Nodes and Codes: The Reality of Cyber Warfare

A Monograph

by

Major Mark A. Cobos

United States Army

School of Advanced Military Studies

United States Army Command and General Staff College

Fort Leavenworth, Kansas

AY 2012-001

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 074-0188

1. AGENCY USE ONLY (Leave blank)	**2. REPORT DATE** 15 May 2012	**3. REPORT TYPE AND DATES COVERED** Monograph, July 2011 – May 2012

4. TITLE AND SUBTITLE
Nodes and Codes: The Reality of Cyber Warfare

5. FUNDING NUMBERS

6. AUTHOR(S)
Major Mark A. Cobos

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
School of Advanced Military Studies (SAMS)
201 Reynolds Avenue
Fort Leavenworth, KS 66027-2134

8. PERFORMING ORGANIZATION REPORT NUMBER

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

Command & General Staff College
731 McClellan Avenue
Fort Leavenworth, KS 66027-1350

10. SPONSORING / MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES

12a. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for Public Release; Distribution Unlimited

12b. DISTRIBUTION CODE

13. ABSTRACT ***(Maximum 200 Words)***

"Nodes and Codes" explores the reality of cyber warfare through the story of Stuxnet, a string of weaponized code that reached through a domain previously associated with information operations to bring about the physical, and potentially lethal, destruction of an adversary's critical infrastructure nodes. Stuxnet served as a proof-of-concept for cyber weapons and provided a comparative laboratory to study the reality of cyber warfare from the military powers most often associated with advanced, offensive cyber attack capabilities. The reality of cyber warfare holds significant operational implications for military forces armed with weapons platforms based on Network Centric Warfare Theory.

This monograph traces the open source story of Stuxnet through the trail of blogs and online articles that served as waypoints for the international digital detectives who deciphered the virus and determined its intentions. It provides a window to view the context of modern cyber warfare according to problematic attribution of actions in cyberspace, ambiguous concepts of cyber attack as acts of warfare, and trends of increasing vulnerability to supposedly sophisticated weapon systems and critical infrastructure.

Three case studies evaluate cyber policy, discourse, and procurement in the US, Russia, and China before and after Stuxnet to illustrate their similar, yet unique, realities of cyber warfare. Evidence suggests that all three nations are taking extraordinary measures to build cyber armies capable of exploiting adversary vulnerabilities in closed and open networks. A final section provides operational considerations for the employment of military force based on the reality of modern "cyber fires."

14. SUBJECT TERMS Cyber Warfare, Stuxnet, Computer Network Attack, Cyber Attack	**15. NUMBER OF PAGES** 58
	16. PRICE CODE

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

SCHOOL OF ADVANCED MILITARY STUDIES

MONOGRAPH APPROVAL

Major Mark A. Cobos

Title of Monograph: Nodes and Codes: The Reality of Cyber Warfare

Approved by:

__________________________________ Monograph Director
Matthew J. Schmidt, Ph.D.

__________________________________ Second Reader
Michael W. Snow, COL, LG

__________________________________ Director,
Thomas C. Graves, COL, IN School of Advanced
Military Studies

__________________________________ Director,
Robert F. Baumann, Ph.D. Graduate Degree
Programs

Disclaimer: Opinions, conclusions, and recommendations expressed or implied within are solely those of the author, and do not represent the views of the US Army School of Advanced Military Studies, the US Army Command and General Staff College, the United States Army, the Department of Defense, or any other US government agency. Cleared for public release: distribution unlimited.

Abstract

NODES AND CODES: THE REALITY OF CYBER WARFARE: by Major Mark A. Cobos, US Army, 58 pages.

"Nodes and Codes" explores the reality of cyber warfare through the story of Stuxnet, a string of weaponized code that reached through a domain previously associated with information operations to bring about the physical, and potentially lethal, destruction of an adversary's critical infrastructure nodes. Stuxnet served as a proof-of-concept for cyber weapons and provided a comparative laboratory to study the reality of cyber warfare from the military powers most often associated with advanced, offensive cyber attack capabilities. The reality of cyber warfare holds significant operational implications for military forces armed with weapons platforms based on Network Centric Warfare Theory.

This monograph traces the open source story of Stuxnet through the trail of blogs and online articles that served as waypoints for the international digital detectives who deciphered the virus and determined its intentions. It provides a window to view the context of modern cyber warfare according to problematic attribution of actions in cyberspace, ambiguous concepts of cyber attack as acts of warfare, and trends of increasing vulnerability to supposedly sophisticated weapon systems and critical infrastructure.

Three case studies evaluate cyber policy, discourse, and procurement in the US, Russia, and China before and after Stuxnet to illustrate their similar, yet unique, realities of cyber warfare. Evidence suggests that all three nations are taking extraordinary measures to build cyber armies capable of exploiting adversary vulnerabilities in closed and open networks. A final section provides operational considerations for the employment of military force based on the reality of modern "cyber fires."

Ultimately, the cyber domain represents an additional, and rapidly evolving, means by which actors can inflict violence and attempt to compel an adversary to their political will through Stuxnet-like attacks. This new phase of conflict, in which adversaries use cyber weapons to create physical destruction, defines the reality of cyber warfare and the expanding number of critical nodes vulnerable to malicious codes.

Table of Contents

Introduction

What is the reality of warfare in the cyber domain? According to James Mulvenon, founder of the Cyber Conflict Studies Association and prominent Chinese military expert, "It's 1946 in cyber. We have these potent new weapons, but we don't have all the conceptual and doctrinal thinking to support those weapons or any kind of deterrence."[1] If Mulvenon is correct, and potent new cyber weapons indicate a shift in the character of warfare analogous to the introduction of nuclear weapons, then what evidence indicates the development of corresponding policy, strategy, military doctrine, or organizations to support a shifting reality of cyber warfare?

The Stuxnet attack is an integral component of this research because it is the first proof of concept to demonstrate that acts of cyber warfare can destroy physical, rather than virtual, targets. The former head of the United States (US) National Security and Central Intelligence Agencies, retired General Michael Hayden, captured the essence of Stuxnet during an interview with *60 Minutes* when he said, "We have entered into a new phase of conflict in which we use a cyber weapon to create *physical* destruction."[2] The five permanent members of the United Nations (UN) Security Council, encompassing the nations with the top five defense budgets, reacted to Stuxnet by signaling their own intentions to develop robust offensive cyber attack capabilities.

This monograph explores the reality of warfare in the cyber domain through the story of Stuxnet and the context in which the attack occurred. Three case studies provide a comparative laboratory to identify changes to the discourse on cyber warfare from the US, Russia, and China, the major military powers most often associated with cyber attack.[3] A final section demonstrates

[1] Mark Clayton, "A US Cyberwar Doctrine? Pentagon Document Seen as First Step, and a Warning," *The Christian Science Monitor*, May 31, 2011.

[2] Michael Hayden, interview by Steve Kroft, *60 Minutes*, CBS, March 4, 2012. Hayden emphasized the word "physical" to describe Stuxnet's destructive capability, italicized in the quote.

[3] Kathryn Stevens and Larry K. McKee Jr., "International Cyberspace Strategies," National Security Cyberspace Institute, http://www.nsci-va.org/WhitePapers/2010-06-28-InternationalCyberspaceStrategies-Stephens-McKee.pdf (accessed February 12, 2012). See also Stockholm

the operational implications of a transformed reality of war and recommends modifications to the current US warfighting theory, Network Centric Warfare.

In order to identify changes in the discourse on cyber warfare, this monograph will analyze the unclassified, open-source literature on cyber warfare published by the US, Russia, and China, as well as academic publications around the world, before and after the Stuxnet attack. It will consider major policy documents and statements, changes in military budgets and procurement, and changes in military doctrine, organization, and training. This monograph will not address or assess responsibility for the Stuxnet attack or speculate about the motivation of the actors involved.[4]

The Story of Stuxnet

The purpose of this section is to tell the story of Stuxnet from the forensic analysis of its code and the logic it used to destroy critical industrial infrastructure in Iran in order to facilitate understanding of the environmental context in which it operated and changes to the discourse on cyber warfare. Analyses of the open-source facts surrounding Stuxnet provide a framework of understanding into why and how the world's major military powers responded to the most-

International Peace Research Institute (SIPRI), "Military Spending and Armaments," *SIPRI Yearbook 2011*, http://www.sipri.org/yearbook/2011/files/SIPRIYB1104-04A-04B.pdf (accessed March 10, 2012). According to Lewis and a McAfee report cited by Stevens and McKee, "five militaries (US, Russia, China, Israel, and France) have advanced cyber-attack capabilities and at least another 30 countries intend to acquire them." SIPRI ranks the US, Russia, China, and France as four of the top five defense spending and exporting countries. Therefore, this monograph considers the discourse from the US, Russia, and China, excluding France due to expected similarities with their NATO ally, the US, and due to space restrictions.

[4] John A. Lynn, *Battle: A History of Combat and Culture* (Boulder: Westview Press, 2003), 331-337. The inspiration for this monograph derives from *Battle*, in which Lynn attributes World War I's stalemate and massive casualty figures to a gap between the discourse on war embraced by political and military leaders (demonstrated through outdated policy, theory, and doctrine) and the reality of warfare in 1914 (dictated by innovation, technology, and industrialization). Lynn demonstrates the power of discourse through system dynamics whereby recognition of war's reality leads to new policies, theories, and doctrines, adjusting the discourse on war and leading to a reformed, perfected reality of war. If Lynn's theory is true, then what evidence demonstrates changes in the reality of modern warfare in the cyber domain or changes to the discourse on cyber warfare through policy, military theory, or the guidelines to military action codified in doctrine? How are states using the latest technological innovations as violent instruments of policy? Do new, violent instruments of policy influence the discourse on war?

exposed cyber weapon to date. Stuxnet is an evolving narrative of sophisticated attack through the cyber domain; much of its plot remains classified or unknown and its ending may not yet be complete. However, the public, open-source version of the story provides insight into the methodology, logic, and means utilized by Stuxnet's creators, and the clues they left behind to shape the discourse on the weaponization of the cyber domain.

Relevant Literature/Primary Sources

Since the initial discovery of Stuxnet in June 2010, a legion of journals, magazines, and bloggers have opined on the composition and significance of the virus, and most are undoubtedly informative. However, this section will attempt to clear away much of the noise and opinion to tell the story through the lenses of the five individuals most responsible for the initial public detection, forensic analysis, and characterization of the intent of Stuxnet. The five primary sources represent five different nationalities and all work for multinational corporations, un-beholden to the authority of any single government. This section will also cite a handful of technical journals and blogs most helpful to prospective researchers looking for concise explanations of otherwise complex information.[5]

Sergey Ulasen was the head of the antivirus division of VirusBlokAda, a small computer security company in Minsk, when he uncovered the malware that would become Stuxnet. He published the details of his discovery on the Wilders Security Forum and on the VirusBlokAda blog site on June 17, 2010. Ulasen, now working for the giant cyber security firm Kaspersky Labs, conducts regular interviews on Stuxnet.[6]

[5] Many of the sources used in this monograph come from web logs (blogs). The most relevant information on the story of Stuxnet exists in the blogosphere, the medium chosen by Stuxnet detectives to collaborate, communicate, and publish their work.

[6] Sergey Ulasen, "Rootkit.TmpHider," Wilders Security Forum Blog, entry posted June 17, 2010, http://www.wilderssecurity.com (accessed October 19, 2011). See also Sergey Ulasen, "Rootkit.TmpHider," VirusBlokAda Blog, entry posted June 17, 2010, http://anti-virus.by/en/tempo.shtml

A trio of malware specialists from the Symantec Security Response Directorate, Liam O Murchu, Eric Chien, and Nicolas Falliere, led the months-long effort to decipher and reverse-engineer Stuxnet. Their approach, techniques, and investigative research comprise the "W32.Stuxnet Dossier," published on the Symantec Security Response blog.[7] The persistent presence of the Symantec Security Response Directorate in almost every chapter of the Stuxnet story, coupled with their enduring service as a hub of information sharing for those willing to contribute to the public decoding of the malware, make the trio authoritative primary sources.

Ralph Langner, a German researcher and expert in industrial control systems, is the fifth and final primary source used in this section. Langner solved a major piece of the puzzle when he personally identified Stuxnet's intended target, Siemens supervisory-control and data acquisition systems (SCADA) used in Iranian uranium enrichment facilities. Langner published his revelation, methodology, and logic on his blog beginning September 16, 2010.[8]

Forensic Analysis

In June 2010, a recent graduate of the Belorussian State Technical University and anti-virus programmer for VirusBlokAda named Sergey Ulasen noticed arbitrary computer reboots and "blue-screens-of-death (BSODS)" on a customer's network near Tehran.[9] Ulasen suspected

(accessed October 19, 2011). See also Sergey Ulasen, interview by Eugene Kaspersky, November 2, 2011, "The Man Who Found Stuxnet – Sergey Ulasen in the Spotlight," Nota Bene Blog, entry posted November 2, 2011, http://eugene.kaspersky.com/2011/11/02/the-man-who-found-stuxnet-sergey-ulasen-in-the-spotlight/ (accessed November 17, 2011).

[7] Nicolas Falliere, Liam O Murchu, and Eric Chien, *W32.Stuxnet Dossier Version 1.4* (Cupertino, California: Symantec Security Response, 2011), 1-4.

[8] Ralph Langner, "September 16, 2010," Stuxnet Logbook Blog, entry posted September 16, 2010, http://www.langner.com/en/2010/09/16/stuxnet-logbook-sep-16-2010-1200-hours-mesz/#more-217 (accessed September 1, 2011).

[9] Lincoln Spector, "What to Do When Windows Gets Really Messed Up," PC World Blogs: Answer Line, entry posted May 5, 2008, http://www.pcworld.com/article/145266/what_to_do_when_windows_gets_really_messed_up.html (accessed September 2, 2011).

that the anomalies were the result of conflicts between computer applications but decided to investigate additional computers on the customer's network by gaining remote access to an infected computer.[10]

Within a few days, Ulasen's team found that the virus consisted of a complex code, sophisticated rootkit technologies, a Microsoft Windows© zero-day vulnerability, and two stolen digital certificates from respected Taiwanese companies.[11] A rootkit is code that allows privileged access to a computer or a network while hiding its presence from administrators, allowing an attacker to mask an intrusion as an authorized function.[12] Zero-days are original vulnerabilities in code unknown to the software developer. They are exceptionally rare, difficult to find in software produced by reliable vendors like Microsoft, and sell in the range of $50,000 to $500,000 on the black market. The stolen security certificates came from RealTek Semiconductor and JMicron Technology, headquartered in the same business park in Taipei.[13] On July 7, 2010, Ulasen contacted Microsoft to report the zero-day vulnerability and published his discovery, while antivirus researchers around the world took samples of the malware to deconstruct and assess.[14]

Among the researchers who continued to examine Stuxnet was the operations manager for Symantec Security Response, Liam O Murchu, a 33-year old Irishman enamored by the virus'

[10] Ulasen, interview.

[11] Ibid.

[12] Dennis Elser and Micha Pekrul, "Inside the Password-Stealing Business: The Who and How of Identity Theft," McAfee Labs Research Report, http://www.mcafee.com/us/resources/reports/rp-inside-password-stealing-biz.pdf (accessed September 2, 2011), 7.

[13] Kim Zetter, "How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History," Wired Threat Level Blog: Privacy, Crime, and Security Online, entry posted July 11, 2011, http://www.wired.com/threatlevel/2011/07/how-digital-detectives-deciphered-stuxnet/all/1 (accessed September 1, 2011). "Out of more than 12 million pieces of malware that antivirus researchers discover each year, fewer than a dozen use a zero-day exploit."

[14] Microsoft Malware Protection Center, "Trojan: WinNT/StuxnetB, July 7, 2010," Threat Research and Response, entry posted July 7, 2010, http://www.microsoft.com/security/portal/threat/Encyclopedia/Entry.aspx?Name=Trojan%3AWinNT%2FStuxnet.B (accessed October 19, 2011). Microsoft named the virus Stuxnet by combining file names (.stub and MrxNet.sys). See also Ulasen, Wilders Security Forum Blog and VirusBlokAda Blog.

size, complexity, and sophistication. After reverse-engineering the first five kilobytes of the 500k code, O Murchu realized that the virus' compartmentalized construction, hidden functions, and encrypted use of ghost files was unlike any known malware, requiring thorough interrogation by a dedicated team of forensic cyber investigators.[15] Eric Chien, technical director of Symantec Security Response, and Nicolas Falliere, a senior code analyst at Symantec's Paris office, joined O Murchu and the trio spent the next several months piecing together the Stuxnet puzzle.[16]

The Symantec team's initial assessment was that Stuxnet represented a form of high tech industrial espionage, an increasingly common form of stealing valuable proprietary information. However, as they continued to deconstruct the code, they found that Stuxnet "phoned home" to allow the attackers to update infected machines and remotely determine whether an infected machine ran Siemens Simatic WinCC Step7 software.[17] Chien and O Murchu mapped the geographical locations of computers infected with Stuxnet, finding that 22,000 of 38,000 infections were in Iran, with only 217 Iranian computers reporting Step 7 software.[18]

The team found three additional Windows zero-day vulnerabilities in the Stuxnet code: a print spooler vulnerability that allowed the virus to spread across internally networked machines that share a common printer and two vulnerabilities in a keyboard file and task scheduler file that

[15] Liam O Murchu, "W32.Stuxnet Variants," Symantec Security Response Blog, entry posted July 28, 2010, http://www.symantec.com/connect/blogs/w32stuxnet-variants (accessed September 2, 2011). See also Zetter.

[16] Nicolas Falliere, Liam O Murchu, and Eric Chien, "W32.Stuxnet Dossier, Version 1.4," Symantec Security Response Blog, entry posted February 3, 2011, http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf (accessed September 2, 2011), 55.

[17] Falliere, O Murchu, and Chien, 5.

[18] Zetter. The Symantec team discovered the numbers of infected computers and their geographical location by intercepting the data and time stamps that the attackers expected to receive. They assessed a high degree of collateral damage to computers and servers around the world, classifying the attack as a high risk operation.

provided the attackers complete, unacknowledged control of a machine.[19] Falliere learned that Stuxnet remained dormant inside of a system unless that system used a device called a Programmable Logic Controller (PLC), used for precision control of industrial motors. The team recreated the attack, learning that it originally hit five organizations in Iran nearly simultaneously with slightly different strains of the virus between June and July 2009.[20] The Security Response Directorate's August 6, 2010 blog warned that Stuxnet represented a targeted attack capable of physically destroying industrial infrastructure by hijacking the PLC in Siemens industrial control systems.[21]

Ralph Langner, a German expert in Siemens industrial control systems picked the information off the Symantec blogs, intent on discovering exactly what kind of device the code intended to destroy. Langner found that Stuxnet contained an embedded dossier targeting a specific technical configuration. If the infected system failed to match the proscribed configuration, Stuxnet became dormant and moved on until it found a target that precisely matched its embedded dossier. Within three weeks, Langner openly speculated that Stuxnet was a precision weapon designed to sabotage Iran's Natanz Uranium Enrichment Facility.[22]

[19] Liam O Murchu, "Stuxnet Using Three Additional Zero-Day Vulnerabilities," Symantec Security Response Blog, entry posted September 14, 2010, http://www.symantec.com/connect/blogs/stuxnet-using-three-additional-zero-day-vulnerabilities (accessed 02 September 2011).

[20] Falliere, O Murchu, and Chien, 1-2, 9.

[21] Nicolas Falliere, "Stuxnet Introduces First Known Rootkit for Industrial Control Systems," Symantec Security Response Blog, entry posted August 6, 2010, http://www.symantec.com/connect/blogs/stuxnet-introduces-first-known-rootkit-scada-devices (accessed 15 September 2011). The Symantec trio publicly compared Stuxnet's destructive capability to an alleged, and unsubstantiated, 1982 CIA digital attack on a Siberian pipeline that resulted in an explosion one-fifth the size of the atomic bomb that fell on Hiroshima.

[22] Ralph Langner, interview by Dale Peterson, December 15, 2010, "Ralph Langner – Stuxnet Interview," http://www.digitalbond.com/2010/12/15/december-podcast-ralph-langner-stuxnet-interview/ (accessed November 3, 2011). See also Ralph Langner, "September 16, 2010," Stuxnet Logbook Blog, entry posted September 16, 2010, http://www.langner.com/en/2010/09/16/stuxnet-logbook-sep-16-2010-1200-hours-mesz/#more-217 (accessed September 1, 2011).

Langner went public with his discoveries in the blogosphere, publishing a technical roadmap that detailed Stuxnet's known path from initial infection in June 2009 through the fall of 2010. Langner argued that publicizing the scope and effects of Stuxnet raised awareness of vulnerable civil infrastructure throughout the world that rely on PLCs or Siemens controllers. However, his characterization of Stuxnet as a precision weapon employed by a state actor openly inferred exposure of a covert state-run operation.[23]

Langner's story became world news headlines despite his speculative claims concerning the origin of the attack. The public became enthralled with the story and with infrastructure security, fascinated by the prospects of attacking industrial control systems on closed networks. Finally, in November 2010, after deciphering all but two small encrypted Stuxnet files, the Symantec team published conclusive evidence that Stuxnet intended to destroy nuclear centrifuges at Natanz.[24] The open-source story of Stuxnet through 2010 provides an intriguing narrative of a savvy attack and shrewd detective work performed by software experts and hobbyists, employed by multinational corporations and small security firms, collaborating in the blogosphere from offices and living rooms around the world to expose the most sophisticated cyber weapon to date.

When evaluated within the context of the attack, Stuxnet exposes shortcomings in current theory, doctrine, and international legal opinions as well as vulnerabilities in sophisticated weaponry, ultimately representing a great leap forward for warfare in the cyber domain. As John Lynn noted in *Battle*, history provides many examples of shifts in the reality of warfare that affect

[23] Zetter.

[24] Falliere, O Murchu, and Chien, 43-48. Stuxnet targeted centrifuges constructed in cascades of 164. After lying dormant in a centrifuge modulator for about two weeks, Stuxnet would attack by increasing converter frequency from 1,064 Hertz to 1,410 Hertz for 15 minutes. The code would lie dormant for 27 days before dropping the frequency to down to 2 Hertz for 50 minutes. Stuxnet would lie dormant for an additional 27 days before repeating its attack.

changes in the discourse on warfare through new theory and doctrine.[25] The context of the Stuxnet attack provides insight to the changing reality of warfare in the cyber domain, prompting further analysis into reciprocating changes to the discourse on cyber warfare by major military powers.

The Context of the Attack

Many elements of strategic context contributed to the response of major military powers to Stuxnet. Variables consisting of International Atomic Energy Agency inspections, compliance with the Nuclear Non-Proliferation Treaty, diplomatic rhetoric, economic sanctions, regional conflicts on Iran's eastern and western borders, and the potential for escalation of conflict provide context for understanding why Stuxnet occurred.[26] However, such analysis is beyond the scope of this monograph. Rather, three contextual elements directly facilitate an understanding of how the Stuxnet attack happened: problematic attribution, ambiguity in the terminology associated with cyber warfare, and trends of increased vulnerability in supposedly sophisticated weaponry and infrastructure. Analysis of these three factors provides a framework for understanding the response to Stuxnet from major military powers.

First, the Stuxnet worm bored into the industrial controllers at Natanz under conditions that made attributing a sophisticated cyber attack to a specific actor difficult and, unlike an attack through conventional weapons, problematic for both the attacker and the recipient. As soft power advocate Joseph Nye notes, the proliferation of information on networks across territorial jurisdictions promotes the diffusion of power from governmental functions to virtual

[25] Lynn, 331-341.

[26] Zetter. See also The United Nations, "Treaty on the Non-Proliferation of Nuclear Weapons," UN Office for Disarmament Affairs, http://www.un.org/disarmament/WMD/Nuclear/NPT.shtml (accessed January 8, 2012). The Nuclear Non-Proliferation Treaty, ratified or acceded by all states except India, Israel, and Pakistan, established the principles of non-proliferation (Articles I and II), disarmament (Article III), and the right to pursue peaceful use of military technology (Article IV). Iran ratified the NPT in 1970.

communities, providing little distinction between governmental and transnational actors, aggressors and bystanders.[27] Nye points to the combination of an exponential increase in internet users since 1992 with a lack of entry or control barriers that create an uncontested environment in large portions of cyberspace. Uncontested nodes, linked across jurisdictions in the cyber domain, provide concealment to cyber attackers and mask their actions, thereby decreasing the probability of attributing specific actions to actors.[28]

In his most recent book, *Cyber War*, former US Cyber Czar Richard Clarke provides a vignette based on simulations run by the Department of Homeland Security and other US governmental organizations. In the scenario, a destructive cyber weapon similar to Stuxnet strikes industrial controllers in the US, crippling electrical grids and communications capacity, creating confusion within governmental institutions and delaying a unified response, while American cyber specialists struggle to attribute the origin of the attack.[29] Although some consider a complex vignette from a former US cyber security czar to be alarmist in nature, there is little argument that the Stuxnet attack occurred within a context of problematic, or at least substantially delayed, attribution.[30]

[27] Joseph S. Nye Jr, *The Future of Power* (New York: PublicAffairs, 2011), 113-114.

[28] Ibid., 123-125. See also William S. Lynn III, interview by Melissa Lee, May 26, 2011, "Code Wars: America's Cyber Threat," CNBC. See also Admiral Lord West, interview by Rob Densmore, April 14, 2011, "The Threat is Imminent: Admiral Lord West Talks About Cyber Terrorism in the UK," Defense IQ, http://www.defenceiq.com/defence-technology/videos/the-threat-is-imminent-admiral-lord-west-talks-abo/ (accessed December 20, 2011). Former US Deputy Secretary of Defense William Lynn and British Security Minister Admiral Lord West agree that uncontested nodes in cyberspace complicate definitive attribution of cyber weapons to their origin and oftentimes the paths they take between nodes.

[29] Richard A. Clarke and Robert K. Knake, *Cyber War: The Next Threat to National Security and What To Do About It* (New York: Harper Collins, 2010), 64-68.

[30] Michico Kakutani, "The Attack Coming from Bytes, Not Bombs," The New York Times Book Reviews, http://www.nytimes.com/2010/04/27/books/27book.html?ref=bookreviews (accessed January 14, 2012). See also Jeff Stein, "Book Review: 'Cyber War' by Richard Clarke," The Washington Post Book Reviews, http://www.washingtonpost.com/wp-dyn/content/article/2010/05/21/AR2010052101860.html (accessed January 14, 2012).

The cyber domain's multifaceted configuration of interconnected, unregulated nodes and chaotic connectivity require equally complex and sophisticated methods to attribute an attack to an attacker. Therefore, disclosure of attribution by the attacked party can also provide attackers with critical feedback on the effectiveness of their weapon or identify supplementary vulnerable networked nodes in defense or infrastructure systems. Additionally, attackers investing considerable resources into sophisticated cyber weapons have little to gain by providing indications of their capacity to conduct offensive attack or to expose vulnerabilities in software that, once patched, no longer present a target for future attack.[31] Given this context, definitive public attribution for the Stuxnet attack may not have been in the interests of any state party involved, including the Iranians. The inability or reluctance to attribute an attack to a specific actor represents a shift in the reality of warfare.

Second, ambiguous definitions and opinions on cyber attack and acts of warfare in the cyber domain provided the Stuxnet attackers with an opportunity to destroy an adversary's material and shape the discourse of future cyber warfare without significant risk of escalation or retaliation from Iran in response to Stuxnet. Despite numerous predictions in the international academic and military communities warning of impending cyber warfare, no authoritative body acting on behalf of a major military power delivered a comprehensive definition of acts of war in the cyber domain prior to Stuxnet. This ambiguity in terminology ultimately led to elastic legal restrictions and allowed the attackers to operate with initiative from a legal sanctuary, while constricting the response options of the attacked party.

In November 2008, the NATO Cooperative Cyber Defense Centre of Excellence (CCDCOE) published an inconclusive legal review entitled "International Cyber Incidents: Legal

[31] Kaspersky Labs, "Cyberthreat Forecast for 2012," http://www.kaspersky.com/images/Kaspersky%20report-10-134377.pdf (accessed January 2, 2012). Kaspersky Labs, a software security industry leader, contends that cyber weapons like Stuxnet are highly unique, limited opportunity codes designed for a specific time and purpose.

Considerations." The NATO report acknowledged ambiguous cyber terminology and discussed the applicability of the Law of Armed Conflict (LOAC) with respect to Russian cyber attacks against Georgia and Estonia, but stopped well short of recommending solutions to the cyber "gaps" in international treaties.[32] In 2009, US Air Force General Kevin P. Chilton, Commander of the US Strategic Command, proclaimed, "the Law of Armed Conflict will apply" to the cyber domain.[33] A 2009 article in the *Berkeley Journal of International Law* thoroughly examined existing treaties and other legal frameworks for establishing definitions of cyber aggression, but acknowledged fundamental difficulties in defining the boundaries of cyber aggression and in extending the assumptions in international law regarding self-defense and the use of force to the cyber domain.[34]

The Prussian war theorist Carl von Clausewitz offered what remains the most widely recognized and complete theory of war, providing a critical resource to evaluate Stuxnet as an act of war. In the first chapter of *On War*, Clausewitz defines war as "an act of force to compel our enemy to do our will."[35] Clausewitz's definition consists of three principal requirements of war: *gewalt*, *zweck*, and *ziel* in his original German text.[36] An action must be violent (*gewalt*) or potentially violent, instrumental as a means to an end (*zweck*), and part of a greater political purpose to compel an adversary (*ziel*). Jack Gibbs, a noted deterrence theoretician, supports

[32] North Atlantic Treaty Organization, "International Cyber Incidents: Legal Considerations," NATO Cooperative Cyber Defense Center of Excellence, http://www.ccdcoe.org/publications/books/legalconsiderations.pdf (accessed February 11, 2012), 102-103.

[33] Jeff Schogol, "Official: No Options 'Off the Table' for US Response to Cyber Attacks," *Stars and Stripes*, May 8, 2009.

[34] Scott Shackelford, "From Nuclear War to Net War," *Berkeley Journal of International Law* no 27.1 (February 2009), http://www.boalt.org/bjil/docs/BJIL27.1_Shackelford.pdf (accessed February 12, 2012), 195.

[35] Karl von Clausewitz, *On War*, ed. Michael Howard and Peter Paret (Princeton: Princeton University Press, 1976), 75.

[36] Antulio J. Echevarria II, *Clausewitz and Contemporary War* (New York: Oxford University Press, 2007), 64-65.

Clausewitz’s three requirements and points out that fear and the threat of violence are war’s instruments, or means, to force an adversary to accept the will of the attacker, based on a political purpose.[37]

As Ralph Langner demonstrated, Stuxnet was most likely an instrument of policy by a state actor to physically destroy Iran’s centrifuges and disrupt or delay that nation’s ability to produce enriched uranium, thereby satisfying Clausewitz’s second and third requirements for acts of war. However, many historians and war theorists, including Thomas Rid of King’s College in London, argue that no public evidence exists to suggest that either Stuxnet or any other cyber attack to date is directly responsible for a human death. Rid points out that while Richard Clarke’s vignettes in *Cyber War* predict substantial violence and collateral damage associated with potential cyber attacks on critical infrastructure, his predictions remain theoretical and not historical.[38] To Rid’s credit, there is no undisputed, open-source evidence to either confirm or deny that the destruction of Iranian centrifuges directly caused human casualties. Nonetheless, as noted in the *Yale Journal of International Law* in the spring of 2011, Stuxnet “was probably used as a substitute for military options” and pushed antagonists to use the malware to destroy centrifuges in a manner similar to kinetic military force.[39] Furthermore, international inspectors verified that Stuxnet destroyed hundreds of nuclear centrifuges, essentially heavy containers that spin highly toxic, corrosive, and radioactive uranium gas (Uranium Hexafluoride) at over 100,000

[37] Jack P. Gibbs, “Deterrence Theory and Research,” in *Law as a Behavioral Instrument,* ed. Gary Melton, Laura Nader, and Richard A. Dienstbier, (Lincoln: University of Nebraska Press, 1986), 87.

[38] Thomas Rid, “Cyber War Will Not Take Place,” *Journal of Strategic Studies* 1-28 (October 2011): 2, 6, 25.

[39] Matthew C. Waxman, “Cyber Attacks and the Use of Force: Back to the Future of Article 2(4),” *Yale Journal of International Law* no. 36.2 (Spring 2011), http://www.yjil.org/docs/pub/36-2-waxman-cyber-attacks-and-the-use-of-force.pdf (accessed July 12, 2012), 443.

rotations per minute.[40] Therefore, it is reasonable to conclude that the Stuxnet attack held the potential for violence.

Georgetown University professors Christopher Joyner and Catherine Lotrionte identified a lack of specificity within modern international law to distinguish "which state actions are permissible as normal computer-generated trans-border data flow from those cyber activities that may qualify as an armed attack against a state." Joyner and Lotrionte suggest that Article 2(4) of the United Nations Charter uses the terminology "use of force" instead of "acts of war" to describe prohibited behavior in international relations between member states in order to include hostile acts that fall short of the common threshold for belligerency. The study concludes by acknowledging the seriousness of ambiguous opinions concerning acts of "armed attack" in the cyber domain and recommending the reevaluation of acceptable definitions of warfare in order to maintain the relevancy of international law.[41] Given the vagueness of the legal threshold for which a cyber attack constitutes an act of war, one can understand how the Stuxnet attackers outmaneuvered the Iranians, taking away conventional retaliatory options and leaving them without a legal charge.

US joint doctrine, both before and after the Stuxnet attack, failed to provide terms that adequately address an attack through networked nodes resulting in the physical destruction of material property or infrastructure. The 2001, 2007, 2010, and 2011 editions of *Joint Publication 1-02: Department of Defense Dictionary of Military and Associated Terms* contain consistent

[40] Zetter. See also Global Security, "Gas Centrifuge Uranium Enrichment," Weapons of Mass Destruction, http://www.globalsecurity.org/wmd/intro/u-centrifuge.htm (accessed March 3, 2012). See also Marshall Brain, "What's a Uranium Centrifuge?" HowStuffWorks, http://science.howstuffworks.com/uranium-centrifuge.htm (accessed March 23, 2012).

[41] Christopher C. Joyner and Catherine Lotrionte, "Information Warfare as International Coercion: Elements of a Legal Framework," *European Journal of International Law* 12, no. 5 (2001): 845, 865. Joyner was Professor of International Law in Georgetown University's Department of Government. Lotrionte was the Assistant General Counsel at the Central Intelligence Agency and Adjunct Professor, National Security Studies Program, Georgetown University. See also The United Nations, "Charter of the United Nations," http://www.un.org/en/documents/charter/chapter1.shtml (accessed January 14, 2012).

definitions of computer network attack (CNA), and electronic attack (EA).[42] Like Stuxnet, CNA includes "actions taken through the use of computer networks to disrupt, deny, degrade, and destroy." However, the definition proceeds to limit the targets of CNA to "information, computers, or networks." Prior to Stuxnet, cyber related attacks targeted information, computers, and networks, but Stuxnet specifically targeted uranium centrifuges set in cascades of 164 and their associated nuclear material at Natanz, and did not attempt to disrupt, deny, degrade, or destroy computers or networks.[43]

Like the joint definition of EA, Stuxnet intended "to attack personnel, facilities, or equipment with the intent of degrading, neutralizing, or destroying enemy combat capability." However, the definition begins by limiting the delivery mechanisms of EA to "the use of electromagnetic energy, directed energy, or anti-radiation weapons," while Stuxnet traveled along networked nodes, never radiating directed energy. Stuxnet seemed to combine the first half of the definition of CNA with the second half of the definition of EA, but clearly represented a new reality with respect to cyber terminology.

Because of the depth of ambiguity concerning cyber attack as an instrument of war, the Stuxnet attack may have set a precedent in the same manner that the launch of Sputnik established a legal precedent concerning space and extension of sovereign airspace prior to 1957. Amid differing legal opinions on the status of satellite over-flights, the Soviet Union launched Sputnik into an orbit that crossed over every nation within 65 degrees of the equator. Over the

[42] Joint Publication (JP) 1-02, *Department of Defense Dictionary of Military and Associated Terms* (12 April 2001, As Amended Through 13 June 2007) (Washington, D.C.: US Government Printing Office) 111, 176. See also JP 1-02, *Department of Defense Dictionary of Military and Associated Terms* (8 November 2010, As Amended Through 15 October 2011) (Washington, D.C.: US GPO) 67, 109.

[43] David Albright, Paul Brannan, and Christina Walrond, "Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant?" Institute for Science and International Security (ISIS), http://isis-online.org/isis-reports/detail/did-stuxnet-take-out-1000-centrifuges-at-the-natanz-enrichment-plant/, December 22, 2010 (accessed January 15, 2012).

next several decades, a multitude of conventions, agreements, and treaties matured the concepts that became International Space Law, based on the precedent and new reality set by Sputnik.[44]

World-renowned telecom executive Rene Obermann appropriately labeled Stuxnet the "digital Sputnik moment." Sputnik demonstrated the risk associated with the weaponization of the space domain, alerted societies to the potentially serious consequences and collateral damage that accompany a new type of threat, and unleashed an expensive space race between the world's major military powers. The launch of Sputnik eventually helped to resolve ambiguous terminology and legal opinions over the use of space to enable acts of war in favor of a handful of major military powers able to afford the expense of developing sophisticated space capabilities. Likewise, Stuxnet powerfully demonstrated the potential for the weaponization of the cyber domain and exposed the vulnerability of industrial and defense infrastructure throughout the world to a new type of threat.[45] Warfare in the cyber domain, unlike the space domain, remains cloaked in ambiguous terminology and legal opinions although changes in the discourse on cyber war began to take shape shortly after Stuxnet became public. The new reality of cyber warfare demonstrated by Stuxnet also hastened a nascent cyber race among the world's major military powers.

Third, a trend of increasing digitization in weaponry and critical infrastructure corresponds to an increase in the number of nodes vulnerable to attack by malicious codes. Locating the point of manufacture and the increasing quantity of computer chips, automated processors, and supervisory control mechanisms of major weapon and infrastructure systems is beyond the scope of this research. However, the available data suggests that formerly analog systems are now digital, complex, and dependent on data obtained from networked systems.

[44] S. Neil Hosenball, "Current Issues of Space Law Before the United Nations," *Journal of Space Law* 2 (1974): 5.

[45] Rene Obermann, "Digital Sputnik Moment," *The New York Times Opinion Pages*, February 27, 2011.

Components of modern, networked weapons systems contain millions of lines of code constructed by manufacturers with global supply chains. Within this context, the Stuxnet attack underscores the reality of a target-rich environment and an expanding number of potential targets on vulnerable, networked nodes.

According to the SIPRI's Arms Transfers Database, the US and Russia exported more arms every year from 1992-2010, in terms of dollar value, than all other nations combined. The US was also the fifth largest arms importer in 2010, demonstrating the multi-dimensional flow of sophisticated weaponry across borders.[46] Therefore, a cross section of weapons sales and purchases by the US and Russia should reasonably indicate any existing trend toward digital, networked weapons and military information systems.

Air defense systems exported by the US and Russia with advanced radar and target acquisition components demonstrate the increasingly digital and network-dependent nature of modern weaponry. According to SIPRI, American and Russian sales of upgraded air defense systems and associated components rose sharply in 1996 and maintained a growing trend through 2010.[47] Sales of advanced avionics systems, upgraded software, and guided missiles also rose, indicating that weapon importers look to replace analog systems with digital, networked systems.

The increased demand for networked, integrated air defense systems and weapons platforms are examples of a larger trend toward weaponry and military information systems built by manufacturers that leverage global supply chains. Global supply chains introduce increased risk to the integrity of electronic components and accompanying software, which often consist of

[46] Stockholm International Peace Research Institute, "Arms Suppliers/Recipients Database," http://armstrade.sipri.org/armstrade/page/toplist.php (accessed January 2, 2012).

[47] Stockholm International Peace Research Institute, "Arms Transfers Database," http://armstrade.sipri.org/armstrade/page/trade_register.php (accessed January 2, 2012).

millions of lines of code programmed in large part by automated processes.[48] Circuit boards, chips, software, and systems built on production lines around the world become integral components to weapon systems, creating vulnerabilities that adversaries look to exploit. Therefore, the trend of sophisticated weapon components developed and assembled by increasingly global supply chains represent an increase in the vulnerability of modern weapon systems to attack or sabotage.

Two articles posted on the "Spectrum: Inside Technology" blog sponsored by the Institute of Electrical and Electronics Engineers prior to Stuxnet demonstrate the trend of increasingly sophisticated software to support advanced war fighting platforms. Robert Charette showed that the avionics systems in the F-22 Raptor and the F-35 Joint Strike Fighter, both fifth generation fighter jets, contain about 1.7 million and 5.7 million lines of code respectively. The avionics in Boeing's 787 Dreamliner require approximately 6.5 million lines of code while the current S-Class Mercedes Benz requires over 20 million lines of code executed on almost 100 microprocessor-based electronic control units.[49] In contrast, SCADA expert Ralph Langner demonstrated that malware targeting supervisory control systems and programmable logic controllers could be a small as four lines of programming code, discretely hidden on a fraction of a single computer chip, manufactured at a relatively unknown node along a global supply chain.[50]

[48] CNA, "Risk Control Industry Guide Series: Electronic Component and Hardware Manufacturing Industry," http://www.cna.com/vcm_content/CNA/internet/Static%20File%20for%20Download/Risk%20Control/Industry%20Guide%20Series/ElectronicComponenent&HdweMfg.pdf (accessed January 15, 2012), 9.

[49] Robert N. Charette, "This Car Runs on Code," Spectrum Inside Technology Blog, Institute of Electrical and Electronic Engineers (IEEE), entry posted February 2009, http://spectrum.ieee.org/green-tech/advanced-cars/this-car-runs-on-code/0 (accessed January 15, 2012). This monograph does not argue that US fifth generation fighters, the Boeing Dreamliner, or advanced Mercedes vehicles are any more vulnerable from attack then similarly sophisticated technologies. These examples merely demonstrate trends in componentry.

[50] Jordan Robertson, "Hackers Cross from Digital to Physical World," *Taipei Times Editorials*, October 27, 2011.

Applied physics and defense technology writer, Sally Adee, provides a summary of the impossible task of inspecting each of the billions of lines of programming code and millions of chips purchased from commercial vendors for mission-critical equipment employed by the US Department of Defense. According to Adee, the US military consumes one percent of all integrated circuits produced worldwide, almost completely through a practice called "semiconductor offshoring," in which chip fabrication takes place in Singapore, Taiwan, and other countries with relatively inexpensive labor but educated workforces. Years before the Stuxnet attack, Adee cited the capacity for chipmakers to build switches into chips designed to allow remote access by a third party.[51] Clearly, the trends indicate an increasing reliance on microprocessors built through global supply chains to execute a greater number of functions, accompanied by an increase in the likelihood that complex malware consisting of even several thousand lines of code can hide undetected in such systems.

Additionally, an increase in industrial and municipal development projects performed by multinational corporations like Siemens and General Electric demonstrate the risk associated with the decentralized manufacture of sophisticated componentry used in modern infrastructure.[52] Records obtained from their websites suggest that Siemens and GE subcontract or distribute the manufacture and assembly of critical automated infrastructure components to global supply chains. Dozens of their product lines utilize web-enabled nodes to facilitate efficient operation of

[51] Sally Adee, "The Hunt for the Kill Switch," Spectrum Inside Technology Blog, Institute of Electrical and Electronic Engineers (IEEE), entry posted May 2008, http://spectrum.ieee.org/semiconductors/design/the-hunt-for-the-kill-switch/0 (accessed October 15, 2011).

[52] Siemens Press Releases, "Presentation: The Company, 2012 (December 2011)," http://www.siemens.com/press/pool/de/homepage/the_company_2012.pdf (accessed December 30, 2011). See also GE Press Releases, "GE Energy Announces More than $3 Billion in New Customer Agreements," http://www.genewscenter.com/content/Detail.aspx?ReleaseID=13175&NewsAreaID=2 (accessed January 2, 2012). Siemens, whose industrial controllers in the Natanz centrifuges were the focus of the Stuxnet attack, produced a 2012 company overview in which it calls itself "a global company with a local footprint in over 190 countries." The Siemens report cites research and development facilities in 30 countries, outsourcing the manufacture of components to 190 countries and €14.3 Billion in sales to US infrastructure projects in fiscal year 2011. GE reports critical power and water projects in both developed and developing countries around the world, along with employees in over 100 countries.

critical infrastructure.[53] Furthermore, industrial manufacturers in both the developed and developing world rely on programmable logic control systems similar to those used in Natanz to control essential electronic components used in factories, power plants, pipelines, dams, traffic control systems, security systems, combat systems, and many more open and closed systems around the world.[54]

Although Siemens and GE invest considerable resources toward software security used in their systems, remote terminal units, and programmable logic controllers, Stuxnet demonstrated the vulnerability of hardware and software widely used in the automation of critical infrastructure.[55] One can reasonably infer that the trends in globally manufactured, automated infrastructure components by multinational corporations indicate an increase in the number of nodes vulnerable to attack or exploitation by malicious codes for the purposes of gaining and maintaining initiative during war.

Problematic attribution, ambiguity in the terminology associated with cyber-warfare, and trends of increased vulnerability in supposedly sophisticated weaponry and infrastructure provide a shifting reality of warfare and the contextual framework to understand the American, Russian, and Chinese responses to Stuxnet. Each of these nations presents a case study, a slightly different

[53] GE Press Releases, "City of Leesburg Launches Grid Modernization Project to Better Manage Electricity Loads and Empower Customers," http://www.genewscenter.com/Press-Releases/City-of-Leesburg-Launches-Grid-Modernization-Project-to-Better-Manage-Electricity-Loads-and-Empower-Consumers-357f.aspx (accessed January 2, 2012). The city of Leesburg, Florida will utilize GE's Grid IQ to integrate an automated power distribution network with online portals to create energy efficiencies. This monograph does not argue that the Grid IQ is an insecure system. Rather, it demonstrates the trend of increasingly sophisticated infrastructure, representing the distributed manufacture of components by multinational corporations.

[54] Ellen Messmer, "Siemens Industrial Control Security Vulnerability Could Be Disclosed Today," Network World Blog, entry posted May 19, 2011, http://www.networkworld.com/news/2011/051911-siemens-security-vulnerability.html (accessed November 22, 2011).

[55] GE Energy Solutions, "Substation Automation," http://www.gedigitalenergy.com/automation.htm (accessed January 2, 2012). Components of GE energy systems, used in the Leesburg, FL grid and in systems around the world, parallel the SCADA systems proved vulnerable by the Stuxnet attack. Proliferation of these automated systems can reasonably substantiate the trend of an increase in the number of infrastructure nodes vulnerable to malicious codes.

change in discourse despite the common understanding of reality, indicative of each nation's projection of future warfare in the cyber domain. Analysis of the policies, strategies, and investments made by these nations to protect their own critical infrastructure and weapon systems against Stuxnet-like attack demonstrates their true perception of threat and vulnerability to networked nodes from malicious codes. Likewise, analysis of these nations' policies, strategies, and investments in offensive cyber capabilities demonstrate their perceived role of cyber attack in future military operations.

Reality of Cyber Warfare in the US

The purpose of this section is to paint a picture that illustrates the American perception of changes in the reality of warfare in the cyber domain by analyzing changes within US policy, strategy, military doctrine, and organization before and after Stuxnet. American political, military, and homeland security leaders recognize the vulnerability of their own infrastructure and power-projection capabilities to cyber attack, they anticipate Stuxnet-like attacks from state and non-state aggressors against the US homeland, and they recognize cyber warfare to be a potential enabling component of US military operations.

Literature Review

The administrations of Presidents George W. Bush and Barack Obama leveraged formal and informal signals to demonstrate changes in policy and posture regarding cyber attack capabilities. However, the most relevant indicators of change in US cyber attack policy emerge from a comparison of the 2006 and 2010 *National Security Strategies*, major Presidential addresses, and the formal remarks delivered by administration officials before and after the Stuxnet attack.

Changes to the capstone publications from the Office of the Secretary of Defense and Joint Staff, along with internal memorandums from key civilian and uniformed military leaders demonstrate important changes to the strategic thought, doctrine, and organization concerning the role of cyber attack in US warfare. The 2006 and 2010 *Quadrennial Defense Reviews*, the 2008 *National Defense Strategy*, the 2004 and 2011 *National Military Strategies*, the 2011 *Cyberspace Policy Review*, and the 2012 Defense Strategic Guidance exhibit conceptual changes within the US defense establishment concerning the role of cyber operations in warfare. Similarly, internal memorandums from senior US military officers following the Stuxnet attack illustrate the cognitive tension within the Joint Staff over the role of cyber attack capabilities that result in the physical damage of material and the potential for violence.

Changes to homeland security policy, strategy, and organizations may present the best indicators of a nation's perceived threat from malicious codes, and therefore offer insight into how that nation may use similar capabilities in an offensive role. The 2010 US Department of Homeland Security's (DHS) *Quadrennial Homeland Security Review* and results of simulations conducted by the DHS's National Cyberspace Security Division provide the best resources to evaluate the US's perceived vulnerabilities to its own infrastructure.

US Cyber Attack Posture Prior to Stuxnet

The 2006 *National Security Strategy* is an ideal starting point for analysis because it is the last of the capstone US publications to omit cyber considerations from policy or military strategy. The lone cyber reference in the document consists of a line copied from the *Quadrennial Defense Review*, published one month earlier, predicting "disruptive challenges from state and non-state actors" that employ innovative cyber technologies to counter US military capabilities.[56] The 2006 *Quadrennial Defense Review* also called for the development of capabilities to tag, track, and locate terrorists in cyberspace; defend the populace, infrastructure, and space assets against cyber attack; and defend against Chinese "high-end, asymmetric military capabilities,

[56] The White House, *National Security Strategy* (Washington, D.C.: The White House, March 2006), 44.

emphasizing electronic and cyber warfare."[57] However, neither of the two 2006 capstone publications called for major changes in organizational structure, military strategy or doctrine, nor the development of cyber capabilities that would allow the US to seize and maintain operational initiative by dictating the tempo or terms of events in the cyber domain.

The 2008 *National Defense Strategy* discussed the impacts of warfare in the cyber domain in terms of the disruption of commerce and economic damage that would follow a major cyber attack. However, the strategy claimed that the Department of Defense (DOD) is neither the best source of resources nor the appropriate authority to "shoulder the burden" of cyber warfare. The strategy discussed China's development of cyber warfare capabilities in a section titled "Managing Risk" but did not include cyber warfare in its discussion of "DOD Capabilities and Means."[58] Although this document pairs the terms "cyber" and "warfare" together, the text pertinent to cyber operations is clearly defensive in nature, suggests that cyber operations are a better fit for other governmental agencies, and stops well short of tying "cyber warfare" to potentially violent actions as an instrument to achieve policy objectives.

In 2009, amid significant tension between US departments and agencies over ambiguous cyber terminology and the burden of responsibility for cyber operations, President Obama ordered a 60-day comprehensive "clean slate" review of US cyber policies and organizational structures. The *Cyberspace Policy Review* confirmed problems in attribution, ambiguous terminology, and trends of increasing vulnerability. It concluded by providing ten defensively-oriented recommendations that focused on reprioritizing the National Security Council agenda and emphasizing cyber threats, incident response, and effective management following successful

[57] Office of the Secretary of Defense, *Quadrennial Defense Review* (Washington, D.C.: The Pentagon, February 2006), 24, 25, 29, 32.

[58] Office of the Secretary of Defense, *National Defense Strategy* (Washington, D.C.: The Pentagon, June 2008), 7, 11, 22.

attacks against the US.[59] The 2010 *Quadrennial Homeland Security Review* reinforced the themes of the *Cyberspace Policy Review*, acknowledged that infrastructure vulnerabilities are a reality of industrialized societies, and declared intent to "manage" risks to the US in cyberspace.[60]

The 2010 US *National Security Strategy*, published two months before Sergey Ulasen publicly identified the Stuxnet worm, allocated four paragraphs to the discussion of US goals in cyberspace. Securing American cyberspace was the last of seven topics that addressed how the White House envisioned advancing American interests through security. The cyber security topics focused on protection of networks, data, intellectual property, and private information by defeating cyber "criminals" through investment in a next-generation digital workforce, strengthening partnerships, and developing international norms and laws. A single sentence acknowledged the vulnerability of US infrastructure and prospective disruption of power grids by potential adversaries, but stopped well short of characterizing cyber attack as a potential act of war.[61]

The 2010 *Quadrennial Defense Review* represented a significant cognitive shift, underscoring perhaps the most significant organizational changes in DOD with respect to cyber warfare prior to public disclosure of the Stuxnet attack. A specified task given to the newly formed US Cyber Command, a sub-unified command under US Strategic Command, was to centralize command of cyber operations and, when ordered, to conduct "full-spectrum cyberspace

[59] US Department of Defense, *Cyberspace Policy Review*, Office of the Secretary of Defense, http://www.defense.gov/home/features/2010/0410_cybersec/docs/nps36-052909-01[1].pdf (accessed January 22, 2012).

[60] US Department of Homeland Security, *Quadrennial Homeland Security Review Report: A Strategic Framework for a Secure Homeland* (Washington, D.C.: Department of Homeland Security, 2010), 57-58.

[61] The White House, *National Security Strategy* (Washington, D.C.: The White House, May 2010), 27-28.

military operations."[62] However, all other references to cyber policy and strategy found in the 2010 *Quadrennial Defense Review* remained focused on defense of networks and assured cyber access, demonstrating that the focus of US cyber operations prior to the public disclosure of Stuxnet continued to focus on networks and data instead of material and infrastructure.[63]

Just days after taking command of US Cyber Command and three weeks before Sergey Ulasen posted the first Stuxnet blogs, General Keith Alexander underscored the ambiguous cyber environment by discussing the lack of clear rules of engagement or jurisdictional boundaries between federal agencies with respect to the cyber domain.[64] Testifying before the House Committee on Homeland Security one week later, the Government Accountability Office Director, Gregory Wilshusen, echoed General Alexander's concerns. Wilshusen talked at great length about the results of a Department of Homeland Security cyber attack exercise called *Cyber Storm* that catalogued organizational deficiencies and highlighted the protection of networks and data. Wilshusen's testimony briefly mentioned critical infrastructure vulnerabilities, but in keeping with the general discourse before the public disclosure of Stuxnet, Wilshusen quickly refocused on crime and network vulnerabilities.[65]

The language used in the major American policy, strategy, and doctrinal publications prior to public disclosure of Stuxnet seems to be consistent with the previously discussed joint definition of computer network attack and reflects the prevailing concepts of attack through the cyber domain. By emphasizing the nonviolent effects to networks and data, the capstone US policy and strategy documents placed the focus of cyber operations on protection. Based solely

[62] Office of the Secretary of Defense, *Quadrennial Defense Review Report* (Washington, D.C.: Government Printing Office, February 2010), 38.

[63] Ibid., v, ix, 2, 15.

[64] Tom Gjeltin, "US Seeks to Define Rules on Cyberwar," National Public Radio June 3, 2010, http://www.npr.org/templates/story/story.php?storyId=127411091 (accessed January 22, 2012).

[65] House Committee on Homeland Security, "Cybersecurity: Continued Attention is Needed to Protect Federal Information Systems from Evolving Threats," 111th Cong., 2d sess., 2010.

on the open source evidence at hand, the US posture toward warfare in the cyber domain prior to the summer of 2010 stressed protective measures and a passive nature. As Clausewitz would say, the characteristic feature of the passive US cyber posture prior to Stuxnet consisted of "awaiting the blow from the enemy," thus demonstrating a negative aim.[66]

Evidence of Changes Following Stuxnet

In the fall of 2010, at the same time the Symantec Trio and Ralph Langner described Stuxnet's systematic progress from infected flash drive to centrifuge destruction in the blogosphere, William Lynn published an eye-opening article in *Foreign Affairs* entitled "Defending a New Domain." The Deputy US Secretary of Defense opened the article by describing a previously classified incident in which a flash drive infected with malicious code established a "digital beachhead" on a US military laptop in the Middle East that it used to send data from classified military networks to servers under foreign control.[67] Lynn emphasized the vulnerability of data in supposedly secure networks that utilize an "air gap," physically separating secure and unsecure networks like the public internet. The article's timing, discussion of infection methods, and revelation of an attack on an "air gapped" US network echoed the Stuxnet themes concurrently debated in the Symantec and Langner blogs. Lynn concluded the article by declaring "the dawn of a transformative new era" and referenced a letter sent from Albert Einstein to President Roosevelt on the eve of World War II, warning of the potential magnitude involved in fission weapons and a subsequent nuclear arms race between the world's major powers.[68]

[66] Clausewitz, 357-359. Clausewitz's use of the term "negative aim" while claiming that the defense is the stronger form of warfare did not imply a value judgment. Rather, it portrayed the reality that defenders do not gain tangible resources and cede the initiative to the attacking party. US cyber policy and strategy prior to Stuxnet contained a negative aim.

[67] William J. Lynn III, "Defending a New Domain," *Foreign Affairs* 89, no. 5 (2010): 97.

[68] Ibid., 97-109. See also Glenn elert, "Albert Einstein's Letters to President Franklin Delano Roosevelt," E-World, http://hypertextbook.com/eworld/einstein.shtml (accessed January 24, 2012).

General James Cartwright, Vice Chairman of the US Joint Chiefs of Staff, followed Lynn’s article with a memorandum addressed to the chiefs of the uniformed services and the combatant commanders acknowledging the inadequate and ambiguous terminology of cyber operations lexicon found in US joint doctrine. Cartwright specifically addressed the inappropriate use of the term “computer network attack” to reference cyber operations that attack physical material instead of virtual assets. Cartwright redefined CNA as a form of “offensive fires,” thereby directly categorizing the destruction of information, systems, and networks as an act of war. Cartwright’s guidance directed the use of the term “cyber attack,” as a part of “offensive cyber operations,” to define hostile acts to destroy an adversary’s systems, assets, or functions that meet “use-of-force” levels through the cyber domain.[69]

General Cartwright’s guidance represents the most significant result of American introspection in the aftermath of the public disclosure of Stuxnet and a fundamental public change regarding the potential role of cyber attacks in future US military operations. Cartwright modified the definition of “advance force operations” to include the delivery of software payloads to facilitate, enable, or provide effects to larger military operations.[70] Within days of Symantec’s initial publication of the “W32.Stuxnet Dossier,” the Vice Chairman of the Joint Chiefs of Staff definitively linked cyber attack, the physical destruction of material through the cyber payloads, and future offensive military operations.

The *National Military Strategy* published shortly thereafter, in January 2011, declared the emergence of cyberspace as a war-fighting domain on the same level as the land, sea, air, and space domains. The strategy included cyberspace among the global commons, comparing it to “the connective tissue upon which all nations’ security and prosperity depend,” within which the

[69] James Cartwright, “Joint Terminology for Cyberspace Operations” (Washington, D.C.: The Pentagon, November 2010), 1-3, 5.

[70] Ibid., 2.

Joint Force's ability to project power and deter aggression depends.[71] The significant changes to the US military's posture toward cyber attack contributed to Congress' requirement, as part of the National Defense Authorization Act of 2011, for the Department of Defense to submit a full review of its military cyberspace policies.[72]

In November 2011, Congress received the "Department of Defense Cyberspace Policy Report" to clarify wording in the *National Military Strategy* with respect to cyberspace operations. The report revealed that the US, along with potential adversaries, maintained offensive cyber attack capabilities and that the DOD anticipated that some nations possessed the capacity to wield such weapons "in an attempt to affect the strategic calculus of the US."[73] The report claimed that legal norms for acts of war, such as Article 2(4) of the UN Charter and the law of armed conflict apply to actions in the cyber domain and that the US reserved the right to respond to hostile acts in cyberspace with "kinetic" military capabilities. Finally, the report suggested that offensive cyber attack by the US should trigger notification and reporting to Congress in accordance with the War Powers Resolution.[74]

In January 2012, President Obama unveiled new strategic guidance for the Department of Defense. Among other requirements, US Joint Forces will use scaled down economy-of-force structures to impose unacceptable costs on opportunistic aggressors by conducting combined arms campaigns across all domains: land, air, maritime, space, and cyberspace. The guidance also

[71] Office of the Chairman of the Joint Chiefs of Staff, *The National Military Strategy of the United States of America, 2011* (Washington, D.C.: The Pentagon, January 2011), 9.

[72] *National Defense Authorization Act for Fiscal Year 2011, Section 934*, Public Law 111-383, 111th Congress, "National Defense Authorization Act for Fiscal Year 2011," http://www.gpo.gov/fdsys/pkg/PLAW-111publ383/pdf/PLAW-111publ383.pdf (accessed January 24, 2012).

[73] US Department of Defense, *Department of Defense Cyberspace Policy Report: A Report to Congress Pursuant to the National Defense Authorization Act for Fiscal Year 2011, Section 934* (Washington D.C.: The Pentagon, November 2011), 2-3.

[74] Ibid., 3-4, 9.

requires power projection into anti-access and area denial regions in which adversaries employ sophisticated weapons and implies that such infrastructure is vulnerable to denial, degradation, and destruction through the cyber domain.[75] The President's proposed 2013 budget includes increased appropriations to offensive and defensive cyber technologies from the current $3.4 billion spent in 2012, according to the *Washington Post*, including cyber weapons that target "offline" military systems.[76]

American perception of the reality of warfare in the cyber domain shifted during the summer and fall of 2010, corresponding to a change in the official US posture toward cyber attack as an act of war. In early 2010, the US clearly exhibited a passive cyber posture, what Clausewitz would call a "negative aim." By the end of 2010 and continuing into 2012, American policy, strategy, and institutions reflected the transition to a modified reality of offensive cyber action, dictating the terms of events and gaining the initiative in cyberspace to help shape broader policy and strategic outcomes, thus operating in what Clausewitz would call a "positive aim."

Reality of Cyber Warfare in Russia

The purpose of this section is to demonstrate the Russian Federation's perception of the changing reality of cyber warfare by analyzing changes to Russian policy, strategy, and the operating doctrine of military and security services following Stuxnet. Russian leaders were among the first to acknowledge the risk and opportunity associated with computer network attack and cyber attack. They anticipate Stuxnet-like attacks from state and non-state actors against the

[75] Department of Defense, *Sustaining US Global Leadership: Priorities for 21st Century Defense* (Washington, D.C.: The Pentagon, January 2012), 4-5.

[76] Ellen Nakashima, "Pentagon Ups Ante on Cyber Front," *The Washington Post*, March 19, 2012. See also US Department of Defense, "2013 Funding Highlights," The White House, http://www.whitehouse.gov/sites/default/files/omb/budget/fy2012/assets/defense.pdf (accessed March 19, 2012).

Russian homeland and they recognize cyber warfare to be a potential enabling component of both military and internal security operations.

Literature Review

References to a cyber domain of military operations are largely absent from Russian open source material outside of citations of Western military theory. Rather, the Russian view of information war, or *informatsionnaya voyna*, is a concept that combines cyber operations, electronic warfare, psychological operations, strategic communications, deception, and influence.[77] Additionally, the policies and strategies developed by Russian leaders reflect military and security cultures that appear unique to Western observers. Russia's *National Security Strategy to 2020* demonstrates the tendency for Russian leaders to consider external and internal threats equally, leading to shared planning among military and internal security organizations to develop similar offensive cyber attack capabilities as instruments of national power and national security.

Capstone publications demonstrate Russian perceptions and concerns, from the *National Security Strategy* to the February 2010 *Military Doctrine of the Russian Federation*. Additionally, statements from the Russian President and Prime Minister, along with papers from major Russian military and internal security theorists, provide an understanding of Russian military actions with respect to offensive cyber operations. However, Russia remains a collection of government institutions and bureaucracies with carefully scripted publications that reflect its secretive history, and censorship of on-line content presents a challenge to efforts aimed at assessing changes in

[77] Kier Giles, "'Information Troops' – a Russian Cyber Command?" Oxford Conflict Studies Research Centre, http://www.conflictstudies.org.uk/files/Russian_Cyber_Command.pdf (accessed January 12, 2012).

posture and perception.[78] Linguistic shortcomings limit the analysis to journals, news articles, and policy documents translated from Russian to English. Because the Stuxnet attack is a relatively recent event, not all relevant publications exist in translated form. Therefore, this chapter pursues the analysis of as many relevant Russian publications as possible to paint the picture of changes to the Russian perception of warfare in the cyber domain.

Russian Cyber Attack Posture Prior To Stuxnet

The Russian Federation was one of the first states that publicly recognized the risks and opportunities associated with information attacks enabled by network operations, demonstrated by their significant investments to develop organizations and promote leaders to focus on cyber-related capabilities. As with other emerging technologies, Russia applied advances in offensive network operations to both their military and internal security organizations. In 1998, the Kremlin created the Directorate for Combating Crimes in the High Technology Sphere, or "Directorate K," the official network information branch of the Ministry of Internal Affairs. Directorate K's initial mission included working closely with Russia's Federal Security Service (FSB), the lead agency for state security and the successor agency of the Soviet Committee of State Security (KGB), to interdict network security threats and develop network information capabilities.[79]

In February 2008, General Aleksandr Burutin, the Russian Deputy Chief of the General Staff and military advisor to Vladimir Putin, delivered a speech entitled "Wars of the Future Will Be Information Wars" to the National Forum of Information Security. General Burutin's comments focused on the similarities between "kinetic force and information operations,"

[78] Open Net Initiative, "Russia," Open Net Research, http://opennet.net/research/profiles/russia (accessed March 4, 2012). See also Press Freedom Index, "Countries Under Surveillance: Russia," Reporters Without Borders, http://en.rsf.org/surveillance-russia,39766.html (accessed March 4, 2012).

[79] Directory of Russian Federation Defense-Related Agencies and Personnel, "Note on MVD Reorganization," Ministry of Internal Affairs (MVD), http://www.fas.org/irp/world/russia/fbis/InternalAffairsMinistry.html (accessed February 6, 2012).

describing future war as “attacking state and military control systems, navigation and communication systems, and other crucial information and facilities.”[80] In another open forum, Burutin referred to electronic warfare units in the FSB and the Ministry of Defense (MOD) and discussed the progress of “special methods” of network information training.[81] Six months later, the world watched the Russian Military Policy on Information Warfare in action.

In the hours before the 2008 South Ossetia War, servers throughout Georgia sustained the coordinated assault of hundreds of millions of network requests that overloaded and shut down its governmental and commercial information networks, isolating the Georgian state from the rest of the world.[82] Known as a distributed denial of service attack (DDoS), this method of saturating a target network with overwhelming amounts of data, making it impossible to function, is often associated with networks of compromised computers, or “botnets,” that can be distributed among computers and servers around the world.[83] Russia officially denied involvement with the DDoS attack although many cyber analysts attributed the attack’s orders to the senior leadership of the Russian government as an extension of military operations against Georgia.[84] The open-source

[80] Aleksandr Burutin, “Russian Military Policy for Information Warfare,” Intellibriefs, http://intellibriefs.blogspot.com/2009_03_22_archive.html (accessed February 11, 2012).

[81] Marina Myakisheva, “What is Russia’s Answer to Cyber Threats?” CNews.ru Reviews, http://eng.cnews.ru/reviews/printEn.shtml?2008/02/12/287829 (accessed February 11, 2012).

[82] Sharon Weinberger, “Hackers are Internet Shock Troops,” Aviation Week, http://www.aviationweek.com/aw/generic/story.jsp?id=news/dti/2010/05/01/DT_05_01_2010_p19-218221.xml&channel=defense (accessed February 5, 2012).

[83] Catherine Hockmuth, “Botnets Threaten National Security,” Ares Defense Technology Blog, http://www.aviationweek.com/aw/blogs/defense/index.jsp?plckController=Blog&plckScript=blogScript&plckElementId=blogDest&plckBlogPage=BlogViewPost&plckPostId=Blog:27ec4a53-dcc8-42d0-bd3a-01329aef79a7Post:c5476b3d-1c5f-41ca-84fd-b7dcceb931bf (accessed February 5, 2012). See also Symatec.Cloud, “Botnets,” Global Threats Blog, http://www.symanteccloud.com/globalthreats/threatmaps/botnets (accessed February 6, 2012). Botnets recruit computers unknowingly by running malicious software, allowing the botnet’s owner remote control over unwitting computers. Botnets can sit idle and appear benign to antivirus checks for months or even years. When a botnet numbers tens of thousands of computers, its owner can direct DDoS operations, sending hundreds of millions of emails from around the world, intentionally overloading or crashing a network.

[84] John Markoff, “Before the Gunfire, Cyberatttacks,” *The New York Times*, August 12, 2008.

intelligence initiative known as Project Grey Goose concluded that the Russian government masked its involvement in the DDoS attack on Georgia by co-opting informal "volunteers" and elements of the Russian Business Network, a "cyber criminal enterprise that provided plausible deniability to a Kremlin-Funded Information Operation," to direct an army of botnets against Georgian networks.[85] Shortly after the Georgia conflict, Vladislav Surkov, the First Deputy Chief of Staff to the President of Russia, said "the Five Day War showed that the Net is a front" and that "August 2008 was the starting point of the virtual reality of conflicts and the moment of recognition of the need to wage war in the information field too."[86]

The computer network attacks against Georgia are not the first example of the Russian government leveraging the cyber capabilities of civilian enterprise or its own internal security organizations to influence the execution of Russian foreign policy. A number of cyber security analysts allege Russian-sponsored DDoS attacks against Estonia, one of the most network-dependent nations on earth, in which Estonian government, media, banks, and private businesses shut down during a 2007 nationalist dispute over a Soviet-era monument in Tallinn's capital square.[87] Jeffrey Carr, a cyber security analyst and founder of Project Grey Goose who lectures regularly at DOD institutions including the US Army War College and the Air Force Institute of Technology, considers the Russian DDoS attacks against Estonia and Georgia early examples of the use of cyber attack as instruments of national policy.[88] However, even if Russia used DDoS

[85] Jeffrey Carr, "Project Grey Goose Phase II Report: The Evolving State of Cyber Warfare," http://www.scribd.com/doc/13442963/Project-Grey-Goose-Phase-II-Report (accessed February 5, 2012). The Russian Business Network and other criminal networks with ties to senior Russian officials "lease" botnets for various purposes. Project Grey Goose proved the affiliation between botnets directed against Georgian websites and Russian criminal organizations, including the RBN.

[86] Jeffrey Carr, *Inside Cyber Warfare: Mapping the Cyber Underworld* (Sebastopol, CA: O'Reilly Media, 2012), 164.

[87] Voice of America, "From Russia with Malice: The Dangers of Russian Hacking," Digital Frontiers Blog, July 18, 2011, http://blogs.voanews.com/digital-frontiers/2011/07/18/from-russia-with-malice/ (accessed February 6, 2012).

[88] Carr, 15-18.

attacks against Estonia and Georgia as instrumental actions aimed at achieving or enabling policy objectives, the targets of DDoS attacks are data and networks and therefore inherently lack the potential for direct violence.

From a policy perspective, the May 2009 *National Security Strategy of the Russian Federation to 2020* addressed the major threats to Russian national security and national interests, established Russian national security priorities, and identified the most likely technological means by which Russian leaders will ensure national security. The strategy characterized the information threat to Russian assets as consisting of "illicit information network activities in the sphere of high technology" and focused national efforts on preventing network crime. Two of the strategy's 112 paragraphs address limiting the effects of network crime and "high technology means of conducting armed warfare," but the policy stops well short of identifying information attack as either a threat to Russian national security or a means of warfare.[89]

The *2010 Military Doctrine of the Russian Federation* predicted an operating environment for Russian military forces with a low probability of conventional or nuclear attack. Rather, the doctrine listed "impeded and disrupted function and operation of state and military command and control systems" as the second major military threat to the Russian Federation. The doctrine described the systems of greatest concern to impeded and disrupted operations, which all rely on networks of interconnected nodes: strategic nuclear forces, missile early warning systems, space systems, nuclear munitions storage facilities, nuclear energy facilities, and atomic and chemical industry facilities.[90] The Russian military doctrine also described the characteristic

[89] Rustrans, *The National Security Strategy of the Russian Federation to 2020*, Rustrans Wikidot http://rustrans.wikidot.com/russia-s-national-security-strategy-to-2020-russian-text (accessed February 5, 2012).

[90] The Russian Federation Ministry of Defense, *Military Doctrine of the Russian Federation*, National Defense University, http://merln.ndu.edu/whitepapers/Russia2010_English.pdf (accessed February 9, 2012), para 10.b.

features of contemporary military conflicts as “the integrated utilization of military force and forces and resources of a nonmilitary character.”[91]

The doctrine stopped short of providing a definition for “forces and resources of a nonmilitary character” and neither of the Russian capstone policy or doctrinal publications explicitly addressed the potential to conduct acts of warfare in cyberspace. However, the doctrine appears to reflect Russian introspective understanding of “information threat” to its networked systems while signaling Russian intent to incorporate computer network attack as an enabling component of Russian military operations, in line with alleged Russian actions against Georgia.

In the years that preceded the Stuxnet attack, the Russian government’s use of resources and investments in doctrine, organization, training, and operations of the MOD and the FSB reflect the expanded role of information operations as an instrument of Russian policy, even if their National Security Strategy did not reflect that reality. Most open-source indications of the Russian pre-Stuxnet posture toward information operations focus on computer network attack, a nonviolent instrument of policy to achieve political objectives, as an enabling component to military information operations. However, the discourse among some Russian officials reflects at least a basic understanding that offensive cyber operations could result in indirect, “kinetic” effects. Stuxnet reinforced General Burutin’s comments and revealed a new reality that offensive networked information operations could result in direct, violent effects.

Evidence of Changes Following Stuxnet

Stuxnet became public amidst an ongoing Russian internal military review of their performance and capabilities during the brief war with Georgia, two years earlier. Despite the relative success of Russian information operations against Georgia and comments by the Commander of the US Cyber Command describing Russia as a “near peer” to the US in offensive

[91] Ibid., para 12.a.

cyber capability, Russian leaders perceived a capabilities gap between Russian information operations and others' cyber operations.[92] Russian leaders embraced a two-pronged approach as early as 2009, designed to limit state actors' development of offensive cyber capabilities through diplomatic efforts while growing a force of "information troops" to increase their own offensive information capabilities. The Stuxnet attack provided an unambiguous impetus to accelerate development in the "sphere of high technology" in order to close a perceived gap between Russian information warfare capabilities and the offensive cyber capabilities of potential western adversaries. As noted by Keir Giles, the Director of the Conflict Studies Research Centre at Oxford, Russia's perceived network vulnerability and their preoccupation with vulnerability to outside influences informed a holistic review of information warfare in the months following the Stuxnet attack.[93]

Russian perceptions of lagging behind potential adversaries in the development of robust information and network warfare capabilities, analogous to American perceptions of a "missile gap" following Sputnik, led Dmitry Rogozin, the Russian Ambassador to NATO, to label Stuxnet an "explosive mine" comparable in scope to the nuclear accident at Chernobyl.[94] Rogozin's initial comments to Russian newspapers introduced suspicion that the Mars-bound Phobos-Grunt spacecraft failed to leave low earth orbit due to subversive pirated microchips purchased from foreign vendors, reflecting ongoing Russian preoccupation to information vulnerability.[95]

[92] Keith B. Alexander, "Statement of General Keith B. Alexander, Commander, US Cyber Command Before the House Committee on Armed Services, 23 September, 2010," http://www.defense.gov/home/features/2010/0410_cybersec/docs/USCC%20Command%20Posture%20Statement_HASC_22SEP10_FINAL%20_OMB%20Approved_.pdf (accessed December 10, 2011).

[93] Giles, 51-53.

[94] Reuters, "Russia Says Stuxnet Could Have Caused New Chernobyl," Reuters US Edition January 26, 2011, http://www.reuters.com/article/2011/01/26/us-iran-nuclear-russia-idUSTRE70P6WS20110126 (accessed February 12, 2012).

[95] Konstantine Bogdanov, "The Phobos Crash was Preprogrammed," *Rianovsti*, February 12, 2012. See also Zakutnyaya Olga, "Herald of Changes," The Voice of Russia Radio, http://english.ruvr.ru/2012/02/03/65244687.html (accessed February 20, 2012).

Andrei Kokoshin, the Deputy Minister of Defense and an advocate for Russian information warfare dominance, encouraged an interdisciplinary approach to develop and implement offensive capabilities across state institutions.[96] According to Alexander Klimburg, a senior advisor at the Austrian Institute for International Affairs, Kokoshin's perspective of overlapping internal jurisdictions, mainly cyber crime, cyber terrorism, information operations, and cyber activism, present commonalities that promote cooperation between MOD, FSB, and other agencies to develop offensive cyber capabilities.[97] Khatuna Mshvidobadze, an analyst at the Georgian Foundation for Strategic and International Studies, claims that "the FSB's 16th Directorate controls a Russian reserve force of hackers," and cites evidence that cultivating talented hackers is one of Vladimir Putin's top priorities.[98] In March 2011, Viktor Ozerov, the head of the Federation Council's Defense and Security Committee said, "there is still no special structure for cyber in the Armed Forces, but this does not mean that we are not dealing with these problems."[99]

The discourse on using emerging cyber capabilities as instruments of Russian national policy circulate at the highest levels of Russian institutions. In November 2011, Russian President Dmitry Medvedev discussed the need for Russia to "develop the capacity for cyber attack against US missile defense systems."[100] Although such a capacity would likely constitute a non-violent shaping operation to enable larger military objectives, Medvedev's comments reflect a perfected reality of warfare due to changes in Russian perceptions of *informatsionnaya voyna*. A December

[96] Andrey Kokoshin, "Kokoshin: Cyberwarfare Threat to Russian National Security," One Russia Party, http://old.er.ru/er/text.shtml?18/2254 (accessed February 18, 2012).

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

[98] Khatuna Mshvidobadze, "The Battlefield on your Laptop," Radio Free Europe Radio Liberty, http://www.rferl.org/content/commentary_battlefield_on_your_desktop/2345202.html (accessed December 13, 2011).

[99] Giles, 55.

[100] Alexander Goltz, "Medvedev Mollifies the West," *The Moscow Times*, November 29, 2011.

2011 article in *Foreign Affairs* credits "patriotic hackers" controlled by the FSB with DDoS attacks against newspapers and websites that depicted Putin's United Russia Party in a negative light prior to parliamentary elections.[101] According to Russia's largest internet search portal, Yandex, the DDoS attack originated from two botnets that turned more than 200,000 computers around the world into "slaves" that overwhelmed election-monitoring sites.[102] In February 2012, Prime Minister and Presidential Candidate Putin published an article in the *Rossiyskaya Gazeta* that summarized strengths and weaknesses in Russia's military posture, predicted requirements for success in 21st Century warfare, and declared that emerging Russian cyber capabilities will play a "decisive role" in future conflicts.[103]

Based on the available evidence of Russian perceptions of warfare in the cyber, or "information" domain since the 1990s, it is reasonable to conclude that Russia's cyber posture reflects a reality in which cyber capabilities encompass important enabling components of military operations and instruments of policy designed to achieve greater political and strategic objectives. Unlike the US, which demonstrated a significant change in posture and organization during 2010, Russia's discourse on cyber warfare reflects a steady crescendo of incorporating emerging offensive cyber capabilities into military and internal security operations. Stuxnet's influence in Russia is a realization that cyber capabilities are likely to play decisive roles in future military operations, rather than shaping roles used by Russia in Georgia in 2008.

[101] Andrei Soldatov, "Vladimir Putin's Cyber Warriors: The Kremlin's Ham-handed Effort to Squelch Online Dissent," *Foreign Affairs* Features, http://www.foreignaffairs.com/articles/136727/andrei-soldatov/vladimir-putins-cyber-warriors?page=show (accessed March 4, 2012).

[102] Hal Roberts and Bruce Etling, "Coordinated DDoS Attack During Russian Duma Elections," The Harvard Law Internet and Democracy Blog, entry posted December 8, 2011, http://blogs.law.harvard.edu/idblog/2011/12/08/coordinated-ddos-attack-during-russian-duma-elections/ (accessed March 4, 2012).

[103] Vladimir Putin, "Be Strong: Guarantee of National Security for Russia," *Rossiyskaya Gazeta*, February 20, 2012, http://www.rg.ru/2012/02/20/putin-armiya.html (accessed March 4, 2012).

Reality of Cyber Warfare in China

The purpose of this section is to demonstrate the reality of cyber warfare in China by analyzing changes to Chinese strategy, military theory and doctrine, and institutional organizations before and after Stuxnet. Chinese leaders and military theorists recognize the vulnerability of their infrastructure and defense networks to cyber attack, they anticipate Stuxnet-like attacks as a part of future warfare, and they recognize cyber warfare to be a potential enabling component of future Chinese military operations.

Literature Review

Limited access exists to open source documents describing the national policy of the People's Republic of China (PRC) regarding offensive cyber operations. The best sources of Chinese cyber policy and strategy are the political officers of the People's Liberation Army (PLA) and the Central Military Commission, who publish extensive works of military theory and doctrine in the journals and white papers of the PLA Academy of Military Science and the Chinese National Defense University. These research institutes provide carefully scripted indications of changes designed to signal Chinese military doctrine, force development, and institutions from the political officers who provide strategic advice to military policymakers, the Politburo, and the Chinese Communist Party leadership. Additionally, Chinese military representatives provide indications of changing perceptions of reality within the Chinese military, although their press releases and news conferences are also carefully scripted events designed to release specific information after rigorous examination by political leaders.

As in the previous Russian case study, linguistic shortcomings limit the analysis of the Chinese cyber attack posture prior to and following the Stuxnet attack to journals, news articles, and policy documents translated from Chinese to English. Because the Stuxnet attack is a relatively recent event, not all relevant Chinese publications exist in translated form. Therefore, this chapter pursues the analysis of as many relevant Chinese publications as possible to paint the picture of changes to Chinese perceptions of cyber warfare.

Chinese Cyber Attack Posture Prior To Stuxnet

The 1991 Gulf War provided Chairman Jiang Zemin and other Chinese Communist Party leaders the explicit realization that the PLA was an obsolete force, and reinforced the need for a "revolution in military affairs" to modernize the Chinese Armed Forces into a force capable of winning "wars under high-tech conditions." Although PLA transformation began two decades earlier under Deng Xiopang, the Gulf War accelerated changes in Chinese strategic, institutional, and operational thinking to fit the realities of Information Age conflict.[104] The PLA of the 1990s was ripe for dramatic doctrinal and structural changes. The writings of many Chinese military professionals in the two decades following the Gulf War reflect the tension between the desire to maintain traditional Chinese asymmetric, indirect operational approaches and the need to modernize military capacity to accomplish Chinese state goals among a competitive field of adaptive, technologically advanced, and networked potential adversaries.

In 1995, two military theorists at the Chinese Academy of Military Science in Beijing, Senior Colonel Wang Baocun and Li Fei co-authored an article in *The Liberation Army Daily* that appears to parallel Network Centric Warfare Theory and predicts smaller organizational structures in future armies due to the force multiplying effects of "informationalized forces." According to Wang and Li, information warfare includes "computer virus warfare" aimed at

[104] Alexander Chieh-cheng Huang, "Transformation and Refinement of Chinese Military Doctrine: Reflection and Critique of the PLA's View," RAND Publications, http://www.rand.org/pubs/conf_proceedings/CF160/CF160.ch6.pdf (accessed February 17, 2012).

destroying a computer's normal operating programs, characterized by problematic detection and attribution, resulting in an increase in vulnerability to combat systems on a digitized battlefield.[105]

In 1999 two PLA Air Force Colonels, Qiao Liang and Wang Xiangsui, published *Unrestricted Warfare*, one of the most influential Chinese military strategy books prior to the Stuxnet attack in which they discuss a variety of innovative options to defeat a technologically superior adversary. In the preface of their book, the Colonels argue that political and technological changes require a new theory of warfare and recommend a departure from Clausewitz. According to Qiao and Wang, "the new principles of war are no longer 'using armed force to compel the enemy to submit to one's will,' but rather are 'using all means, including armed force or non-armed force, military and non-military, and lethal and non-lethal means to compel the enemy to accept one's interests.'" The authors discount the potentially violent nature of warfare by arguing that in war, "methods that are not characterized by the use of the force of arms, nor by the use of military power, nor even by the presence of casualties and bloodshed, are just as likely to facilitate the successful realization of the war's goals, if not more so." The authors endorse American precedents and claim that attacks on financial assets, social systems, and the networks that support them are in keeping with Chinese traditions of warfare, although by nature they are not violent.[106]

Qiao and Wang acknowledge the reality that states must "fight the fight that fits one's weapons," but they also argue that China must develop new concepts of weapons that fit their definition of warfare, including information weapons "used to obtain or suppress information," in

[105] Wang Baocun and Li Fei, "Information Warfare," *The Liberation Army Daily*, June 20, 1995, http://www.fas.org/irp/world/china/docs/iw_wang.htm (accessed February 18, 2012). See also Timothy Thomas, *The Dragon's Quantum Leap: Transforming from a Mechanized to an Informationized Force* (Fort Leavenworth: Foreign Military Studies Office, 2009), 2. According to Thomas, "several terms (cyber, digital, network) that are information-related in English translate from Chinese to English in a number of ways (informationization, informationalization)."

[106] Qiao Liang and Wang Xiangsui, *Unrestricted Warfare* (Beijing: PLA Literature and Arts Publishing House, 1999), http://cryptome.org/cuw.htm (accessed February 17, 2012).

an effort to “make weapons that fit the fight.”[107] *Unrestricted Warfare* demonstrates that Chinese military theorists wrestled with the relationship between the reality and discourse of warfare as new capabilities and vulnerabilities emerged in the years following Desert Storm, well before Stuxnet. However, by rejecting the Clausewitzian requirement for potential violence and labeling information weapons as tools to obtain or suppress information, the PLA theorists unambiguously endorse a concept of cyber warfare in line with the traditional American definition of computer network attack.

The concept of using informationalized instruments of warfare in an asymmetric manner to achieve Chinese policy objectives is in line with the traditional Chinese approach called *shi*, which advocates “potential born of disposition,” avoiding an adversary’s strength by exploiting their vulnerabilities, and dominating an adversary indirectly.[108] Two network attacks prior to Stuxnet, attributed to the PRC by McAfee’s Threat Research Department, demonstrate the concept of *shi* in the cyber domain. According to McAfee, in late 2009 “Operation Aurora” used malicious payloads to gain access and modify source code repositories at high-tech, security, and defense contractors in the US and Taiwan including Google, Symantec, Northrop Grumman, Morgan Stanley, and DOW Chemical.[109] An article in the *New York Times* suggested that the American Embassy in Beijing had reason to believe the Chinese Politburo directed the Aurora attack.[110] “Operation Shady RAT,” a second network attack attributed directly to China by

[107] Ibid.

[108] SANS Institute, “Redefining the Role of Information Warfare in Chinese Society,” InfoSec Reading Room, http://www.sans.org/reading_room/whitepapers/warfare/redefining-role-information-warfare-chinese-strategy_896 (accessed February 18, 2012).

[109] McAfee, “Protecting Your Critical Assets: Lessons Learned From Operation Aurora,” McAfee Labs, http://www.mcafee.com/us/resources/white-papers/wp-protecting-critical-assets.pdf (accessed February 19, 2012). See also Kim Zetter, “Google Hackers Had Ability to Alter Source Code,” Wired Threat Level Blog, http://www.wired.com/threatlevel/2010/03/source-code-hacks/ (accessed February 19, 2012).

[110] Scott Shane and Andrew Lehren, “Leaked Cables Offer Raw Look at US Diplomacy,” *The New York Times*, November 28, 2010.

McAfee, used a Remote Access Tool (RAT) to steal intellectual property, negotiation plans, and secrets of at least 72 sovereign governments, defense contractors, think tanks, and the UN.[111]

In the years before the Stuxnet attack, Chinese officials advocated for, and exhibited an active posture toward warfare in the cyber domain within the traditional Chinese *shi* approach and allocated considerable resources in the 12th Five Year Plan (2011-2015) to build indirect cyber capabilities.[112] However, when evaluated from a Clausewitzian perspective, Chinese cyber theory and doctrine lacked the potential for violence, suggesting a role for cyber capabilities closer to the US doctrinal definition of computer network operations than cyber attack. That would change in the fall of 2010 following the publications by the Symantec trio and Ralph Langner.

Evidence of Changes Following Stuxnet

A few weeks after Stuxnet become a major news story, China's *Liberation Army Daily* published a story that claimed the PLA's outdated mode of warfare theory reflected conservative and traditional Chinese culture, required modernization, and called for audacious changes to leverage "recent innovations."[113] The concept of using a cyber weapon in a direct attack against material resources received a high degree of attention from the Chinese government, military, and society following a series of September 2010 publications in Chinese newspapers that summarized the threat to industrial control systems and PLC-dependent infrastructure throughout

[111] Dmitri Alperovich, "Revealed: Operation Shady RAT," McAfee Threat Research, http://www.mcafee.com/us/resources/white-papers/wp-operation-shady-rat.pdf (accessed February 19, 2012).

[112] Willy Lam, "Beijing Bones Up it Cyber-Warfare Capacity," The Jamestown Foundation, http://www.jamestown.org/programs/chinabrief/single/?tx_ttnews%5Btt_news%5D=36007&tx_ttnews%5BbackPid%5D=414&no_cache=1 (accessed February 2, 2012).

[113] Reuters, "China Paper Warns Military Thinking Outmoded," *Reuters US Edition*, http://www.reuters.com/article/2010/08/15/us-china-military-idUSTRE67E07020100815 (accessed February 10, 2012).

China.[114] Not knowing Stuxnet's benign character outside of Natanz, the *South China Morning Post* referenced a news release from the official Xinhua News Agency that claimed Stuxnet infected over one thousand Chinese industrial computer networks, including the Three Gorges Dam hydroelectric facility, nuclear plants, airports, and power facilities.[115] China's *Global Times* quoted Eugene Kaspersky saying, "Stuxnet proves that we have now entered the age of cyber warfare."[116] Chinese military theorists and government officials quickly agreed.

The March 2011 review of Chinese defense publicly recommitted China to a policy of active cyber defense and revealed China's concerns, implicitly referencing Stuxnet, that 2010 marked the moment in which other major military powers developed "enhanced cyber operations capabilities to occupy new strategic commanding heights."[117] Chinese National Defense University professor and space power theorist, Colonel Li Daguang, referred to the Stuxnet attack as a "Pandora's Box" of cyber warfare and predicted an arms race to develop cyber weapons capable of paralyzing an adversary's networks and their military and economic capabilities, thereby influencing a society's willpower.[118]

Almost one year after the Stuxnet attack became public, two PLA scholars, Ye Zheng and Zhao Baoxian, published an article in the *Zhongguo Qingnian Bao* to reassure their comrades of

[114] Guo Qiang, "Web Superbug Seeking to Access China," *Global Times*, http://china.globaltimes.cn/society/2010-09/577487.html (accessed February 19, 2012). See also Stephen Chen and Stephan Finsterbusch, "Hackers Warn of Holiday Strike by Cyber Worm," *South China Morning Post Online* (English), http://www.aaj.tv/2010/10/holiday-concerns-in-china-over-cyber-superweapon/ (accessed February 19, 2012).

[115] Xinhua, "Super Virus Hits 6 Million Computers in China," Xinhua News, http://news.xinhuanet.com/english2010/china/2010-10/01/c_13538835.htm (accessed February 18, 2012). See also Chen and Finsterbusch.

[116] Guo.

[117]The PRC Central Military Commission, *China's National Defense in 2010* (Beijing: Information Office of the State Council, 2011), http://news.xinhuanet.com/english2010/china/2011-03/31/c_13806851.htm (accessed February 18, 2012).

[118] Li Daguang, "After One Opens 'Pandora's Box' of Cyber Warfare," Jiefangjun Bao Online, http://www.chinamil.com.cn/ (accessed February 19, 2012). See also Timothy Thomas, email message to author, February 7, 2012.

Beijing's efforts to avoid falling behind potential adversaries' developments in cyber warfare capabilities. Ye and Zhao acknowledged problems of attribution in cyberspace and the challenges associated with responding to an attack through multiple unregulated jurisdictions, but stressed Beijing's commitment to honing the PLA's cyber warfare skills. The reality of modern warfare, they argue, is that "every military cannot afford to be passive (in the cyber domain) but must make preparations to fight (through) the internet."[119]

In May 2011, Chinese Defense Ministry Spokesman Geng Yansheng announced the formation of a new cyber warfare unit called the "On-Line Blue Army." Open source evidence suggests that the cyber unit is small, with an annual budget of about 10 million Yuan.[120] Li Li, a military theorist at the Chinese National Defense University told *The People's Daily* that when compared to the offensive capabilities of other cyber powers, the Online Blue Army "is currently at its fledgling state," but added that it will be applied in an "online maneuver mode" and expressed optimism for future offensive capabilities.[121]

The Online Blue Army, although small, represents institutional, organizational, and doctrinal changes in the PLA and a shift from an offensive, network-focused cyber warfare strategy based on *shi* to a more direct offensive cyber attack strategy. Although translated versions of open source documents demonstrate Chinese anticipation that offensive cyber attack capabilities will be an instrumental component to achieve policy goals through military operations, no translated evidence exists to suggest that those theorists, or their military leaders, expect offensive cyber attack operations to hold the potential for violence. Additionally, the lack

[119] Ye Zheng and Zhao Baoxian, "How do you Fight a Network War," *Zhongguo Qingnian Bao*, June 1, 2011. See also Timothy Thomas, email message to author, February 7, 2012.

[120] Hannah Beech, "Meet China's Newest Soldiers: An Online Blue Army," *Time*, http://globalspin.blogs.time.com/2011/05/27/meet-chinas-newest-soldiers-an-online-blue-army/ (accessed November 20, 2011).

[121] Su Jie, "PLA 'Online Blue Army Gets Ready for Cyber Warfare," ECNS.cn, http://www.ecns.cn/2012/01-16/6254.shtml (accessed February 19, 2012).

of empirical evidence of China's willingness to use cyber warfare capabilities to enable conventional military operations stems from a lack of observable Chinese conventional military operations since the beginning of their cyber discourse in 1991.

Chinese cyber posture changed slightly in late 2010. Open-source publications suggest that the perceptions of cyber warfare held by many Chinese leaders and military theorists demonstrate a shift in the reality of cyber warfare. Additionally, Chinese investments in institutional organizational reforms reflect the power of discourse amid shifting perceptions of reality.

The Operational Significance of Stuxnet

When James Mulvenon said, "It's 1946 in cyber," he would have been just as accurate to suggest that it is the 1920s in cyber. Technological advances in weaponry and innovation in warfighting capacity prior to 1914, to include the emergence of lethal capacity from the new air domain, forced military theorists to reevaluate their warfighting theories and doctrine during the interwar period. Perhaps the best example of change generated by the shifting reality of warfare was Soviet Deep Battle Theory, developed through years of problem framing, reframing, and synthesis by Red Army theorists under the tutelage of Mikhail Tukhachevsky.[122]

Deep Battle served as the basis for weapon systems design and procurement, altered the organizational structure of Soviet combined arms forces, and provided the intellectual foundation for the Soviet campaigns of 1943 and 1944 that allowed the Red Army to seize the initiative from the Germans on the Eastern Front.[123] The Soviet military model, based on Deep Battle Theory

[122] Richard W. Harrison, *Architect of Soviet Victory in World War II: The Life and Theories of G.S. Isserson* (Jefferson, North Carolina: McFarland and Company, 2010), 4-5, 123-140. Captured by G.S. Isserson in *The Evolution of Operational Art* and *Fundamentals of the Deep Operation*, Deep Battle Theory resulted in a new combined arms Soviet military doctrine of operational shock and deep strike by 1936.

[123] David M. Glantz and Jonathan M. House, *When Titans Clashed: How the Red Army Stopped Hitler* (Lawrence, Kansas: University Press of Kansas, 1995), 148-169.

and exported to Soviet-aligned nations during the Cold War, inspired multiple changes in American theory and doctrine, most notably "Active Defense," "Air-Land Battle," and most recently "Network Centric Warfare" (NCW) Theory.[124]

NCW emerged from the rapid increase in corporate and industrial efficiency attributed to networked systems during the 1990s and the effectiveness of precision weapons during the 1991 Gulf War, embraced as the US theory of warfare in *Joint Vision 2020.*[125] NCW drove investment of hundreds of billions of dollars in weapons procurement across DOD, changes to force structure and doctrines, and production of networked weapons systems sold to allies through the US Foreign Military Sales Program and used in coalition environments like NATO.[126] Former Air Force Chief of Staff Ronald Fogleman summarized NCW during Congressional testimony in 1997 saying, "In the first quarter of the 21st century you will be able to find, fix or track, and target – in near real time – anything of consequence that moves upon or is located on the face of the Earth."[127]

Adam Elkus explained significant problems with NCW in a *Small Wars Journal* article entitled "The Rise and Decline of Strategic Paralysis." According to Elkus, NCW attempted to translate information superiority, gained through information advantages, into competitive advantages through network-dependent platforms, systems, and sensors but exposed critical US

[124] Brian M. Linn, *Echo of Battle: The Army's Way of War* (Cambridge, MA: Harvard University Press, 2007), 201-232.

[125] Joint Chiefs of Staff, "Joint Vision 2020: America's Military – Preparing for Tomorrow," *Joint Force Quarterly* (Summer, 2000): 62, 65-66. See also Arthur K. Cebrowski and John H. Garstka, "Network Centric Warfare: Its Origin and Future," *US Naval Institute Proceedings Magazine* 124 (January 1998), http://www.usni.org/print/3675 (accessed March 10, 2012).

[126] US Department of Defense, *The Implementation of Network-Centric Warfare*, Office of Force Transformation, Office of the Secretary of Defense (Washington, DC, 2005). In summary, networking forces improves information sharing. Collaborative information sharing allows shared situational awareness. Shared situational awareness allows real-time synchronization across all domains and facilitates rapid command decisions. Synchronization is a necessary component to mission success.

[127] Michael O'Hanlon, *Technological Change and the Future of Warfare* (Washington, D.C.: Brookings Institution Press, 2000), 13.

military capabilities and vulnerabilities to the computer network operations that became common long before Stuxnet. Military networks under attack, or sometimes just closed for routine maintenance, introduced compounding effects of chaos and complexity to military operations built around networked platforms. Compounding elements of chaos and complexity occasionally thickened the fog of war, requiring land component commanders to move away from their primary war fighting systems on occasion, in order to remain adaptive to events on the battlefield.[128]

Although considerable, the risk presented by such computer network attacks amounted to moderate inconveniences for battlefield commanders in comparison to cyber weapons that can reach through a digital system or weapons platform to inflict physical destruction, thus turning a critical requirement into a critical vulnerability.[129] According to SIPRI, trends indicate that emerging weaponry in nearly every country reflect NCW-inspired interoperability and networked synchronization.[130] Additionally, non-state actors from terrorist organizations to opposition movements and drug cartels leverage networked capabilities to extend their reach, synchronize their operations, and adapt their operational tempo by attempting to translate information advantages into competitive advantages.[131] Furthermore, current and future military operations

[128] Adam Elkus, "The Rise and Decline of Strategic Paralysis," *Small Wars Journal*, September 17, 2011, http://smallwarsjournal.com/jrnl/art/the-rise-and-decline-of-strategic-paralysis (accessed March 23, 2012). See also Antoine Bosquet, *The Scientific Way of Warfare: Order and Chaos on the Battlefields of Modernity* (New York: Columbia University Press, 2009), 169-173.

[129] Joint Publication 5-0, *Joint Operation Planning* (Washington, D.C.: Government Printing Office, 2011), III-24. Critical capabilities are "crucial enablers for a (center of gravity) to function and essential to the accomplishment of the adversary's assumed objective(s)." Critical requirements are "means, conditions, and resources that enable a critical capability to become fully operational." Critical vulnerabilities are "aspects or components of critical requirements that are deficient or vulnerable to direct or indirect attack in a manner achieving decisive or significant results."

[130] SIPRI Yearbook, http://www.sipri.org/research/armaments/transfers/databases/armstransfers (accessed March 11, 2012).

[131] Robert Bunker, "Mexican Cartel Operational Note No. 1: Mexican Military Operations Against Los Zetas Communications Networks," Small Wars Journal Blog Posts, December 17, 2011, http://smallwarsjournal.com/blog/mexican-cartel-operational-note-no-1 (accessed March 11, 2012). See

involving the US and its NATO allies are likely to take the form of a coalition, leveraging networked platforms and information-sharing tools among partnered countries, many of whom deploy forces with a great disparity in cyber defense capabilities, norms, and regulations.[132] Therefore, it is reasonable to expect that as more actors embrace NCW theory and associated weaponry, the character of attacks on critical capabilities, critical requirements, and critical vulnerabilities through the cyber domain will transition from an information threat to a physical threat.

Conclusion

Leon Panetta recently said, "the one thing I worry about most right now is knowing that a cyber attack is possible, and feeling that we have not taken the necessary steps to protect this country." The Defense Secretary and former director of the Central Intelligence Agency continued, "I think the capabilities are available in cyber warfare to virtually cripple this nation, and literally paralyze this country."[133] Panetta's comments underscore Michael Hayden's assertion that the reality of cyber warfare is physical destruction through cyber weapons, and reinforces James Mulvenon's concern that "we don't have all the conceptual and doctrinal thinking to support those weapons."

From the 1990s through 2010, leaders and theorists from the US, Russia, and China largely considered offensive network operations to be shaping operations designed to deny an

also Strategic Studies Institute, "Key Strategic Issues List, 2011-2012," US Army War College, http://www.strategicstudiesinstitute.army.mil/pubs/ksil.cfm?sortBy=organization (accessed March 11, 2012).

[132] Robert Riscassi, "Principles for Coalition Warfare," *Joint Forces Quarterly* (Summer, 1993), http://www.dtic.mil/doctrine/jel/jfq_pubs/jfq0901.pdf (accessed March 10, 2012). As far back as 1994, the Vice Chairman of the US Joint Chiefs of Staff, Robert Riscassi, predicted a future dominated by coalition warfare that required synchronization, interoperability, and precision information sharing to allow unified action.

[133] Hyun Soo Suh, "The 3 a.m. Call Panetta Fears the Most," CNN Security Clearance Blog, entry posted March 2, 2012, http://security.blogs.cnn.com/2012/03/02/the-3-a-m-call-panetta-fears-the-most/ (accessed March 10, 2012).

adversary network-centric capabilities or to establish conditions that enable other forms of direct military action. However, their conceptions of nonviolent and indirect (*shi*) applications of cyber power changed during the course of 2010. Stuxnet demonstrated that the reality of cyber warfare consists of potentially violent cyber actions that are difficult to attribute, ambiguous in nature, and directed at the trends of supposedly sophisticated weaponry and infrastructure that essentially turn critical capabilities and requirements into critical vulnerabilities. Today, leaders and theorists from the US, Russia, and China seem to share Panetta's concerns and agree that the character of modern warfare includes violent instruments of policy that attack through the cyber domain in order to compel an adversary to accept one's will.

Evidence suggests that the US, Russia, and China are taking extraordinary measures to build cyber armies capable of exploiting adversary vulnerabilities in closed and open networks. Cyber-related concerns and issues in all three countries constitute a priority topic in the newspapers, journals, and public forums as well as among top officials because tangible cyber vulnerabilities intersect across all elements of their modern societies and those of their potential adversaries. The Russians and Chinese both consider cyber capabilities to be useful tools to ensure internal security and order, although no evidence exists to suggest that their security leaders or theorists intend to pursue violent cyber weapons for use as domestic policy tools. Russia already demonstrated its will to use cyber tools to enable military achievement of political objectives and their leaders publicly endorse the pursuit of offensive cyber weapons to use against American targets. China takes a more subtle approach to the changes in cyber warfare but acknowledges that "informationalized" warfare must include the capacity for a direct attack through cyberspace.

The pursuit of answers to the narrowly focused research question at the heart of this monograph overturned additional questions that deserve further study. First, what efforts are nations or multinational organizations taking to increase attribution and decrease the ambiguity associated with cyber attack? How will those efforts affect cyber warfare? Second, is it reasonable to expect that sophisticated cyber weapons will become an effective strategic or operational deterrent? Third, does the US Army’s shift from “battle command” toward “mission command” and commander-centric operations represent a pivot away from NCW theory? How would such a move alter the American theory of warfare and associated procurement, doctrine, and organization?

Finally, Stuxnet provoked significant discourse on cyber warfare from the world’s major military powers. This monograph attempted to capture a snapshot of the evolving narrative of cyber warfare and the unique role that Stuxnet played as a proof of concept for what General Cartwright considered the cyber component of “operational fires.” The discourse on cyber warfare will expand and evolve, as will the number and nature of vulnerable nodes, and continue to approach what James Mulvenon referred to as “all the conceptual and doctrinal thinking” to support potent, weaponized codes.

BIBLIOGRAPHY

Albright, David, Paul Brannan, and Christina Walrond. “Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant?” Institute for Science and International Security. http://isis-online.org/isis-reports/detail/did-stuxnet-take-out-1000-centrifuges-at-the-natanz-enrichment-plant/ (accessed January 15, 2012).

Alexander, Keith B. “Statement of General Keith B. Alexander, Commander, US Cyber Command Before the House Committee on Armed Services, 23 September, 2010.” http://www.defense.gov/home/features/2010/0410_cybersec/docs/USCC%20Command%20Posture%20Statement_HASC_22SEP10_FINAL%20_OMB%20Approved_.pdf (accessed December 10, 2011).

Alperovich, Dmitri. “Revealed: Operation Shady RAT.” McAfee Threat Research. http://www.mcafee.com/us/resources/white-papers/wp-operation-shady-rat.pdf (accessed February 19, 2012).

Beech, Hannah. “Meet China’s Newest Soldiers: An Online Blue Army.” *Time*. http://globalspin.blogs.time.com/2011/05/27/meet-chinas-newest-soldiers-an-online-blue-army/ (accessed November 20, 2011).

Brain, Marshall. “What’s a Uranium Centrifuge?” HowStuffWorks. http://science.howstuffworks.com/uranium-centrifuge.htm (accessed March 23, 2012).

Bosquet, Antoine. *The Scientific Way of Warfare: Order and Chaos on the Battlefields of Modernity*. New York: Columbia University Press, 2009.

Burutin, Aleksandr. “Russian Military Policy for Information Warfare.” Intellibriefs. http://intellibriefs.blogspot.com/2009_03_22_archive.html (accessed February 11, 2012).

Carr, Jeffrey. *Inside Cyber Warfare: Mapping the Cyber Underworld*. Sebastopol, California: O’Reilly Media, 2012.

Carr, Jeffrey. “Project Grey Goose Phase II Report: The Evolving State of Cyber Warfare.” http://www.scribd.com/doc/13442963/Project-Grey-Goose-Phase-II-Report (accessed February 5, 2012).

Cartwright, James. “Joint Terminology for Cyberspace Operations.” Washington, D.C.: The Pentagon, 2010.

Cebrowski, Arthur K. and John H. Garstka. “Network Centric Warfare: Its Origin and Future.” *US Naval Institute Proceedings Magazine* 124 (January 1998). http://www.usni.org/print/3675 (accessed March 10, 2012).

Chen, Stephen and Stephan Finsterbusch. "Hackers Warn of Holiday Strike by Cyber Worm." *South China Morning Post Online* (English). http://www.aaj.tv/2010/10/holiday-concerns-in-china-over-cyber-superweapon/ (accessed February 19, 2012).

Chieh-cheng Huang, Alexander. “Transformation and Refinement of Chinese Military Doctrine: Reflection and Critique of the PLA’s View.” RAND Publications. http://www.rand.org/pubs/conf_proceedings/CF160/CF160.ch6.pdf (accessed February 17, 2012).

Clarke, Richard A. and Robert K. Knake. *Cyber War: The Next Threat to National Security and What To Do About It*. New York: Harper Collins, 2010.

Clayton, Mark. “A US Cyberwar Doctrine? Pentagon Document Seen as First Step, and a Warning.” *The Christian Science Monitor*, May 31, 2011.

CNA. “Risk Control Industry Guide Series: Electronic Component and Hardware Manufacturing Industry.” CAN Financial Corporation. http://www.cna.com/vcm_content/CNA/internet/Static%20File%20for%20Download/Risk%20Control/Industry%20Guide%20Series/ElectronicComponenent&HdweMfg.pdf (accessed January 15, 2012).

Directory of Russian Federation Defense-Related Agencies and Personnel. “Note on MVD Reorganization.” Ministry of Internal Affairs (MVD). http://www.fas.org/irp/world/russia/fbis/InternalAffairsMinistry.html (accessed February 6, 2012).

Echevarria II, Antulio J. *Clausewitz and Contemporary War*. New York: Oxford University Press, 2007.

Elert, Glenn. “Albert Einstein’s Letters to President Franklin Delano Roosevelt.” E-World. http://hypertextbook.com/eworld/einstein.shtml (accessed January 24, 2012).

Elkus, Adam. “The Rise and Decline of Strategic Paralysis.” *Small Wars Journal.* http://smallwarsjournal.com/jrnl/art/the-rise-and-decline-of-strategic-paralysis (accessed March 23, 2012).

Elser, Dennis and Micha Pekrul. “Inside the Password-Stealing Business: The Who and How of Identity Theft.” McAfee Labs Research Report. http://www.mcafee.com/us/resources/reports/rp-inside-password-stealing-biz.pdf (accessed September 2, 2011).

Falliere, Nicolas, Liam O Murchu, and Eric Chien. "W32.Stuxnet Dossier Version 1.4." Cupertino, California: Symantec Security Response, 2011.

Falliere, Nicolas. “Stuxnet Introduces First Known Rootkit for Industrial Control Systems.” Symantec Security Response Blog. Entry posted August 6, 2010. http://www.symantec.com/connect/blogs/stuxnet-introduces-first-known-rootkit-scada-devices (accessed 15 September 2011).

GE Energy Solutions. “Substation Automation.” General Electric. http://www.gedigitalenergy.com/automation.htm (accessed January 2, 2012).

GE Press Releases. “City of Leesburg Launches Grid Modernization Project to Better Manage Electricity Loads and Empower Customers,” General Electric. http://www.genewscenter.com/Press-Releases/City-of-Leesburg-Launches-Grid-Modernization-Project-to-Better-Manage-Electricity-Loads-and-Empower-Consumers-357f.aspx (accessed January 2, 2012).

GE Press Releases. “GE Energy Announces More than $3 Billion in New Customer Agreements.” General Electric. http://www.genewscenter.com/content/Detail.aspx?ReleaseID=13175&NewsAreaID=2 (accessed January 2, 2012).

Gibbs, Jack P. “Deterrence Theory and Research.” In *Law as a Behavioral Instrument*. Edited by Gary Melton, Laura Nader, and Richard A. Dienstbier. Lincoln, Nebraska: University of Nebraska Press, 1986.

Giles, Kier. “‘Information Troops’ – a Russian Cyber Command?” Oxford Conflict Studies Research Centre. http://www.conflictstudies.org.uk/files/Russian_Cyber_Command.pdf (accessed January 12, 2012).

Gjeltin, Tom. “US Seeks to Define Rules on Cyberwar.” National Public Radio. http://www.npr.org/templates/story/story.php?storyId=127411091 (accessed January 22, 2012).

Glantz, David M., and Jonathan M. House. *When Titans Clashed: How the Red Army Stopped Hitler*. Lawrence, Kansas: University Press of Kansas, 1995.

Global Security. “Gas Centrifuge Uranium Enrichment.” Weapons of Mass Destruction. http://www.globalsecurity.org/wmd/intro/u-centrifuge.htm (accessed March 3, 2012).

Guo, Qiang. “Web Superbug Seeking to Access China.” *Global Times*. http://china.globaltimes.cn/society/2010-09/577487.html (accessed February 19, 2012).

Harrison, Richard W. *Architect of Soviet Victory in World War II: The Life and Theories of G.S. Isserson*. Jefferson, North Carolina: McFarland and Company, 2010.

Hosenball, S. Neil. “Current Issues of Space Law Before the United Nations.” *Journal of Space Law* 2 (1974): 5.

Joint Publication 1-02. *Department of Defense Dictionary of Military and Associated Terms*. Washington, D.C.: US Government Printing Office, 2007.

Joint Publication 1-02. *Department of Defense Dictionary of Military and Associated Terms*. Washington, D.C.: US Government Printing Office, 2011.

Joint Publication 5-0. *Joint Operation Planning*. Washington, D.C.: Government Printing Office, 2011.

Joyner, Christopher C. and Catherine Lotrionte. “Information Warfare as International Coercion: Elements of a Legal Framework.” *European Journal of International Law* 12, no. 5 (2001): 845, 865.

Kakutani, Michico. Review of *Cyber War* by Richard Clarke and Robert K. Knake. *New York Times Book Reviews*, January 14, 2012.

Kaspersky Labs. “Cyberthreat Forecast for 2012.” Kaspersky Labs Forecasts. http://www.kaspersky.com/images/Kaspersky%20report-10-134377.pdf (accessed January 2, 2012).

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

Kokoshin, Andrey. “Kokoshin: Cyberwarfare Threat to Russian National Security.” One Russia Party. http://old.er.ru/er/text.shtml?18/2254 (accessed February 18, 2012).

Lam, Willy. “Beijing Bones Up it Cyber-Warfare Capacity.” The Jamestown Foundation. http://www.jamestown.org/programs/chinabrief/single/?tx_ttnews%5Btt_news%5D=36007&tx_ttnews%5BbackPid%5D=414&no_cache=1 (accessed February 2, 2012).

Langner, Ralph. "September 16, 2010." Stuxnet Logbook Blog. Entry posted September 16, 2010. http://www.langner.com/en/2010/09/16/stuxnet-logbook-sep-16-2010-1200-hours-mesz/#more-217 (accessed September 1, 2011).

Li, Daguang. "After One Opens 'Pandora's Box' of Cyber Warfare." *Jiefangjun Bao Online*. http://www.chinamil.com.cn/ (accessed February 19, 2012).

Linn, Brian M. *Echo of Battle: The Army’s Way of War*. Cambridge, Massachusetts: Harvard University Press, 2007.

Lynn, John A. *Battle: A History of Combat and Culture*. Boulder, Colorado: Westview Press, 2003.

Lynn III, William J. "Defending a New Domain." *Foreign Affairs* 89, no. 5 (2010): 97.

McAfee. "Protecting Your Critical Assets: Lessons Learned From Operation Aurora." McAfee Labs. http://www.mcafee.com/us/resources/white-papers/wp-protecting-critical-assets.pdf (accessed February 19, 2012).

Mshvidobadze, Khatuna. "The Battlefield on your Laptop." Radio Free Europe Radio Liberty. http://www.rferl.org/content/commentary_battlefield_on_your_desktop/2345202.html (accessed December 13, 2011).

Myakisheva, Marina. "What is Russia's Answer to Cyber Threats?" CNews.ru Reviews. http://eng.cnews.ru/reviews/printEn.shtml?2008/02/12/287829 (accessed February 11, 2012).

North Atlantic Treaty Organization. "International Cyber Incidents: Legal Considerations." NATO Cooperative Cyber Defense Center of Excellence. http://www.ccdcoe.org/publications/books/legalconsiderations.pdf (accessed February 11, 2012).

Nye Jr, Joseph S. *The Future of Power*. New York: PublicAffairs, 2011.

Office of the Chairman of the Joint Chiefs of Staff. *The National Military Strategy of the United States of America, 2011*. Washington, D.C.: The Pentagon, 2011.

Office of the Secretary of Defense. *National Defense Strategy*. Washington, D.C.: The Pentagon, 2008.

Office of the Secretary of Defense. *Quadrennial Defense Review*. Washington, D.C.: The Pentagon, 2006.

Office of the Secretary of Defense. *Quadrennial Defense Review Report*. Washington, D.C.: The Pentagon, 2010.

O'Hanlon, Michael. *Technological Change and the Future of Warfare*. Washington, D.C.: Brookings Institution Press, 2000.

Olga, Zakutnyaya. "Herald of Changes." The Voice of Russia Radio. http://english.ruvr.ru/2012/02/03/65244687.html (accessed February 20, 2012).

O Murchu, Liam. "Stuxnet Using Three Additional Zero-Day Vulnerabilities." Symantec Security Response Blog. Entry posted September 14, 2010. http://www.symantec.com/connect/blogs/stuxnet-using-three-additional-zero-day-vulnerabilities (accessed 02 September 2011).

O Murchu, Liam. "W32.Stuxnet Variants." Symantec Security Response Blog. Entry posted July 28, 2010. http://www.symantec.com/connect/blogs/w32stuxnet-variants (accessed September 2, 2011).

Open Net Initiative. "Russia." Open Net Research. http://opennet.net/research/profiles/russia (accessed March 4, 2012).

People's Republic of China Central Military Commission. *China's National Defense in 2010*. (Beijing: Information Office of the State Council, 2011). http://news.xinhuanet.com/english2010/china/2011-03/31/c_13806851.htm (accessed February 18, 2012).

Press Freedom Index. "Countries Under Surveillance: Russia." Reporters Without Borders. http://en.rsf.org/surveillance-russia,39766.html (accessed March 4, 2012).

Putin, Vladimir. "Be Strong: Guarantee of National Security for Russia." *Rossiyskaya Gazeta*, February 20, 2012. http://www.rg.ru/2012/02/20/putin-armiya.html (accessed March 4, 2012).

Qiao, Liang and Wang Xiangsui. *Unrestricted Warfare*. Beijing: PLA Literature and Arts Publishing House, 1999. http://cryptome.org/cuw.htm (accessed February 17, 2012).

Reuters. "China Paper Warns Military Thinking Outmoded." Reuters US Edition. http://www.reuters.com/article/2010/08/15/us-china-military-idUSTRE67E07020100815 (accessed February 10, 2012).

Reuters. "Russia Says Stuxnet Could Have Caused New Chernobyl" Reuters US Edition. http://www.reuters.com/article/2011/01/26/us-iran-nuclear-russia-idUSTRE70P6WS20110126 (accessed February 12, 2012).

Rid, Thomas. "Cyber War Will Not Take Place." *Journal of Strategic Studies* 1-28 (October 2011): 2-25.

Riscassi, Robert. "Principles for Coalition Warfare." *Joint Forces Quarterly* (Summer, 1993). http://www.dtic.mil/doctrine/jel/jfq_pubs/jfq0901.pdf (accessed March 10, 2012).

Roberts, Hal, and Bruce Etling. "Coordinated DDoS Attack During Russian Duma Elections," The Harvard Law Internet and Democracy Blog. Entry posted December 8, 2011. http://blogs.law.harvard.edu/idblog/2011/12/08/coordinated-ddos-attack-during-russian-duma-elections/ (accessed March 4, 2012).

Russian Federation Ministry of Defense. *Military Doctrine of the Russian Federation*. National Defense University. http://merln.ndu.edu/whitepapers/Russia2010_English.pdf (accessed February 9, 2012.

Rustrans. *The National Security Strategy of the Russian Federation to 2020*. Rustrans Wikidot. http://rustrans.wikidot.com/russia-s-national-security-strategy-to-2020-russian-text (accessed February 5, 2012).

SANS Institute. "Redefining the Role of Information Warfare in Chinese Society." InfoSec Reading Room. http://www.sans.org/reading_room/whitepapers/warfare/redefining-role-information-warfare-chinese-strategy_896 (accessed February 18, 2012).

Shackelford, Scott. "From Nuclear War to Net War." *Berkeley Journal of International Law* no 27.1 (February 2009). http://www.boalt.org/bjil/docs/BJIL27.1_Shackelford.pdf (accessed February 12, 2012).

Siemens Press Releases. "Presentation: The Company, 2012 (December 2011)." Siemens. http://www.siemens.com/press/pool/de/homepage/the_company_2012.pdf (accessed December 30, 2011).

Soldatov, Andrei. "Vladimir Putin's Cyber Warriors: The Kremlin's Ham-handed Effort to Squelch Online Dissent." *Foreign Affairs* Features. http://www.foreignaffairs.com/articles/136727/andrei-soldatov/vladimir-putins-cyber-warriors?page=show (accessed March 4, 2012).

Stein, Jeff. Review of *Cyber War* by Richard A. Clarke and Robert K. Knake. *Washington Post Book Reviews*, May 21, 2010.

Stevens, Kathryn and Larry K. McKee Jr. "International Cyberspace Strategies." National Security Cyberspace Institute. http://www.nsci-va.org/WhitePapers/2010-06-28-InternationalCyberspaceStrategies-Stephens-McKee.pdf (accessed February 12, 2012).

Stockholm International Peace Research Institute. "Arms Suppliers/Recipients Database." *SIPRI Yearbook*. http://armstrade.sipri.org/armstrade/page/toplist.php (accessed January 2, 2012).

Stockholm International Peace Research Institute. "Arms Transfers Database." *SIPRI Yearbook*. http://armstrade.sipri.org/armstrade/page/trade_register.php (accessed January 2, 2012).

Stockholm International Peace Research Institute. "Military Spending and Armaments." *SIPRI Yearbook*. http://www.sipri.org/yearbook/2011/files/SIPRIYB1104-04A-04B.pdf (accessed March 10, 2012).

Strategic Studies Institute. "Key Strategic Issues List, 2011-2012. US Army War College. http://www.strategicstudiesinstitute.army.mil/pubs/ksil.cfm?sortBy=organization (accessed March 11, 2012).

Su, Jie. "PLA 'Online Blue Army Gets Ready for Cyber Warfare." China News Service (English). http://www.ecns.cn/2012/01-16/6254.shtml (accessed February 19, 2012).

The United Nations. "Charter of the United Nations." Chapter 1: Purposes and Principles. http://www.un.org/en/documents/charter/chapter1.shtml (accessed January 14, 2012).

The United Nations. "Treaty on the Non-Proliferation of Nuclear Weapons." UN Office for Disarmament Affairs. http://www.un.org/disarmament/WMD/Nuclear/NPT.shtml (accessed January 8, 2012).

The White House. *Cyberspace Policy Review*. Washington, DC: The White House, 2012.

The White House. *National Security Strategy*. Washington, DC: The White House, 2006.

The White House. *National Security Strategy*. Washington, DC: The White House, 2010.

Thomas, Timothy. *The Dragon's Quantum Leap: Transforming from a Mechanized to an Informationized Force*. Fort Leavenworth: Foreign Military Studies Office, 2009.

Turabian, Kate L. *A Manual for Writers of Research Papers, Theses, and Dissertations*. 7th ed. Chicago: University of Chicago Press, 2007.

Ulasen, Sergey. "Rootkit.TmpHider." Wilders Security Forum Blog. Entry posted June 17, 2010. http://www.wilderssecurity.com (accessed October 19, 2011).

Ulasen, Sergey. "Rootkit.TmpHider." VirusBlokAda Blog. Entry posted June 17, 2010. http://anti-virus.by/en/tempo.shtml (accessed October 19, 2011).

US Congress. House Committee on Homeland Security, *Cybersecurity: Continued Attention is Needed to Protect Federal Information Systems from Evolving Threats.* 111th Cong., 2d sess., 2010.

US Department of Defense. *Department of Defense Cyberspace Policy Report: A Report to Congress Pursuant to the National Defense Authorization Act for Fiscal Year 2011, Section 934*. Washington D.C.: The Pentagon, 2011.

US Department of Defense. *The Implementation of Network-Centric Warfare*. Office of Force Transformation. Washington, D.C.: The Pentagon, 2005.

US Department of Defense. *Sustaining US Global Leadership: Priorities for 21st Century Defense*. Washington, D.C.: The Pentagon, 2012.

US Department of Defense Budget. “2013 Funding Highlights.” The White House. http://www.whitehouse.gov/sites/default/files/omb/budget/fy2012/assets/defense.pdf (accessed March 19, 2012).

US Department of Homeland Security. *Quadrennial Homeland Security Review Report: A Strategic Framework for a Secure Homeland*. Washington, D.C.: Department of Homeland Security, 2010.

US Joint Chiefs of Staff. “Joint Vision 2020: America’s Military – Preparing for Tomorrow.” *Joint Force Quarterly* (Summer, 2000): 62, 65-66.

Von Clausewitz, Karl. *On War*. Edited by Michael Howard and Peter Paret. Princeton: Princeton University Press, 1976.

Wang, Baocun and Li Fei. “Information Warfare.” *The Liberation Army Daily*, June 20, 1995. http://www.fas.org/irp/world/china/docs/iw_wang.htm (accessed February 18, 2012).

Waxman, Matthew C. “Cyber Attacks and the Use of Force: Back to the Future of Article 2(4).” *Yale Journal of International Law* no. 36.2 (Spring 2011): 443.

Weinberger, Sharon. “Hackers are Internet Shock Troops.” Aviation Week. http://www.aviationweek.com/aw/generic/story.jsp?id=news/dti/2010/05/01/DT_05_01_2010_p19-218221.xml&channel=defense (accessed February 5, 2012).

Xinhua. “Super Virus Hits 6 Million Computers in China.” Xinhua News. http://news.xinhuanet.com/english2010/china/2010-10/01/c_13538835.htm (accessed February 18, 2012).

Zetter, Kim. “How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History.” Wired Threat Level Blog: Privacy, Crime, and Security Online. Entry posted July 11, 2011. http://www.wired.com/threatlevel/2011/07/how-digital-detectives-deciphered-stuxnet/all/1 (accessed September 1, 2011).