO was markedly broader than Russia had historically operated within. The initial years of the conflict expanded the scope to include the full spectrum of legal military targets such as the electrical grid, and some blatant cyber-enabled violations of Ukraine's sovereignty, most notably a current hallmark of Russian foreign policy, election interference.

The OCO targeting the Ukrainian electrical grid showed incredible sophistication, ranging from social engineering cyberattacks to expansive and efficient malware such as BlackEnergy.[111] The cyberattacks on the power grid in 2015 and 2016 align with the Chekinov-Bogdanov framework objective of socio-psychological impact. The first attack occurred at 3:30 pm over a holiday just prior to Christmas, when most Ukrainians would be at home.[112] Repeating the attacks nearly exactly a year later in 2016 only exacerbated the framework objective of socio-psychological impact on Ukrainian civilians. Furthermore, as the first-ever successful cyberattack on a power grid, Russia met another

---

[110] Giles, Sherr, and Seaboyer, "Russian Reflexive Control," 18.

[111] Lawson and Macak, "ICRC Expert Meeting Transcript - Avoiding Civilian Harm From Military Cyber Operations During Armed Conflicts," 49–50.

[112] Robert M. Lee, Michael J. Assante, and Tim Conway, *Analysis of the Cyber Attack on the Ukrainian Power Grid* (Washington, D.C.: Electricity Information Sharing and Analysis Center, March 18, 2016), iv.

framework-derived objective of re-anchoring and complicating the rules and customs of war.

In 2014, a failed attempt at compromising Vybory, the Ukrainian Central Election Commission's computer-aided vote tallying system, was attributed to a hacking group with ties to the GRU.[113] As votes were being tallied, Ukrainian officials discovered and quietly eradicated a virus intended to overwrite the election tally with false results of a 37% vote for a far-right candidate, rather than the less than 1% he did actually receive. Immediately following the election, Russia undertook an offensive cyber operation resulting in the defacement, then disabling, of the Central Election Commission's results website for several hours, delaying the official announcement of the next president of Ukraine.[114] Concurrent to the operation denying the election results from being published, Russian media announced false results for the election, misinforming the global and Ukrainian audience with the exact fake tally as was coded into the virus. Apart from the violation of Ukraine's sovereignty and gross attempts at destabilizing social situations, the offensive cyber operation met the Chekinov-Bogdanov framework objective of adjusting public opinion, particularly on the election's legitimacy, with the

---

[113] Russian Active Measures Campaigns and Interference in the 2016 U.S. Election, vol. 1, Russian Efforts against Election Infrastructure with Additional Views, 116th Cong., 1st sess., Report 116-XX (Washington, DC: Select Committee on Intelligence), 64, http://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume1.pdf.

[114] NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), "Ukraine Parliamentary Election Interference (2014)," International Cyber Law in Practice: Interactive Tool Kit, last updated March 26, 2019, https://cyberlaw.ccdcoe.org/wiki/Ukrainian_parliamentary_election_interference_(2014); US Congress. Senate, *Russian Active Measures Campaigns and Interference in the 2016 U.S. Election*, 64.

deeper context of casting doubt on the widespread support for progressive pro-Western movements. It is worthy of mention that the cyberattack's enduring result was antithetical, specifically in that it validated the Ukrainian election system's anti-fraud methods and encouraged Ukraine to continue to enhance their election commission's cybersecurity, including a pledge for $10 million from the U.S. State Department.[115]

As the conflict continued, the restraint shown in the initial period of war was less prevalent. OCO were indiscriminate, often spreading beyond the borders of Ukrainian government, such as with the NotPetya data-wiping malware. The distribution mechanism of the attacks utilized custom software stolen from the National Security Agency by the Shadow Brokers hacking group, and were incredibly effective when used to spread the infection.[116] As the malware spread beyond the target networks, from government computers to industry controllers to personal devices across the globe, the damage resulting in the mass data-wiping caused billions of dollars' worth of damage. This, potentially accidentally but quite effectively, aligns with the objective of destroying the adversary's economy in a particularly low-risk fashion, as well as re-anchoring and complicating the rules and customs of war.

---

[115] Office for Democratic Institutions and Human Rights, *Ukraine - Early Presidential Election 25 May 2014 - OSCE/ODIHR Election Observation Mission Final Report* (Warsaw: Organization for Security and Cooperation in Europe, May 24, 2014), 35; Ukrainian Election Task Force, *Foreign Interference in Ukraine's Democracy* (Washington, DC: The Atlantic Council, May 2019), 12, https://www.atlanticcouncil.org/in-depth-research-reports/report/foreign-interference-in-ukraine-s-election.

[116] The MITRE Corporation, "Enterprise tactics," ATT&CK, sec. S0368, accessed April 1, 2022, https://attack.mitre.org/tactics/enterprise.

Key Inferences from Case Studies

The case studies show that Russia's use of OCO have distinct trends, despite the scale and scope distinctions between the two case study subjects. OCO against Georgia in 2008 showed a lack of sophistication with limited goals and a focus on semi-deniability in order to avoid impediments by customary, international, and humanitarian laws. For example, the two primary areas of international law that were exploited in support of the 2008 operations were use of force and violation of sovereignty. These operations, taken individually, do not constitute a use of force as outlined in the Charter of the United Nations, Article 2(4). In customary international law, use of force is generally attributed to armed military forms of coercion.

Observed in their entirety, however, the OCO were accompanied by an armed military use of force, in this case, the Russian belligerence associated with the 8 August 2008 invasion of South Ossetia. This complicated the application of international law to the cyber operation as it would have been subsumed by the UN Security Council complaint against their destructive use of force or physical breach of sovereignty. The pretext for engaging in the destructive use of force or breach of sovereignty was dubious but *prima facie* legal. Chronologically applying the framework to historical incidents cannot appropriately capture the increased sophistication and escalation expected of future cyber conflicts. In order to better address developments in cyber warfare tactics and techniques in the future, the researcher used the Chekinov-Bogdanov framework objectives to identify the international laws being exploited.

As a broad effort to manipulate the opponent's decision-making process, RCT does not need to inherently exploit any international laws, though it benefits from the

maneuver space afforded by ambiguity in international law's application to cyberspace. Cyber-enabled reflexive control methods, used more aggressively in the future, could stay within international law and international humanitarian law while still achieving their objectives of influencing adversary decision-making. Continued utilization of cyber-enabled espionage and cyber-enabled gray-zone tactics such as disinformation, election interference attributed to criminal organizations or hacktivists, utilization of proxy forces and botnets for denials of service, all complicate the attribution of a State for the violation of sovereignty for their opponent, exploiting customary international law, as well as established practices from International Court of Justice rulings. Furthermore, Russia will be able to continue to exploit a loophole that exists regarding international humanitarian law only applying during armed conflict. If they can successfully deny that the conflict is armed, through denial of communications or media sources, they will be able to enact OCO on the general population with impunity, as evidenced by hostilities in 2008 and 2015. Finally, considering the speed of opponent decision-making at the operational and tactical levels, Russia may exploit the requirements of Article 2(3) of the Charter of the United Nations, requiring States to seek nonviolent remedies under Article 33, such as "negotiation, enquiry, mediation, conciliation, arbitration, judicial settlement" and more to support reflexive control methods, due to the incredible amount of time required to address such a conflict, since "the invocation of the responsibility of a State for an internationally wrongful act involves complex technical, legal and political

considerations."[117] By the time the arbitration begins, the reflexive control methods have already had an opportunity to influence the targeted critical decisionmaker.

Concealment of operations also need not explicitly violate international norms, considering the tactics of ruse and camouflage is a specifically allowed practice under the Geneva Conventions. Current methods, such as the Pterandon malware used in Ukraine as early as 2013, are initially viewed as criminal activities or espionage, and do not directly violate use of force prohibitions in and of themselves, even when attributed to a State. When the pilfered intelligence is weaponized, passed on to military units for kinetic action, the cyberattack and malware would be subsumed under the greater violation of the use of force prohibition in international law such as the Charter of the United Nations. Even then, it is unlikely that international law would consider the weaponized intelligence an attack in its own right, due to inflexible legal definitions of terms such as attack, armed conflict, hostilities, violence, and harm. Concealing operations in the future may not be limited simply to concealing the physical presence of troops (an international law violation as a breach of sovereignty in and of itself) by enacting internet blackouts to deny journalists the ability to report and upload media. Instead, concealing operations is likely to broadly include actions such as fostering misattribution by using code stolen from other State actors, launching attacks intended to be misattributed to destabilize an opponent's tenuous relations with an adversary, or hiring proxy cybercriminals to threaten or terrorize the general population while masking

[117] United Nations (UN), *Charter of the United Nations and Statute of the International Court of Justice* (San Francisco, CA, June 26, 1945), https://www.un.org/en/about-us/un-charter/full-text; UN General Assembly, *Advancing Responsible State Behaviour in Cyberspace in the Context of International Security*, 18.

the benefactor. These actions challenge State responsibility as codified by the International Court of Justice, discussed below as Article 4 and Article 8, and also leverage the lack of inclusion of cyber effects in the same key terms, such as attack, listed above.

Destruction of the opponent's economy evokes imagery such as indiscriminate shelling or area bombing, which are prohibited by a variety of international laws. Despite the billions of dollars of loss associated with the NotPetya data-wiping malware attacks in 2017, no effort was expended to apply the principles of State responsibility to provide restitution for the effects of the attack. Furthermore, cyberattacks under this objective again leverage the insufficient definition of attack, which prevents the Geneva Conventions requirements for discriminating between military and civilian objects. Future attacks intended to destroy an opponent's economy may involve manipulating and attacking stock markets or hacking supply management and logistics databases without necessarily running afoul of international law, again exploiting the lack of a use of force or violation of sovereignty in cyberattacks.

Socio-psychological impact, destabilizing social situations, and adjusting public opinion covers a wide range of political and military objectives in the two studied conflicts, ranging from defacing government websites, to power grid attacks, to leaks of pilfered private data by a State, and even election interference. The scope of these three Chekinov-Bogdanov framework objectives cover violations of customary international law, the Charter of the United Nations, the Geneva Conventions and International Court of Justice rulings, and all of them leverage the lack of an armed attack enacting international humanitarian law, plausible deniability, proxy forces, and misattribution.

Future conflicts will likely see State-sponsored cybercriminals leaking private health or financial data of an opponent's civilians, and cyber-enabled influence or disinformation campaigns creating destabilized social situations that offer Russia *prima facie* legality to step in with military force. The most likely pretexts will be language, religion, and race, borrowing from Article 1 of the Charter of the United Nations.[118]

Another Chekinov-Bogdanov framework objective, re-anchoring and complicating the rules and customs of war, was significantly more precisely described than the other framework objectives. They refer to making the "defending country's political and economic system made ungovernable, its population demoralized" in order to "achieve the military and political aims of its campaign within the shortest possible time frame," while "these nonmilitary options will lessen, and ultimately remove military hazards and threats by peace treaties" and when those efforts do not sufficiently achieve their objectives, Russia "must be ready to use every kind of power containment."[119] It is not difficult to envision a scenario that could avoid a use of force distinction while violating sovereignty in a multi-pronged offensive cyber operation on the general population of a country, targeting examples such as tax records, health records, stock markets, financial institutions, and telecommunication. Leveraging their opponent's adherence to existing rules and customs of war ensures Russia can maintain a permissive cyberspace environment and is likely to feature heavily in future conflict with limited aims.

---

[118] United Nations, *Charter of the United Nations and Statute of the International Court of Justice*.

[119] Chekinov and Bogdanov, "Nature and Content of a New Generation War," 22.

International Law

Several critical areas of international humanitarian law are relevant to how OCO are conducted, generally or against civilians. Customary international humanitarian law, International Court of Justice rulings and adopted Draft Articles, the Charter of the United Nations, and the Geneva Conventions serve as the foundation for the rules that nations at war are held to. Analyzing these documents with the key inferences from the case studies provides a baseline for OCO Russia is likely to undertake while continuing to project the image of compliance with international law and international humanitarian law, as well as highlight loopholes, ambiguities, and gaps that are exploited in these operations. While relevant to the topic in general, determining the status of cyber-attackers, State or Non-State, within the concepts of *jus in bello* and *jus ad bellum* is outside the scope of this thesis.

Customary international laws are "general practices accepted as law" and are universally applicable, as opposed to treaty laws, which are intended to bind States consenting to them.[120] The rules set forth under customary international law find their foundations in normalized practices and a variety of legal sources such as the Hauge Conventions of 1907 or International Court of Justice case law.

The International Court of Justice is the "principal judicial organ of the United Nations," and as such sets legal precedent that can establish customary international law,

[120] ICRC, *Study on Customary International Humanitarian Law*, 1.

as well as interpretations of existing international laws.[121] The International Court of Justice has formally adopted the *Draft Articles on the Responsibility of States for Internationally Wrongful Acts*, which contain two articles relevant to this thesis: Article 4, and Article 8. Article 4 links the conduct of a State organ with responsibility as an act of that State.[122] Therefore, when Russian military members, as organs of the State, conduct OCO, they make Russia responsible for their actions. This is not singularly sufficient justification to prosecute a State for the actions of a State-directed cybercriminal, therefore Article 8 must also be considered. Article 8 identifies that "the conduct of a person or group of persons shall be considered an act of a State under international law if the person or group of persons is in fact acting on the instructions of, or under the direction or control of, that State in carrying out the conduct."[123] This covers the scenario of attacks by CyberBerkut, a hacking group based in Ukraine with ties to Russian military forces. If it can be proven that Russia directed the actions of CyberBerkut, and potentially provided the cyber toolkit to accomplish the offensive operation, CyberBerkut's actions may be legally attributed to Russia as the responsible State.

---

[121] United Nations (UN), *Statute of the International Court of Justice*, International Court of Justice, 1945, 1, https://legal.un.org/avl/pdf/ha/sicj/icj_statute_e.pdf.

[122] United Nations (UN) General Assembly, *Report of the International Law Commission* (New York, NY: UN, 2001), 84, https://legal.un.org/ilc/texts/instruments/english/commentaries/9_6_1996.pdf.

[123] UN General Assembly, *Report of the International Law Commission*, 103.

The Charter of the United Nations is an example of treaty law, and binds UN member states to it. A small number of nations or states are not members of the UN, such as the Holy See, and some states with limited recognition such as Taiwan, Palestine, and Kosovo. Russia, however, is a member of the UN and therefore subject to its laws. The aspects of the Charter of the United Nations that are most relevant to conducting OCO are Article 2(4) and Article 51.

The Charter's Article 2(4) directs that member States "shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state" while also prohibiting actions inconsistent with Article 1, which identifies purposes of the UN.[124] Within Article 1, the phrases vulnerable to exploitation are the elements that discuss removal of threats to the peace or suppression of acts of aggression.[125] As discussed in this chapter, asserting that an action is taken to protect persons from threats to the peace or acts of aggression becomes a narrative-dependent opportunity to exploit international humanitarian law.

The Charter's Article 51 reaffirms customary international law in codifying the right to self-defense during an armed attack.[126] While the Article relies on customary international law for the definition of armed attack, it is widely accepted that not every cyber-incursion constitutes an attack. A more moderate viewpoint may be the consequence-based determination of whether a cyberattack has breached some threshold

---

[124] United Nations, *Charter of the United Nations and Statute of the International Court of Justice*.

[125] Ibid.

[126] Ibid.

defining attack, but even that enables low-risk offensive cyberattacks due to the difficulty of quick and accurate attribution. A recently-emerging consensus among States seems to be that cyberattacks causing physical injury or damage may be considered armed attacks.[127]

The Geneva Conventions of 1949, and the three additional protocols are another example of treaty law, even though many of the rules overlap with customary international humanitarian law. Geneva Convention IV, on protecting civilians in a time of war, was insufficient when considering the novel methods of warfare since 1949, and therefore Additional Protocol I, on protecting victims of international armed conflict, was adopted. Additional Protocol I of the Geneva Conventions of 1949 is the most relevant facet of the Geneva Conventions to this analysis. Three concerns complicate the applicability of international humanitarian law to OCO as accomplished by Russia. First, international humanitarian law only comes into effect during an armed conflict. Second, customary and treaty law only delineates between international armed conflict, and non-international armed conflict, neglecting damaging cyber operations in phases under the threshold of armed conflict. Finally, while Russia has withdrawn its Article 90 declaration, which acknowledged the powers of the International Fact-Finding

[127] Charlie Dunlap, "International Law and Cyber Ops: Q & A with Mike Schmitt about the Status of Tallinn 3.0," *Lawfire*, October 3, 2021, https://sites.duke.edu/lawfire/2021/10/03/international-law-and-cyber-ops-q-a-with-mike-schmitt-about-the-status-of-tallinn-3-0.

Commission, it is not absolved from their responsibilities under Additional Protocol I.[128] The Article 90 declaration withdrawal does, however, allow Russia to selectively approve of International Fact-Finding Commission evidence that might rule against Russia and reduce the maneuver space they enjoy in cyberspace.

Summary

Utilizing the two case studies, the researcher found several key inferences useful in assessing Russian military thought as it applies to international law. These inferences were: reflexive control, concealing operations, destruction of economy, socio-psychological impact, adjusting public opinion, destabilizing social situations, and re-anchoring and complicating the rules and customs of war.

Those inferences then helped identify general tactics associated with Russia's OCO. Inferences common to OCO in both conflicts were: concealing operations, adjust public opinion, destabilize social situations, re-anchor, and complicate rules and customs of war. Inferences unique to OCO in the escalated conflict of the second case study were: reflexive control techniques, destruction of opponent economy, and socio-psychological impact. This suggests a plausible ladder of escalation for Russia's OCO, with low-risk and low-cost operations that do not amount to a use of force against civilians setting the baseline. RCT operations that are task-intensive, such as successfully creating socio-psychological impact, or destruction of an opponent economy, run the risk of easier

[128] Russian Federation, "Notification to the Governments of the States Parties to the Geneva Conventions of 12 August 1949 for the Protection of War Victims" (Swiss Federal Council, October 23, 2019), 1, https://www.dfae.admin.ch/dam/eda/fr/documents/aussenpolitik/voelkerrecht/genevenotifications/191030-GENEVE_e.pdf.

attribution due to the complexity of the task, and greater risk of being addressed with international law, potentially permanently creating a more restrictive cyberspace environment. Reflexive control methods against large populations can vary significantly in risk of violation of international law and efficacy.

CHAPTER 5

CONCLUSIONS AND RECOMMENDATIONS

Introduction

Modern societies rely on the digital presence of governments, militaries, civilians, financial institutions, media, and critical infrastructure, making these networks and their data valuable targets for malicious actors. This thesis sought to identify how a State actor, Russia, maintains an image of compliance with international law while undertaking OCO against an opponent. Additionally, it pursued an assessment of which loopholes were being exploited in international law, and how RCT applies to Russia's OCO.

The research conducted during the case studies, cross-case synthesis, and structured document analysis provided sufficient data to answer the primary research question. The utilization of the Chekinov-Bogdanov commentaries to establish a framework for the case studies was a valuable tool, but with certain limitations. The framework aided in developing a baseline for which international laws Russia is currently exploiting, and identifying general OCO Russia is likely to take in future limited conflict, as well as proposing which escalatory measures can reasonably follow while still ascribing by international law. The exploitation of several aspects of customary international law, treaty law, and international humanitarian law were all found in both case studies, and demonstrated the maneuver space created by the stringent textualism in applying existing international law, intended for physical conflict, to conflicts in cyberspace.

Conclusions

Russia has been able to maintain an image of compliance and, therefore, the ability to act with impunity while conducting OCO due to an established practice of precision application of gray-zone conflict tactics to cyberspace. Furthermore, the image of compliance is supported by the lack of evidence in either case study of directly harming civilians in or via cyberspace, with the exception of indirect harm via power grid attacks and elections interference. While the case studies considered conflict with limited aims, the results already show escalation in scale and impact of cyberattacks that is only likely to increase unless international law is updated with considerations for future cyber conflict.

Both case studies inferred an offensive cyber operation, followed by a narrowly-scoped use of force. Any nondestructive impacts from the offensive cyber operation are subsumed under the UN Security Council complaint of the destructive use of force or physical breach of sovereignty, creating space where Russia continued conducting OCO. The physical breach of sovereignty, which would typically violate international law, then had a supportive narrative launched through defacement, denial of media and government websites, or redirecting traffic to Russian servers. This supportive narrative offered justification for the physical breach under tenets that would generally follow international law, such as acting in defense of ethnicity or race, or removal of threats to peace, from customary international law and the Charter of the United Nations. OCO on telecommunications then prevents competing ground-truth narratives from being widely released. The primary caveat is that the cyberattacks must be subsumed under the physical use of force or breach of sovereignty UN Security Council complaint.

Expanding from the baseline, Russia leverages textualism, whereby the specific definition of a term is valued over the intent of the law, as effective loopholes, ambiguities, and gaps in the application of international humanitarian law to cyberspace. The definitions for armed attack, use of force, hostilities, physical violence, damage, and breach of sovereignty are too narrowly defined to apply to cyberspace, de facto creating a permissive environment for cyberattacks on governments, militaries, and even civilians. International humanitarian law's reliance upon activation by armed conflict also exploits the definition of armed conflict, restricting any protections of civilians that would otherwise apply in a physical conflict between two States. These operations embody gray-zone conflict tactics, achieving strategic effect while staying below the threshold of armed conflict, specifically leveraging the strict definitions of armed attack, use of force, or armed conflict.

Finally, the research and analysis suggested a beneficial relationship between OCO and Reflexive Control methods due to the potential for viable feedback mechanisms, computer-aided modeling of reflexion, and the existing efforts in the case study that align with the Reflexive Control method of Selecting Messages. In fact, even though Russia likely utilizes multiple warfighting theories to support its strategic goals, a majority of its actions in cyberspace are supported under the construct of RCT. Despite this inference of a link between the two, the case studies lacked specific evidence of whether or not any previous OCO were verifiably reflexive control methods.

Recommendations

As demonstrated in the case studies, Russian OCO leverage loopholes, ambiguities, and gaps in international law to achieve strategic political and military goals,

at the cost of tangible harm to civilians. Other malicious actors are likely to utilize the same cyber maneuver space Russia operates within, turning the practice into a norm. The researcher recommends minimizing the maneuver space for belligerent impunity in cyberspace with a two-part solution.

First, upgrade contemporary domestic and international institutions, as well as treaties, to address cyber operations, gray-zone conflict tactics in cyberspace, and feigned compliance with international law. While governments would be generally responsible for effecting this change, other stakeholders such as the technology industry, utility providers, and telecommunications services are valuable advocates. This suggestion expands on the scope of the ICRC's talking point highlighted in the literature review, as limiting the adaptation solely to international humanitarian law still allows significant room for exploitation. If the conflict is not considered an armed conflict, international humanitarian law will not come into force. For this reason, policy changes must be made to the trio of international law, treaties, and international humanitarian law to minimize the maneuver space for adversary OCO.

Second, codify an effects-based determination of hostile cyberspace actions that do not meet the strict definitions of armed conflict, armed attack, hostilities, damage, violence, and actual harm. As an example, if Russia were to attack Poland's power grid, causing widespread and lengthy power outages, impacting emergency services, governing, finance, and essential services, then Poland would be empowered to swiftly determine whether the effects of the attack are comparable to an armed attack, enabling international humanitarian law protections and international support for armed or digital self-defense. Due process and appropriate attention to attribution will still be challenges

to this recommendation in practice, but the goal of limiting maneuver space will have been achieved regardless.

Shortfalls in Research or Scope

The Chekinov-Bogdanov commentaries served as a valuable foundation to organize operations into strategic objectives. A concern, however, is that their most recent work is 2017, and considering escalation of conflicts and significant changes in Russian military actions within the past ten years, insight into Russian military thought from 2017 may be dated. As additional perspectives on Russian military thought surface from the aftermath of the Russo-Ukrainian conflict, it would be beneficial to revisit the framework to confirm its continued validity. Additionally, Colonel S.G. Chekinov and Lieutenant General (ret.) S.A. Bogdanov's writings occasionally forecasted too far forward to a type of technology or level of war that is not yet customary or has recently been proved inaccurate. As an example, they believed that quantum computers would "easily crack all codes and gain free, and virtually instant, access to all networks supporting the operation and security of government and military control agencies."[129] This has been proved incorrect, evidenced by algorithms such as lattice-based cryptography.[130] While the structured document analysis and case studies were impartial

[129] Chekinov and Bogdanov, "Nature and Content of a New Generation War," 18.

[130] Lattice-based cryptography is one of several cryptographic functions known as post-quantum, and accomplishes its task by easily creating a problem that is difficult to solve, even with quantum computers. An excellent primer on lattice-based cryptography can be found via New York University's Courant Institute of Mathematical Sciences at https://cims.nyu.edu/~regev/papers/pqc.pdf

and objective, the Chekinov-Bogdanov commentaries being distilled into a framework by the researcher leaves it subject to the author's and the researcher's cognitive biases.

Furthermore, the question of a modern and universal definition of harm arose. The interconnectivity and reliance on cyberspace allow adversaries to conduct operations to create cyber-enabled socio-psychological impact without distinction of military or civilian targets. Harm, in this sense, can manifest in a variety of ways, such as financial or psychological. Financial harm, enabled by malware or stolen digital credentials, is easily captured in the recommendation for a shift to effects-based determinations. On the other hand, psychological harm is not so easily captured in an effects-based determination, and increasing concern today compared to the 1949-era perspectives on mental health. Could mass psychological harm, such as mass-created deepfakes, or cyberattacks enabling false missile warning sirens, meet the threshold for a physical response?

Topics for Further Study

In his 1984 book introducing RCT, Lefebvre envisioned a future for computer-aided reflexive control, performing aspects of the analysis while leaving the creativity up to the human.[131] Over the past 40 years, Lefebvre's assessment of the capabilities of computers has been challenged, as complex algorithms and narrow artificial intelligence are developed that can arrive at novel conclusions, even when confined to the same

[131] Lefebvre and Lefebvre, *Reflexive Control*, 144-145, quoted in McCroskey, "Decision Space Operations," 70.

rulebook as their human counterparts.[132] A future cyber-enabled reflexive control system, ascribing by Lefebvre's rules, that seeks to influence whole populations would be an interesting concept to dedicate further study towards.

This evolution of reflexive control might be a system that uses cyber-enabled information warfare to determine a subgroup's cognitive map, categorize the group by required inputs to manipulate decision-making, then move on to the next group. The required inputs could be sourced from social media, or leverage existing information extrapolated from publicly-available research on biases associated with zip codes and socioeconomic status. This type of process could systematically proceed through large portions of connected society via social media, categorizing required inputs along the way, ideally capturing at least one social group leader in each group, exploring their cognitive map until a positive reflexion score is obtained.

When the system is tasked to support a narrative, it simply adjusts the narrative to include a perspective that targets the social leader in each group, or the group as a whole, repeatedly via social media or targeted advertising, to sway an entire population's decision-making process while remaining well within the bounds of international law as simple espionage and influence operations. A hypothetical system such as this could be used to placate, sway, or manipulate domestic and foreign populations. It could also be used to combat similar adversary systems, automatically inoculating the population from adversary information warfare campaigns. Future research on this topic may come from

[132] Bowen Baker, Ingmar Kanitscheider, Todor Markov, Yi Wu, Glenn Powell, Bob McGrew, and Igor Mordatch, "Emergent Tool Use From Multi-Agent Autocurricula," (Paper, last revised February 2020): 1–2, https://arxiv.org/abs/1909.07528.

the realm of Department of Defense and Intelligence Community convergence, algorithmic warfare, or simply the synthesis of artificial intelligence and information warfare.

Summary

The research conducted on this topic shows evidence of Russian exploitation of textualism in international law, enabling maneuver space for OCO, and leveraging military use of force to subsume complaints of cyberspace breaches of sovereignty. While textualism and imprecise analogs between physical and cyberwar may be the problem, implicitly adapting those definitions to include cyberattacks is a detrimental solution. Instead, allowing an effects-based determination of legal terms such as armed attack and armed conflict from cyberattacks enables flexibility in responding with military force. This presents its own set of challenges in the legal sense, but the threat of a legal military response to a cyber operation minimizes the maneuver space that adversaries currently exploit.

Furthermore, the case studies identified a defined baseline for OCO. First, OCO to enable presence and future action. Then, OCO to complicate the legality of a response to a military use of force. Finally, OCO to obscure military and political goals, adjust their opponent's public opinion, and enforce permissive Russian narratives.

Finally, Russia is likely to continue OCO in order to further develop reflexive control methods and structures, due to the low risk of attribution, plausible deniability, low effort and cost, and high reward offered by their successful use. RCT is greatly benefitted by the reach afforded in cyberspace, and the ability to misattribute actions. If

Russia is not already pursuing cyber-enabled reflexive control, it would be to its strategic benefit to do so.

BIBLIOGRAPHY

Baker, Bowen, Ingmar Kanitscheider, Todor Markov, Yi Wu, Glenn Powell, Bob McGrew, and Igor Mordatch. "Emergent Tool Use From Multi-Agent Autocurricula." Paper, last revised February 2020. https://arxiv.org/abs/1909.07528.

Blanchard, Marc-André. "Explanation of Vote on Resolution L.27/Rev1: Developments in the Field of Information and Telecommunications in the Context of International Security." Government of Canada, November 7, 2018. https://www.international.gc.ca/world-monde/international_relations-relations_internationales/un-onu/statements-declarations/2018-11-07-telecommunications.aspx.

Bowen, Andrew S. "Russian Cyber Units." Congressional Research Service, Washington, DC, last updated February 2, 2022. https://crsreports.congress.gov/product/details?prodcode=IF11718.

Burt, Tom. "New Activity from Russian Actor Nobelium." *On the Issues*, November 13, 2021. https://blogs.microsoft.com/on-the-issues/2021/10/24/new-activity-from-russian-actor-nobelium.

CGSC Learning Resource Center. Combined Arms Research Library. E-mail submission. April 18, 2022. Reviewed for grammar, punctuation, and clarity of expression.

Chairman of the Joint Chiefs of Staff. Joint Publication 3-12, *Cyberspace Operations*. Washington, DC: Joint Chiefs of Staff, 2018.

Chankvetadze, Natia, and Ketevan Murusidze. "Re-Examining the Radicalizing Narratives of Georgia's Conflicts." Carnegie Europe, Brussels, Belgium, May 12, 2021. https://carnegieeurope.eu/2021/05/12/re-examining-radicalizing-narratives-of-georgia-s-conflicts-pub-84508.

Chekinov, Colonel S. G., and Lieutenant General S. A. Bogdanov. "A Forecast for Future Wars: Meditations on What They Will Look Like." *Military Thought*, no. 4 (2015).

———. "Initial Periods of War and their Influence on a Country's Preparations for Future War." *Military Thought*, no. 11 (2012).

———. "Military Strategy: A Look into the Future." *Military Thought*, no. 11 (2016).

———. "Nature and Content of a New Generation War." *Military Thought*, no. 10 (2013): 12-23.

———. “Predicting the Nature and Content of Future Wars: Problems and Opinions.” *Military Thought*, no. 10 (2015).

———. “Strategic Deterrence and Russia’s National Security Today.” *Military Thought*, no. 3 (2012): 21-31.

———. “The Art of War in the Early 21st Century: Issues and Opinions.” *Military Thought*, no. 1 (2015).

———. “The Evolution of the Essence and Content of ‘War’ in the 21st Century.” *Military Thought*, no. 1 (2017).

———. “The Influence of the Indirect Approach on the Nature of Modern Warfare.” *Military Thought*, no. 6 (2011).

Chotikul, Diane. “The Soviet Theory of Reflexive Control in Historical and Psychocultural Perspective.” Technical Report, Naval Postgraduate School, July 1986. https://apps.dtic.mil/sti/citations/ADA170613.

Cyber Security Situational Centre, The Security Service of Ukraine (SSU). *Gamaredon/Armageddon Group*. Kyiv, Ukraine: SSU, 2021.

Department of Defense (DoD). *Summary: Department of Defense Cyber Strategy.* Washington, DC: DoD, 2018. https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/cyber_strategy_final.pdf.

Douhet, Giulio. *The Command of the Air*. Eastford, CT: Martino Fine Books, 1921.

Dunlap, Charlie. “International Law and Cyber Ops: Q & A with Mike Schmitt about the Status of Tallinn 3.0.” *Lawfire*, October 3, 2021. https://sites.duke.edu/lawfire/2021/10/03/international-law-and-cyber-ops-q-a-with-mike-schmitt-about-the-status-of-tallinn-3-0.

Fox, Amos C. “Hybrid Warfare: The 21st Century Russian Way of Warfare.” Monograph, School of Advanced Military Studies, U.S. Army Command and General Staff College, 2017. https://apps.dtic.mil/sti/pdfs/AD1038987.pdf.

Giles, Keir. *Handbook on Russian Information Warfare*. Fellowship Monograph. Rome: NATO Defense College, Research Division, November 2016.

Giles, Keir, James Sherr, and Anthony Seaboyer. “Russian Reflexive Control.” Royal Military College of Canada, Kingston, Ontario, October 2018.

Guterres, Antonio. “Remarks to the General Assembly on the Secretary-General’s Priorities for 2020 (As Delivered).” Transcript, United Nations, January 22, 2020. https://www.un.org/sg/en/content/sg/speeches/2020-01-22/remarks-general-assembly-priorities-for-2020.

Hollis, David. “Cyberwar Case Study: Georgia 2008.” *Small Wars Journal* (January 6, 2011). https://smallwarsjournal.com/jrnl/art/cyberwar-case-study-georgia-2008.

International Committee of the Red Cross (ICRC). *Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I).* Geneva, Switzerland: ICRC Headquarters, June 8, 1977. https://www.refworld.org/docid/3ae6b36b4.html.

———. *Solferino and the International Committee of the Red Cross: Background, Facts and Figures.* Geneva, Switzerland: ICRC Headquarters, January 6, 2010. https://www.icrc.org/en/doc/resources/documents/feature/2010/solferino-feature-240609.htm.

———. “Special Series: Avoiding Civilian Harm During Military Cyber Operations.” *Law and Policy* (blog). Blog. *International Committee of the Red Cross*, June 15, 2021. https://blogs.icrc.org/law-and-policy/category/special-themes/avoiding-civilian-harm-during-military-cyber-operations.

———. *Study on Customary International Humanitarian Law*. Geneva: ICRC Headquarters, August 15, 2005. https://www.icrc.org/en/doc/resources/documents/misc/customary-law-q-and-a-150805.htm.

Kasza, Anthony, and Doninik Reichel. “The Gamaredon Group Toolset Evolution.” Unit 42. Last updated February 27, 2017. https://unit42.paloaltonetworks.com/unit-42-title-gamaredon-group-toolset-evolution.

Lawson, Ewan, and Kubo Macak. *Avoiding Civilian Harm From Military Cyber Operations During Armed Conflicts*. ICRC Expert Meeting. Geneva, Switzerland: ICRC, January 21-22, 2020. https://shop.icrc.org/download/ebook?sku=4539/002-ebook.

Lee, Robert, Michael Assante, and Tim Conway. *Analysis of the Cyber Attack on the Ukrainian Power Grid*. Washington, D.C.: Electricity Information Sharing and Analysis Center, March 18, 2016.

Lefebvre, Vladimir, and Victorina Lefebvre. *Reflexive Control: The Soviet Concept of Influencing an Adversary’s Decision Making Process*. Englewood, CO: Science Applications Inc., 1984.

Mazarr, Michael. “Mastering the Gray Zone, Understanding a Changing Era of Conflict.” Monograph, U.S. Army War College, 2015. https://press.armywarcollege.edu/monographs/428.

McCroskey, Erick D. “Decision Space Operations: Campaign Design Aimed at an Adversary’s Decision Making.” Monograph, School of Advanced Military Studies, U.S. Army Command and General Staff College, 2003.

Miles, Mark, and Charles Miller. “Global Risks and Opportunities - The Great Power Competition Paradigm.” *Joint Force Quarterly* 94 (3rd Quarter): 80-85. https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-94/jfq-94_86-91_Miles-Miller.pdf.

The MITRE Corporation. “Enterprise tactics.” ATT&CK. Accessed April 1, 2022. https://attack.mitre.org/tactics/enterprise.

North Atlantic Treaty Organization (NATO). *Bucharest Summit Declaration*. Bucharest, Romania: NATO, April 3, 2008. Accessed May 5, 2022. https://www.nato.int/cps/en/natolive/official_texts_8443.htm.

NATO Cooperative Cyber Defence Centre of Excellence. “A Surprising Turn of Events: UN Creates Two Working Groups on Cyberspace.” *INCYDER*, March 11, 2019. https://ccdcoe.org/incyder-articles/a-surprising-turn-of-events-un-creates-two-working-groups-on-cyberspace.

———. “The Tallinn Manual.” Research. Accessed May 6, 2022. https://ccdcoe.org/research/tallinn-manual.

———. “Ukraine Parliamentary Election Interference (2014).” International Cyber Law in Practice: Interactive Toolkit. Last updated March 26, 2019. https://cyberlaw.ccdcoe.org/wiki/Ukrainian_parliamentary_election_interference_(2014).

Office for Democratic Institutions and Human Rights. *Ukraine - Early Presidential Election 25 May 2014 - OSCE/ODIHR Election Observation Mission Final Report*. Warsaw: Organization for Security and Cooperation in Europe, May 24, 2014.

Popescu, Nicu, and Stanislav Secrieru, eds. “Hacks, Leaks and Disruptions: Russian Cyber Strategies.” Chaillot Paper No. 148, European Union Institute for Security Studies, Paris, France, October 2018. https://www.iss.europa.eu/sites/default/files/EUISSFiles/CP_148.pdf.

Posard, Marek, Marta Kepe, Hilary Reininger, James Marrone, Todd Helmus, and Jordan Reimer. *From Consensus to Conflict: Understanding Foreign Measures Targeting U.S. Elections*. Santa Monica, CA: RAND Corporation, 2020. https://www.rand.org/pubs/research_reports/RRA704-1.html.

Russian Federation. Notification to the Governments of the States Parties to the Geneva Conventions of 12 August 1949 for the Protection of War Victims. Geneva: International Committee of the Red Cross Headquarters, October 30, 2019. https://www.dfae.admin.ch/dam/eda/fr/documents/aussenpolitik/voelkerrecht/genevenotifications/191030-GENEVE_e.pdf.

Schmitt, Michael N. “Taming the Lawless Void: Tracking the Evolution of International Law Rules for Cyberspace.” *Chicago Journal of International Law* 3, no. 3 (Summer 2020): 32-47. https://tnsr.org/2020/07/taming-the-lawless-void-tracking-the-evolution-of-international-law-rules-for-cyberspace.

———. “‘Virtual’ Disenfranchisement: Cyber Election Meddling in the Grey Zones of International Law.” *Chicago Journal of International Law* 19, no. 1 (August 16, 2018). https://chicagounbound.uchicago.edu/cjil/vol19/iss1/2.

Schmitt, Michael N., ed. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. 2nd ed. New York: Cambridge University Press, 2017.

Scott Brady. *United States v. Yuriy Sergeyevich Andrienko, et al.* U.S. District Court, Western District of Pennsylvania, 2020.

Smith, Brad. “The Need for a Digital Geneva Convention at the RSA Conference (As Delivered).” Transcript of Keynote Address at the RSA Conference, San Francisco, CA, February 14, 2017. https://blogs.microsoft.com/wp-content/uploads/2017/03/Transcript-of-Brad-Smiths-Keynote-Address-at-the-RSA-Conference-2017.pdf.

Snegovaya, Maria. *Putin’s Information Warfare in Ukraine: Soviet Origins of Russia’s Hybrid Warfare*. Russia Report 1. Washington, DC: Institute for the Study of War, September 2015.

Thomas, Timothy. *The Chekinov-Bogdanov Commentaries of 2010-2017: What Did They Teach Us About Russia’s New Way of War*. Technical Report, The MITRE Corporation, McLean, VA, November 1, 2020. https://apps.dtic.mil/sti/citations/AD1141587.

———. “Information Security Thinking: A Comparison of U.S., Russian, and Chinese Concepts.” Foreign Military Studies Office, Fort Leavenworth, KS, July 2001. https://community.apan.org/wg/tradoc-g2/fmso/m/fmso-monographs/240293.

———. *Recasting the Red Star: Russia Forges Tradition and Technology Through Toughness*. Fort Leavenworth, KS: Foreign Military Studies Office, 2011. https://community.apan.org/wg/tradoc-g2/fmso/m/fmso-books/195632.

———. “Russian Military Thought: Concepts and Elements.” Technical Paper, The MITRE Corporation, McLean, VA, August 2019. https://www.mitre.org/publications/technical-papers/russian-military-thought-concepts-and-elements.

———. “Russia’s Reflexive Control Theory and the Military.” *The Journal of Slavic Military Studies* 17, no. 2 (June 2004): 237-256. https://www.rit.edu/~w-cmmc/literature/Thomas_2004.pdf.

Ukrainian Election Task Force. *Foreign Interference in Ukraine's Democracy*. Washington, DC: The Atlantic Council, May 2019. https://www.atlanticcouncil.org/in-depth-research-reports/report/foreign-interference-in-ukraine-s-election.

Unit 42. "Russia's Gamaredon AKA Primitive Bear APT Group Actively Targeting Ukraine." PaloAltoNetworks. Last updated February 16, 2022. https://unit42.paloaltonetworks.com/gamaredon-primitive-bear-ukraine-update-2021.

United Nations (UN). *Charter of the United Nations and Statute of the International Court of Justice.* San Francisco, CA, June 26, 1945.https://www.un.org/en/about-us/un-charter/full-text.

———. *Statute of the International Court of Justice.* International Court of Justice, 1945. https://legal.un.org/avl/pdf/ha/sicj/icj_statute_e.pdf.

United Nations General Assembly. *Advancing Responsible State Behaviour in Cyberspace in the Context of International Security.* New York, NY: UN, October 10, 2018. https://undocs.org/A/C.1/73/L.37.

———. *Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security*. New York, NY: UN, July 14, 2021. https://undocs.org/A/76/135.

———. *Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security*. Final Substantive Report. New York, NY: UN, March 10, 2021. https://undocs.org/A/75/816.

———. *Report of the International Law Commission*. New York, NY: UN, 2001. https://legal.un.org/ilc/texts/instruments/english/commentaries/9_6_1996.pdf.

U.S. Army Training and Doctrine Command (TRADOC). TRADOC Pamphlet 525-3-1, *The U.S. Army in Multi-Domain Operations 2028*. Fort Eustis, VA: TRADOC, 2021.

US Congress. Senate. *Hearing to Review Testimony on United States Special Operations Command and United States Cyber Command in Review of the Defense Authorization Request for Fiscal Year 2020 and the Future Years Defense Program*. Washington, DC: Committee on Armed Services, February 14, 2019. https://www.armed-services.senate.gov/hearings/19-02-14-united-states-special-operations-command-and-united-states-cyber-command.

———. Putin's Asymmetric Assault on Democracy in Russia and Europe: Implications for U.S. National Security. A Minority Staff Report Prepared for the use of the Committee on Foreign Relations, 115th Cong., 2nd sess. January 10, 2018. S Prt.

115-21. Washington, DC: U.S. Government Publishing Office, 2018. https://www.foreign.senate.gov/imo/media/doc/FinalRR.pdf.

———. *Russian Active Measures Campaigns and Interference in the 2016 U.S. Election*. Vol. 1, *Russian Efforts against Election Infrastructure with Additional Views*. 116th Cong., 1st sess. Report 116-XX. Washington, DC: Select Committee on Intelligence, 116th Congress. http://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume1.pdf.

U.S. President. *Interim National Security Strategy of the United States of America*. Washington, DC: Executive Office of the President, March 2021. https://www.whitehouse.gov/wp-content/uploads/2021/03/NSC-1v2.pdf.

Vasara, Antti. "Theory of Reflexive Control: Origins, Evolution and Application in the Framework of Contemporary Russian Military Strategy." National Defence University, 2020. https://www.doria.fi/handle/10024/176978.

Yin, Robert K. *Case Study Research and Applications: Design and Methods*. 6th ed. Los Angeles: SAGE, 2018.