1s and 0s, A Part of War's Equation

A Monograph

by

Major Nathan Folgert
US Army

School of Advanced Military Studies
US Army Command and General Staff College
Fort Leavenworth, KS

2020

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From-To)*
21-05-2020	Master's Thesis	JUN 2019-MAY 2020

4. TITLE AND SUBTITLE
1s and 0s, A Part of War's Equation

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
MAJ Nathan Folgert

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: ATXL-SWD-GD
Fort Leavenworth, Kansas 66027-2301

8. PERFORMING ORG REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)
Advanced Military Studies Program

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.
1s and 0s, A Part of War's Equation, by MAJ Nathan Folgert, US Army, 56 pages.

In 1965 two researchers connected computers over telephone lines, giving birth to the internet and ultimately cyberspace. Since its conception cyberspace has become fundamental to the American way of life and has progressively asserted itself into warfare. This reliance on cyberspace in everyday life and military technology provides opportunities for exploitation. Adversaries, such as Russia, play an active role in the development of cyber warfare theories and their application in conflicts around the world. The US military struggles to integrate cyber warfare into conventional military operations while Russia employs it within its information warfare branch. The rapidity of change within cyberspace requires that the US military develop and employ cyber warfare within its doctrine, or risk losing its asymmetric advantage over adversaries.

This monograph focuses on this problem by analyzing incidents of cyber warfare and contributing factors. Because computers are becoming an increasingly important part of everyday life, they will achieve an increasing role in warfare moving forward. The analyzed cases demonstrate the evolution of cyber warfare and its increasing integration into military operations. The ability to look at historical cases, identify the forward evolutional trends, and adopt them is critical to maintaining relevancy and advantage in the world. .

15. SUBJECT TERMS
Cyber warfare

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
					MAJ Nathan Folgert
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			**19b. PHONE NUMBER** *(include area code)*
(U)	(U)	(U)	(U)	63	906-235-8570

Monograph Approval Page

Name of Candidate: MAJ Nathan Folgert
Monograph Title: 1s and 0s, A Part of War's Equation

Approved by:

_____, Monograph Director
Adam B. Lowther, PhD

_____, Seminar Leader
Aimee S. DeJarnette, COL

_____, Director, School of Advanced Military Studies
Brian A. Payne, COL

Accepted this 21st day of May 2020 by:

_____, Acting Director, Office of Degree Programs
Prisco R. Hernandez, PhD

Abstract

1s and 0s, A Part of War's Equation, by MAJ Nathan Folgert, US Army, 56 pages.

In 1965 two researchers connected computers over telephone lines, giving birth to the internet and ultimately cyberspace. Since its conception cyberspace has become fundamental to the American way of life and has progressively asserted itself into warfare. This reliance on cyberspace in everyday life and military technology provides opportunities for exploitation. Adversaries, such as Russia, play an active role in the development of cyber warfare theories and their application in conflicts around the world. The US military struggles to integrate cyber warfare into conventional military operations while Russia employs it within its information warfare branch. The rapidity of change within cyberspace requires that the US military develop and employ cyber warfare within its doctrine, or risk losing its asymmetric advantage over adversaries.

This monograph focuses on this problem by analyzing incidents of cyber warfare and contributing factors. Because computers are becoming an increasingly important part of everyday life, they will achieve an increasing role in warfare moving forward. The analyzed cases demonstrate the evolution of cyber warfare and its increasing integration into military operations. The ability to look at historical cases, identify the forward evolutional trends, and adopt them is critical to maintaining relevancy and advantage in the world.

Contents

Abbreviations

ARPA	Advanced Research Projects Agency
ARPANET	ARPA Network
CERT	Computer Emergency Response Team
CTC	Combat Training Center
DCO	Defensive Cyber Operations
DDoS	Distributed Denial of Services
DoD	Department of Defense
EMS	Electromagnetic Spectrum
FNC	Federal Network Council
FM	Field Manual
FSB	Federal Security Service (Russia)
GPS	Global Positioning System
GRU	Main Intelligence Directorate (Russia)
IAEA	International Atomic Energy Agency
IT	Information Technology
IW	Information Warfare
IXP	Internet Exchange Point
MIT	Massachusetts Institute of Technology
NATO	North Atlantic Treaty Organization
PLC	Programmable Logic Controller
OCO	Offensive Cyber Operations
OODA	Observe, Orient, Decide, Act
SCADA	Supervisory Control and Data Acquisition
SDC	Systems Development Corporation

SVR	Foreign Intelligence Service (Russia)
US	United States

Introduction

In 1965, two researchers, Lawrence Roberts from the Massachusetts Institute of Technology (MIT) and Thomas Merrill from the Systems Development Corporation (SDC), used low-speed dial-up Western Union telephone lines to connect computers in California and Massachusetts.[1] This connection experiment is the first recorded wide-area computer network, which paved the way for the modern internet.[2] The event generated national interest in connecting computers to share information. This interest then led to the creation of the Advanced Research Projects Agency (ARPA) network (ARPANET) and ultimately to the internet as we know it today.[3] Roberts and Merrill could not foresee the evolutionary direction their achievement would take in becoming the internet. The internet, within the theory of warfare and warfare itself, continues to evolve as it struggles to find its niche.

The term cyberspace was originally coined as a phrase to describe the virtual world behind computer screens by fiction novelist, William Gibson, in his 1984 book *Neuromancer*.[4] Cyberwar, as a concept, was first discussed in 1993 as the internet took hold and became mainstream.[5] Cyberspace, recognized as a domain in 2011 by the US Army, came into being in conjunction with the advent of the internet.[6] Just as the air domain and airpower existed before

---

[1] Barry M. Leiner et al., "Brief History of the Internet," *Internet Society*, last modified 1997, accessed September 17, 2019, https://www.internetsociety.org/internet/history-internet/brief-history-internet/; Giovanni Navarria, "How the Internet Was Born: The ARPANET Comes to Life," *The Conversation*, accessed February 25, 2020, http://theconversation.com/how-the-internet-was-born-the-arpanet-comes-to-life-68062.

[2] Leiner et al., "Brief History of the Internet."

[3] Ibid.

[4] John Naughton, "The Evolution of the Internet: From Military Experiment to General Purpose Technology," *Journal of Cyber Policy* 1, no. 1 (May 8, 2016): 12–13.

[5] Kim Zetter, *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon*, First Edition. (New York: Crown Publishers, 2014), 205.

[6] Headquarters, Department of the Army, *Army Doctrine Publication (ADP) 3-0, Operations* (Washington DC: Government Printing Office, 2019), 1–6; Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, *Defense Science Board Task Force on Cyber Deterrence* (Department of Defense, February 2017), 3.; Zetter, *Countdown to Zero Day*, 215; US Department of

the First World War's inaugural air combat, cyberspace existed before being officially defined by a governmental organization as a warfighting domain or used in any major conflict.

The cyberspace domain is manmade, depending entirely on technologies and physical infrastructure created and used by humans, whereas the other recognized warfighting domains are physical and immutable.[7] Various authors make different cases as to the exact time and place of origin, but this paper recognizes the establishment of this domain concurrent with the creation of ARPANET in the late 1960s.[8] Both nation-state and non-state actors have increased their presence and activity within this domain at an ever-escalating rate and are increasingly using it for hostile intent. Cyberspace, like aircraft, will shape the future, and its use in warfare changes battlefields, but it is incapable of producing victory on its own, as with airpower.[9]

American society and the Department of Defense, since the creation of ARPANET, interweave cyber into all functions and capabilities at an exponentially increasing rate. The pace of interconnectedness is commensurate with technological innovations, providing opportunities for cyber-savvy adversaries in future conflicts. Opportunities take the form of, but are not limited to, vulnerabilities in code, overreliance on equipment or technology, and the creative uses of emerging technologies to bridge capability gaps. War will inevitably reflect the characteristics of the participating societies, so the greater the technological dependence today, the greater the role

---

Defense, *The Department of Defense Cyber Strategy* (Washington DC: Government Printing Office, 2015), 4.

[7] P. W. Singer, *Cybersecurity and Cyberwar: What Everyone Needs to Know* (Oxford ; New York: Oxford University Press, 2014), 13–14; Lior Tabansky, "The Current State of Cyber Warfare," *Cyber Security Review*, last modified May 2015, accessed December 19, 2019, https://www.cybersecurity-review.com/articles/the-current-state-of-cyber-warfare/.

[8] Leiner et al., "Brief History of the Internet."

[9] Kenneth Geers, ed., *Cyber War in Perspective: Russian Aggression against Ukraine* (Tallinn, Estonia: NATO Cooperative Cyber Defence Centre of Excellence, 2015), 46.

of cyber in war tomorrow.[10] The 2018 *National Cyber Strategy* recognizes and illustrates this concept:

> For the past quarter-century, the ingenuity of the American people drove the evolution of cyberspace, and in turn, cyberspace has become fundamental to American wealth creation and innovation. Cyberspace is an inseparable component of America's financial, social, government, and political life…They view cyberspace as an arena where the United States' overwhelming military, economic, and political power could, and where the United States and its allies and partners are vulnerable.[11]

Russia, one of the leading actors in cyberspace and one of the top three most capable cyber nations is developing and testing a holistic cyber warfare doctrine that integrates cyber capabilities with other service components.[12] The Russian Federation demonstrated this capability to the world in Georgia in 2008 and Ukraine in 2014 by coordinating cyber-attacks with military attacks and deploying ground forces to secure cyber-isolated objectives. The former is an instance of cyber attacks coordinated with military attacks. The latter is an instance of cyber warfare cutting off a target from communicating its predicament to the outside world while seizing it with military troops. There is no precedent for this combined warfare approach in the pursuit of national objectives, bringing about an unprecedented innovation to the world of cyber warfare. Russia is also a country with a diametric theory of cyber warfare compared to that of the Western world, particularly the US, which views cyber as a distinct domain.[13]

Russia's theory, within its military, places cyber capabilities subordinate to its information warfare branch. The overarching goal of this branch is to influence an adversary's

---

[10] Jarno Limnéll and The Society of Digital Information and Wireless Communication, "The Exploitation of Cyber Domain as Part of Warfare: Russo-Ukrainian War," *International Journal of Cyber-Security and Digital Forensics* 4, no. 4 (2015): 521.

[11] Office of the President of the United States, *National Cyber Strategy 2018* (Washington, DC: The White House, 2018), 1.

[12] Michael Connell and Sarah Vogler, "Russia's Approach to Cyber Warfare" (CNA, March 2017), i, accessed December 17, 2019 https://www.cna.org/cna_files/pdf/DOP-2016-U-014231-1Rev.pdf; Limnéll and The Society of Digital Information and Wireless Communication, "The Exploitation of Cyber Domain as Part of Warfare," 525.

[13] Connell and Vogler, "Russia's Approach to Cyber Warfare," 4–5.

public behavior, its strategic decision making, and risk calculations.[14] This approach prioritizes influencing an opponent's decision making processes over achieving physical destruction through a cyberattack. This divergent cyber warfare theory, the active use of cyber warfare in the last decade, and the existing US-Russia great power competition is the reason for Russia's central role in this paper.

The US military currently struggles with the complications of coordinating and integrating cyber warfare into military operations. It is used more as a strategic capability and a means of national power rather than an operational or tactical approach to large-scale conflict. While cyber warfare is seeing limited use around the world today, it remains an emerging capability that is not yet fully integrated into military doctrine. As with all emergent warfare capabilities, cyber warfare's integration into operations at all levels is the key to creating an asymmetric advantage in large scale conflict.[15] Small scale conflicts provide nations a venue to validate their theories and emerging doctrine, as with Russia's employment of cyber warfare in Georgia and Ukraine.[16]

James Corum, a professor of military history at various institutions, notes that air doctrine changes more than any other military doctrine due to its dependence on technological factors.[17] This claim is even more applicable to cyber warfare, which relies on technology to an even greater degree. Based on the use of cyber warfare in recent small scale conflicts, a war which fully integrates cyber is certain to exceed anticipated implications.[18]

---

[14] Blagovest Tashev, Michael Purcell, and Brian McLaughlin, "Russia's Information Warfare: Exploring the Cognitive Dimension," *MCU Journal* 10, no. 2 (December 10, 2019): 133–134.

[15] Limnéll and The Society of Digital Information and Wireless Communication, "The Exploitation of Cyber Domain as Part of Warfare," 523.

[16] Timothy J. Williams, "Cyberwarfare and Operational Art" (Monograph, School of Advanced Military Studies, US Army Command and General Staff College, 2017), 22–35.

[17] James S. Corum, *The Luftwaffe: Creating the Operational Air War, 1918-1940*, Modern war studies (Lawrence: University Press of Kansas, 1997), 72.

[18] Qiao Liang and Wang Xiangsui, *Unrestricted Warfare* (Beijing: PLA Literature and Arts Publishing House, 1999), 43.

The United States needs to develop an effective cyber warfare approach and integrate it into doctrine to maintain an asymmetric advantage over its adversaries. Military leaders contribute to this endeavor by discussing multiple emerging concepts of cyber warfare to identify and capitalize on asymmetric advantages before the next major conflict. Such discussion facilitates preparation for cyber warfare in future large-scale conflict through the development of staunch cyber warfare doctrine that is capable of surviving the initial onset of hostilities while remaining flexible enough to adapt and seize the initiative in the new emerging environment.[19] Consequently, this paper will answer the research question: How can the United States gain an asymmetric advantage in its next large-scale conflict through the employment of cyber warfare?

[19] Carl von Clausewitz, Michael Eliot Howard, and Peter Paret. *On War*. (Princeton, NJ: Princeton University Press, 1989), 95–100.

Methodology

This paper utilizes Alexander George's structured, focused comparison case study framework to answer the research question. Alexander George was a behavioral scientist and political science professor at Stanford University who focused on nuclear studies and their political connections during the Cold War. This methodology derives structure from reflection on the research objective through questions asked of each case study.[20] It achieves focus through limiting the cases to specific aspects of the case studies that answer the questions.[21] This structure and focus allow for analysis of varied cases as they pertain to the initial research question.

This method provides for an overview of the cases to provide context and a situational understanding before it begins to focus in on answering a set of questions. The structure comes through this method's employment of a set of questions answered by each case to address the research question. This paper evaluates each case according to these questions and attempts to draw out the variables and their empirical relationships.

Research focuses on analyzing current and past doctrine, policy, and history to answer the proposed research question through Alexander George's method. Each case study is analyzed only insofar as is required to answer these questions, giving it the necessary focus. The final answer to the thesis comes through comparing the results of each case study, one question at a time, to analyze and compare the results to identify congruence and divergence. The summary of this analysis and comparison forms the basis for recommendations.

Each case begins with an account of the case's story to provide context and set the stage for the analysis to follow. Then, the paper analyzes each case according to the questions set forth. Each question is asked and analyzed with the available information for each case study. Finally, each case study concludes with a summary overview and discussion as relates the value of the

[20] Alexander L. George and Andrew Bennett, "Case Studies and Theory Development in the Social Sciences," *Perspectives on Politics* (n.d.): 67.

[21] Ibid.

particular case to the hypothesis. The conclusion section then summarizes, by hypothesis and value to the research question, each case's analysis for the comparative results.

With the advent of the global internet, as named and defined by the Federal Network Council (FNC) in 1995, a new field of competition emerged within the world of warfare.[22] The United States initially dominated this field as American corporations owned much of the backbone infrastructure supporting the nascent internet.[23] Cyber activities have expanded from the initial incidents of the 1980s and 1990s to the more complex activities of the last 15 years. Cyber warfare began with espionage such as the Cuckoo's Egg (1986), Moonlight Maze (1998), Solar Sunrise (1998) and Buckshot Yankee (2008). Cyber warfare expanded to include deliberate war-like actions such as in the attacks on Estonia 2007, the Russo-Georgia war of 2008, Stuxnet (2010) and the on-going Ukraine conflict (2014-present).[24] Given this global environment of increasing cyber activity, it is doubtful that the US will face a future conflict that does not involve the use of cyber warfare. This condition leaves the US military with the prospects of simultaneously fighting a war in multiple domains, crossing domains, and in ways that defy traditional concepts of boundaries.

To better understand how to achieve an asymmetric advantage under these conditions, this paper examines the use of cyber warfare in four cases and asks the questions: How were cyber attacks employed to achieve political objectives or enable military operations? What kind of staffing structure facilitated the use of cyber to ensure collaboration rather than combativeness? What was the civil-military cyber relationship, and how it supported the use of cyber attacks? How well did military leaders understand both cyber and its role and effects in the operations within which they participated? What lessons did actors glean from their experiences?

---

[22] Leiner et al., "Brief History of the Internet."

[23] Naughton, "The Evolution of the Internet: From Military Experiment to General Purpose Technology," 12.

[24] Omry Haizler, "The United States' Cyber Warfare History Implications on.Pdf," *32Cyber, Intelligence, and Security* 1, no. 1 (January 2017): 32–34.

Case Selection

Selected cases met four criteria and had adequate research materials available. These criteria are:

1. Cyber activities must either achieve physical damage or appear in conjunction with military operations.
2. It must not be for espionage alone.
3. It cannot be merely criminal activities but must advance a larger purpose.
4. These activities must originate with a nation-state or other actor capable of fielding a military force.

Stuxnet, Outside the Box/Orchard, Russo-Georgia war and the Ukraine conflict were selected for study for various reasons. The first and most important criteria stipulated that cyber activities achieved physical damage as part of a strategy or were conducted in conjunction with military operations in the other domains. This criterion eliminated a large number of cyber incidents while leaving room for many other incidents meeting this criterion through effects incidental to the primary aims of the cyber weapon. The second criterion further limited the number of possible cases in eliminating those designed for cyber espionage alone, removing many other inter-governmental incidents. The third criterion further reduced the number of non-governmental cases in stipulating that civilians and corporations were not the primary targets for financial gains, such as identity theft, monetary theft, or ransom. The final criterion provided conditions that the activities originate from, at the behest of, or appear to be coordinated by a nation-state government or similar organization capable of fielding a military force.

Eight separate cases meet the selection criteria established above. The cases begin with the US invasion of Iraq (2003), Aurora generator test (2007), Stuxnet (2010), Outside the Box/Orchard (2007), Russo-Georgia war (2008), US Military dismantling of a Saudi website (2008), the Syrian Civil War (2011-present), and the Ukraine conflict (2014-present). Initial research material availability reduced this and provided a focus for selecting the final cases to analyze. Little information is publically available on the Iraq, Aurora, US dismantling of a Saudi

website, and the Syrian civil war cases. This paper analyzes Stuxnet, Orchard, Russo-Georgia War, and the Ukraine conflict out of the eight plausible cases.

Current US military doctrine, specifically that of unified land operations and large scale combat operations, provided the baseline for describing military operations.[25] These cases, in addition to meeting the selection criteria, most closely resemble such operations and activities for which the US military trains according to this doctrine. The Ukraine conflict provides the most examples of cyber warfare and military cooperation as well as applicable research material available.

Questions:

Five questions asked of each selected case:

1. How were cyber attacks employed to achieve political objectives or enable military operations?
2. What kind of staffing structure facilitated the use of cyber to ensure collaboration rather than combativeness?
3. What was the civil-military cyber relationship, and how did it support the use of cyber attacks?
4. How well did military leaders understand both cyber and its role and effects in the operations within which they participated?
5. What lessons did actors glean from their experiences?

Assumptions and Constraints

The Department of Defense (DoD), and subordinate to it the individual services, doctrines are the primary comparison tool for current US practice. Open source public sources are assumed adequate to convey an accurate picture of current US policy and operations. These sources fit within the constraints of the classified and restricted nature of many cyber warfare related works in existence. The US Navy, for example, classifies its related doctrinal and warfare

[25] Headquarters, Department of the Army, *Field Manual (FM) 3-0, Operations* (Washington DC: Government Printing Office, 2017), ix, 1–16.

related publications. This constraint set conditions for identification of cases, eliminating otherwise good examples due to the overly classified nature of the pertinent information. A major assumption, derived from this constraint, is that this public information is adequate for each case study with enough reliable detail and data to address the research question and hypotheses.

Joint publications identify cyberspace as an interdependent domain alongside the other four traditional domains of air, land, sea, and space.[26] The Army, in its capstone FM 3-0, discusses cyberspace and differentiates the electromagnetic spectrum (EMS) as a domain of increasing contest with proximity to the conflict.[27] The US Air Force agrees that cyberspace is a separate domain, setting the requirement of cyberspace freedom of action for any mission, which is interconnected with all other domains and links them through the effects they can produce.[28] The same USAF cyberspace operations manual goes on to discuss the inherent difficulties associated with cyberattack attribution, something this paper does not delve into. This research focuses on conflict-associated cyber activities consistent with nation-state activities and assumes they are so sanctioned, to avoid the issue of attribution.

Joint doctrine discusses the interrelated nature of information and cyberspace to usurp an adversary's decision-making cycle, yet acknowledges them as separate because cyberspace operations may achieve non-information operation related objectives.[29] The Air Force acknowledges by stating that "in modern warfare, all domains are interconnected via cyberspace operations."[30] This view is Western and acknowledged as opposed to some Eastern views such as

---

[26] US Department of Defense, Joint Staff, *Joint Publication (JP) 3-12, Cyberspace Operations* (Washington DC: Government Printing Office, 2018), I–2.

[27] Headquarters, Department of the Army, *FM 3-0*, 1–7.

[28] LeMay Center for Doctrine, "Cyberspace Operations," *Annex 3-12 - Cyberspace Operations*, last modified November 30, 2011, accessed December 31, 2019, https://www.doctrine.af.mil/Portals/61/documents/Annex_3-12/3-12-Annex-CYBERSPACE-OPS.pdf.

[29] US Department of Defense, Joint Staff, *JP 3-12*, I–5.

[30] LeMay Center for Doctrine, "Cyberspace Operations," 18.

those of Russia and China, which view cyber as a subordinate of information warfare.[31] This thesis accepts all of this and eschews the discrepancy by assuming that cyberspace, the information environment, and the intertwined domains as a distinct and comprehensive aspect of war.

Delimitations

Cyber warfare has many elements and varying terminology which change with time and within the US and international community. Computer network attacks, offensive and defensive cyber operations, hacking, hacktivist, intrusion, vulnerability, and information assurance are just a few of the terms. This thesis uses a common and consistent language, concurrent with the latest US military doctrine and publications. There are three main categories of cyber activities: crime, espionage, and attack. Cyber activities are judged by the legal framework of an existing conflict, in becoming elements of cyber warfare.[32] This rule means that otherwise classified crime and espionage cyber activities become supporting elements of cyber warfare. The predominant feature in cyber attack, bringing them into cyber warfare, is the offensive nature of the tools used to achieve effects within the conflict or the context of the political aims.

This thesis focuses on cyber attacks as a form of cyber warfare, at the direction or behest of the government, to achieve military or national policy objectives. Cybercrime is typical of an individual or illicit group or organization seeking monetary gain or status recognition, therefore outside the purview of this work. Cyber espionage, while sometimes conducted at the behest of a government, is the theft or absconding of information rather than effects on an adversary. Cybercrime and espionage, in some cases, use overlapping or identical ways and means to achieve their ends; however, it is the actor and intent that distinguish and classify it.

---

[31] Connell and Vogler, "Russia's Approach to Cyber Warfare," 4–5.

[32] Geers, *Cyber War in Perspective*, 124.

Cyber attacks need to demonstrate destruction or use in coordination with military and national policy objectives to be relevant in this study. The cases selected for this thesis were picked based on the amount of research information publically available. Additionally, case selection criteria limited selection to those tied to military operations or those resulting in physical damage and destruction, thereby eliminating several potential cases such as Estonia in 2007. Russia is the most prolific actor that meets these criteria, so for the preservation of this work, distinctness was an added criterion for cases involving Russia.

Case Study Analyses

Stuxnet, 2010

In 2010 Iran's Natanz uranium enrichment plant was replacing centrifuges for its nuclear uranium enrichment program, almost 2,000 in a few months as opposed to the normal 800 a year.[33] The excessive replacement baffled both the Iranians and the International Atomic Energy Agency (IAEA) inspectors who noticed it. By late in the year, several computer security companies uncovered a complex digital code that was spreading throughout the corporate world.[34] A complex code, fifty times larger than the average computer virus, was responsible for this feat.[35] It was finally detected when it spread beyond its intended targets remaining concentrated in systems primarily in Iran.[36]

Because the Iranian uranium enrichment program within Natanz operated on a closed network, not connected to the larger world wide web, hackers needed to find an alternate way to achieve effects. Stuxnet, as it became known, was specifically designed to spread over local area networks via removable media, rather than through emails or internet connections, to target the isolated network.[37] Computer security technicians took several months to reverse-engineer Stuxnet, initially working to stop its spread and identify its source.[38] Technicians from Symantec

[33] Zetter, *Countdown to Zero Day*, 1–3.

[34] David Kushner, "The Real Story Of Stuxnet," *Institute of Electrical and Electronics Engineers (IEEE)Spectrum*, last modified February 23, 2013, accessed November 1, 2019, https://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet.

[35] Kim Zetter, "How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History," *Wired*, July 11, 2011, accessed October 31, 2019, https://www.wired.com/2011/07/how-digital-detectives-deciphered-stuxnet/.

[36] Ibid.

[37] Ibid.

[38] Kushner, "The Real Story Of Stuxnet."

ultimately named the virus Stuxnet from a text file written into its code but remained unable to determine the weapon's developer beyond doubt and yet suspecting US and Israel.[39]

Stuxnet used four zero-day exploits to spread between systems, identify required conditions, and access the supervisory control and data acquisition (SCADA) program to influence Programmable Logic Controller (PLC) of specific hardware to damage it beyond repair.[40] This code was the first time, outside of theory and strictly controlled experiments, that a string of digital coding directly damaged equipment existing in the physical domain, a cyber weapon, digital weapon striking a physical target.[41] Iran does not publically admit the extent of damage to its uranium enrichment program; however, the estimates average out to a two-year setback.[42]

Stuxnet was the first instance of a cyber tool producing physical damage and being targeted against an adversary, classifying it as a weapon.[43] This creation of a cyber weapon designed specifically to produce damage took the cyber world by storm despite limited proof of concept testing, writings, and even Hollywood movie productions hinting at similar possibilities.[44]

---

[39] William J. Broad, John Markoff, and David E. Sanger, "Israeli Test on Worm Called Crucial in Iran Nuclear Delay," *New York Times*, last modified January 15, 2011, accessed November 1, 2019, https://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html.

[40] Zetter, "How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History"; Kushner, "The Real Story Of Stuxnet."

[41] Shane Harris, *@WAR: The Rise of the Military-Internet Complex* (Boston: Houghton Mifflin Harcourt, 2014), 11; Zetter, *Countdown to Zero Day*, 3.

[42] Broad, Markoff, and Sanger, "Israeli Test on Worm Called Crucial in Iran Nuclear Delay."

[43] Michael P Carvelli, "A Smarter Approach to Cyber Attack Authorities," *Joint Force Quarterly* 4th Quarter 2018, no. 91 (2018): 69.

[44] Michael Swearingen et al., "What You Need to Know (and Don't) About the AURORA Vulnerability," *Power: Business & Technology for the Golbal Generation Industry Since 1882*, last modified September 1, 2013, accessed November 19, 2019, https://www.powermag.com/what-you-need-to-know-and-dont-about-the-aurora-vulnerability/?printmode=1.

How were cyber attacks employed to achieve political objectives or enable military operations?

The presumed intent of this weapon was to delay the Iranian nuclear program without starting a war. Intent presumption results from the lack of any government or organization assuming responsibility or credit for this cyber-attack. Software engineers, to achieve this goal, developed a worm that would damage equipment without causing loss of life.[45] Such a precise and non-lethal option provides national decision-makers with a tempting option that avoids the repercussions of applying military force.

This weapon achieved a goal, destruction of Iranian centrifuges, without the involvement of any military forces.[46] Using this cyber attack mitigated two of the major risks any politician faces when deciding to attack an adversary; risk to soldier's lives and risk to policy. This cyber-attack avoided putting troops or military equipment in the line of fire as a conventional attack requires, This option also reduced risk to policy by providing plausible deniability to the government, because of the difficulty of attribution.

What kind of staffing structure facilitated the use of cyber to ensure collaboration rather than combativeness?

Stuxnet provides an example of an extremely complex computer worm that incorporated multiple vulnerabilities to cross multiple academic disciplines to achieve destructive results in the real world. Stuxnet, compared in parallel to conventional military parlance, is the epitome of the US Army's emerging multi-domain operations and concept of convergence.[47] Conventional military operations at all levels require large staffs working together to synchronize capabilities and produce effects on enemy targets. Cyber warfare, as demonstrated in the complexity of Stuxnet, is no different.

---

[45] Zetter, *Countdown to Zero Day*, 366–370.

[46] Tabansky, "The Current State of Cyber Warfare."

[47] Headquarters, Department of the Army, *TRADOC Pamphlet 525-3-1: The U.S. Army in Multi-Domain Operations 2028* (Washington DC: Government Printing Office, December 6, 2018), iii, viii–x.

Deconstruction of this particular cyber weapon, to reveal its purpose and target, required nearly a year and a large number of computer security experts around the world.[48] This particular cyber attack required knowledge of SCADA and PLC programs, uranium refinement technical knowledge, familiarity with the hardware involved and fluency in any of the proprietary software coding languages used throughout the entire process. This easily covers the disciplines of computer science, nuclear science, electrical engineering, and the electromagnetic spectrum, amongst others.

Creating such a cyber weapon, with its deliberate targeting and processes to minimize collateral damage and risk of detection, requires a large and well-integrated staff. To reduce risk to a level acceptable for decision-makers requires that the staff possesses the expertise to fulfill each of these discipline's functions and even test the weapon in a controlled environment. Stuxnet, still a disavowed operation, could only have succeeded with this level of support and a significant amount of time for developing and testing. United States military staff structures cannot currently support this. They need to be adjusted to integrate and synchronize cyber capabilities with effects and targets through time, space, and purpose

What was the civil-military cyber relationship, and how did it support the use of cyber attacks?

There is no proof that any military was involved in the creation of Stuxnet, so government agencies take the place of the military. Stuxnet's discovery is a perfect example of a failure to integrate civilian and military or government agencies and organizations to achieve political ends. The Stuxnet worm was discovered and revealed by an anti-virus corporation, which was focused solely on serving its customers regardless of the intentions of whomever or whatever government created the worm.[49] Beyond Symantec's focus on protecting its customers, Microsoft owned part of the vulnerability and immediately, once notified, took steps to remediate

[48] Zetter, *Countdown to Zero Day*, 3.

[49] Ibid., 5–6, 31–32.

it.[50] The presumption here is that the government agency responsible for Stuxnet did not coordinate with these companies.

This lack of synchronization and integration resulted in a short lifespan for the worm once it inadvertently spread beyond the target computer network. Coordination with Symantec and Microsoft could result in measures to reduce further the visibility of this worm and smoother integration of its processes within affected systems. Coordination between these various entities would enable further refining targeting, constrain direction, and enhance the accuracy and efficiency of the cyberweapon itself. Based on available information, this coordination did not occur and ultimately resulted in its public discovery and reverse-engineering.

How well did military leaders understand both cyber and its role and effects in the operations within which they participated?

Lacking the proof or implication of military involvement, government agencies replace it in the context of this question. Stuxnet's designer and agent are still unknown; however, the method of its discovery supports the conclusion that military leaders require an understanding of cyber warfare, regardless of their concentration or occupational specialty. From international inspectors to anti-virus programmers and large corporations, many players participated in the identification, defeat, and analysis of the Stuxnet worm.[51]

Stuxnet's designers took into account the political situation and risks, deliberately tailoring their worm to avoid propagation into the larger world and to avoid collateral damage. In military parlance, this equates to applying the concepts of proportionality, in the just war

[50] Zetter, *Countdown to Zero Day*, 14, 31–32.

[51] Zetter, "How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History"; Kim Zetter, "An Unprecedented Look at Stuxnet, the World's First Digital Weapon," *Wired*, November 3, 2014, accessed August 2, 2019, https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/.

tradition.[52] The amount of effort applied to build this weapon belays the effort applied to adhere to this tradition and reduce unforeseen consequences, risk, upon discovery.

On Iran's part, it was individuals who did not understand the basics of cybersecurity or adhere to the policies and regulations which contributed to Stuxnet's spread. Leaders who understand weapons systems make better-informed decisions that enhance both protection and effectiveness. This understanding is one of the reasons that the US military employs a robust staff and seeks to incorporate all disciplines into its planning processes. Cyber awareness programs and professional military education are ways to bridge this understanding gap, and simple demonstrations can reduce security lapses such as the Iranians at Natanz experienced.

What lessons did actors glean from their experiences?

Proficiency increases only through practice. Computer experts dissecting Stuxnet employed computer systems set up in isolation of any live network to reverse engineer the worm. It is reasonable to assume that Stuxnet's creators did likewise to ensure the cyber weapon achieved the intended results before firing the weapon, knowing it was a matter of time until the discovery and the vulnerabilities enabling its success remedied. Using an isolated network to test the worm did not prevent its unintentional propagation upon release for execution. Further testing in a controlled but live environment may uncover more of these unintended side effects.

Cyber attacks can result in physical damage and achieve strategic objectives. Stuxnet delayed Iran's uranium enrichment program through deliberate engineering and avoided unnecessary collateral damage. Military force was not required to achieve this objective, adding the benefit of plausible deniability to the use of this cyber attack.

Isolated networks, commonly referred to as air-gapped, are not safe from cyber attacks. The network at the Natanz uranium enrichment plant was isolated from the internet. The term

[52] Brian Orend and Robert M. Martin, *The Morality of War*, Second edition, Second edition expanded and updated, 2/e expanded and updated. (Peterborough, Ontario, Canada; Buffalo, NY, USA: Broadview Press, 2013), 34, 125.

'air-gap' provides a mental visualization of the physical disconnection of one network from another designed to increase network security. Actors bridged this gap using other conventional means to get Stuxnet onto this isolated network.

Summary

This case demonstrates the first effective use of a cyberweapon in public knowledge. This case is a good example of an emerging capability employed in its domain, seemingly ahead of its time, and limited in scale and scope to mitigate collateral damage. This case provides a clear look at the use of a cyber weapon and, with regards to the thesis, provides areas of study to achieve an asymmetric advantage in the next cyberwar salvo. US military failure to professionally discuss and advance this theory remains, to this day, evidenced through limited cyber doctrine and establishment of a major cyber command in 2017.[53] The United States should adjust its training centers to incorporate unrestrained cyber warfare during unit rotations, both to acclimate and educate the units, as well as for testing both offensive and defensive capabilities.

Israeli Operation Outside the Box / Orchard, 2007

On 5 September 2007, just before midnight, eight Israeli F-15s and F-16s crossed the border into Syria to bomb a nuclear reactor and remained undetected throughout the covert strategic bombing mission.[54] Dropping bombs on a target is both the easy part for the military instrument of national power and the final act in a sequence of events and decisions. This operation traced its roots back to 2004 as intelligence, and various Israeli agencies set the stage

[53] Office of U.S. Cyber Command, "U.S. Cyber Command History," *U.S. Cyber Command*, accessed November 19, 2019, https://www.cybercom.mil/About/History/.

[54] Barbara Opall-Rome, "Declassified: How an Israeli Operation Derailed Syria's Nuclear Weapons Drive," *Defense News*, last modified March 21, 2018, accessed October 29, 2019, https://www.defensenews.com/global/mideast-africa/2018/03/20/just-declassified-how-an-israeli-operation-derailed-syrias-nuclear-weapons-drive/; Fred M. Kaplan, *Dark Territory: The Secret History of Cyber War*, First Simon & Schuster hardcover edition. (New York: Simon & Schuster, 2016), 160–162.

for the subsequent application of military power against a potential national threat.[55] The jets used in this attack were not stealth aircraft, so Israel found a different way to hide their presence. This mission incorporated electronic attack jamming, and computer network intrusion to compromise and defeat key Syrian systems allowing aircraft to fly unmolested through Syrian airspace.[56]

The main objective of these Israeli offensive cyber capabilities was to neutralize the Syrian air defense systems manipulating and inserting false data protecting the strike aircraft, thus enabling deniability by the national government afterward.[57] An electronic attack, or jamming, essentially blinds a system but is noticeable to alert, trained, and proficient system operators, as the Syrian air defense radar operators were.[58] Jamming alone was, therefore, not enough as the Israelis needed to keep the Syrians from discovering anything at all until the bombs fell. They achieved this by synchronizing computer network intrusion with the air sorties, compromising the computer control programs, thereby allowing Israeli cyber warriors to manipulate the Syrian air defense network data and hide Israeli aircraft.[59] It is an indisputable fact that Israeli aircraft

[55] Opall-Rome, "Declassified: How an Israeli Operation Derailed Syria's Nuclear Weapons Drive."

[56] Yossi Melman, "OUTSIDE THE BOX: Israel's Strike on Syria's Nuclear Plant," *The Jerusalem Post*, last modified April 6, 2018, accessed October 29, 2019, https://www.jpost.com/Arab-Israeli-Conflict/OUTSIDE-THE-BOX-Israels-strike-on-Syrias-nuclear-plant-547870; David A. Fulghum and Robert Wa, "U.S. Electronic Surveillance Monitored Israeli Attack On Syria," *World Security Network*, last modified February 7, 2014, accessed October 29, 2019, https://web.archive.org/web/20140207060836/http://www.worldsecuritynetwork.com/Israel-Palestine/David-A.-Fulghum-and-Robert-Wall-/U.S.-Electronic-Surveillance-Monitored-Israeli-Attack-On-Syria.

[57] Yaakov Katz, "And They Struck Them with Blindness," *The Jerusalem Post*, last modified September 29, 2010, accessed October 29, 2019, https://www.jpost.com/Magazine/Features/And-they-struck-them-with-blindness; Joseph Trevithick, "Israel Details Long Secret Raid On Syrian Nuclear Reactor, Says It's Willing To Do It Again," *The Drive*, accessed October 30, 2019, https://www.thedrive.com/the-war-zone/19492/israel-details-long-secret-raid-on-syrian-nuclear-reactor-says-its-willing-to-do-it-again.

[58] Richard A. Clarke and Robert K. Knake, *Cyber War: The next Threat to National Security and What to Do about It*, 1st ed. (New York: Ecco, 2010), 5–8.

[59] Ibid., 6–8.

navigated the Syrian skies without air defense systems targeting them, yet Israel maintains the classification on how exactly they achieved this effect.[60]

Syrian President Bashar Assad denied any nuclear-related operations, following the attack.[61] Israel remained quiet, until 2018, about the attack allowing Syria to save face in the political realm.[62] Israel censored its media from reporting on the incident and Syria admitted there had been an attack, without sharing much detail, and only proffered weak protests before returning to silence on the subject.[63] As the dust settled, this operation faded into oblivion.

How were cyber attacks employed to achieve political objectives or enable military operations?

Cyber attacks, in conjunction with other means, rendered Syrian air defense systems ineffective and enabling conventional attack aviation to reach its target.[64] In this case, cyber attacks played a supporting role in a kinetic operation. These Israeli cyber attacks lowered the level of political risk by eliminating the need to strike the Syrian air defense systems kinetically. Shutting down Syrian air defenses also allowed Israeli combat aircraft to traverse the skies freely, bomb their targets, and egress without fear of being shot down.

Cyber attacks gave politicians on both sides the ability to exercise further political diplomacy to resolve the situation, due to the reduced loss of life and overt military action. Loss of either aircraft or the need to deliberately engage Syrian air defense systems would eliminate the political deniability of either Syrian or Israeli activities and could escalate the situation.

---

[60] Judah Ari Gross, "Ending a Decade of Silence, Israel Confirms It Blew up Assad's Nuclear Reactor," *The Times of Israel*, accessed October 30, 2019, https://www.timesofisrael.com/ending-a-decade-of-silence-israel-reveals-it-blew-up-assads-nuclear-reactor/.

[61] Melman, "OUTSIDE THE BOX: Israel's Strike on Syria's Nuclear Plant."

[62] Ibid.

[63] Clarke and Knake, *Cyber War*, 2–3.

[64] George Perkovich and Ariel Levite, eds., *Understanding Cyber Conflict: 14 Analogies* (Washington, DC: Georgetown University Press, 2017), 52.

Silence, from both sides, for the next 10 year confirmed success, until Israel officially recognized the operation in 2018.[65]

What kind of staffing structure facilitated the use of cyber to ensure collaboration rather than combativeness?

Israeli operation Outside The Box / Orchard demonstrated the integration of electronic warfare, cyber within the United States military establishment, and conventional capabilities at the point of attack.[66] Research does not reveal the extent to which Israel compromised the Syrian air defense computer network and, therefore, the effort poured into this cyber attack.[67] Coordinating cyber attacks with combat aviation operations requires deliberate planning and trust on the part of pilots flying past enemy air defense systems. Israeli pilots had limited information before they flew the mission, only a few being privy to the planning outside of a few hours' notice.[68]

These facts imply that senior leadership coordinated the activities of independent agencies and elements of the military to synchronize the timing and placement of effects to achieve the desired effects. This synchronization resulted from national government prioritization and attention, not from systems, processes, procedures, or other frameworks to establish collaboration. This coordination and synchronization was deliberate, planned out, and executed in a compartmentalized fashion. This process works for a strategic military strike but may fall short in war. If such synchronization of cyber warfare and conventional warfare is the desired and continual product, then a revision of command and staffing structures is necessary.

---

[65] Melman, "OUTSIDE THE BOX: Israel's Strike on Syria's Nuclear Plant."

[66] Clarke and Knake, *Cyber War*, 8–9; Kaplan, *Dark Territory*, 160–162.

[67] Opall-Rome, "Declassified: How an Israeli Operation Derailed Syria's Nuclear Weapons Drive."

[68] Ibid.

What was the civil-military cyber relationship, and how did it support the use of cyber attacks?

Israeli Unit 8200, a clandestine governmental cyber warfare organization, breached Syria's air defense radar system ahead of the attack using a computer program originally obtained from the US.[69] To reach the Syrian air defense radar systems, Israel needed both international cooperation and the use of civilian infrastructure. The commercial telecommunications industry provides the backbone for internet and telephone services, which this unit used to reach the Syrian air defense systems.

This case demonstrates a covert government agency employing a cyber attack against an adversary. The research did not uncover any deliberate roles for non-governmental or military agencies involved. The use of civilian infrastructure to reach cyber attack targets inextricably links civilian and military within the cyberspace domain.

How well did military leaders understand both cyber and its role and effects in the operations within which they participated?

The covert nature of Operation Outside The Box / Orchard, at the time of execution, resulted in an extremely limited number of individuals being aware of the full nature of the mission.[70] This operational security precluded an emerging concept and cross-concentration training manifestation or coordination. A reasonable deduction is that Israeli planners had a well-developed understanding of cyber attacks, as it played a pivotal role in reducing operational risk.

Israeli leadership would not execute this operation at the risk of war should the cyber attack fail and result in a shoot-out between Israeli aircraft and Syrian air defense systems. Israel employed air-to-ground on-board technology and ground-based computer network links to breach the Syrian air defense systems and compromise the data which Syrian operators received.[71]

---

[69] Kaplan, *Dark Territory*, 160–161.

[70] Opall-Rome, "Declassified: How an Israeli Operation Derailed Syria's Nuclear Weapons Drive"; Gross, "Ending a Decade of Silence, Israel Confirms It Blew up Assad's Nuclear Reactor."

[71] Zetter, *Countdown to Zero Day*, 215–216.

Decision-makers placed their trust in this capability. This trust implies an understanding and confidence in the utilized capability.

Despite the implications that planners and decision-makers had a cyber understanding, this did not translate into the pilots flying the mission. The pilots were unaware of the cyber attack role, learning of the mission itself a short while before taking off.[72] These pilots exhibited trust in their leadership; however, it is plausible that they did not fully understand the cyber attack and its role in their mission. In a large scale conflict, leaders seeking effects on targets need to know how to request and receive those effects.

What lessons did actors glean from their experiences?

Israel used this airstrike against a Syrian nuclear reactor as an opportunity to use both cyber warfare and conventional warfare capabilities in a single operation to achieve national political aims. Military leaders no doubt learned from this operation and have incorporated lessons into future operations as of yet classified. This operation tested an Israeli theory without committing the nation to a large scale conflict.

This operation taught Israel countless lessons regarding the integration of cyber attacks with conventional means, particularly in strategic operations. Details on the finer points of these lessons are speculative, lacking published research material on the matter. In addition to taking away successful integration, this operation undoubtedly increased decision-makers and military leaders trust and confidence in using cyber attacks to enable military operations.

Summary

This case demonstrates a small scale yet effective integration of cyber and conventional military capabilities to achieve a lethal mission. The evidence in this case adequately answers the posed questions, and yet, due to the still overly classified nature of research materials, it provides a relatively weak baseline for some of the conclusions. Some of these answers require deduction

[72] Melman, "OUTSIDE THE BOX: Israel's Strike on Syria's Nuclear Plant."

from the available information, yet they remain valid until new evidence surfaces to challenge them. This case critically identifies that cyber attacks can support conventional operations to achieve strategic and political objectives while reducing risk to an acceptable level. Given the increasing world-wide use and reliance on information technology, it is reasonable to assume that the use of cyber attacks to support strategic military strikes will continue to increase and may even see use in place of kinetic options.

Russo-Georgia war, 2008

Georgia, on 7 August 2008, invaded South Ossetia and began shelling Tskhinvali.[73] Russia responded to this aggression by deploying both conventional military forces and cyber warfare against the Georgian government and its armed forces.[74] In the cyber domain, Russia encouraged its citizens to conduct attacks against Georgian targets deliberately identified to cause inconvenience but short of provoking an international response.[75] Simultaneous with Russian armored forces advancing against Georgian forces, Russian cyber warfare crippled Georgian websites and internet services.[76] These attacks ranged from Distributed Denial of Service (DDoS) to website defacing, all strategically designed to interfere with Georgian internal processes without provoking the international community.[77]

Russia's cyber attacks seized and maintained the initiative from Georgia in information, communication, and military control.[78] Throughout the short conflict, Russia capitalized on this

---

[73] David Hollis, "Cyberwar Case Study: Georgia 2008," *Small Wars Journal* (January 6, 2011): 1.

[74] Ibid., 1–5.

[75] Sarah P. White, *Understanding Cyberwarfare: Lessons from the Russia-Georgia War* (West Point, NY: Modern War Institute, March 20, 2018), 7–8, 12.; Gregg Keizer, "Russian Hacker 'militia' Mobilizes to Attack Georgia," *Network World*, last modified August 12, 2008, accessed December 12, 2019, https://www.networkworld.com/article/2274800/russian-hacker--militia--mobilizes-to-attack-georgia.html.

[76] Kaplan, *Dark Territory*, 164–165.

[77] Hollis, "Cyberwar Case Study: Georgia 2008," 3–4.

[78] Kaplan, *Dark Territory*, 164–165.

information warfare advantage to reinforce its legitimacy and to undermine the Georgian government.[79] Russia also targeted Georgian hackers early on in the conflict, seeking to degrade their adversary's ability to respond and retaliate.[80] Cyber attacks against Georgian targets began simultaneous with the first airstrikes and ended with the declaration of a cease-fire.[81] The cyber warfare focused on isolating Georgia digitally and providing an element of surprise for Russian military forces.[82] The Georgia-Russia war ended after about one week with Georgia's decisive defeat, at all levels of war, following the battle of Tskhinvali.[83]

How were cyber attacks employed to achieve political objectives or enable military operations?

Russia's use of cyber warfare directly contributed to military campaigns in a heretofore unprecedented manner, illustrative of potential for future cyber warfare possibilities.[84] Georgia was a target for these non-persistent cyber attacks as much as a month before ground combat ensued, indicating that Russia was preparing and testing its tools.[85] Those cyber attacks did not last long in the face of cyber defense activities. This preparation of the battlefield undoubtedly also served as a warning to the Georgian government, one which went unheeded. Russia employed non-state actors, to reduce political risk and generate plausible deniability for the cyber attacks.[86]

---

[79] Small Wars Journal, "Russia-Georgia: Early Take," *Small Wars Journal*, n.d., accessed December 17, 2019, https://smallwarsjournal.com/blog/russia-georgia-early-take.

[80] Andreas Hagen, "The Russo-Georgian War 2008: The Role of the Cyber Attacks in the Conflict" (AFCEA, May 24, 2012), 7–9.

[81] Oscar Jonsson and Robert Seely, "Russian Full-Spectrum Conflict: An Appraisal After Ukraine," *The Journal of Slavic Military Studies* 28, no. 1 (January 2, 2015): 15.

[82] Sergei A. Medvedev, "Offense-Defense Theory Analysis of Russian Cyber Capability" (Master's Thesis, Naval Postgraduate School, 2015), 23–24.

[83] Hollis, "Cyberwar Case Study: Georgia 2008," 1.

[84] Medvedev, "Offense-Defense Theory Analysis of Russian Cyber Capability," 22.

[85] Hollis, "Cyberwar Case Study: Georgia 2008," 3–4.

[86] Keizer, "Russian Hacker 'militia' Mobilizes to Attack Georgia."

These attacks, while non-persistent, enabled Russia's military forces to gain the element of surprise over Georgian forces. This surprise came from attacks disrupting Georgian ability to command and control its military forces.[87] When Georgia disentangled itself from the cyber attacks, Russian troops had already achieved their military objectives.

Cyber attacks against Georgia proved that non-persistent cyber attacks have a limited duration unless coupled with, and followed by, conventional military force.[88] Cyber attacks may still convey a message when disconnected from military operations. They may also serve as a form of military deception, distracting the enemy to allow military forces to achieve their mission.[89]

What kind of staffing structure facilitated the use of cyber to ensure collaboration rather than combativeness?

Russia sees cyber as an element of information warfare, already well within its existing staff structure.[90] This approach relies on existing staff structures to employ a new capability. The US is creating multi-discipline organizations as they incorporate targeting warrant officers into cyber formations.[91] The Russian incorporation of cyber warfare into conventional operations, both government organizations and the hacker underground, indicates a highly integrated planning and coordinating staff system capable of capitalizing on cross-domain gains.[92]

The Russian-Georgia war demonstrates a high degree of coordination between strategic and tactical level organizations to achieve results by controlling tactical military operations and strategic yet decentralized cyber warfare operations.[93] At the operational level, Russian airstrikes

---

[87] Kaplan, *Dark Territory*, 164.

[88] Medvedev, "Offense-Defense Theory Analysis of Russian Cyber Capability," 24.

[89] Headquarters, Department of the Army, *FM 3-0*, 2–28.

[90] White, *Understanding Cyberwarfare*, 2.

[91] Ibid., 12.

[92] Hagen, "The Russo-Georgian War 2008: The Role of the Cyber Attacks in the Conflict," 6–9.

[93] Ibid., 13–17.

and cyberattacks occurred simultaneously against Georgian targets, further implying a direct and well-coordinated link between the Russian military and individual hackers.[94] This indicates a well developed and utilized structure to support the cross-coordination of military and cyber operations.

The Russian model of a 'cyber militia,' independently acting out of nationalism in support of military and governmental force operations, provides an interesting concept that the US should further explore, both in legal ramifications and as an option to augment its Department of Defense in times of need.[95] The use of non-governmental entities to carry out cyber attacks against Georgia provided Russian leadership with plausible deniability. The proximity and overlap of cyber and military attacks belie a collaboration between this 'cyber militia' and the Russian government. Available research material did not provide the exact means of collaborating these efforts.

What was the civil-military cyber relationship, and how did it support the use of cyber attacks?

In this case, Russia deliberately employed cyber warfare against civilian and government components of Georgia, rather than against military capabilities.[96] Russia coordinated both government and non-government cyber attacks against Georgia's websites and communications systems.[97] Corporate support of these attacks came in the form of the information technology infrastructure supporting internet-based services and connecting Russia and Georgia.

More than ever, private entities own and control the hardware, software, and infrastructure that support cyberspace, indicating that failure to include them in future strategies

---

[94] Hagen, "The Russo-Georgian War 2008: The Role of the Cyber Attacks in the Conflict," 17–18.

[95] Ibid., 17–20; Connell and Vogler, "Russia's Approach to Cyber Warfare," 17–18.

[96] White, *Understanding Cyberwarfare*, 4.

[97] Hollis, "Cyberwar Case Study: Georgia 2008," 2–5.

may result in upset efforts, as learned in the Stuxnet case.[98] The Russia-Georgia war demonstrates the interwoven nature of corporations and government, transferring capabilities to corporate Tulip Systems TSHost servers physically located within the US.[99] The move of Georgian cyber interests to US information technology infrastructure by a private company potentially changes national conflict status without the government's involvement.[100]

Russia's denial of cyber warfare operations may change the nature of future war as nations follow its example and prime individuals to carry out cyber warfare operations, allowing deniability of government action.[101] This Russian 'cyber militia' actively assists the government, as evidenced in the Russian-Georgian 2008 war in supporting the military in achieving its conventional objectives.[102] This case provides plausibility to the idea that a patriotic information technology company may become a participant in war depending on the services it offers or denies to customers in the opposed nation.

How well did military leaders understand both cyber and its role and effects in the operations within which they participated?

This case demonstrates the integration of cyber warfare activities and conventional military force. Military leaders need to have a sound understanding of cyber warfare and be as comfortable speaking cyber as they are with conventional maneuvers and combined arms.[103] Cyber attacks induced general population communications interference, caused problems for the Georgian government's communications with its military, and the internal military

---

[98] White, *Understanding Cyberwarfare*, 17; Zetter, "How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History."

[99] White, *Understanding Cyberwarfare*, 8–9.

[100] Stephen W. Korns and Joshua E. Kastenberg, "Georgia's Cyber Left Hook," *www.Army.Mil*, last modified April 7, 2009, accessed December 13, 2019, https://www.army.mil/article/19351/georgias_cyber_left_hook.

[101] Ibid.

[102] Hagen, "The Russo-Georgian War 2008: The Role of the Cyber Attacks in the Conflict," 13–15, 18.

[103] White, *Understanding Cyberwarfare*, 17.

communications throughout the conflict.[104] The Russian military capitalized on this communications confusion as its forces carried out air attacks and ground movements.

Cross-training military leaders in cyber warfare helps to construct a more holistic operational approach, lines of effort and operations, and campaign plans. Russia, in this case, showed exactly how this comes together on a limited scale.[105] The close coordination between cyber and conventional military attacks indicates that military leaders understood enough about cyber warfare to maximize the advantages it provided their forces.[106] This example covers the operational level of war, as it coordinates the strategic and tactical. Leaders, at the tactical level, with a good understanding of cyber warfare, will have an increased reaction time, facilitating the military's ability to exploit opportunities and multiple dilemmas outlined in FM 3-0.[107]

What lessons did actors glean from their experiences?

Russia utilized the 2008 conflict with Georgia as a testbed to exercise its unique cyber militia approach to cyber warfare.[108] Russia used online blogs and forums to post directions, tools, codes, and targets allowing individuals to contribute to the national enterprise. [109] Russia's use of its cyber militia in this limited war gave both the government and the individuals composing the militia experience, allowing them to refine their cyber warfare tactics, techniques, and procedures.[110] Small scale testing, as exemplified in this case, builds confidence and capability through exposure betwixt the various military, governmental, and militia components that coordinated to bring about the decisive Georgian defeat.

---

[104] Hollis, "Cyberwar Case Study: Georgia 2008"; Korns and Kastenberg, "Georgia's Cyber Left Hook."

[105] White, *Understanding Cyberwarfare*, 11.

[106] Jonsson and Seely, "Russian Full-Spectrum Conflict."

[107] Headquarters, Department of the Army, *FM 3-0*, 1–17, 1–21, 5–4.

[108] Keizer, "Russian Hacker 'militia' Mobilizes to Attack Georgia."

[109] Ibid.

[110] Connell and Vogler, "Russia's Approach to Cyber Warfare," i.

The movement of Georgian cyber assets to the United States through a civilian information technology corporation, without US Government approval, identifies an unresolved area of cyber warfare theory regarding neutrality.[111] The movement of critical Georgian web-based services to US locations only brought the ongoing cyber attacks to American networks.[112] Current international law conventions leave this a grey area codified before the internet emerged, requiring additional resolution to address conflict implications. It appears that to Russia, the key element is the customer, not the provider, as the target for web-services and legitimacy as a target.

Russia employed a tactic to target and eliminate Georgia's hackers at the outset of the conflict, though to limited success.[113] This strategy aimed to eliminate the enemy's cyber counter-attack capabilities while the government concentrated on attack recovery and reconsolidation. Despite the limited success, this is a clear lesson Russia learned and is likely to repeat in the future.

Summary

This case has good information to address the identified questions. It provides value in the area of civil-military integration as Russian civilians participating in cyber warfare synchronized with military operations and the various sovereign nations involved. The integration of Russian military and non-military elements, ranging from the strategic through the tactical level, directly dovetails with the research question in demonstrating how to go about developing an emerging capability. Key points in this case study are the cyber militia, coordination between military forces and cyber operations, and the Russian integration of cyber warfare into conventional disciplines, such as information warfare and psychological operations.

---

[111] Korns and Kastenberg, "Georgia's Cyber Left Hook."

[112] White, *Understanding Cyberwarfare*, 9.

[113] Ibid., 8.

In opposition to the United States, Russia did not realign its staff but rather integrated cyber into its information warfare operations.[114] This integration of cyber into its already existing information warfare branch influenced the application of cyber attacks in this case. Russia refrained from overt employment of its state cyber warfare capabilities rather relying on proxies to carry out low-level, non-destructive, cyberattacks orchestrated by the state's cyber warfare capable organizations.

Overall, Russia effectively integrated cyber warfare into its doctrine, coordinated between military and civilian entities, and used this case to test its tactics, techniques, and procedures in a limited-scale conflict. The United States should follow these lessons. Author Sarah White calls for a reconsideration of doctrine in her lessons-learned paper on the Russia-Georgia war, supporting the idea that the current US theory and doctrinal approach requires additional work.[115] Andreas Hagen agrees, concluding that the United States is very unprepared in the cyber domain, and to participate in cyber warfare.[116]

Ukraine Conflict, 2014-2016

In February 2014, Russia wrested control of the Crimea region away from Ukraine and annexed it on 18 March.[117] In April 2014, cyber warfare exponentially increased with significant and obvious correlation to land operations.[118] Leading up to this, civil unrest, resulting from the Ukrainian president's controversial decision first to join the European Union and then to renege on this decision.[119] This situation provided a prime information warfare battleground heavily

---

[114] Connell and Vogler, "Russia's Approach to Cyber Warfare," 3.

[115] White, *Understanding Cyberwarfare*, 16.

[116] Hagen, "The Russo-Georgian War 2008: The Role of the Cyber Attacks in the Conflict," 22.

[117] Andreas Goldthau and Tim Boersma, "The 2014 Ukraine-Russia Crisis: Implications for Energy Markets and Scholarship," *Energy Research & Social Science* 3 (September 2014): 13.

[118] Lookingglass Cyber Threat Intelligence Group, *Operation Armageddon: Cyber Espionage as a Strategic Component of Russian Modern Warfare* (Lookingglass, April 28, 2015), 4.

[119] Timothy Thomas, "Russia's Military Strategy and Ukraine: Indirect, Asymmetric—and Putin-Led," *The Journal of Slavic Military Studies* 28, no. 3 (July 3, 2015): 446.

exploited in the domain of cyberspace. Russia, closely following the situation, began to get involved using an information and psychological warfare approach to influence the international community, Ukrainians, and domestic audiences and keep progressing events below the level of kinetic warfare.[120] Allegedly independent actors, of a pro-Russian persuasion, executed website defacing, online trolling, and delivery of cyber warfare tools and guidance to exacerbate the situation.[121]

Telecommunications infrastructure and systems were primary targets isolated by cyber-attacks and seized by Russian forces.[122] Continuous attacks against Ukrtelecom, Ukraine's telecommunications organization, allowed Russian special forces to gain control of the Crimean Simferopol internet exchange points (IXP) and ultimately seize control over incoming and outgoing land-based communications within the region.[123] Concurrent with Russian troops crossing into Crimea, cyberattacks shut down traffic to Ukranian government websites and other communications systems, preventing effective or timely reactions.[124] The Russian troops that moved in and seized the cyber-isolated targets did not wear any insignia, giving Russia plausible deniability in the physical world just as the non-state proxy cyber actors conducting cyber warfare did in cyberspace.[125] Once Russia 'owned' the Crimean networks, there was no need to attack any

[120] Jānis Bērziņš, "Russia's New Generation Warfare in Ukraine: Implications for Latvian Defense Policy" (National Defense Academy of Latvia, Center for Security and Strategic Research, April 2014), 4–7.

[121] Limnéll and The Society of Digital Information and Wireless Communication, "The Exploitation of Cyber Domain as Part of Warfare," 527–528.

[122] András Rácz, *Russia's Hybrid War in Ukraine: Breaking the Enemy's Ability to Resist*, Senior Research Fellow (Helsinki: The Finnish Institute of International Affairs, June 16, 2015), 81; Williams, "Cyberwarfare and Operational Art," 29–30.

[123] Williams, "Cyberwarfare and Operational Art," 26–32; Geers, *Cyber War in Perspective*, 25.

[124] Limnéll and The Society of Digital Information and Wireless Communication, "The Exploitation of Cyber Domain as Part of Warfare," 527–528.

[125] Jonsson and Seely, "Russian Full-Spectrum Conflict," 10; Limnéll and The Society of Digital Information and Wireless Communication, "The Exploitation of Cyber Domain as Part of Warfare," 526–527.

of it kinetically when they could use it themselves.[126] These coordinated activities assured Russian information superiority using cyberspace, one small part of information space according to Russian doctrine, to gather intel against Ukraine.[127]

Rocket strikes destroyed two Ukranian mechanized brigades on 11 July 2014 as they assembled, using drones and cyber warfare to geolocate the units.[128] The cyber warfare aspect of this employed malware within an artillery mobile phone application that transmitted location information back to Russian forces.[129] Russian forces confirmed this using drones to provide real-time information to guide their multiple launch rocket systems onto the Ukranian brigades.[130] This particular incident depicts the coordination between the Russian military and cyber warfare elements to culminate in a tactical battlefield effect.

In December 2015, Russian hackers caused power outages by attacking power facilities.[131] They attacked three separate sites in Western Ukraine, causing power outages for 220,000 residents and in some instances, they deleted the operating systems at the power distribution sites.[132] The obvious message from the power outages is to sway public support away

---

[126] Geers, *Cyber War in Perspective*, 24.

[127] Ibid., 8–9, 16.

[128] Liam Collins and Harrison Morgan, "King of Battle: Russia Breaks Out the Big Guns," *Association of the United States Army*, last modified January 22, 2019, accessed October 3, 2019, https://www.ausa.org/articles/king-battle-russia-breaks-out-big-guns.

[129] Itai Barsade et al., "Prevention in the Cyber Domain" (Perry World House Student Fellows 2016-2017, University of Pennsylvania, n.d.), 7–8, accessed December 19, 2019, https://global.upenn.edu/sites/default/files/perry-world-house/CyberPolicyProjectReport.pdf.

[130] Shawn Woodford, "The Russian Artillery Strike That Spooked The U.S. Army," *Mystics & Statistics*, March 29, 2017, accessed December 22, 2019, http://www.dupuyinstitute.org/blog/2017/03/29/the-russian-artillery-strike-that-spooked-the-u-s-army/; Amos Fox, "The Russian–Ukrainian War: Understanding the Dust Clouds on the Battlefield," *Modern War Institute*, last modified January 17, 2017, accessed December 22, 2019, https://mwi.usma.edu/russian-ukrainian-war-understanding-dust-clouds-battlefield/.

[131] Peter Fairley, "Unplugging From Digital Controls To Safeguard Power Grids," *Institute of Electrical and Electronics Engineers (IEEE)Spectrum*, last modified July 22, 2019, accessed November 19, 2019, https://spectrum.ieee.org/energywise/energy/the-smarter-grid/unplugging-digital-networks-to-safeguard-power-grids.

[132] Connell and Vogler, "Russia's Approach to Cyber Warfare," 20.

from the Ukranian government by demonstrating it cannot take care of its people, and to pave the way for favorable negotiations with Russia. As the conflict expanded into the Donbas region, conventional attacks targeted IT infrastructure while cyberattacks continued their disruptive work and added the capability to coordinate artillery to adjust fire missions.[133]

These operations gave Russia control over all information within the targeted regions, enabling strong propaganda information operations, and disrupted Ukranian government and military communications abilities.[134] These cyberattacks, in conjunction with Russia's international propaganda and political rhetoric, curtailed the public perception of what was taking place until it was too late.[135] The primacy of these attacks appears intended to deny Ukranian services, promote defection to support Russia and its backed rebel cause, and to promote Russia's narrative both domestically and internationally.[136]

How were cyber attacks employed to achieve political objectives or enable military operations?

The Russian use of cyber operations as a facilitator or enabler for information operations within Ukraine demonstrates the fluidity and flexibility of cyber warfare, challenging current conceptions and theories.[137] Cyber attacks, especially those utilizing proxy or patriotic actors, bring a degree of plausible deniability to the table for national leadership.[138] Russian special forces coordinated with cyber attacks by seizing key cyber terrain in the physical world, inhibiting network traffic and isolating the Crimea from the larger internet.[139]

---

[133] Geers, *Cyber War in Perspective*, 62–63.

[134] Rácz, *Russia's Hybrid War in Ukraine: Breaking the Enemy's Ability to Resist*, 80–82; Connell and Vogler, "Russia's Approach to Cyber Warfare," 19.

[135] Kristin Ven Bruusgaard, "Crimea and Russia's Strategic Overhaul," *Parameters* 44, no. 3 (2014): 84.

[136] Connell and Vogler, "Russia's Approach to Cyber Warfare," 19.

[137] Geers, *Cyber War in Perspective*, 28.

[138] Ibid., 96.

[139] Medvedev, "Offense-Defense Theory Analysis of Russian Cyber Capability," 29.

Russia used cyber warfare, as a component of information warfare in Ukraine, achieving the US Army FM 3-0 operational concept of presenting multiple dilemmas to the enemy, delaying any NATO response until one would be ineffectual.[140] Cyber attacks supported information operations by disrupting Ukrainian decision making and government cohesion and in encouraging lack of trust in the government, such as sending text messages to soldiers encouraging their defection.[141] Coordinating these cyber attacks with military forces enabled Russia to seize the Crimea and shape public opinion to undermine any popular support against this annexation.

Russia further employed cyber attacks to deliver political messages and force the Ukrainian government to acquiesce by causing power outages.[142] Operationally, Russia demonstrated the supporting role of cyber attacks in the July 2014 rocket strike. This application of cyber warfare expands upon the lessons of the Russo-Georgia war, bringing cyber warfare to a higher level.

What kind of staffing structure facilitated the use of cyber to ensure collaboration rather than combativeness?

Russia folds cyber operations under its traditional information warfare division where it is just another tool used in psychological, electronic, and informational warfare.[143] Cyber warfare, within this paradigm, is an enabler to facilitate achieving information supremacy throughout all stages of a conflict, setting the stage for victory, and supporting the long term strategic narrative.[144] This structure places cyber subordinate to information and thereby allows national

---

[140] Geers, *Cyber War in Perspective*, 38; Headquarters, Department of the Army, *FM 3-0*, 1-16-1–17.

[141] Connell and Vogler, "Russia's Approach to Cyber Warfare," 19.

[142] Ibid., 20.

[143] Ibid., 3–6; Geers, *Cyber War in Perspective*, 23–24.

[144] Connell and Vogler, "Russia's Approach to Cyber Warfare," 5–6.

and strategic planners to oversee all the data and operations as well as capitalizing on a historically close military relationship.[145]

Russia has four organizations, outside of the military, involved in cyber operations with the military and changed its focus from electronic warfare to information warfare as a result of this conflict and the Russo-Georgia war.[146] Russia has aligned its organizations against this information warfare theory and collaborates between the Federal Security Service (FSB), Foreign Intelligence Service (SVR), and the military's Main Intelligence Directorate (GRU) to achieve effects.[147] These organizations have, in contrast to US cyber organizations, greater authorities and freedom of action due to the subordinate nature of cyber to information warfare. These flexible authorities enabled Rusian organizations to coordinate non-government and military actions, as occurred in Crimea.

In the Donbas region, Russia employed signals intelligence in conjunction with cyber warfare to gather position location information on Ukranian military forces through cell phone, Wi-Fi, and GPS networks and then adjust artillery fire onto those formations.[148] Achieving this capability requires close coordination between cyber warfare and artillery organizations to collect, analyze, understand, transmit, target, and execute such a decisive operation.

What was the civil-military cyber relationship, and how did it support the use of cyber attacks?

Russia's deliberate targeting, isolation, and seizure of the Simferopol IXP demonstrate that civilian information technology and internet infrastructure require just as much offensive and defensive military planning consideration as other strategic key terrains.[149] Inside of Russia, internet service providers work with the government as laws require them to install monitoring

---

[145] Geers, *Cyber War in Perspective*, 88, 91.

[146] Connell and Vogler, "Russia's Approach to Cyber Warfare," 7–8.

[147] Medvedev, "Offense-Defense Theory Analysis of Russian Cyber Capability," 2–4.

[148] Geers, *Cyber War in Perspective*, 63.

[149] Geers, *Cyber War in Perspective*, 25.

and back-door hardware.[150] This relationship between the state and the corporate world, albeit legally based, enables Russia greater freedoms without requiring coordination.

Russia utilized non-state actors, as in the 2008 Russo-Georgia war, to serve as proxies and provide plausible deniability to the government; patriots inside Ukraine followed suit.[151] Non-state cyber actors enabled Russia's activities in Ukraine through the defacement of web pages, DDoS, and other attacks tied to physical operations and information warfare objectives.[152] These cyber attacks facilitated military operations, but the Russian government retained plausible deniability due to the nature of attack origins. Independent actors identified online forums, registered in multiple countries, which the Russian government supposedly used to coordinate and synchronize these attacks.[153]

The Ukranian computer emergency response team (CERT) worked closely with network security corporations to find, fix, and eliminate malicious software, viruses, and worms that hackers used.[154] Ukranian CERT personnel recognizes the cyber warfare they are involved with poses both technical and content-related aspects of ever-increasing technical complexity with which the nation is struggling to cope.[155] Various network security companies, such as Symantec and Kaspersky Lab, found, traced, cataloged, exposed, and otherwise became involved in the cyber warfare taking place between Ukraine and Russia.[156]

This civilian corporate work to identify and expose cyber operations has the potential to destroy US cyber warfare operations if the US does not secure their cooperation. Ukraine has

---

[150] Connell and Vogler, "Russia's Approach to Cyber Warfare," 7.

[151] Geers, *Cyber War in Perspective*, 101, 132.

[152] Connell and Vogler, "Russia's Approach to Cyber Warfare," 19.

[153] Jonsson and Seely, "Russian Full-Spectrum Conflict."

[154] Geers, *Cyber War in Perspective*, 56.

[155] Ibid., 58.

[156] Limnéll and The Society of Digital Information and Wireless Communication, "The Exploitation of Cyber Domain as Part of Warfare," 528.

been unable to effectively leverage the cyber skills, the resources, and the capabilities resident within its sector.[157] This shortfall contributes to the nation's inability to mount an effective cyber defense or counter-campaign. To get after this shortfall, Ukraine established a ministry of information on 2 December 2014 devoted to information technology, including all things cyber.[158]

How well did military leaders understand both cyber and its role and effects in the operations within which they participated?

The conflict taking place in Ukraine provides a good example of coordinated cyber warfare blending with conventional warfare and politics.[159] The Russian approach to cyber warfare is holistic with cyber as an integral element of information warfare and crosses domains with soldiers seizing critical infrastructure restricting information pathways.[160] This approach addresses both attacks on political targets and attacks against military infrastructure, including civilian infrastructure that supports the military. This well-developed doctrine provides an existing structure for Russian officers to coordinate efforts across the force and with non-military entities.[161]

Russian military leaders participate in ongoing discussions regarding the role of cyber warfare, with their publications focusing on gaining information superiority in cyberspace as an air force does in the air domain.[162] These leaders have an understanding of cyber warfare and grasp how to integrate it into conventional and irregular operations to disrupt and gain an

---

[157] Geers, *Cyber War in Perspective*, 84.

[158] Ibid., 116; Christopher Miller, "Ukraine Just Created Its Own Version of Orwell's 'Ministry of Truth,'" *Mashable*, last modified December 2, 2014, accessed December 23, 2019, https://mashable.com/2014/12/02/ukraine-ministry-of-truth/.

[159] Geers, *Cyber War in Perspective*, 168.

[160] Ibid., 23–25.

[161] Ibid., 96.

[162] Ibid., 88.

advantage over their adversary. Russian special forces, to achieve this end, exploited key cyber critical infrastructure during the invasion and annexation of Crimea.[163]

The 11 July 2014 cyber guided artillery strikes, which proved devastating to the Ukrainians, demonstrate the required need for military leaders to have an understanding of cyber warfare.[164] Leaders needed to understand the information gathered via cyber warfare and then share it with the appropriate military force in time to capitalize on it, making it actionable intelligence with a limited lifespan of usefulness. Interdisciplinary cross-training facilitates accurate and timely exploitation of opportunities, a key concept discussed in the US Army's FM 3-0.[165] The Russian targeting cycle operated swiftly due to the interdisciplinary understanding that decision-makers possessed.

What lessons did actors glean from their experiences?

Russia used the annexation of the Crimea to refine the techniques, tactics, and procedures they had evolved since its previous rendition in the Russian-Georgian war of 2008.[166] It was conducting cyber attacks using viruses against civilian entities as well as in coordination with military operations, rounding out its hybrid warfare doctrine and experience while improving it each year the conflict drags on.[167] For Russian leadership, this conflict has validated the use of non-state actors to achieve effects without needing a large standing cyber capability.

Russian military leaders and theorists wrote about coordinating electronic isolations of adversary governments and military in sequence with conventional attacks to overwhelm and

[163] Williams, "Cyberwarfare and Operational Art," 29–30.

[164] Barsade et al., "Prevention in the Cyber Domain," 6–9.

[165] Headquarters, Department of the Army, *FM 3-0*, 1–17.

[166] Bruusgaard, "Crimea and Russia's Strategic Overhaul," 86.

[167] Roman Rukomeda, "Russia's Hybrid War Against Ukraine: The Latest Developments and Trends," *Norwegian Centre for Integrity in the Defence Sector (CIDS)*, last modified September 28, 2018, accessed December 20, 2019, https://cids.no/2018/09/28/russias-hybrid-war-against-ukraine-the-latest-developments-and-trends/.

destroy them, exactly what took place in 2014 in Ukraine.[168] Russian special operation forces, unrecognizable today from 2008, provide physical proof that Russia is learning, adapting, and improving from its war with Georgia.[169] The stark contrast between the 2014 seizure of Crimea and the 2015 power blackouts exemplifies Russian learning and adapting inside of this conflict. Cyber attacks supported a military objective in the former case while delivering a political statement in the latter.

One of the key lessons from Russia's use of cyber warfare is its ability to restore a fog of war for the targeted opponent by confusing, severing, and disrupting both governmental and civilian IT systems, networks, and capabilities.[170] Increasing confusion and system and network distrust allow one to act faster and more effectually than their adversary can react, a key concept of Boyd's well known OODA loop.[171] This confusion serves to prolong and preserve the element of surprise and the asymmetric advantage one has over their adversary.

Finally, Russia's conflict with Ukraine has provided it with a playground for experimenting on how best to achieve political aims and military objectives through integrated operations and strategy.[172] The repeated hacking and defacement of Ukrainian government websites, trolling, and attacks on power stations find merit inside of information warfare. Previously addressed military-cyber coordinated operations also achieved national objectives, securing Russia access to the Black Sea.

---

[168] Rácz, *Russia's Hybrid War in Ukraine: Breaking the Enemy's Ability to Resist*, 37–39.

[169] Geers, *Cyber War in Perspective*, 20.

[170] Ibid., 35.

[171] Tracy A. Hightower, "Boyd's O.O.D.A Loop and How We Use It," *Tactical Response*, accessed December 21, 2019, https://www.tacticalresponse.com/blogs/library/18649427-boyd-s-o-o-d-a-loop-and-how-we-use-it.

[172] Geers, *Cyber War in Perspective*, 48.

Summary

This case provides the most recent and comprehensive review of cyber warfare during a limited scale conflict. It reinforced by the execution of various elements of cyber warfare between the belligerents and integration with military operations. The disparity between the integration of cyber into strategy and military operations, and the Russian philosophy of subordination to information warfare, provides an interesting perspective that theorists should consider as cyber warfare doctrine and organizational structures continue to evolve.[173] Russian dominance of internal networks and the integration of criminal entities as proxies for low-level cyber warfare have intriguing implications concerning potential ways forward within the US and merit further discussion.[174] The major weakness of this case is the limited scope of both the conflict and the lack of overt destruction through cyber means, yet this remains characteristic of all conflicts involving cyber warfare to this day.

[173] Medvedev, "Offense-Defense Theory Analysis of Russian Cyber Capability," 47–48.

[174] Ibid., 43–45.

Analysis

This section provides a consolidated summary of the findings for each hypothesis. Each question is analyzed and summarized. The final summary ties this analysis into the research question. This paper finally ends with recommendations for the US military going forward.

How were cyber attacks employed to achieve political objectives or enable military operations?

Low-level cyber attacks generally have a disruption lifespan commensurate with the duration of the attack and need to be tethered to conventional military operations. Cyber-attacks produce physical damage against civilian or military equipment, depending on the target and political or military aim, such as with stuxnet. The damage they produce is not limited to geographical borders or military targets and crosses into the cognitive domain. Cyber attack targets are not limited to military or government but will include all aspects of a society involved in the conflict. US cyber theory and doctrine address some, but far from all, of these aspects of cyber warfare.

Geographical borders are less important than the patriotic, ethnic, and nationalistic ties of individuals and organizations, motivating their participation. The case studies involving Russia demonstrate that properly motivated civilians are capable of contributing to the nation's strategy through cyber attacks. National boundaries do not constrain internet-based services or these non-state cyber actors, providing governments plausible deniability.

Cyber warfare is unlikely to occur in isolation, rather in close coordination with military operations, as a shaping operation.[175] The US cyber warfare theory and doctrine appears constrained to a war context, relying heavily on military forces or organizations to gain superiority in this domain. As the case studies demonstrated, cyber warfare is not constrained to the same degree as military operations and can occur in the form of a proxy attack against civilian

[175] Limnéll and The Society of Digital Information and Wireless Communication, "The Exploitation of Cyber Domain as Part of Warfare," 531.

power generation infrastructure far from the battlefield to achieve a psychological effect. Cyber attacks are just as likely to achieve cognitive effects as they are to enable kinetic strikes, as demonstrated in each case study.

What kind of staffing structure facilitated the use of cyber to ensure collaboration rather than combativeness?

Stuxnet was extremely complex, deliberately designed to discriminate its targets, and crossed multiple disciplines and technical fields to achieve results in a different domain. It could not achieve this without a dedicated staff to research, develop, and test the weapon before releasing it into the wild. The design of this one weapon was both labor and resource-intensive, not something rapidly repeatable in a large scale conflict.

Israel coordinated electronic warfare, cyber warfare, and conventional combat aircraft to breach Syria's air defense network and carry out an airstrike. Russia integrates cyber warfare into its military's information warfare branch to gain information supremacy early on in its conflicts. Russia also augments its cyber warfare with non-military proxies and three separate federal agencies to achieve effects in coordination with conventional military operations. All of this requires staffing and support structures that coordinate between the cyber actors and the military leaders' decision-making and executing operations.

The complexity of creating and using cyber weapons, such as Stuxnet, and coordinating cyber warfare effects in time and space will require a close relationship and trust between all the disparate cyber capable elements of the federal government, as the Russians have demonstrated in Georgia and Ukraine. The hierarchal nature of the current US military staff is conducive to incremental and iterative processing that cannot achieve the needed results when dealing with cyber warfare. Further study is required to design a decentralized process that integrates into and across the hierarchal levels of the US military rapidly and fastidiously with kinetic operations despite reciprocal adversary cyber actions.

What was the civil-military cyber relationship, and how did it support the use of cyber attacks?

Cyberspace spans the globe and connects adversaries, militaries, governments, corporations, and motivated individuals in a domain where all can compete. A national strategy that eschews the integration of civilian and governmental organizations and capabilities is tantamount to fighting a tank battle without fuel. Civilian cyber corporations and government cyber organizations bring complementary skills to the fight, which, if integrated, can drastically tip the balance in cyber warfare.

Cyber warfare is present in all phases of conflicts, at different levels and threats, and executed by military, governmental, and non-military or governmental actors.[176] The Stuxnet case indicates a potential outcome should a government exclude network security corporations from its cyber warfare; the operation was identified, deconstructed, and prematurely exposed to the world. Corporations today tend to focus their loyalty on their customer bases, as Symantec did in publicizing Stuxnet and Microsoft in rapidly notifying consumers and remediating the vulnerability.

Russian literature theorizes that defense alone is inadequate, so the government constrains its networks and focuses on retaliatory preparations, coopting corporations into this system.[177] Georgia, in the Russo-Georgia War, employed a private corporation which relocated information technology services overseas. Network security organizations, like Symantec in the Stuxnet case, are a vital part of national cybersecurity and will inevitably be involved in any cyber warfare.

Russia employed cyber militias composed of patriotic civilians and cybercriminals as well as targeting civilian information technology infrastructure both in Georgia and Ukraine. Its seizure of Internet Exchange Points and occupation of telecommunications centers in the Ukraine

[176] Medvedev, "Offense-Defense Theory Analysis of Russian Cyber Capability," 62–63.

[177] Ibid., 51–52.

conflict blur the divide between combatant and non-combatant within the confines of war. Finally, Ukraine's employment of civilian network security corporations to bolster its cybersecurity against Russian cyber warfare draws these corporations closer to the status of a combatant.

How well did military leaders understand both cyber and its role and effects in the operations within which they participated?

The Russo-Georgian War provides examples of close coordination between cyber and conventional warfare as Russia dominated the battlefield. In Ukraine, Russian soldiers seized critical cyber infrastructure, damaged others to constrain information flow, and employed it to gather actionable intelligence on Ukranian forces. Russian understanding of cyber warfare provided leaders with cross-discipline understandings, which are paramount in this ever technologically advancing world where the lines between civilian and military technology begin to blur.[178]

Military leaders, just as in combined arms, need to understand the basic operations, capabilities, and constraints inherent in cyber warfare as they direct their organization towards accomplishing its mission. Cyber warfare simultaneously occurs in all domains and can produce effects in any of them, something fundamental which leaders need to understand and anticipate. The Stuxnet case provides an example of leaders failing to understand even the basics, thereby contributing to the cyber attack's success.

Russian leaders understand this, to some extent, and they participate in ongoing academic discussions regarding the role of cyber warfare and its place within their nation and military. This understanding bridges the government-military gap and extends even to the individual civilians composing Russia's cyber militia. The US military needs to become more

[178] Geers, *Cyber War in Perspective*, 52.

engaged in cyber warfare discussion regardless of military discipline to enhance both understanding and potential capabilities as warfighters and technicians collaborate.

What lessons did actors glean from their experiences?

The Russian-Georgian war of 2008 provides an example where maneuver overcomes the confusion and disruption of attacks more effectively than a hardened defensive orientation.[179] This knowledge resurrects the adage that a moving target is harder to hit than a stationary one, reinforcing the corporate movement of internet-based services during cyber attacks. This complicates the current paradigm of war and the definition of legitimate targets.

Russia's experience in the Russo-Georgian War and the Ukraine conflict have shaped its understanding, doctrine, and application of cyber in conducting information warfare and power projection.[180] These conflicts have refined the tactics, techniques, and procedures used in its execution of cyber warfare. Russia used Georgia to validate its centralized direction of decentralized cyber attacks through proxies. The Ukraine conflict validated Russian military leader professional writings about cyber warfare and paved the way for cyber-conventional warfare coordination to achieve political aims and military objectives as in the annexation of Crimea.

Cyber warfare is not alone in using small scale conflicts to test theory and doctrine, as history shows Russia and Germany used the 1936-1939 Spanish Civil War as a testing grounds for their airpower theories between the world wars. The US military has its combat training centers (CTC) to replicate this without the loss of life and equipment, but it needs to incorporate unconstrained cyber warfare into the rotations instead of the restrained version currently incorporated. US cyber warfare operators need to build experience, confidence, and capability

[179] Geers, *Cyber War in Perspective*, 25.

[180] Ibid., 50.

through practice and experimentation on a living breathing adversary without risk of retribution, and a CTC rotation has the potential to provide this.

Summary

In summary, just like the rifle, artillery, aircraft, radios, and nearly every technical invention that impacts the way nations fight wars, leaders must develop ways to integrate cyber warfare with existing capabilities to sequence effects across time, space, echelon, and frequency and overwhelm the enemy's decision making cycle. This integration and sequencing is the true asymmetric advantage posed by cyber warfare, given its depth and breadth. The more fluid, seamless, and synchronized the execution is with other domains, the more decisive the results and asymmetric the advantage.

Integration and sequencing provide the answer to the initial research question of how the US can gain an asymmetric advantage in the next large-scale conflict through cyber warfare. Russian cyber warfare theory subordinates it to information warfare, which provides insight into cyber evolution and innovation to come. This fundamentally different view on capability employment and the analytical lens with which they view the existing application of cyber provides insight into the future of cyber warfare, reflecting on the development of theory and doctrine.[181]

Future conflicts, the history of emerging capabilities can attest, will involve cyber warfare and most likely some hybrid combination of the currently existing theories; military doctrines and organizations need to include this in their operational arts or risk irrelevance.[182] The US needs to invest more effort and intellectual power into developing and refining its cyber warfare theory in light of events taking place throughout the world; take a serious look at the US military staff structure and how it integrates with cyber warfare; consider legislation to coopt

[181] Medvedev, "Offense-Defense Theory Analysis of Russian Cyber Capability," 51.

[182] Ibid., 59–61.

government and non-government cyber entities to coordinate efforts and capabilities; develop a cyber warfare education program for military leadership of all levels and occupational specialties; and conduct larger-scale testing of existing doctrine in unconstrained environments to garner realistic feedback for application in technique, tactic, and procedure refinement.

Recommendations

The United States can take a few steps to gain an asymmetric advantage over other cyber powers in the world. The cases identified that advantages in cyber warfare come from the side that both practices it and coordinates it throughout all involved parties to the greatest extent. Three areas for improvement emerge from this: inter-governmental cooperation, government-corporate collaboration, and tapping into a nation's full cyber potential.

Inter-governmental cooperation

The United States needs to capitalize on the aforementioned proven hypotheses to gain an asymmetric advantage in the next large-scale conflict. Matt Graham, a US Army strategist serving on the joint staff, writes that the United States should establish a cyber component simultaneously focused on cyber warfare and interfaced with the existing military service branches, government, and civilian organizations.[183] This concept is not only possible but a likely outcome of the next large-scale conflict involving the United States.

US cyber personnel from all branches of government should coordinate, analyze previous and ongoing conflicts, and incorporate lessons learned into cyber warfare theory. It is not enough to study from afar, rather the United States should send these experts, in purpose-built and capable teams, to where the cyber warfare is occurring to interface with, assist, learn, and gain experience dealing with the activities taking place. Sending cyber experts to assist friendly nations not only helps to build US cyber prowess but also extends US influence across the world.

[183] Matt Graham, "U.S. Cyber Force: One War Away," *Military Review*, no. May-June 2016 (n.d.): 118.

The lessons learned from these conflicts and the teams sent in to get a close look at cyber warfare can shape US policy, doctrine, and organizational structuring to better protect the nation in a future conflict. Interwar Germany proved this concept in developing an effective air force and air power doctrine, despite lacking a functional branch. Staying on top of the emerging strategies ensures that the US maintains a relevant and potent doctrine to employ across the range of military operations.

Governmental - Corporate collaboration

The United States should nationalize cybersecurity in a way that enables corporate autonomy but also promotes cybersecurity collaboration at a national level. This concept integrates companies and corporations and their capabilities into the larger national construct for defending the United States, collaborative information sharing, and a mutual interest to keep the nation safe through a secure internet. Corporations dubiously volunteer, so some form of policy or legislation is necessary to accomplish this grand task. The more holistic the look at our national cybersecurity, the better prepared the network for cyber attacks and recuperation.

Capitalizing on the untapped potential

The United States has untapped reserves of cyber-savvy civilians and businesses that could facilitate cyber defense and potentially augment offense in times of war. During World War Two, the United States mobilized the industry to support the war effort, however noting today exists for the cyber field. The problem is how to reach these civilians and businesses and garner their support for the nation.

The United States should consider a construct similar to its national guard or reserve components, but one where individuals with an information technology background or degree can work part-time for the government within the cyber discipline. Such federal employees could function, while on-shift, under Title 10 or 50 authorities as needed before ending their shift and relinquishing such authorities. This construct would enable private citizens to bolster their resume, gain experience, contribute to the nation out of patriotism, and facilitate bridging the

divide between individual and national narratives. They could achieve this while the government benefits from their skills in cyber warfare and without the need to build and sustain a large cyber warfare organization.

This concept gives individuals otherwise unable to serve in the armed forces an opportunity to demonstrate their patriotism through their technical skills and abilities while freeing up the government from long term and expensive contracts. It saves the military from the legal battles over deployability and individual readiness measures. The tasks and duties performed at such organizations may vary but would nonetheless provide the nation with a large reserve of capable cyber warfare technicians should the need arise. Such a construct also eschews the Russian practice of employing cybercriminals and proxies to do the government's bidding while developing a robust national capability.

Bibliography

Barsade, Itai, Louis Davis, Kathryn Dura, Rodrigo Ornelas, and Ariel Smith. "Prevention in the Cyber Domain." Perry World House Student Fellows 2016-2017, University of Pennsylvania, n.d. Accessed December 19, 2019. https://global.upenn.edu/sites/default/files/perry-world-house/CyberPolicyProjectReport.pdf.

Bērziņš, Jānis. "Russia's New Generation Warfare in Ukraine: Implications for Latvian Defense Policy." National Defense Academy of Latvia, Center for Security and Strategic Research, April 2014.

Broad, William J., John Markoff, and David E. Sanger. "Israeli Test on Worm Called Crucial in Iran Nuclear Delay." *New York Times*. Last modified January 15, 2011. Accessed November 1, 2019. https://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html.

Bruusgaard, Kristin Ven. "Crimea and Russia's Strategic Overhaul." *Parameters* 44, no. 3 (2014): 81–90.

Carvelli, Michael P. "A Smarter Approach to Cyber Attack Authorities." *Joint Force Quarterly* 4th Quarter 2018, no. 91 (2018): 7.

Clarke, Richard A., and Robert K. Knake. *Cyber War: The next Threat to National Security and What to Do about It*. 1st ed. New York: Ecco, 2010.

Collins, Liam, and Harrison Morgan. "King of Battle: Russia Breaks Out the Big Guns." *Association of the United States Army*. Last modified January 22, 2019. Accessed October 3, 2019. https://www.ausa.org/articles/king-battle-russia-breaks-out-big-guns.

Connell, Michael, and Sarah Vogler. "Russia's Approach to Cyber Warfare." CNA, March 2017. https://www.cna.org/cna_files/pdf/DOP-2016-U-014231-1Rev.pdf.

Corum, James S. *The Luftwaffe: Creating the Operational Air War, 1918-1940*. Modern war studies. Lawrence: University Press of Kansas, 1997.

Fairley, Peter. "Unplugging From Digital Controls To Safeguard Power Grids." *Institute of Electrical and Electronics Engineers (IEEE)Spectrum*. Last modified July 22, 2019. Accessed November 19, 2019. https://spectrum.ieee.org/energywise/energy/the-smarter-grid/unplugging-digital-networks-to-safeguard-power-grids.

Fox, Amos. "The Russian–Ukrainian War: Understanding the Dust Clouds on the Battlefield." *Modern War Institute*. Last modified January 17, 2017. Accessed December 22, 2019. https://mwi.usma.edu/russian-ukrainian-war-understanding-dust-clouds-battlefield/.

Fulghum, David A., and Robert Wa. "U.S. Electronic Surveillance Monitored Israeli Attack On Syria." *World Security Network*. Last modified February 7, 2014. Accessed October 29, 2019. https://web.archive.org/web/20140207060836/http://www.worldsecuritynetwork.com/Israel-Palestine/David-A.-Fulghum-and-Robert-Wall-/U.S.-Electronic-Surveillance-Monitored-Israeli-Attack-On-Syria.

Geers, Kenneth, ed. *Cyber War in Perspective: Russian Aggression against Ukraine*. Tallinn, Estonia: NATO Cooperative Cyber Defence Centre of Excellence, 2015.

George, Alexander L., and Andrew Bennett. "Case Studies and Theory Development in the Social Sciences." *Perspectives on Politics* (n.d.). Accessed October 3, 2019. https://www.academia.edu/19264308/Case_Studies_and_Theory_Development_in_the_Social_Sciences.

Goldthau, Andreas, and Tim Boersma. "The 2014 Ukraine-Russia Crisis: Implications for Energy Markets and Scholarship." *Energy Research & Social Science* 3 (September 2014): 13–15.

Graham, Matt. "U.S. Cyber Force: One War Away." *Military Review*, no. May-June 2016 (n.d.): 111–118.

Gross, Judah Ari. "Ending a Decade of Silence, Israel Confirms It Blew up Assad's Nuclear Reactor." *The Times of Israel*. Accessed October 30, 2019. https://www.timesofisrael.com/ending-a-decade-of-silence-israel-reveals-it-blew-up-assads-nuclear-reactor/.

Hagen, Andreas. "The Russo-Georgian War 2008: The Role of the Cyber Attacks in the Conflict." AFCEA, May 24, 2012. Accessed December 17, 2019. https://www.afcea.org/committees/cyber/documents/TheRusso-GeorgianWar2008.pdf.

Haizler, Omry. "The United States' Cyber Warfare History Implications on.Pdf." *32Cyber, Intelligence, and Security* 1, no. 1 (January 2017): 31–45.

Harris, Shane. *@WAR: The Rise of the Military-Internet Complex*. Boston: Houghton Mifflin Harcourt, 2014.

Headquarters, Department of the Army. *Army Doctrine Publication (ADP) 3-0, Operations*. Washington DC: Government Printing Office, 2019.

———. *Field Manual (FM) 3-0, Operations*. Washington DC: Government Printing Office, 2017.

———. *TRADOC Pamphlet 525-3-1: The U.S. Army in Multi-Domain Operations 2028.* Washington DC: Government Printing Office, December 6, 2018.

Hightower, Tracy A. "Boyd's O.O.D.A Loop and How We Use It." *Tactical Response*. Accessed December 21, 2019. https://www.tacticalresponse.com/blogs/library/18649427-boyd-s-o-o-d-a-loop-and-how-we-use-it.

Hollis, David. "Cyberwar Case Study: Georgia 2008." *Small Wars Journal* (January 6, 2011): 10.

Jonsson, Oscar, and Robert Seely. "Russian Full-Spectrum Conflict: An Appraisal After Ukraine." *The Journal of Slavic Military Studies* 28, no. 1 (January 2, 2015): 1–22.

Kaplan, Fred M. *Dark Territory: The Secret History of Cyber War*. First Simon & Schuster hardcover edition. New York: Simon & Schuster, 2016.

Katz, Yaakov. “And They Struck Them with Blindness.” *The Jerusalem Post*. Last modified September 29, 2010. Accessed October 29, 2019. https://www.jpost.com/Magazine/Features/And-they-struck-them-with-blindness.

Keizer, Gregg. “Russian Hacker ‘militia’ Mobilizes to Attack Georgia.” *Network World*. Last modified August 12, 2008. Accessed December 12, 2019. https://www.networkworld.com/article/2274800/russian-hacker--militia--mobilizes-to-attack-georgia.html.

Korns, Stephen W., and Joshua E. Kastenberg. “Georgia’s Cyber Left Hook.” *Army.Mil*. Last modified April 7, 2009. Accessed December 13, 2019. https://www.army.mil/article/19351/georgias_cyber_left_hook.

Kushner, David. “The Real Story Of Stuxnet.” *Institute of Electrical and Electronics Engineers (IEEE)Spectrum*. Last modified February 23, 2013. Accessed November 1, 2019. https://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet.

Leiner, Barry M., Vinton G. Cerf, David D. Clark, Robert E. Kahn, Leonard Kleinrock, Daniel C. Lynch, Jon Postel, Larry G. Roberts, and Stephen Wolff. “Brief History of the Internet.” *Internet Society*. Last modified 1997. Accessed September 17, 2019. https://www.internetsociety.org/internet/history-internet/brief-history-internet/.

LeMay Center for Doctrine. “Cyberspace Operations.” *Annex 3-12 - Cyberspace Operations*. Last modified November 30, 2011. Accessed December 31, 2019. https://www.doctrine.af.mil/Portals/61/documents/Annex_3-12/3-12-Annex-CYBERSPACE-OPS.pdf.

Liang, Qiao, and Wang Xiangsui. *Unrestricted Warfare*. Beijing: PLA Literature and Arts Publishing House, 1999.

Limnéll, Jarno, and The Society of Digital Information and Wireless Communication. “The Exploitation of Cyber Domain as Part of Warfare: Russo-Ukrainian War.” *International Journal of Cyber-Security and Digital Forensics* 4, no. 4 (2015)

Lookingglass Cyber Threat Intelligence Group. *Operation Armageddon: Cyber Espionage as a Strategic Component of Russian Modern Warfare*. Lookingglass, April 28, 2015. Accessed December 20, 2019. https://www.lookingglasscyber.com/wp-content/uploads/2015/08/Operation_Armageddon_Final.pdf.

Medvedev, Sergei A. “Offense-Defense Theory Analysis of Russian Cyber Capability.” Master’s Thesis, Naval Postgraduate School, 2015.

Melman, Yossi. “OUTSIDE THE BOX: Israel’s Strike on Syria’s Nuclear Plant.” *The Jerusalem Post*. Last modified April 6, 2018. Accessed October 29, 2019. https://www.jpost.com/Arab-Israeli-Conflict/OUTSIDE-THE-BOX-Israels-strike-on-Syrias-nuclear-plant-547870.

Miller, Christopher. “Ukraine Just Created Its Own Version of Orwell’s ‘Ministry of Truth.’” *Mashable*. Last modified December 2, 2014. Accessed December 23, 2019. https://mashable.com/2014/12/02/ukraine-ministry-of-truth/.

Naughton, John. “The Evolution of the Internet: From Military Experiment to General Purpose Technology.” *Journal of Cyber Policy* 1, no. 1 (May 8, 2016).

Navarria, Giovanni. “How the Internet Was Born: The ARPANET Comes to Life.” *The Conversation*. Accessed February 25, 2020. http://theconversation.com/how-the-internet-was-born-the-arpanet-comes-to-life-68062.

Office of the President of the United States. *National Cyber Strategy 2018*. Washington, DC: The White House, 2018.

Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics. *Defense Science Board Task Force on Cyber Deterrence*. Department of Defense, February 2017. Accessed September 5, 2019. https://www.acq.osd.mil/dsb/reports/2010s/dsb-cyberdeterrencereport_02-28-17_final.pdf.

Office of U.S. Cyber Command. “U.S. Cyber Command History.” *U.S. Cyber Command*. Accessed November 19, 2019. https://www.cybercom.mil/About/History/.

Opall-Rome, Barbara. “Declassified: How an Israeli Operation Derailed Syria’s Nuclear Weapons Drive.” *Defense News*. Last modified March 21, 2018. Accessed October 29, 2019. https://www.defensenews.com/global/mideast-africa/2018/03/20/just-declassified-how-an-israeli-operation-derailed-syrias-nuclear-weapons-drive/.

Orend, Brian, and Robert M. Martin. *The Morality of War*. Second edition expanded and Updated. Peterborough, Ontario, Canada ; Buffalo, New York, USA: Broadview Press, 2013.

Perkovich, George, and Ariel Levite, eds. *Understanding Cyber Conflict: 14 Analogies*. Washington, DC: Georgetown University Press, 2017.

Rácz, András. *Russia’s Hybrid War in Ukraine: Breaking the Enemy’s Ability to Resist*. Senior Research Fellow. Helsinki: The Finnish Institute of International Affairs, June 16, 2015.

Rukomeda, Roman. “Russia’s Hybrid War Against Ukraine: The Latest Developments and Trends.” *Norwegian Centre for Integrity in the Defence Sector (CIDS)*. Last modified September 28, 2018. Accessed December 20, 2019. https://cids.no/2018/09/28/russias-hybrid-war-against-ukraine-the-latest-developments-and-trends/.

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

Small Wars Journal. “Russia-Georgia: Early Take.” *Small Wars Journal*, n.d. Accessed December 17, 2019. https://smallwarsjournal.com/blog/russia-georgia-early-take.

Swearingen, Michael, Steven Brunasso, Joe Weiss, and Dennis Huber. “What You Need to Know (and Don’t) About the AURORA Vulnerability.” *Power: Business & Technology for the Golbal Generation Industry Since 1882*. Last modified September 1, 2013. Accessed November 19, 2019. https://www.powermag.com/what-you-need-to-know-and-dont-about-the-aurora-vulnerability/?printmode=1.

Tabansky, Lior. “The Current State of Cyber Warfare.” *Cyber Security Review*. Last modified May 2015. Accessed December 19, 2019. https://www.cybersecurity-review.com/articles/the-current-state-of-cyber-warfare/.

Tashev, Blagovest, Michael Purcell, and Brian McLaughlin. “Russia’s Information Warfare: Exploring the Cognitive Dimension.” *MCU Journal* 10, no. 2 (December 10, 2019): 129–147.

Thomas, Timothy. “Russia’s Military Strategy and Ukraine: Indirect, Asymmetric—and Putin-Led.” *The Journal of Slavic Military Studies* 28, no. 3 (July 3, 2015): 445–461.

Trevithick, Joseph. “Israel Details Long Secret Raid On Syrian Nuclear Reactor, Says It’s Willing To Do It Again.” *The Drive*. Accessed October 30, 2019. https://www.thedrive.com/the-war-zone/19492/israel-details-long-secret-raid-on-syrian-nuclear-reactor-says-its-willing-to-do-it-again.

US Department of Defense. *The Department of Defense Cyber Strategy*. Washington DC: Government Printing Office, 2015.

US Department of Defense, Joint Staff. *Joint Publication (JP) 3-12, Cyberspace Operations*. Washington DC: Government Printing Office, 2018.

White, Sarah P. *Understanding Cyberwarfare: Lessons from the Russia-Georgia War*. West Point, NY: Modern War Institute, March 20, 2018. Accessed December 10, 2019. https://mwi.usma.edu/understanding-cyberwarfare-lessons-russia-georgia-war/.

Williams, Timothy J. “Cyberwarfare and Operational Art.” Monograph, School of Advanced Military Studies, United States Army Command and General Staff College, 2017.

Woodford, Shawn. “The Russian Artillery Strike That Spooked The U.S. Army.” *Mystics & Statistics*, March 29, 2017. Accessed December 22, 2019. http://www.dupuyinstitute.org/blog/2017/03/29/the-russian-artillery-strike-that-spooked-the-u-s-army/.

Zetter, Kim. “An Unprecedented Look at Stuxnet, the World’s First Digital Weapon.” *Wired*, November 3, 2014. Accessed August 2, 2019. https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/.

———. *Countdown to Zero Day: Stuxnet and the Launch of the World’s First Digital Weapon*. First Edition. New York: Crown Publishers, 2014.

———. “How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History.” *Wired*, July 11, 2011. Accessed October 31, 2019. https://www.wired.com/2011/07/how-digital-detectives-deciphered-stuxnet/.