CYBER WARFARE: ARMAGEDDON IN A TEACUP?

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

MASTER OF MILITARY ART AND SCIENCE
General Studies

by

BRADLEY L. BOYD, MAJOR, USA
B.A., University of California, Irvine, California, 1996

Fort Leavenworth, Kansas
2009-02

REPORT DOCUMENTATION PAGE

Form Approved OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From - To)*
11-12-2009	Master's Thesis	FEB 2009 – DEC 2009

4. TITLE AND SUBTITLE

CYBER WARFARE: ARMAGEDDON IN A TEACUP?

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Major Bradley L. Boyd

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

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

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

8. PERFORMING ORG REPORT NUMBER

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

10. SPONSOR/MONITOR'S ACRONYM(S)

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

12. DISTRIBUTION / AVAILABILITY STATEMENT

Approved for Public Release; Distribution is Unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

Security concerns over the growing capability of Cyber Warfare are in the forefront of national policy and security discussions. In order to enable a realistic discussion of the topic this thesis seeks to analyze demonstrated Cyber Warfare capability and its ability to achieve strategic political objectives. This study examines Cyber Warfare conducted against Estonia in 2007, Georgia in 2008, and Israel in 2008. In all three cases Cyber Warfare did not achieve strategic political objectives on its own. Cyber Warfare employed in the three cases consisted mainly of Denial of Service attacks and website defacement. These attacks were a significant inconvenience to the affected nations, but the attacks were not of sufficient scope, sophistication, or duration to force a concession from the targeted nation. Cyber Warfare offensive capability does not outmatch defensive capability to the extent that would allow the achievement of a strategic political objective through Cyber Warfare alone. The possibility of strategic level Cyber Warfare remains great, but the capability has not been demonstrated at this time.

15. SUBJECT TERMS

Cyber Warfare, Information Warfare, IW, CW, Cyber Space, Cyber Security

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			**19b. PHONE NUMBER** *(include area code)*
(U)	(U)	(U)	(U)	106	

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

MASTER OF MILITARY ART AND SCIENCE
THESIS APPROVAL PAGE

Name of Candidate: Bradley L. Boyd

Thesis Title: Cyber Warfare: Armageddon in a Teacup?

Approved by:

_____, Thesis Committee Chair
Jack D. Kem, Ph.D.

_____, Member
John R. Schatzel, M.S.A.

_____, Member
Commander Christopher R. Vega, B.S.

Accepted this 11th day of December 2009 by:

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

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

ABSTRACT

CYBER WARFARE: ARMAGEDDON IN A TEACUP?, by Bradley L. Boyd, 106 pages.

Security concerns over the growing capability of Cyber Warfare are in the forefront of national policy and security discussions. In order to enable a realistic discussion of the topic this thesis seeks to analyze demonstrated Cyber Warfare capability and its ability to achieve strategic political objectives. This study examines Cyber Warfare conducted against Estonia in 2007, Georgia in 2008, and Israel in 2008. In all three cases Cyber Warfare did not achieve strategic political objectives on its own. Cyber Warfare employed in the three cases consisted mainly of Denial of Service attacks and website defacement. These attacks were a significant inconvenience to the affected nations, but the attacks were not of sufficient scope, sophistication, or duration to force a concession from the targeted nation. Cyber Warfare offensive capability does not outmatch defensive capability to the extent that would allow the achievement of a strategic political objective through Cyber Warfare alone. The possibility of strategic level Cyber Warfare remains great, but the capability has not been demonstrated at this time.

ACKNOWLEDGMENTS

This thesis would not have been possible without the valuable opinions, advice, and guidance from some of the best instructors available to the United States Army. My Staff Group Advisor, Mr. John Schatzel provided some of the best instruction and insight that I have received in my entire military career. His words were like gold, and I learned something every time we interacted.

Several of the instructors throughout my tour at the Command and General Staff College either directly or indirectly helped with the formulation and production of this thesis. Specifically Dr. Jack Kem, Dr. Bill McCollum, Dr. Tony Mullis, LTC Loye Gau, and especially CDR Christopher Vega. Their effort and insight helped keep me on the right track.

The last group that provided grounding and guidance for this thesis was my classmates in Staff Group 6D. They were always eager to allow me to test ideas with them. Especially MAJ Christopher Filipietz, whose insight and experience always gave me something to think about.

And of course, this thesis would never have been completed without the tolerance and support of my wife Celeste. She kept me going and kept me focused. I thank her and the rest of the professionals who helped me from the bottom of my heart.

TABLE OF CONTENTS

Page

ACRONYMS

CERT	Computer Emergency Response Team
CII	Critical Information Infrastructure
CNA	Computer Network Attack
CNO	Computer Network Operations
CSIRT	Computer Security Incident Response Team
CW	Cyber Warfare
DDoS	Distributed Denial of Service
DIME	Diplomatic, Information, Military, Economic
DNS	Domain Name System
DoS	Denial of Service
EU	European Union
GDP	Gross Domestic Product
GTEP	Georgia Train and Equip Program
IDF	Israeli Defense Force
IO	Information Operations
IT	Information Technology
IW	Information Warfare
JP	Joint Publication
NATO	North Atlantic Treaty Organization
SQL	Structured Query Language
SSOP	Sustainment and Stability Operations Program
U.S.	United States

TABLES

Page

CHAPTER 1

INTRODUCTION

The Birth of Cyber Warfare

Cyber warfare did not begin with the construction of the Internet. Cyber warfare (CW) really finds its roots in hacking. To understand CW, hacking must be understood first. “Hacking” and “hacker” have become terms that most people associate with talented computer programmers who have learned to exploit systems that the average person does not completely understand. But, the term hacker pre-dates the emergence of the silicon chip based computers most people are currently familiar with.

> In the late 1950s, the MIT model railroad club was given a donation of parts, mostly old telephone equipment. The club’s members used this equipment to rig up a complex system that allowed multiple operators to control different parts of the track by dialing in to the appropriate sections. They called this new and inventive use of telephone equipment *hacking*; many people consider this group to be the original hackers. (Erickson 2008, 2)

The hacker culture stayed with telephone equipment as their medium of choice through the 1980s. The Bell phone networks became a target for hackers who specifically called themselves phone phreaks (Goldstein 2009, xxxvii). Early phone phreaks would whistle a sound at 2600 hertz into a telephone, which the system would recognize and allow access to the long distance phone network (Goldstein 2009, xxxvii). The phone phreak would then have access to the entire system the way an operator would (Goldstein 2009, xxxvii). This iconic frequency has become the title of one of the more influential hacker publications titled simply: 2600. Steve Jobs and Steve Wozniak were some of these early hackers exploring the phone networks and tricking the system into doing what they wanted (Wozniak 2006, 103).

As home computers began to emerge in the 1980s, hackers began to explore their potential and possibilities. The most recognizable early instance of this in popular culture was the movie “War Games.” In this movie, the main character uses his computer and the phone networks to enter into a military computer and wreak havoc. There is also a scene in this movie where the main character hacks a pay phone to make a free long distance call.

With the advent of the computer in homes, hackers began to learn more and more about computer code. This is essentially where the skill of the hacker lies today. The concept of modern hacking is quite simple. Exploit errors or loopholes in a computer system’s operating code thus allowing access to and manipulation of the system. Early hackers seemed more concerned with what could be done rather than hacking a system to get something from that system (Erickson 2008, 1). The possibilities of hacking became obvious very quickly as government, financial, educational, and security systems became more connected in the 1980s to promote efficiency of information transfer. In the 1990s the Internet granted the public unprecedented access to a variety of networks for financial transactions, communication, and commerce. Hackers quickly began to categorize themselves into different groups based on different goals. Hackers who are oriented towards increasing security and testing systems so that they might be strengthened called themselves White Hat Hackers. Those more criminally minded were termed Black Hat Hackers. And, of course those that dabble in both became Grey Hat Hackers.

The hacker community continued to grow throughout the 1980s and 1990s. Hacking became more public with the advent of malicious code in the form of viruses and software (malware). As people began to use the Internet more and more, personal

computers began to be affected. Self Replicating Computer Viruses had been present since the early 1970s, but mainstream citizens did not take notice until the Happy99 worm and the ILOVEYOU worm appeared in the 1990s. These worms had global effects that reached the lives and systems of everyday citizens. This self replicating global reach signals the start of real concern about a strategic level attack capable of striking throughout the globe, paralyzing systems, and preventing the flow of accurate information. People and governments started to fear computer hackers and their potential to disrupt systems that governments and economies relied on. Governments started to worry that if a single hacker can wreak havoc with an ILOVEYOU worm, then what could a nation accomplish with the full weight of national spending. In the late 1990s CW appeared to be a viable way to disrupt other nations, though how and to what extent were unclear.

What is Cyber Warfare?

Simply put, Cyber Warfare is war in cyber space. The definition of cyber space is more complicated. National Security Presidential Directive 54/Homeland Security Presidential Directive 23 (NSPD-54/HSPD-23) defines cyber space as, “The interdependent network of information technology infrastructures, and includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers in critical industries (Cyberspace Policy Review 2009, 1). This definition focuses on the hardware that creates cyber space, and not cyber space itself. This definition is technically accurate, but it automatically limits full appreciation for the potential of cyber space. This study will consider cyber space under the following definition. Cyber space is the electronic environment created by the interaction of

electronic networks, computer systems, communication arrays, and information storage devices. This definition implies that cyber space is greater than the sum of its parts. Any estimation of the capabilities and possibilities in cyber space must focus on cyber space as an environment with its own unique terrain, rather than a collection of systems.

If CW is warfare in cyber space, then is CW the same as Information Warfare (IW) or Information Operations (IO)? The answer is no. CW is related to IW and IO in much the same way as naval warfare and land warfare are particular components of warfare in general. CW is IW and IO, but IW and IO are not only CW. This distinction is important in any discussion about CW, because the terms are often used as describing the same act. IW and IO are much broader terms used to describe the use of information in any form, to conduct war or operations against another entity. CW specifically requires the use of cyber space to conduct war.

If CW is war in cyber space, then what does CW actually do? Formal doctrine and studies on CW are rare in an open source environment. However, many security professionals are asking questions about what CW actually does, or what CW is for. Martin C. Libicki from the RAND Corporation has classified CW into four basic capabilities. According to Libicki, CW can be used to conduct espionage, cause disruption, cause corruption, and cause distraction (Libicki 2007, 79). The specifics of these four capabilities will be discussed further in chapter 3.

Why is Cyber Warfare Important?

AT&T Research labs estimate that traffic and capacity of the Internet has grown at rates on average of 100 percent per year with some years in the mid 1990s seeing growth rates of 1000 percent per year (Coffman and Odlyzko 2009, 2). Essentially

capability and use of the Internet is at least doubling every year. Nokia/Siemens reports that the United States is the most interconnected nation in the world. In four of six measured categories, the United States was in first place (LECG, 2). Particularly the U.S. is in first place for Government and Business interconnectivity (LECG, 2). Table 1 illustrates the measure of U.S. interconnectivity.

Table 1. U.S. Interconnectivity Ranking

Component	Score	Weight
Consumer Infrastructure	0.57 (0.88)*	0.18
Consumer Usage and Skills	0.69 (0.69)*	0.18
Business Infrastructure	0.89 (0.89)*	0.44
Business Usage and Skills	0.65 (0.72)*	0.11
Government Infrastructure	0.93 (0.93)*	0.06
Government Usage and Skills	0.94 (0.94)*	0.02

Source: LECG, *Connectivity Scorecard 2009* (London: LECG, 2009), 2.
NOTE: * The score of the leading performer for this component.

As the world increases its connectivity, particularly in government and financial systems, policy makers have begun to sense a threat. Since this interconnectivity links several strategic systems throughout government and finance, policy makers have started to perceive a strategic vulnerability in this interconnectivity. The Chairman of the Senate Commerce, Science, and Transportation Committee, Senator John D. Rockefeller IV said, “It’s an understatement to say that cybersecurity is one of the most important issues we face; the increasingly connected nature of our lives only amplifies our vulnerability to

cyber attacks and we must act now" (Press Release 1 April 2009, 1). The President's Cyberspace Policy Review states that, "Threats to cyberspace pose one of the most serious economic and national security challenges of the 21st century for the United States and our allies" (Cyberspace Policy Review 2009, 1). As policy makers become more aware of CW and its potential, they begin to organize the government, allocate assets, and designate funding. A key issue is if CW's potential has been demonstrated, or is the government attributing a capability to CW that has not been demonstrated?

Primary Research Question

Most of the clamor over CW is based on estimated capability. Security blogs and movies are overloaded with possible scenarios that have CW causing Armageddon by infiltrating government or financial systems through the Internet. However, there is little in the way of demonstrated capability with which to develop solid CW policy. The implication of CW is that in skilled hands, with the backing of an enemy's national assets, a targeted nation can be brought to its knees by an attacker, or perhaps, simply the threat of attack. The most logical comparison for a weapon with this capability is nuclear weapons. Nuclear weapons are strategic assets and strategic weapons, but is CW the same? Libicki compares nuclear warfare to CW by comparing a firestorm to a snowstorm, "Nuclear warfare creates firestorms, destroying people and things for miles around. By contrast, even a successful widespread information attack has more the character of a snowstorm" (Libicki 2007, 39). He continues by explaining that, ". . . the effect of snowstorms, apart from a few heart attack and accident victims, is entirely temporary and rapidly over" (Libicki 2007, 39). No one knows what the aftermath of a strategic CW attack would look like. Would it resemble the aftermath of a firestorm or

the aftermath of a snowstorm? “People have seen the detritus left by small-scale hacker attacks, but no one has ever seen it work at the scale often claimed for it” (Libicki 2007, 41). This is the problem when discussing CW. What is needed is a real estimation of CW capabilities based on a demonstrated capability in order to develop policy, doctrine, and funding to properly deal with CW. This study will attempt to provide that estimation by asking: Can cyber warfare achieve a strategic political objective? In answering this question, this study will answer three secondary questions. First, is CW a strategic weapon? Second, has a nation been attacked with CW and subsequently conceded a strategic advantage to the attacker? Lastly, has CW been employed with the intent to achieve a strategic objective?

Definitions

Cyber Corruption: The use of CW to alter the intended purpose of a system.

Cyber Disruption: The use of CW to prevent a system from performing its intended purpose.

Cyber Distraction: The use of CW to use a targeted system to disrupt the decision making cycle of that system’s end users.

Cyber Espionage: The use of CW to gather information as part of or in preparation of a cyber attack.

Cyber Space: Cyber space is the electronic environment created by the interaction of electronic networks, computer systems, communication arrays, and information storage devices.

Cyber Warfare: Warfare conducted in cyber space.

Limitations

A great deal on the employment of cyber warfare is not open source information. In order to promote discussion about the topic, this study will only deal with unclassified and open source information.

Delimitations

This study will not address CW in the context of cyber terrorism or cyber crime. According to O. Sami Saydjari, small organizations and individuals do not have the funding or equipment necessary to conduct CW at the strategic level (Saydjari 2006).

The first step in answering the primary research question is to determine what current literature says about the subject. Chapter 2 will review the literature available on CW and its employment for strategic political gains.

CHAPTER 2

LITERATURE REVIEW

Cyber warfare continues to be an emerging field, and as such has little traditional literature associated with it. In fact there is little to be found in print that discusses the emerging possibilities, threats, and issues of cyber warfare. This study seeks to answer the question, “Can Cyber Warfare achieve a Strategic Political Objective?” The challenge in conducting a literature review on the subject is that there is very little demonstrated capability to be studied and analyzed in an open source forum. There are many opinions to be found, but few with supporting scholarship. The literature reviewed for this study was gathered from open source materials. Many of the open sources used were Internet-based, which leads to another challenge when dealing with the subject of cyber warfare. The preponderance of information related to cyber warfare is available on the Internet and not traditional print. Government agencies and the more prominent security professionals continue to produce printed materials about the subject, but many sources with valid and accurate information on the subject present their material solely on the Internet. The challenge becomes vetting these sources to determine who is credible and who is not.

The most significant obstacle to the conduct of a literature review in relation to this study’s primary research question is that no one has directly dealt with this subject by conducting research and then publishing their results. In fact the cyber security community in general seems to make the assumption that cyber warfare can achieve objectives at all levels of warfare. Consequently, they believe effort should be focused on defending against cyber warfare rather than first determining if such warfare is even

possible. As a result of this thinking there is little available to review that evaluates the strategic capabilities of this new form of warfare. However, there are a few security professionals, scholars, military thinkers, and politicians who are beginning to ask tough questions on cyber warfare's actual capabilities. This literature review will focus on their emerging questions and thoughts.

This literature review is divided into three sections. The first section reviews the literature associated with policy makers, primarily in the United States, Western Europe, and China. The second section will review military doctrine associated with cyber warfare to provide a military consensus on cyber warfare capabilities. The last section will deal with the broad world of cyber security professionals and academics. The review will then summarize the findings to provide a broad picture of the current view on cyber warfare's capabilities in relation to the primary research question.

Political Literature

Literature that is published by various governments is key to understanding how nations are posturing themselves to deal with cyber warfare. Policy statements and reviews give insight into how governments view cyber warfare's capabilities, and how they plan to exploit or deny those capabilities. Most governments protect their knowledge of and plans for cyber warfare with robust levels of information security. Governments do not seem especially interested in revealing how sophisticated their cyber warfare programs are, or what their long term plans are for the employment of cyber warfare. Most governments put forth information in the form of generalities and basic concepts. The political literature in this review will be divided by regional cyber warfare leaders who have demonstrated a willingness to publish their views on cyber warfare: United

States, Western Europe, and China. There are other powerful nations with significant cyber warfare capability such as Russia, Taiwan, and North Korea, but they are unwilling to reveal policy in regards to this issue.

United States

U.S. policy makers are still struggling to understand what cyber warfare is and why the government should be concerned. President Obama recently directed a *Cyberspace Policy Review* because, "It is the fundamental responsibility of our government to address strategic vulnerabilities in cyberspace and ensure that the United States and the world realize the full potential of the information technology revolution" (Cyberspace Policy Review, iii). The *Cyberspace Policy Review* fails to explain what the danger is because the policy makers do not understand what cyberspace is or what cyber warfare's capabilities are. The *Cyberspace Policy Review* repeatedly declares that the U.S. government must protect cyberspace. The language used in the Review demonstrates the lack of understanding by the administration. This lack of understanding is also present in the House of Representatives. When the House Committee on Science and Technology's Subcommittee on Research and Science Education reviewed the President's *Cyberspace Policy Review*, the Subcommittee Chairman David Wu said, "A secure and resilient cyberspace is vital not only for the federal government, but for business . . . and every single American" (Press Release, 16 June 2009). Both Presidential Policy and House Subcommittee review focus their statements on cyberspace as the vulnerable system, rather than focusing on U.S. security systems and infrastructure. The Senate Committee on Commerce, Science, and Transportation takes a more nuanced view as the Committee Chairman, Senator Rockefeller published in a press release that

states, “Currently, the U.S. has systems in place to protect our nation’s secrets and our government networks against cyber espionage, and it is imperative that those cyber defenses keep up with our enemies’ capabilities” (Press Release, 1 April 2009).

U.S policy makers appear divided on what is actually at risk in regards to cyber warfare, as most literature and policy statements fail to have a unified description on what is at risk and what capability exists. Even though the problem is not clearly defined in policy there is a consensus on what action the U.S. government should take. The President’s *Cyberspace Policy Review* and the Senates impending legislation *The Cybersecurity Act of 2009*, generally state the same goals: To raise awareness, appoint leadership, develop capability, provide funding, and provide oversight.

According to the available political literature, the U.S. is moving forward on cyber policy, but has failed to develop a unified vision and description of the problem. This difficulty with defining the cyber problem across agencies is not as prevalent in other parts of the world.

Western Europe

The European Union is much more advanced in the field of cyber warfare when compared to the United States. European Union Policy is much more comprehensive and direct in describing the threats posed by cyber warfare and what cyber warfare’s capabilities actually are.

European Union Policy is directed towards the protection of Critical Information Infrastructures (CII) and acknowledges that the disruption of these CIIs is essentially a strategic level victory. The *Communication From the Commission (of the European Communities at the Conference on Cyber-warfare Tallinn 2009) to the European*

Parliament, the Council, The European Economic and Social Committee and the Committee of the Regions on Critical Information Infrastructure Protection (March 2009) outlines the strategic nature of the threat and acknowledges cyber attacks as means to disrupt or destroy these strategic systems. Additionally, the European Community summarized the Conference on Cyber Warfare, Tallinn, Estonia, June 2009 with the document, *Towards a European Union Policy on Critical Information Infrastructure Protection* (June 2009). This summary includes the same basic points as in the previous communication from the Commission of European Communities, but specifically states a course of action to deal with the strategic threat posed by cyber warfare.

The European Union commissions use the attack against Estonia as their prime validation of cyber warfare to achieve strategic objectives. However, no such case study (open source) appears to exist. Regardless, the European Union is convinced that cyber warfare has achieved strategic objectives in the past, and will do so in the future. European Union Policy is oriented towards mitigating that strategic threat.

China

Evaluating Chinese policy in regards to using cyber warfare to achieve strategic objectives is inherently difficult due to language constraints. Therefore, to review Chinese views on strategic cyber warfare, intermediate sources must be used. Timothy L. Thomas has created a summary of Chinese cyber policy in his book *"Cyber Silhouettes: Shadows Over Information Operations"* (2005). Thomas describes two key aspects that demonstrate China's belief that cyber warfare can achieve strategic objectives. First, the Chinese government is transforming its army from a mechanized force to an informationized force (Thomas 2005, 80). If the assumption is made that China's main

effort for any strategic victory through warfare would be through its army, then the fact that the army is beginning to focus on its cyber warfare capability suggests that China sees cyber warfare as a means to achieve strategic ends. Second, according to Thomas, China's leaders have made policy that describes the use of Information Warfare as a means to achieve victory without war. This suggests that Chinese policy makers view cyber warfare (in the context of information warfare) as a tool to achieve victory without resorting to conventional armed conflict. This policy appears to require Chinese confidence in cyber warfare's ability to produce strategic results without other forms of warfare.

Military Literature

This study's review on military literature will focus on publications produced by military organizations and exclude analysis of military intentions by civilian scholars. This is to insure that only viewpoints articulated by the military are considered when establishing a consensus on military literature regarding the strategic capabilities of cyber warfare. In some cases, civilian literature quoting military literature may be used due to the lack of availability of military literature from certain nations. In this case only direct quotations will be considered and civilian analysis will be set aside. Military Literature will be divided into U.S., Western European, Chinese, and Russian sources.

United States

The U.S. military's primary publication that relates to cyber warfare is Joint Publication (JP) 3-13, *Information Operations* (February 2006). This publication essentially describes the way the U.S. military will relate to cyber warfare. This

publication does not use the term cyber warfare, and instead refers to Information Warfare, Information Operations, and Computer Network Attack. JP 3-13 describes Information Warfare (IW) as a task that the U.S. military performs in conjunction with other forms of warfare. JP 3-13 infers that the U.S. military will treat IW as an integral part of a combined campaign. JP 3-13 describes in detail many aspects of IW (and consequently cyber warfare) but does not describe any ability of IO, IW, or CNA to achieve any level of objective on its own.

Western Europe

Western European Military literature on cyber warfare is not prevalent. The European Union has created committees and studies to develop the European Union's cyber warfare capability, but the way European militaries view cyber warfare and information warfare appears to be fundamentally different than U.S. or eastern counterparts. Western European militaries appear to view cyber warfare as a criminal action, and not as a component of military doctrine. The British Ministry of Defence's most recent publication on European Defense comes in the form of "Ministry of Defence Policy Paper Number 3: *European Defence*." In this document the British Ministry of Defence makes no mention of cyber warfare, information warfare, information operations, or computer network attack. The British Ministry of Defence makes no real statement about cyber warfare in any available publication or on its website. Other militaries such as the German, Swedish, or French have not published documents that are open source regarding cyber warfare. Perhaps the European Militaries view cyber warfare as a criminal issue not a military issue. Clearly Europe is not ignoring the potential for

cyber warfare, but the European militaries do not currently appear to be contributing to the generation of doctrine relating to cyber warfare

China

The primary source for Chinese military doctrine is Timothy L. Thomas' book *Cyber Silhouettes: Shadows Over Information Operations.* Thomas describes Chinese military doctrine by quoting the Chinese People's Liberation Army Information Warfare Staff Proponent, General Dai Qingmin, ". . . General Dai Qingmin, listed six forms of IW in the authoritative Chinese journal Chinese Military Science: operational security, deception, computer network attack, electronic warfare, intelligence, and physical destruction" (Thomas 2005, 83). Thomas also quotes General Dai as describing three characteristics of Information Warfare: IW is an integrated combat posture that can greatly affect the war as a whole, it allows freedom of movement in the information dimension, and it influences events in the information dimension so as to affect events in the physical dimension (Thomas 2005, 84). Though not a doctrinal publication, the Chinese Military Science journal is important as it allows the Chinese Military's Staff Proponent, General Dai to indicate Chinese military doctrine in regards to cyber warfare. From this reference, it can be surmised that Chinese cyber warfare doctrine is similar to U.S. doctrine, but it also appears to play a more prominent role for the Chinese military. The Chinese see cyber warfare as an effective means to gain strategic parity with the United States and Western Europe.

Russia

Russia revamped its military policy in 2003 and 2004 focusing on avoiding overt conflicts and adhering to an independent line of behavior in foreign policy (Odnokolenko 2003). Timothy Thomas quotes the Russian journal "Military Thought," "the goals of contemporary armed struggle were obtainable by military, economic, and information-technical and information-psychological measures" (Thomas 2005, 79). Thomas also describes how the Russians view information conflict at different levels. Information weapons have a place at the strategic, operational, and tactical levels according to Russian military thinkers (2005, 79-80). As long as ten years ago, the Russians were considering the implications of CW.

In 1999 Russian Defense Minister Igor Sergeyev listed four priorities for the Russian Military: Guided and Electromagnetic Energy Weapons, Cyber Weapons, Stealth Unmanned Combat Platforms, All-Weather Reconnaissance and Accurate Long-Range Weapons (Thomas 2005, 81). Cyber Weapons claimed a more prominent position in Russian Military Officials minds compared to Western Military Officials in 1999.

Cyber Security Professionals

Cyber Security Professionals is a broad term that is claimed by just about anyone who voices an opinion on any word with "cyber" in front of it. In the case of this study, Cyber Security Professionals will mean individuals who are neither military nor governmental personnel, and who conduct scholarly research into the subject, perform cyber security work for business, government, or military communities, and are generally recognized as experts in their field. Most Cyber Security Professionals have a body of work and commentary from which to draw information. Some professionals write books,

but most post their analysis on web logs on their website, or a host website that they work for. This study will review literature from Martin C. Libicki, Bruce Schneier, and O. Sami Saydjari.

Martin C. Libicki

Libicki directly deals with the real capabilities of cyber warfare in his book *Conquest in Cyberspace*. This book is significant because it is the only academic source that applies academic rigor to cyber warfare to determine its ability to turn theory into capability. Libicki specifically states that cyber warfare is not strategic, because it cannot affect the strategic environment the way a true strategic weapon can (Libicki 2007, 37). Libicki specifically measures the non-demonstrated capability of cyber warfare to attain strategic objectives against the demonstrated capability of nuclear weapons to achieve strategic objectives. Libicki's analysis finds cyber warfare incapable of achieving strategic results like nuclear warfare. Libicki goes on to suggest that the defenses created in response to the threat of cyber attack are capable of neutralizing a cyber offense completely, and that this process is continuous. He suggests that cyber warfare is not "weaponized" yet (Libicki 2007, 98). The book ultimately suggests that no nation can develop a significant enough advantage in offensive or defensive capability to allow cyber warfare to gain a strategic advantage. He contrasts this with nuclear warfare, where there is essentially no viable defense.

Libicki does not completely discount cyber warfare as a tool for strategic influence. Libicki discusses long-term effects from corruption of data to noise generated by constant cyber activity such as worms, viruses, and others.

Bruce Schneier

Schneier's writings on cyber warfare are primarily on his web log, and have been compile into a book called, *Schneier on Security*. Although his opinions evolved over time, essentially he writes that cyber warfare may be capable of the sort of strategic effects that are generally suggested, but that no demonstrated capability of cyber warfare has taken place. He includes the conflicts in Estonia and Georgia in that assessment. Schneier takes a minority view in that he stipulates that warfare (including cyber warfare) by definition requires destruction and death. Cyber attacks that destroy networks and disrupt systems he does not classify as cyber warfare, but as cyber crime, or cyber terrorism depending on the incident. Schneier's main requirement for classifying and action as cyber warfare is human death. This implies that policy would be written to classify non-lethal cyber attacks as criminal and lethal cyber attacks as warfare. Schneier agrees that cyber attacks can achieve strategic objectives, but that without human death, the objectives were not achieved through warfare. Schneier also suggests that cyber attacks against strategic targets are not necessarily warfare, because no government would want to destroy financial networks for strategic advantage since all nations are dependent on the same networks.

O. Sami Saydjari

Saydjari is a cyber security consultant and has testified before congress on the strategic implications of cyber warfare. In his testimony, Saydjari states, "The U.S. is vulnerable to a strategically crippling cyber attack from nation-state-class adversaries." Saydjari is also the author of the Dark Angel study, which simulated a strategic attack on the United States by another nation-state. Dark Angel specified that cyber warfare would

be strategic in nature, but would be economic and social warfare. Meaning that strategic attacks would focus on civilian targets and infrastructure, with military targets secondary. The Dark Angel study was a watershed in research for cyber warfare as a strategic weapons system, and is one of the only simulations that is open source on the strategic capabilities of cyber warfare.

Summary

In general there is consensus in the available literature that cyber warfare can achieve strategic objectives on its own. Different sources view cyber warfare as more or less preeminent based on their own strategic position. Western nations with a surplus of military and economic power acknowledge cyber warfare's potential, but tend to view it as subordinate to conventional forms of warfare. Eastern nations that have a deficit of military and economic power when compared to the west tend to give cyber warfare a higher priority than their western counterparts. Civilian experts in the field tend to agree that cyber warfare has strategic implications, but cannot agree on whether cyber warfare as warfare can have the same strategic affect as conventional forms.

Literature on the subject of CW in regards to the primary research question is limited, hence the impetus for this study. The lack of literature makes research a challenging task. Chapter 3 will describe in detail the research methodology used in this study and will lay the groundwork for answering the primary and secondary research questions.

CHAPTER 3

RESEARCH METHODOLOGY

This chapter discusses the method for collecting the information that will answer the primary research question: Can nations use Cyber Warfare to obtain a Strategic Political Objective? As discussed, there is very little open source information on any strategic level cyber warfare. There are many examples of the employment of cyber warfare, but most of these incidents are firmly planted in the realm of nuisance warfare, which fail to produce any results of strategic importance. This research is intended to focus exclusively on cyber warfare that has strategic level effects.

Organization and Assumptions

The research will be organized into two parts. The first part will center around three CW case studies. The second part is an analysis of the three case studies, looking for patterns, commonalities, and differences. The concept of cyber warfare includes a broad field of activity. In order to narrow the field of research and obtain pertinent information about cyber warfare with strategic ramifications, certain assumptions must be made.

The first assumption is that any cyber attacks that achieved a strategic objective were of significant scope and effect that the attacks and their results were known to the world community. This eliminates the daunting task of trying to find attacks that no one knew occurred, and that achieve objectives so far reaching and subtle that their impact cannot be realized for years, or even decades. This is not implying that such attacks are not possible, but that they are not readily classifiable into demonstrated capability for the

purpose of research. The next assumption is the research must deal with demonstrated capability only, and not theoretical capability. While theoretical capability such as the destruction of the world financial system through a virus or denial of service attack may be possible, it is not known whether anyone has ever achieved results even closely approximating that goal. This makes the information available about such attacks speculative at best and propaganda at worst. In order to determine real conclusions about the strategic capabilities of cyber warfare, only cases that have demonstrated capability to attack targets with strategic significance will be considered as appropriate for research.

Part One

Part One begins with research focused around three case studies. Each case study consists of a demonstrated use of cyber warfare that is widely acknowledged by the world community and experts in the field. The first case study will be on the cyber attack on Estonia that occurred in April-May of 2007. The second case study will be on the cyber attack against Georgia that occurred in conjunction with the conventional attack by Russia in 2008. The last case study will research the cyber attacks that were conducted against Israel in 2008. Each case will follow an identical research format designed to help answer the primary research question. The format for each case study will consist of a general synopsis of the event that provides the context for the study. The study will then go on to answer several subordinate research questions.

The first question will be, “What were the conditions of National Power that existed for the target nation leading up to the cyber attack?” This question will be designed to lay the strategic framework for the impending cyber attack. This portion of the case study will describe the strategic situation in the target country by using the

DIME (Diplomatic, Intelligence, Military, Economic) model of analysis. The DIME model will describe the requirements that must exist for a successful cyber attack to occur. Specifically, what conditions existed politically, and what conditions existed technologically that allowed cyber warfare to be employed. This portion of the case study will also provide a set of strategic conditions that existed prior to the cyber attack that can then be used to compare against new conditions that existed after the cyber attack. The expected change in conditions will be used to evaluate the effectiveness of cyber warfare in achieving strategic objectives in the case study.

The second question, "What was the nature of the attack?" will be used to determine how the attack was conducted. This question will dip into the operational level as it discusses the operational goals of the cyber attack as means to achieve strategic objectives. This portion of the research will be organized according to the four types of cyber warfare that occur. Those categories are Espionage, Disruption, Corruption, and Distraction. The types of the cyber attack will be classified into one of these four categories, so that cyber warfare's effectiveness may be evaluated by type. Types that are categorized as Espionage will be types that are specifically designed to gather information in preparation or as part of a cyber attack. Types that are categorized as Disruption will be those that prevent a system from performing its intended purpose. This system can be an information system or it can be a mechanical system. Types that are classified as Corruption will be those that are designed to alter a system's intended purpose, whether the new purpose is for an enemy's purpose or simply against the target nation's purpose. Lastly, the types classified as Distraction will be those that use target systems to confuse the decision making cycle of system users.

The last question asked is, “What were the new conditions of National Power after the cyber attack?” This question will also employ the DIME model to provide direct comparison between conditions before and after the cyber attack. Key strategic political issues will be compared directly in this portion.

Part Two

Part Two of the research is analysis of the three case studies. All three case studies will be evaluated in relation to each other. Emerging patterns will be documented for analysis. This pattern analysis will be used to answer the primary research question, “Can cyber warfare be used against nations to achieve strategic political objectives?” The pattern analysis will be organized into three categories based on the secondary research questions: (1) Was CW employed in the case studies with the intent to achieve a strategic political objective? (2) Was the case study nation attacked with CW and subsequently conceded a strategic political objective? (3) Was CW a strategic weapon?

The first question will evaluate whether CW was employed by an aggressor intent on using CW as a tool to gain a strategic political objective. The second question will evaluate whether such an attack actually occurred. The third question will evaluate whether CW was a weapon capable of strategic affect in the case study, or just an incidental player in a larger conflict.

Table 2 graphically depicts the results of the analysis in chapter 4. Each section will be answered with a simple yes or no. The yes or no answers will indicate a trend to answer the primary research question.

Table 2. Shell: Summary of Case Studies Relative to Subordinate Research Questions			
	Q1: Weaponized	Q2: Intent	Q3: Concession
Estonia			
Diplomatic			
Information			
Military			
Economic			
Georgia			
Diplomatic			
Information			
Military			
Economic			
Israel			
Diplomatic			
Information			
Military			
Economic			
Trend			

Source: Created by Author.

Strengths and Weaknesses of Research Method

This research method has several strengths that make it suitable for this topic. First, by using case studies, the research will consist of demonstrated capability of cyber warfare rather than speculation and hypothesis. Second, all the case studies are on events that have taken place in the last two years. This makes the information relevant and timely. Technology changes rapidly, but with research conducted on recent events, the conclusions from the study will be useful immediately. Comparing three case studies rather than a single study, a pattern analysis is used to generate relevant conclusions that can be applied to future conflicts that employ cyber warfare. As cyber warfare policy is modernized and implemented there is precedent that can be used to justify decisions made by policy makers.

Along with the strengths, there are a few weaknesses in this methodology. First, the amount of quantifiable data available is not enough to decisively conclude an answer to the research question. This means that the qualitative data will have a much more prominent role. This carries the danger that qualitative data will be called into question because it comes close to opinion. Second, data on the case studies are difficult to gather, because most nations do not want to reveal their vulnerabilities (past or present), and the attacking party is not willing to identify itself, much less explain its objectives and techniques. This makes the case study more of a crime scene analysis than a traditional case study. The research into the incident becomes an exercise in forensic cyber analysis.

Despite these weaknesses, the case study methodology will provide the most accurate assessment of cyber warfare as a tool for nations to achieve strategic political

objectives. The next chapter will implement the research methodology, and set the conditions to answer the primary research question.

CHAPTER 4

ANALYSIS

In order to answer the primary research question, data must be gathered from known cyber attacks that have a strategic level nature, a demonstrated capability, and are primarily attacks between nation states. These criteria will provide the proper framework to determine if CW can be used to obtain a strategic political objective between nations. This paper will review three case studies: The cyber attack against Estonia in 2007, the Russia-Georgia War of 2008, and the Gaza War of 2008-2009. This chapter will be divided into two parts. The first will include the three case studies. The second part will be a review of the case studies looking for general trends of the three cases.

Part One Analysis of Case Studies

Case Study Number 1: Estonia 2007

Overview of Cyber Attack on Estonia

Estonia is a small Baltic country, formally a Soviet satellite state that received its independence from the Soviet Union in 1991. Estonia has about 1.4 million inhabitants spread over 45,226 square kilometers (Link 2009, 4). Estonia became a member of NATO on 2 April 2004, and joined the European Union on 1 May 2004 (Link 2009, 4). In early 2007, the government of Estonia decided to relocate a World War II Soviet War Memorial from the capital city of Tallinn to a military cemetery outside of the city (Link 2009, 6). The Russian government as well as many Russia citizens were outraged at the perceived slight (Traynor 2007). It is generally accepted that this was the catalyst for the cyber attacks that occurred soon after the uproar over the war memorial. The attacks did

not occur as part of a concerted effort. This is apparent when trying to determine the exact dates of the attack. Since the attacks typically manifested in increased usage of Estonian servers to the point of collapse, it is difficult to determine when the attack actually started, as usage is continuous. A line can be drawn at the point where usage surged to the point that service was no longer possible. Additionally, the nature of the attack can be used to estimate the start of the battle. An obvious malicious attack can be indicative, but it is difficult to determine whether the attack is related to a concerted effort. In most instance though, the attackers wanted it known that the attack was in response to the Russian War Memorial issue. They accomplished this by not only shutting down Estonian websites, but defacing them as well. All these factors serve to give the approximate dates that encompass the cyber attack. The period from 27 April 2007 through 21 May 2007 generally encompasses the cyber attack against Estonia.

Once the attacks ended, Estonia began to take stock of its condition. Did the attacks achieve anything for the attackers? Was the Estonian government or nation actually damaged from the attacks? To understand this, a snapshot must be taken of Estonia prior to the issue with the War Memorial and the subsequent cyber attacks. This snapshot will be taken through the lens of instruments of national power. The DIME model will be this lens.

Conditions of National Power Prior to 27 April 2007

To assess the strategic success of the cyber attacks against Estonia in 2007, the DIME model of National Power will be used to compare conditions before the attack and conditions after the attack. With this comparison conclusions can be drawn as to whether

the attacker or attackers were able to gain a strategic objective through employment of CW.

Diplomatic

In 2006 and leading up to early 2007 the diplomatic situation in Estonia centers on relations with the European Union (EU) and Russia (Ehin 2006, 9). European Enlargement created unique diplomatic problems for the Estonian government as it seeks to further its interests. European Enlargement is the process that is still occurring as the EU increases its number of member states (Ehin 2006, 9). Estonian was against European Enlargement in the 2003-2004 timeframe even as it sought to join the EU (Ehin 2006, 23). Increased engagement with the West was seen as more beneficial than looking towards Russia and the East. Engagement with the EU and the West would bring immediate aid in the form of financial and technological assistance, where Russia could not supply those incentives (Kononenko 2006, 83). European Enlargement would bring unwanted changes as the systems in place would adapt to new norms imposed by the presence of new member states and additional social and cultural norms. The Estonian Government in 2004 saw European Enlargement as bringing closer political union with the West, common policies that Estonia would have to abide by, and common positions in dealing with external national politics (Ehin 2006, 23).

In 2005 a new government came to power in Estonia, a government that was not against European Enlargement (Ehin 2006, 25). This new Estonian government was pro EU Constitution, pro globalization, and accepting of the EU social model (Ehin 2006, 24). Acceptance into the EU in 2004 and full support in 2005 allowed the Estonian government to redefine its role with Russia. In order to deal with Estonian issues

diplomatically, Russia was required to go through the EU (Kuusik 2006, 67). Estonia could now deal with Russia as a full partner (through the EU) and not as a former satellite state (Kuusik 2006, 66). Russia still attempted to exert control over Estonia by professing concern of the one hundred thousand ethnic Russians living in Estonia (Kuusik 2006, 67).

Estonia began to increase its support for European Enlargement by contributing diplomatic support to new prospects for entry into the EU (Orav 2006, 81). Estonia began to increase relations with Georgia, Ukraine, and Moldova with presidential visits and support for their entry into the EU (Orav 2006, 81). Estonia also saw an increase in diplomatic relations with Macedonia, Bosnia, Kosovo, Serbia, and Montenegro, because Estonia sees them as future EU and NATO partners (Orav 2006, 82).

Estonia began to distance itself from Russia diplomatically from 2005 through 2007. The movement of a Russian War Memorial in 2007 may have sparked the CW attacks in 2007, but the Estonian disrespect of the Russian Victory Day for World War II was not a new issue. In 2005 Russia insisted that Estonia celebrate Victory Day on 9 May by attending celebrations in Russia (Kuusik 2006, 69). The Estonian government refused on the grounds that the Soviet Union illegally annexed Estonia in 1940 (Kuusik 2006, 69). This argument was repeated in 2006 (Kuusik 2006, 69). In 2007 the argument was not revisited, because it was overshadowed by the cyber attacks in April and May.

Estonia's diplomatic efforts and focus immediately prior to the cyber attacks in 2007 were towards developing joint activities through the EU. Estonia sees the EU as a source of diplomatic strength and protection, as demonstrated by the Estonian Political Director Aivo Orav:

> It is becoming ever more obvious that bilateral relations can be developed more effectively through the joint activities of the EU, especially its common foreign policy. The common foreign and security policy of the European Union provides us with better opportunities for protecting our interests more effectively. But at the same time, it also imposes on us a certain framework for our relations with third countries. (Orav 2006, 83)

Estonian diplomacy was directed towards the West and the EU in the spring of 2007. Estonia was working diplomatically to increase its ability to interact with Russia as an equal nation, and achieve its interests. The EU was a tool to do this. This action by Estonia is seen in Russia in a larger context of central European influence. If the Baltic states, Ukraine, Georgia, and Moldova are absorbed by the EU, Russia would lose the greater part of its ability to affect diplomatic action in central Europe.

Information

Estonian information power is closely related to Estonian security. Estonia is one of the few countries in the world to allow voting to occur over the Internet (Link 2009, 7). Estonia allowed Internet voting to occur for local elections in 2005, and then it allowed Internet voting for national Parliamentary elections in 2007 (Link 2009, 7). This is rare for a government to trust its information systems enough that it allows elections to be conducted via these systems. This willingness demonstrates that Estonia has aggressively embraced the information age. 90 percent of people aged twelve to twenty-four use the Internet, and 58 percent of those aged twenty-five to forty-nine use the Internet in early 2007 (Link 2009, 7-8). 95 percent of Estonian banking transactions were conducted electronically. 90 percent of the population used mobile phones, and 50 percent of parking fees were collected via mobile networks (Link 2009, 8).

Estonia was rapidly increasing its information interconnectivity up through 2007. Estonia was fully embracing the benefits of information technology in the private sector, and even more so in the government sector. 100 percent of all central government agencies were equipped with information technology needed to perform their functions (Link 2009, 8). Estonia's rapid employment of information technologies was increasing their ability to employ information power, but it was also creating security vulnerabilities that were not being addressed quite as rapidly. The evidence for this exists in the initial results of the cyber attacks in 2007. Estonian information security procedures were not capable of preventing the attacks, but once started they were able to respond effectively.

Military

Estonia's military power in 2006 and early 2007 is oriented around Estonia's desire to be a contributing partner in NATO and the EU. Estonia sought to increase its military capability, and "further advance European security cooperation and to assist the democratic countries beyond the Eastern borders of the EU and NATO" (Baltic Security and Defence Review 2007, 274). Estonia identified the defense and military assistance to Ukraine, Georgia, and Moldova as top security priorities (Baltic Security and Defence Review 2007, 274). Estonia assisted Ukraine and Georgia with the construction of modern defense systems in 2006 and early 2007 (Baltic Security and Defence Review 2007, 274). Estonia saw itself as a potential defense benefactor to other former Soviet satellite states who were struggling towards democracy. 2006 was an extremely strong year economically for Estonia and resulted in the forecasting of increased defense spending to support the previously mentioned programs (Baltic Security and Defence Review 2007, 277). Estonia approved a 33 percent increase in defense spending for 2007

from 2006 (Baltic Security and Defence Review 2007, 277). The majority of this budget increase was earmarked for purchasing military equipment and enticing volunteers to join the military by increasing salaries 15 percent (Baltic Security and Defence Review 2007, 277). Estonia specifically wanted to increase its ability to fight at night with night vision equipment and advanced light weaponry, and was purchasing systems to do so (Baltic Security and Defence Review 2007, 277).

In addition to increasing the capabilities and size of its military, Estonia was contributing what assets it had available to NATO missions in Afghanistan and Coalition efforts in Iraq (Baltic Security and Defence Review 2007, 276). Estonia contributed roughly reinforced company sized units to each conflict, reaffirming its commitment to the international security stage in support of democracy (Baltic Security and Defence Review 2007, 276).

Estonia's military actions indicate an effort to distance itself from security reliance on its Russian neighbor. Estonia pursued a military policy that looked towards the West, not only to secure itself, but as a chance to assist other nations to throw off reliance on Russian security institutions and norms that were left over from the Cold War. Estonia was working towards becoming a catalyst for change in Eastern Europe from old Russian paradigms to new EU models.

Economic

Estonia was rapidly becoming a Baltic economic powerhouse in 2006. Estonia's economy grew almost twelve percent in 2006, and its Gross Domestic Product (GDP) grew over 11 percent (The Baltic Times 2007).

Estonia's most significant economic sectors are Information Technology (IT), Transportation, Energy, Tourism, and Banking. Estonia was a leading adapter of new information technologies. In 2006 Estonian telecommunications companies were adapting 3G mobile communications networks for the largest cities in Estonia granting unprecedented mobile Internet access for Estonian users (Estonian Economy 2006, 3). The Estonian state controlled power company also announced that it would soon allow Internet access over its power lines using new Power Line Communication technology (Estonian Economy 2006, 3). This technology would allow Internet speeds approaching 200 mbps, hundreds of times faster than what was then available in most households, or via the 3G network (Estonian Economy 2006, 3).

In the Transportation sector Estonia decided not to privatize its railway systems, because the private company involved did not meet all the obligations for the sale (Estonian Economy 2006, 4).

In the energy sector Estonia only imports about one third of its energy needs (Fabian-Marks 2006, 1). Estonia generates 56 percent of its energy from its own deposits of oil, but Estonia does rely on Russia to provide natural gas. Of the one third of its energy needs that Estonia imports, 48 percent is oil and 41 percent is natural gas (Fabian-Marks 2006, 1). Russia is the sole supplier of natural gas to Estonia, which creates unique security concerns and reliance on Russia (Fabian-Marks 2006, 1).

The Nature of the Cyber Attack

Summary

The cyber attack against Estonia in 2007 was primarily oriented towards government and government related Internet sites (Toth 2007, 1). Civilian sights were

also targeted, but not to the same extent as the government sites (Toth 2007, 1). No military sites were attacked, perhaps demonstrating that the attackers were trying to manage their aggression and reduce provocation (Link 2009, 5). Tables 3 through 5 present a picture of the attacks by location, date, and duration.

Table 3. Volume of Cyber Attacks in Estonia 27 April 2007–21 May 2007

Number of Unique Attacks (128)	Location of Attack
36	Estonian State Portal
35	Estonia Police Website
35	Ministry of Finance Website
7	Estonian Parliament Website
6	Ministry of Agriculture Website
4	Estonian Informatics Center
2	Ministry of the Environment Website
2	Social Ministry Website
1	Starman Internet Server Estonia (Commercial Internet)

Source: Beatrice Toth, *Estonia Under Cyber Attack,* www.cert.hu/dmdocuments/ Estonia_attack2.pdf (accessed 18 July 2009), 1.

Table 4. Summary of Unique Attacks by Date (significant volume)	
Number of Attacks (128)	Date
21	3 May 2007
17	4 May 2007
31	8 May 2007
58	9 May 2007
1	11 May 2007

Source: Beatrice Toth, *Estonia Under Cyber Attack,* www.cert.hu/dmdocuments/ Estonia_attack2.pdf (accessed 18 July 2009), 2.

Table 4 shows that this was not a continuous attack, but that the attacks surged on various days. Particularly on 9 May 2007, which is the day that Russia commemorates the defeat of Hitler in Europe (Toth 2007, 1). The distribution of attack volume suggests that the attacks were definitely related to the conflict over the Soviet War Memorial and the Estonian Governments decision to move the memorial from the capitol.

Table 5. Attack Durations	
Number of Attacks	Duration of Attacks
78	1 minute – 60 minutes
17	< 1 minute
16	1 hour – 5 hours
8	5 hours – 9 hours
7	> 10 hours

Source: Beatrice Toth, *Estonia Under Cyber Attack,* www.cert.hu/dmdocuments/Estonia_attack2.pdf (accessed 18 July 2009), 2.

Table 5 shows 61 percent of the attacks lasted under one hour. That does not necessarily mean that the affected site was operating again as soon as the attack ceased, but it does imply that the attacks could not be sustained for long periods without significant effort, or that Estonian countermeasures possibly had some effect.

Estonian Internet Security Professionals were not unable to defend their system. The attacks were coming from the .ru domain, so Estonia blocked all Russian domains (.ru) in order to prevent Russian interaction with Estonian systems (Toth 2007, 4). Estonia believed it was a concerted effort by the Russian government. There has been no unclassified evidence to support that claim, but it is generally accepted as accurate. Regardless, the attackers either quickly circumvented that countermeasure, or the countermeasure was misguided to begin with. The attacks continued as part of a botnet with origins from around the world. Toth quotes Estonian officials as suggesting that attacks were coming from bots located in the U.S, China, Vietnam, Egypt, and Peru (Toth

2007, 5). Eventually, Estonian security professionals shut down traffic coming into Estonia from the international community as well (Traynor 2007).

Estonia acted politically to get the international community to intervene on its behalf. Estonia asked allies in the European Union, and NATO to come to its aid with little result (Toth 2007, 5).

One interesting countermeasure that has also been seen in other cyber conflicts is the reaction from Estonian civilian "hackers." Similar to U.S. hackers who counterattacked China during the conflict over a wayward EP-3 and Chinese fighter jet collision in 2000, Estonian hackers began to attack Russian sites (Toth 2007, 6). There is no evidence that these counterattacks by Estonian civilian hackers had any effect on neutralizing the cyber attacks against Estonia.

The attacks against Estonia did not occur across the spectrum of CW capabilities. Using the classification suggested by Martin Libicki, CW can be used to conduct espionage, disruption, corruption, and distraction (Libicki 2007, 79). The attacks against Estonia appear to have focused on disruption and corruption. Evidence is not plentiful of attacks that occurred with the intent of espionage or distraction.

Espionage

One of the key capabilities of CW is that of espionage. In the case of Estonia there is no unclassified evidence that shows any sort of cyber espionage took place between 27 April 2007 and 21 May 2007. After Action Reviews conducted by Estonia's Computer Emergency Response Teams (CERTs) and international CERTs involved with the attacks do not acknowledge any espionage related attacks against Estonia during the period in question (Link 2009, 9 and Toth 2007, 1-3).

Disruption

This element of CW was the primary element employed against Estonia during the 27 April 2007 to 21 May 2007 attacks. The attackers used various types of Distributed Denial of Service (DDoS) attacks to prevent Estonia websites from functioning properly (Toth 2007, 1). A DDoS attack floods a website with traffic causing it to be unable to interact with users or to potentially shut down. Within the first twenty-four hours of the Estonian attacks six government websites were unreachable due to DDoS attacks (Link 2009, 11). Also interesting is that nine government websites remained reachable despite being attacked (Link 2009, 11).

While the British Guardian newspaper reported that three of Estonia's largest news organizations, two of its largest banks, and several political party websites were temporarily unable to provide service (Traynor 2007) there is no official evidence to support that the DDoS attacks had any lasting impact on website functionality within Estonia. The DDoS attacks appeared to resemble Martin Libicki's "snow storm" concept, in that Estonian Internet users were extremely inconvenienced during the duration of the DDoS, but security workers were able to mitigate the effects and return operations to normalcy within days. The DDoS attacks were not new techniques, so Estonian CERT and Internet Security Professionals were able to quickly deal with the various techniques, but the persistence and duration of the attacks made the task more difficult (Kaeo 2009, 16).

Corruption

In the case of Estonia, several political and government websites were corrupted to display pro Soviet propaganda rather than their true content (Toth 2007, 3). This

corruption was relatively benign in that the only effect was the display of the propaganda. Once the propaganda was removed from the sites, the functioning of the systems remained intact (Toth 2007, 3). This corruption was more a case of cyber graffiti. Toth states that, “The pages were nevertheless restored in short order” (Toth 2007, 3).

Distraction

Distraction is difficult to identify, because it can use deceit or the truth to affect the decision making cycle of system users. In Estonia there are no identified cases of the employment of distraction during the attacks in 2007. There is the potential that the entire event was a distraction effort to influence Estonian policy makers’ decision cycle on other issues unrelated to the attack. In that case, distraction becomes the key strategic element of the attacks against Estonia. It is clear that no distraction was employed to affect the Estonian government’s decision regarding the Russian War Memorial issue. Were the attacks an attempt to gain a strategic objective from Estonia by affecting the Estonian government’s decision-making process through distraction? Analysis of the elements of national power post-attack may demonstrate this potential.

Conditions of National Power After 21 May 2007

The conditions of national power after the cyber attacks will be used as a yardstick to compare the possible strategic results from the attack. If the cyber attack was effective at the strategic level, then there should be some change in the elements of Estonia’s national power.

Diplomatic

Estonia's diplomatic stance towards Russia deteriorated immediately after the cyber attacks in 2007 and continued to remain cool throughout the following year (Woerhel 2007, 3). Ethnic Russians living in Estonia have not been integrated into Estonian citizenry, because they are legally forbidden to become citizens. Russia is still frustrated with this aspect of Estonian law, but appears unable to change the situation (Woerhel 2007, 3). Estonia still enjoys close relations with its Scandinavian, Baltic, and Finnish neighbors, and continues to be an advocate for Westernization of Ukraine, Moldova, and Georgia (Woerhel 2007, 3). In 2007 Estonia continued to push for closer relations with the U.S. to include a waiver for a visa requirement for Estonian citizens (Woerhel 2007, 5). If the cyber attacks were a strategic effort by Russia to influence Estonian diplomatic relations, it was counterproductive. Estonian diplomatic ties with Western allies strengthened immediately following the attacks as Western governments went to Estonia's aid. Assistant Secretary of State Daniel Ford said in 2007 the Baltic states, "will never be left alone again, whether threatened by old, new, or virtual threats. . . ." (Woerhel 2007, 5).

Information

The immediate response to the cyber attacks in regards to the Estonian information infrastructure was to look for aid in combating the effects of the attacks. Within a month after the start of the cyber attacks Estonia sought aid from NATO and the EU (Toth 2007, 5). Several western nations provided Computer Security Incident Response Teams (CSIRTs) to stave off the attacks and recover the sites affected (Toth 2007, 5). Estonia looked to NATO and the EU for increased protection of its information

infrastructure, going so far as to call for unified approaches to the problem. Estonian Defense Minister Jaak Aaviksoo said in May 2007, “Taking into account what has been going on in Estonian cyber space, both the EU and NATO clearly need to take a much stronger approach and cooperate closely to develop practical ways of combating cyber attacks” (Toth 2007, 6).

In response NATO established a “Center of Excellence” in Tallinn within one year of the attacks to conduct training and research into CW (NATO News 2008). In the same timeframe Estonia developed sophisticated policies and strategies to safeguard its information infrastructure, specifically through published information security strategy doctrine (Cyber Security Strategy, Estonian Ministry of Defence 2008).

Military

Estonian military developments and commitments remained stable throughout the attacks and for the following year (Woerhel 2007, 5). Estonia maintained all EU and NATO military commitments and did not modify any weapons procurement or development programs (NATO site 2007).

The biggest change in Estonian military posture came in relation to its attitude towards CW. Estonia is one of the only countries that published an unclassified strategy for Cyber Security. This strategy is a thorough and innovative look at CW, and it places Estonia clearly at the cusp of doctrine related to CW. Specifically the Estonian Defense Ministry outlines very clearly (within a year of the cyber attacks) a sophisticated set of policy objectives to frame CW and the security associated with it:

> In advance of our strategic objectives on cyber security, the following policy fronts have been identified: • application of a graduated system of security measures in Estonia; • development of Estonia’s expertise in and high awareness

> of information security to the highest standard of excellence; • development of an appropriate regulatory and legal framework to support the secure and seamless operability of information systems; • promoting international co-operation aimed at strengthening global cyber security. (Estonian Ministry of Defence 2008)

Rather than avoid the potential dangers of CW as a result of the cyber attack, Estonia moved aggressively to develop measures to prevent CW within a year of the attacks.

Economic

The Estonian economy remained vibrant immediately following the cyber attacks and continued to perform well for the rest of 2007 with a growth rate of almost ten percent in GDP and a budget surplus of two percent of GDP for 2007 (Woerhel 2007, 2). In 2007 Estonia ranked twelfth in the world for economic freedom by the Wall Street Journal/Heritage Foundation Index of Economic Freedom (Woerhel 2007, 2). Russia made efforts in 2007 to weaken the Estonian economy within the six months following the cyber attacks (Woerhel 2007, 4). Russia is the largest provider of oil and the sole provider of natural gas to Estonia (Fabian-Marks 2006, 1). In the six months following the cyber attacks, Russia decided to transit more of its oil exports through its own ports rather than use Estonian ports (Woerhel 2007, 4). Russia also attempted to impose unofficial economic sanctions against Estonia following the cyber attack by reducing the amount of freight traffic from Russia to Estonia and limiting the amount of traffic over a key bridge linking the two countries (Woerhel 2007, 4). These actions do not appear to have significantly affected the Estonian economy for 2007.

Estonia received monetary aid from the U.S. of 5.8 million dollars for 2007 to improve Estonia's military capabilities, including training and education. The cyber attacks in spring 2007 did not appear to significantly affect the Estonian economy.

Case Study Number 2: Georgia 2008

Overview of Cyber Attack on Georgia

Unlike the CW in Estonia, the CW in Georgia was a part of a larger conventional campaign in action, though not necessarily by design. As with the attacks in Estonia, the cyber attacks in Georgia were not officially linked to the Russian government (Grey Goose Report 2008, 3). The cyber attacks did occur in conjunction with the conventional attacks, so it is reasonable to assume that the cyber attacks were an element of the larger conflict. The attacks may have been organized and carried out strictly by Russian patriots with CW knowledge, or by Russian state controlled entities, or some combination thereof. There currently is no unclassified information to suggest that the Russian government actively participated in the cyber attacks against Georgia in 2008.

Despite no conclusive evidence as to the origin of the cyber campaign against Georgia in 2008, there most certainly was a campaign (Grey Goose Report 2008, 5). This campaign began at roughly the same time as the Russian conventional campaign. Russia and Georgia were in political conflict over the areas of Abkhazia and South Ossetia, and by the end of July 2008 South Ossetia was the center of Russian-Georgian tensions (Cornell and Starr 2009, 149). Both Abkhazia and South Ossetia were seeking Russian aid to gain independence from Georgia (Cornell and Starr 2009, 123). From late July to 7 August 2008, Georgian and South Ossetian forces traded gunfire sporadically until Georgia declared a ceasefire in order to make political contact with the leaders in South

Ossetia (Cornell and Starr 2009, 151). By 2300 on 7 August 2008, Russian military forces began to move into South Ossetia (Cornell and Starr 2009, 151). Georgian forces advanced to prevent the Russian forces from seizing the separatist capital of Tskhinvali (Cornell and Starr 2009, 151). By mid day on 8 August 2008, Russian forces were initiating the invasion of Georgian territory (Cornell and Starr 2009, 152). Russian forces overwhelmed the Georgian military in a few days seizing South Ossetia and Abkhazia (Cornell and Starr 2009, 153). By 10 August 2008, Georgian officials asked for a ceasefire, but Russia continued to consolidate its gains finally ceasing hostility sometime around 16 August 2008 (Cornell and Starr 2009, 153).

The cyber attacks that accompanied these conventional attacks began approximately 8 and 9 August 2008 (Evron 2008). Some sources say the attacks started as early as July 2008 (Markoff 2008). Again it is difficult to determine when the attacks actually started, similar to Estonia. A site may not realize it is under attack until it is deluged with so much traffic that it shuts down. The attacks appear to have diminished by 12 August 2008, and Georgian sites began to return to normal traffic (Markoff 2008).

The cyber attacks appear to be linked with the Russian conventional campaign against Georgia, and appear to be directed against Georgian information flow and control of information (Markoff 2008). To determine if the cyber attacks were able to affect Georgia strategically the Georgian elements of national power must be evaluated before and after the conflict.

Conditions of National Power Prior to 7 August 2008

Diplomatic

The conditions of diplomatic power in Georgia before 7 August 2008 were dominated by Georgia's desire to Westernize and Russia's desire to maintain regional influence over states once under its control as part of the Soviet Union. Prior to the Russian-Georgian War, "Georgia was under severe Russian political, economic, and military pressure" (Cornell and Star 2009, 122). This pressure was designed to prevent Georgia from joining NATO and the EU, because membership in these Western institutions meant that Georgia would have to "embrace the Western paradigm," and association with the West implies dissociation with Russia (Cornell and Starr 2009, 111 and 123). Abkhazia and South Ossetia's move towards independence from Georgia was fueled by Russian desires to prevent Georgia from joining NATO (Cornell and Starr 2009, 122-123). The Russian Government made it clear to the Georgian president that Russian policy was oriented towards NATO, the U.S. and the EU in response to perceived Western encroachment on Russian influence and security as stated by Vladimir Putin:

> As for the disputed territories of Abkhazia and South Ossetia, in this regard we shall respond not to you (Georgia), but to the West–America and NATO, and in connection to Kosovo. You should not worry, it shouldn't bother you. What we do will not be directed against you but will be our response to them. (Cornell and Starr 2009, 67)

Georgian goals may have been based on assumptions that Russia would not resort to armed conflict to prevent Georgia's move Westward indicated by an optimistic set of goals focused on independence from Russia:

> 1) Commitment to reintegration of Russian-backed separatist Georgian territories. 2) Implementation of a Western-oriented security policy centered on NATO. 3)

> Exploit geography to establish Georgia as an energy transit state. 4) Liberalization of the economy-Democratization and membership in EU and NATO memberships. (Cornell and Starr 2009, 123)

These goals were antagonizing the Russian government, specifically the move towards NATO membership. Dmitry Rogozin, the Russian envoy to NATO stated that, "As soon as Georgia gets some kind of prospect from Washington of NATO membership, the next day the process of real secession of these two territories from Georgia will begin" (Cornell and Starr 2009, 125). Putin put it more succinctly, "The emergence of a powerful military bloc at our borders will be seen as a direct threat to Russian security" (Cornell and Starr 2009, 126).

To placate Russian security concerns and perhaps defuse some of the volatility surrounding Georgia's Western ambitions, the Georgian government did not recognize the independence of Kosovo, and subsequently announced that it would withdraw its 160 soldiers from the NATO peacekeeping mission in Kosovo (Cornell and Starr 2009, 128-129).

Georgia also attempted to make deals with the separatist states Abkhazia and South Ossetia. The Georgian President Saakashvili proposed:

> 1) Free economic zones in certain cities. 2) Abkhaz representation at all levels of the Georgian government. 3) Right to veto any decision regarding Abkhazian constitutional status. 4) Merger of Abkhaz security structures with Georgian structures. 5) Joint customs-border space. 6) Full autonomy on the ground. (Cornell and Starr 2009, 132)

Soon after these proposals were made, the Georgians participated in a NATO summit in Bucharest (Cornell and Starr 2009, 132). At this summit NATO agreed that Georgia would become a member of NATO (along with Ukraine) (Cornell and Starr 2009, 135). By April 2008 Russia began to solidify the separation of Abkhazia and South

Ossetia from Georgia and their annexation by Russia, including the build up of military forces in Abkhazia and South Ossetia (Cornell and Starr 2009, 133).

The Georgians attempted to placate the Russians again in June 2008 by agreeing to an international force to supervise the separatist territories, but requiring Russian troops to withdraw along with Georgian troops (Cornell and Starr 2009, 140). However, the Georgians did not modify their stance on joining NATO and the EU, and continued to look to the West for diplomatic support (Cornell and Starr 2009, 137).

Information

Georgian information capability is generally described as defensive in nature (Cornell and Starr 2009, 183). Georgian Internet capability was not as extensive as other former Soviet Bloc states like Estonia. Georgia ranked seventy-fourth of two hundred and thirty-four nations in Internet usage in 2008 (Markoff 2008). This meant that Georgia was less connected than Bangladesh, Nigeria, Bolivia, and El Salvador (Markoff 2008). Lack of connectivity is in itself a defense against CW. The Georgians did use the Internet to operate government websites and control information through those sites (Markoff 2008).

Georgia also had a very small media with which to engage the world (Cornell and Starr 2009, 186). There were also very few Western journalists present in Georgia to carry information and provide objectivity (Cornell and Starr 2009, 186). The fact that Georgia could not go on the offensive with an information apparatus meant the government had to act defensively by shutting down Russian media access and Russian sites accessed from Georgian Internet hubs (Cornell and Starr 2009, 186). Georgia had very few methods of distributing and controlling information making them prime targets for exploitation by a competent CW opponent. Georgia also did not seem to have the

same CERT professionals available to respond to any sort of cyber attack, since their activities are not mentioned in accounts of the cyber attacks.

To counter Russia information efforts, Georgia had to publish information through friends in Western cities and agencies (Cornell and Starr 2009, 191). Georgia also adapted well to their lack of information infrastructure by quickly establishing web logging sites (blogs) outside of Georgian networks, so that information could be disseminated to the world (Cornell and Starr 2009, 191).

Overall, Georgia was ill prepared to conduct information operations during the Russian-Georgian War in 2008. Their information infrastructure was not robust or effective enough to act offensively and decisively win the information battle.

Military

The Georgian military was divided in two prior to the war in 2008. Georgia's armed forces consisted of a professional portion with few soldiers, who were well equipped and surrounded by American advisors, while the other portion of the military was manned by conscripts; poorly paid, and poorly led (Francois 2008, 5). The Georgian military was and is backed by funding from the U.S. which does not prepare the Georgian military for large scale combat operations, but for security and stability operations (Francois 2008, 5). There are two programs: Georgia Train and Equip Program (GTEP) and the Sustainment and Stability Operations Program (SSOP) (Francois 2008, 5). The GTEP is designed to train and equip 2600 men from the Georgian Ministries of Defense and Interior in counter terrorism (Francois 2008, 5). The SSOP is designed to prepare Georgian units to operate alongside coalition forces in Iraq (Francois 2008, 5).

Cooperation with the U.S. has transformed the Georgian military budget from a meager thirty-six million Euros in 2000 to 714 million Euros in 2008 (Francois 2008, 6).

Georgian military commitments included two thousand soldiers sent to Iraq to support operations there, while approximately twenty-five thousand soldiers remained in Georgia (Francois 2008, 6). Military forces remaining in Georgia consisted of four infantry brigades, a special operations group, and an artillery brigade. The infantry brigades consisted of two infantry battalions, an armor battalion, an artillery battalion, an engineer company, and a communications company (Global Security 2009).

Economic

President Saakashvili stated in 2008 that his "major vision (is) to turn Georgia into the Dubai and Singapore of this region (Caucuses/Black Sea)" (Cornell and Starr 2008, 136). Georgia's main effort to make this vision a reality was membership in the EU and NATO, as well as becoming an energy transit node between resources in the Caspian and markets in Europe (Cornell and Starr 2009, 110). Georgia provides transit corridors for Caspian energy supplies and Central Asia commodities to Europe and the Atlantic (Cornell and Starr 2009, 110). Georgia also attracted foreign investment by providing opportunities of open routes to Azerbaijan and other states in the region (Cornell and Starr 2009, 125). In order to join the EU Georgia had to remake its economic norms to fall in line with EU requirements, specifically regarding market oriented, liberal democratic political and economic systems (Cornell and Starr 2009, 111). The Georgian President promised to offer "life without corruption, wherein no one will ever be able to extort bribes from you, or shares from your businesses" (Cornell and Starr 2009, 137).

Georgia pursued Western values and economic norms to foster integration into Western institutions.

GDP in Georgia was valued at thirteen billion dollars in 2008, and GDP grew at 3 percent for 2008, down from 12 percent in 2007 (World Fact Book 2009). Georgia's economy was mostly agrarian in 2008 and imported all of it oil and natural gas requirements (World Fact Book 2009). Georgia's intent in 2008 was to make the best use of the Baku-T'bilisi-Ceyhan oil pipeline completed in 2005 and the Baku-T'bilisi-Erzerum gas pipeline completed in 2006 to generate economic growth (World Fact Book 2009). Georgia also intended to profit from the Nabucco gas pipeline and the Kars-Akhalkalaki Railroad (Nabucco Gas Pipeline International 2009). Economic growth in Georgia was driven mostly by foreign direct investment and expanding bank credit (Transparency International 2009).

Economic policy in Georgia was heavily focused on integrating Georgian institutions with EU and other Western establishments. This policy may have benefited Georgia economically, but it jeopardized Georgia's short-term security.

The Nature of the Cyber Attack

Much less information is known about the cyber attacks in Georgia than in Estonia. Some of the gap in information is probably due to the amount of time required to publish detailed analysis, but some may be due to resistance by the Georgian government to discuss the details of the attack and its results. What does seem apparent is that the attacks against Georgia were more sophisticated and better coordinated than the attacks against Estonia. Georgia's connectivity to the Internet is much less than Estonia's

(Markoff 2008). This has a clear impact on the damage done by the attacks, but the systems that were present were exploited by more technically advanced methods.

Espionage

The cyber attacks against Georgia were predominantly in the form of DDoS attacks (Evron 2008). What is interesting about the DDoS attacks used against Georgia is that they were carrying another unique code possibility with them. In the case of Georgia, the attackers were using Structured Query Language (SQL) Injection attacks coupled with the large volume DDoS attacks (Grey Goose Report 2008, 4). An SQL technique exploits poor secure application coding practices (Grey Goose Report 2008, 10). That means that if a system does not effectively validate a user, then the user could input commands within parameters passed from the web application to the backed database (Grey Goose Report 2008, 10). An SQL injection effectively compromises the system housing the database (Grey Goose Report 2008, 10). Unlike a DDoS that uses a botnet of thousands of systems to overwhelm a targeted system and cause it to shut down, and SQL injection can achieve the same effect with only a few systems (Grey Goose Report 2008, 4). The injected commands can be used to order the system to tie itself up with command cycles, or it can be used for espionage (Grey Goose Report 2008, 10). SQL attacks are extremely hard to detect when covered by a large scale DDoS (Grey Goose Report 2008, 4).

The SQL injection attacks that occurred against Georgian systems may have compromised all of the data stored in back end databases. This data may have been stolen or altered (Grey Goose Report 2008, 9). Information stored in these databases often times consists of username and password combinations that could be stolen and later used for

long term intelligence gathering inside other systems (Grey Goose 2008, 9). The information that the attackers may have gained is not available or known in unclassified sources. What seems clear is that many Georgian systems' security was compromised. This is an excellent example of CW being used to conduct espionage, despite our lack of knowledge as to what was collected.

The CW espionage conducted against Georgia also consisted of Internet traffic being rerouted through Russian telecommunications sites (Markoff 2008). The destination and purpose of this traffic is unknown.

Disruption

The cyber attack on Georgia was primarily an operation of disruption. The overwhelming majority of attacks were in the form of DDoS attacks against Georgian government websites. While no hard data is available, the Georgian President's website was shut down for at least twenty-four hours during the conflict (Markoff 2008). Several other government websites were also reported shut down, but no reports exist to depict which sites and for how long (Markoff 2008).

The Georgian government did not rely on Internet capacity for indispensible government functions except for information control, so the attacks against the government websites only disrupted the government's ability to disseminate information to its people and the world community and some communications that relied on phones and Internet (Markoff 2008). DDoS attacks significantly disrupted communications via email, landline, and cellular phone traffic (US-CCU 2009, 6).

Georgian banks and transportation agencies were also attacked, but few Georgian transactions occur over the Internet making the attacks mostly irrelevant to the overall campaign (Markoff 2008).

Corruption

There were a few examples of Corruption in the Georgian conflict. Similar to the Estonian conflict these manifested in cyber vandalism. The National Bank of Georgia's website was defaced with pro Russian ideology (Markoff 2008). The Bank site also was vandalized with imagery of Georgian President Saakashvili's head placed on Adolph Hitler's body.

There is also some possibility of overlap from the SQL injection attacks. Some systems may have been altered in their purpose without user knowledge by SQL injection attacks. There is no evidence to support this claim. It is purely speculation based on what is possible and probable.

Distraction

Once again the SQL injection attacks open up the possibility that some form of distraction may have occurred, but there are no documented cases to support this. On a larger scale, the attacks themselves do not appear to have any purpose of distraction, since the CW campaign appears to have played a subordinate role to the conventional campaign that was occurring simultaneously.

Conditions of National Power After 16 August 2008

Diplomatic

The Russia-Georgia War did not result in Georgia acquiescing to Russia desires to keep its former satellite states out of NATO. Georgia did not seek to avert Russian power by supplicating itself to Russia, but instead looked Westward for assistance from the EU, the UN and the U.S (Cornell and Starr 2008, 139). President Saakashvili did not see resolution to the overall conflict in the region coming from Russia, but from intervention from the West:

> Nothing will hamper the peaceful unification of our country. We will continue working with all our partners. We expect and demand that the Russian Federation revise all those decisions which breach Georgia's sovereignty and territorial integrity. We need not only statements; we need serious diplomatic actions from our partners, our friends. We expect and hope that these actions will be made in the coming days and coming weeks. (Cornell and Starr 2008, 137)

Within five months of the ceasefire concluding the war, Georgia signed a strategic partnership agreement with the U.S. affirming security cooperation, special trade status between the two nations, and support for Georgia's desire to become a member of NATO (Foreign Policy 2009). In September 2008, NATO and Georgia agreed to establish the NATO-Georgia Commission (NGC) to supervise assistance to Georgia following the war with Russia (NATO 2009).

Diplomatic relations with the EU were not as strong as those with NATO and the U.S. Despite Georgia's request for intervention by the EU on Georgia's behalf, the EU seems to be remaining un-provocative towards Russia. The EU issued a message from the office of the EU presidency regarding continued tensions and possible cross boundary shooting between Russia and Georgia in March 2009:

> The EU reaffirms the importance it attaches to all sides participating fully in the framework of the Incident Prevention and Response Mechanism (IPRM) and calls on all parties to cooperate fully with the IPRM in clarifying incidents, including those over the past few days. The EU further calls on all sides to give the EUMM (European Union Monitoring Mission) unrestricted access to both sides of the South Ossetian administrative boundary line. (European Union 2009)

The EU has pledged six million Euros in aid for humanitarian assistance in Georgia (European Union 2009).

Collectively, Georgia was not dissuaded from its goals of increased diplomatic and political ties with the West. The conflict has solidified Georgia's plans to seek its economic and security goals diplomatically through the West. There are no indications that these policies changed after the war in August of 2008.

Information

At the conclusion of the war with Russia, the Georgian government felt that it had won the content portion of the information war, but lost the technical portion of the information war (Cornell and Starr 2009, 194). Information security experts in Russia assessed that Russia had lost the information war with Georgia and must take immediate steps to correct their mistakes. (Cornell and Starr 2009, 193) Both assessments are related to content and not technological exploitation via a cyber campaign. Georgia was caught unprepared for the CW employed against its websites and Internet infrastructure, since it focused its cyber defense primarily on the sustainment of websites and ignoring the espionage potential of the attacks (US-CCU 2009, 6).

In immediate response to the CW attacks, Georgia moved most of the hosting of its websites to overseas locations so that it would be easier for the websites to filter malicious traffic (US-CCU 2009, 7). Many websites that were finding themselves under

attack switched their format from interactive websites to blogs (Cornell and Starr 2009, 191). This prevented many DDoS as there was no service to be denied. Content could be corrupted, but bloggers were most likely watching their content closely and guarding against that type of attack.

During the war and in the month following, President Saakashvili took further steps to control information flow and access (Cornell and Starr 2009, 186). Some observers suggested that President Saakashvili used the war as a reason to tighten his control over information systems in Georgia (Cornell and Starr 2009, 186).

Internet usage in Georgia has remained relatively small compared to most European Countries with 7.9 percent of the population connected as of 2009 (Internet World Stats 2009). It is not clear if this is due to lack of confidence in the systems or simply a problem of physical connectivity. CISCO systems Vice President for Europe East reports that Georgia has a "mountainous terrain and a low penetration of copper and optical wire line networks, wireless solutions are virtually the only way to help eliminate the digital divide" (Market Wire 2009). Georgia may be leaping into wireless connectivity in order to boost its population's access to the Internet.

Military

Georgia's military commitments remain focused towards the West and the Global Community. Georgia currently allows logistic support to flow through its borders to Afghanistan, though it no longer contributes to security forces there (NATO 2009). In September 2008 Georgia and NATO signed an agreement establishing the NGC to supervise NATO support to Georgia following the war with Russia (NATO 2009). By February 2009 Georgia signed a strategic partnership agreement with the U.S. affirming

security cooperation, special trade status between the two nations, and support for Georgia's desire to become a member of NATO (Foreign Policy 2009).

Georgia's loss to Russia in 2008 became "a catalyst for significant personnel change within the Georgian armed forces" (Hamilton 2009). Georgia appointed a new chief of staff of the armed forces (Vladimer Chachibaia) who was a military officer with battalion command experience in Iraq and was a graduate of the U.S. Army War College (Hamilton 2009). Chachibaia's deputy Devi Chankotadze replaced him in March 2009 (Radio Free Europe 2009). While Chachibaia was in charge he focused his efforts on developing "doctrinal and institutional foundations of a modern military force rather than focusing on the purchase and deployment of weapons and equipment (Hamilton 2009). Georgia has maintained its military relationship with the U.S. demonstrated by a cadre of western trained officers emplaced to help with the transformation (Hamilton 2009).

Georgia did experience a small military mutiny attempt in May 2009 (Radio Free Europe 2009). This mutiny or coup was designed to disrupt the NATO Partnership for Peace exercise occurring in Georgia (Radio Free Europe 2009). The Georgian government arrested thirteen civilians and fifty officers in connection with the attempt (Radio Free Europe 2009). The mutiny did not appear to have a major affect on the Georgian military in general.

Economy

According to Transparency International the Russia-Georgia War caused the Georgian economy to shrink significantly (Transparency International 2009). Georgian economic growth slowed to three percent in 2008 (World Fact Book 2009). Growth was projected as 4 percent for 2009 (Transparency International 2009). However, the CIA

World Fact Book projects Georgia's economic growth to be even less than 3 percent for 2009 (World Fact Book 2009).

One of the prime movers of the Georgian economy, Foreign Direct Investment, has plummeted since the war with Russia, most likely due to the instability from the conventional fighting (Transparency International 2009). Credit flow was greatly reduced after the war, and banks were unable to move cash (Transparency International 2009). One hundred thousand Georgians may lose their jobs in 2009 as investment drops and growth slows (Transparency International 2009).

The Georgian government faces a budget shortfall for 2009, because it is collecting less revenue as the economy shrinks (Transparency International 2009). Transparency International quotes the Joint Needs Assessment (JNA) conducted by the World Bank, European Commission and the United Nations as saying that reduced confidence in private sector business "will lead to a precipitous decline in private sector investment, bank lending, and private consumption" (Transparency International 2009).

Georgia's attempts to turn geography into economic power were proceeding as planned after the war. The Nabucco Gas Pipeline is still planned to start construction in 2011 and be complete by 2015 (Nabucco Gas Pipeline International 2009). This gas pipeline will have strategic effects for Europe in that it will alleviate Europe's dependency on Russia for natural gas.

Georgia received pledges of aid from international donors in the amount of 4.55 billion dollars to assist in recovery from the war (Transparency International 2009).

Georgia's economy suffered serious problems as a result of the war with Russia. Georgia continues to solidify ties with the West in spite of these problems. Georgia

appears to follow a policy suggesting that the West can ultimately solve all of Georgia's economic difficulties. This is in evidence from the continuation of energy infrastructure construction through Georgia to Europe and the strategic partnership agreements with the U.S. and NATO. Also Western dominated institutions like the World Bank, EU, and the UN continue to be key donors in monetary relief efforts for Georgia. After the war in 2008, Georgia still looks westward.

Case Study Number 3: Israel 2008-2009

Overview of Cyber Attack on Israel

The cyber attacks against Israel in late 2008 and early 2009 were not a coordinated CW campaign against the Israeli government. The cyber attacks were in conjunction with the conventional armed conflict occurring in Gaza. On 18 December 2008, the ceasefire between Israel and Hamas ended (Catignani 2009, 1). Hamas launched seventy rockets into Israeli territory on 21 December 2008 (Catignani 2009, 1). On 27 December 2008, Operation Cast Lead began with the Israeli Air Force attacking Hamas government and infrastructure targets in Gaza (Catignani 2009, 3). On 3 January 2009, the IDF began its ground invasion of Gaza with infantry and armor forces (Catignani 2009, 3).

Cyber attacks began soon after the Israeli bombing campaign began (Warner 2008). Within a few days, three hundred Israeli websites were attacked (Warner 2008). In response, the Israelis attacked Palestinian media websites (Krangel 2009). As the war continued, video from both combatants emerged on Youtube (Information Warfare Monitor 2009). Civilians and journalists began posting accounts of the war on micro blog site Twitter in an effort to shape the information battle (Information Warfare Monitor

2009). Israelis and Palestinians began social networking pages on Facebook to contribute to the information battle (Information Warfare Monitor 2009).

The ground campaign met with some tactical success, but limited strategic success. The Israeli incursion into Gaza succeeded in killing 709 known Islamic Jihad operatives, but it also killed 295 personnel known to be civilians (Catignani 2009, 6). Israel was unable to stop the rocket attacks during the war. Hamas succeeded in firing over six hundred rockets into Israel during the twenty-two day conflict (Catignani 2009, 6). Israel failed to win the information war, and under international pressure instituted a ceasefire on 17 January 2009 (Catignani 2009, 6).

"Crowd sourced cyber armies" on both sides carried out cyber attacks during the conflict (Information Warfare Monitor 2009). The conflict started with web defacements and DOS attacks, then escalated to more sophisticated computer network attacks (CNA) (Information Warfare Monitor 2009). Unclassified details regarding sophisticated CNAs are not forthcoming, but some possible examples may be the Domain Name System (DNS) server attacks that led to the rerouting of traffic to other websites.

Conditions of National Power Prior to 27 December 2008

Diplomatic

The exercise of Israeli diplomatic power is complex with a long history. For the purpose of this case study, Israeli diplomatic power will be viewed in the narrow context of just before the war in Gaza. Specifically, this case study will look at Israeli diplomatic power in relation to the Arab world and the West. This is a significant view, because immediately prior to the conflict in Gaza, Israeli politicians had a real opportunity to normalize relations with the Arab world provided the Israeli government made certain

significant concessions. These concessions appeared to be seriously considered by the Israeli government until the conflict erupted.

The Saudi Arabian government proposed a peace plan to the Israelis in 2002 granting the state of Israel normal relations with all twenty-two nations of the Arab world (O'Loughlin 2008). In exchange, Israel would withdraw to its pre-1967 borders and acknowledge the Palestinian State (O'Loughlin 2008). This plan was favored by the Labor Party and the Kadima Party, but was rejected by the conservative Likud Party (Heller 2009). Israel was set to have elections in February 2009, and the Kadima Party was the front-runner for those elections prior to the Gaza War (Mahnaimi and Baxter 2008).

The U.S. government was in transition just before the Gaza War, as the Bush Administration was transferring authority to the Obama administration. President-elect Obama made it clear that the U.S. under his administration would support the adoption of a plan similar to the Saudi Plan to secure peace in the region (Mahnaimi and Baxter 2008). President Obama stated to Mahmoud Abbas (the Palestinian Leader), "The Israelis would be crazy not to accept this initiative. It would give them peace with the Muslim world from Indonesia to Morocco" (Mahnaimi and Baxter 2008).

Israeli diplomatic efforts created a way towards peace just prior to December 2008. Israeli President Shimon Peres continued to strengthen the diplomatic solution during a conference at the United Nations in November 2008 when he told the conference and Saudi King Abdullah, "I wish that your voice will become the prevailing voice of the whole region. Of all people" (Mahnaimi and Baxter 2008). As long as the more liberal

political parties remained in power, it seemed that diplomatic peace was possible in late 2008 and moving into 2009.

Information

The Israeli government and particularly the Israeli military were very aware and proactive regarding information power prior to the Gaza War in 2009. In fact the entire Palestinian-Israeli conflict is a watershed event in the use of information as a tool of national power. This study's analysis of Israeli information power will narrow the focus to Israeli information power in regards to CW, and the ability of Israel to use CW as part of its information campaigns leading up to the 2008-2009 Gaza War.

The head of the IDF's Foreign Press branch, MAJ Avital Leibovich told the Jerusalem Post, "The blogosphere and new media are another war zone. We have to be relevant there" (Information Warfare Monitor 2009). The Israeli consulate in New York held a press conference via the microblog Twitter, demonstrating that the Israeli government understands how many individuals can be mobilized on a topic with simple short messages (Information Warfare Monitor 2009).

Israel also controlled information operations before the war by limiting the presence of foreign journalists into Gaza (Information Warfare Monitor 2009). In this way, Israel could control the message that was being given to the world.

Israel's information operations were designed to portray Israel as the victim of Hamas led terrorism, and thus garner sympathy and support from the global community (Shlaim 2009). Israel was effective at this, in that the U.S. and the EU imposed economic sanctions against the government of Hamas when it came to power (Shlaim 2009).

Most importantly, Israel had the quiet support of the U.S. and the EU when it first began operations against Hamas on 27 December 2008 (Margolis 2009). Israeli information power had succeeded in framing the conflict as one of Israeli self-defense against a terrorist-led government.

Military

Israel's military performance against Hezbollah in 2006 is characterized as "uninspiring" (Matthews 2009, 41). By 2008, Israeli ground forces underwent a major cultural change "toward decisiveness, aggressiveness, commitment to the mission, and willingness to accept casualties" (Matthews 2009, 41). The Israeli government directed a committee to investigate IDF shortcomings in the war against Hezbollah in Lebanon in 2006 (Matthews 2009, 42). The report concluded:

> All in all, the IDF failed, especially because of the conduct of the high command ad the ground forces, to provide an effective military response to the challenge posed to it by the war in Lebanon, and thus failed to provide the political echelon with a military achievement that could have served as a basis for diplomatic action. (Matthews 2009, 42)

So, essentially, the Israeli government determined that the IDF of 2006 was not capable of generating conditions on the ground that would be favorable to a political victory through diplomatic action. The Israeli government identified several reasons for this failure. The IDF created fact-finding teams that determined that "doctrine used during the 2006 campaign created 'confusion in terminology and misunderstanding of basic military principles'" (Matthews 2009, 43). According to Israeli Brigadier General Shimon Naveh, the "core of this document is the theory of SOD (Systemic Operational Design)" (Matthews 2009, 43). The IDF of 2008 discarded the SOD doctrine and returned to its doctrine prior to 2006 (Matthews 2009, 43). From there, the IDF began

training again on fundamental conventional warfighting skills (Matthews 2009, 43). Tank units focused on speed and firepower (Matthews 2009, 43). Battalions participated in realistic training on terrain that simulated terrain they would likely encounter (Matthews 2009, 43).

The reserve force was also revamped to be more effective at integrating with active component forces (Matthews 2009, 43). The Israeli government invested in procuring all weapons and equipment that reserve units lacked prior in 2006 (Matthews 2009, 43). The IDF purchased "tens of thousands of ballistic helmets and vests and night vision goggles, as well as significant quantities off grenades, small arms ammunition, and magazines" (Matthews 2009, 43).

The IDF that existed in 2008 had completed a transformation to becoming a more effective fighting organization based on usable doctrine and fundamental warfighting techniques (Matthews 2009, 44). The IDF effectively fixed the shortcomings of the 2006 war, and in 2008 were well prepared to take military action in Gaza as part of a military based strategy to achieve political goals (Mathews 2009, 50).

Economic

The Israeli economy suffered a reduction in growth in 2008 compared to the previous five years (World Fact Book 2009). 2008 saw Israeli GDP grow at 3.9 percent compared to an average of 5 percent in each year from 2003 (World Fact Book 2009). This is likely attributable to the Global Economic Crisis in 2008 (World Fact Book 2009).

The Israeli economy is reliant on the import of raw materials, oil, grain, and military equipment (World Fact Book 2009). Israel is a key competitor in the technology

industries, and rates itself as a high-tech center following the Silicon Valley in California and Route 128 in Boston (Israel Ministry of Industry, Trade, and Labor 2009). Israel's economy is reliant on exports to generate growth (Israel Ministry of Industry, Trade, and Labor 2009). Israeli exports declined by 13 percent in 2008 due to the Global Economic Crisis (Israel Ministry of Industry, Trade, and Labor 2009). Israel has free trade agreements with the U.S., Canada, Mexico, the EU, Turkey, and Jordan (Israel Ministry of Industry, Trade, and Labor 2009).

Israel's economy is oriented around services primarily. Agriculture generates just under 3 percent of GDP, industry 32 percent, and services 65 percent (World Fact Book 2009).

The Nature of the Cyber Attack

The cyber attacks against Israel in 2008 and 2009 were not as sophisticated or organized as the attacks against Estonia and Georgia. The cyber attacks were not oriented around destroying Israeli cyber capability or information infrastructure. Rather the attacks appear to have been designed to win the information war that accompanied the conventional Gaza War. The information war itself may have had strategic impact on Israel, but it is unclear if the cyber attacks contributed to IW success.

Espionage

There were no reported cases of CW being used to conduct espionage during the Gaza War. There were also no indications of an undetected espionage attempt as was seen with Georgia and the SQL injection attacks. It does not appear that Hamas used CW to conduct espionage against Israel.

Disruption

The Information Warfare Monitor reported that the CW campaign against Israel in 2008 began with website defacements and denial of service (DOS) attacks (Information Warfare Monitor 2009). The attacks then escalated into “more sophisticated computer network attacks (CNA)” (Information Warfare Monitor 2009). Information regarding these “sophisticated” CNAs is not available, but they could be referring to DNS server attacks conducted by Muslim groups outside Israel.

The Project Grey Goose Phase II Report states that as many as ten thousand websites may have been attacked by the first week of January 2009 (Project Grey Goose Phase II Report 2009, 8). The majority of the attacks appear to be corruption in the form of website defacement, but some of the attacks have been DDoS. In the Grey Goose Project Report Phase II the existence of DDoS attacks against Israel during the Gaza War is clearly stated, but no specific incidents are mentioned. The Grey Goose Report does mention that the Ashianeh Security Group hacked four hundred Israeli websites, including websites for the Mossad and the Israeli Defense Minister (Project Grey Goose Phase II Report 2009, 12). The Grey Goose Report also suggests that the Ashianeh Security Group might be an Iranian Government sponsored hacker group, because the group does not participate in online hacker forums (Project Grey Goose Phase II Report 2009, 12).

The Grey Goose Report also suggests that an Iraqi hacker named Nimr al-Iraq is responsible for updating DDoS tools for use during the Gaza War (Project Grey Goose Phase II Report 2009, 12).

The Grey Goose Report suggests that “anti Israeli hackers would like to carry out serious cyber attacks against Israeli targets, however, they do not have a demonstrated capability to carry out such attacks.” The Grey Goose Report goes on to suggest that “Instead, their actions have been limited to small to mid scale denial of service attacks and website defacements” (Project Grey Goose Phase II Report 2009, 12). This may account for the lack of spectacular DDoS attacks that would have garnered international media attention.

Israel conducted its own DDoS attacks, but these attacks do not appear to be state sponsored (Project Grey Goose Phase II Report 2009, 13). The DDoS attacks were unusual in that pro Israeli computer users could contribute to the DDoS attacks by signing up to allow their computer to be used to attack Palestinian websites (Project Grey Goose Phase II Report 2009, 13-14). The user would download software that would allow their computer to become part of a botnet (Project Grey Goose Phase II Report 2009, 13-14). These voluntary botnets could be joined from anywhere in the world.

Corruption

Corruption during the Gaza War was most prevalent in the form of website defacements. Three hundred Israeli websites were defaced in forty-eight hours following the air attacks on 27 December 2008 (Warner 2008). Hackers employing website defacement came from several known hacker entities. Project Grey Goose lists Palestinian, Egyptian, Saudi, Turkish, Moroccan, Algerian, Iranian, and Iraqi (Project Grey Goose Phase II Report 2009, 9-12).

Hackers downloaded vulnerability scanners and scanned Israeli websites looking for known vulnerabilities (Project Grey Goose Phase II Report 2009, 13). Once a known

vulnerability was discovered, the hacker would then use a known exploit to execute his planned defacement (Project Grey Goose Phase II Report 2009, 13). Patch codes were quickly emplaced to defend against these attacks, and only websites whose administrators were "lax in updating their software and downloading their patches" remained vulnerable (Project Grey Goose Phase II Report 2009, 13). This illustrates the fact that the CW attacks against Israel were not sophisticated, and failed to generate significant coverage in the media. Israel was also able to easily counter the attacks and mount their own attacks against Palestinian targets.

The Jewish Internet Defense Force disabled social networking sites that promote anti-semitism or Islamic terrorism (Information Warfare Monitor 2009). According to the Grey Goose Report, the IDF itself hacked a television station belonging to Hamas (Project Grey Goose Phase II Report 2009, 14). No details were given as to the result.

Distraction

Distraction is a very sophisticated element of CW. As mentioned before, the cyber attacks against Israel during the Gaza War were not especially sophisticated. No examples of distraction during the Gaza War were uncovered.

Conditions of National Power After 17 January 2009

Diplomatic

In February 2009 Israel held national elections that determined the Kadima Party would hold the most seats in parliament, and the Likud Party would have the best chance for forming a new government (Marcus 2009, 55). Eventually the Israeli President Shimon Peres asked Binyamin Netanyahu to form the next government as Prime Minister

(Marcus 2009, 64). This was a significant change in government as the Likud Party was considered a conservative party and the Kadima Party considered liberal. The Kadima Party was more agreeable to the Saudi posed peace plan that would create normal relations between the Arab world and Israel (Heller 2009). Netanyahu as leader of the Likud party was opposed to the concessions required in the Saudi plan (Benn 2009). This placed the Saudi sponsored/American backed peace proposal in jeopardy (Bar'el 2009). The Saudis demanded that Israel make progress on implementing the peace plan by 2011, and President Obama supported the demand (Bar'el 2009). As of June 2009, Israel had not made any progress that would indicate acceptance of the peace plan (Bar'el 2009).

The Gaza War most likely frightened the Israeli populace into supporting a more conservative government. The rise of Netanyahu to Prime Minister means that the Saudi plan has little chance of being implemented in the aftermath of the Gaza War. Israeli diplomatic power is now focused on maintaining relations with the U.S. and neutralizing the nuclear threat from Iran (Marcus 2009, 68).

Information

Israeli information power has moved further towards employment of Internet based media following the Gaza War. Israel employed YouTube and Facebook as tools to propagate their message during the Gaza War, and they still use these tools (Information Warfare Monitor 2009). The IDF is "crafting a real-life master plan to invade social media" after the Gaza War (Information Warfare Monitor 2009). A quick search of the relevant sites shows that Israel maintains information ability on YouTube, Facebook, and Twitter. The popularity and effectiveness of these tools may not be as great as planned. Israel's Twitter account has 32,383 followers as of October 2009. In comparison, U.S.

President Obama has 2,410,667 followers. The Israeli Foreign Ministry Facebook page has 1,445 fans as of October 2009. The comedian Carrot Top has 3,151 fans as of October 2009. The Israeli government may be attempting to use Internet means to propagate their message, but they have not effectively reached a large population to validate their employment of these Internet based media. Israel has effectively mobilized a large population of civilians to get state the Israeli message. A search of Facebook, YouTube, and Twitter will yield hundreds and in some cases thousands of results for pro (and anti) Israeli messages. This information falls in line with other parts of CW in that most active participants appear to be civilian rather than government sponsored. Israeli information power appears to be heavily civilianized on the Internet.

Military

The IDF has maintained the reforms it made after the 2006 war in Lebanon (Matthews 2009, 51). The IDF maintains a policy of "commitment to the mission and simplicity" (Matthews 2009, 50).

The IDF is fully capable of maintaining a credible military deterrence force for national security in the Middle East, and it can defeat Palestinian and regional threats for the near future (Matthews 2009, 50).

The IDF has branched into information warfare as stated by Major Avital Leibovich, the head of the IDF Foreign Press Branch, "The blogosphere and new media are another war zone. We have to relevant there" (Information Warfare Monitor 2009). The IDF views CW and IO as branches of warfare, not civilian security problems and plans to use the IDF as a force in CW and IO (Ben-Ari 2008, 52).

Economic

The Israeli economy is expected to contract for 2009 with GDP growth estimated at -1.747 percent (Economy Watch 2009). Unemployment is estimated to rise from 6 percent in 2008 to 7 percent in 2009. These numbers are likely from the Global Economic Crisis during the past year. There are no indicators that would suggest that any economic issues are directly related to the CW conducted during the Gaza War.

Part Two

This portion of the research will serve to summarize findings from the previous case studies so that patterns and commonalities may be observed. The method will focus on orienting each case study around the subordinate research questions, ultimately leading to the primary research question.

Subordinate Research Questions:

1. Was CW a strategic weapon?

2. Was CW employed with the intent to achieve a strategic political objective?

3. Did the targeted nation concede a strategic political objective as a result of CW?

Table 6 compiles presents answers to the three subordinate questions by case study and element of national power.

Table 6. Summary of Case Studies Relative to Subordinate Research Questions			
	Q1: Weaponized	Q2: Intent	Q3: Concession
Estonia			
Diplomatic	No	Yes	No
Information	No	Yes	No
Military	No	No	No
Economic	No	Yes	No
Georgia			
Diplomatic	No	No	No
Information	No	Yes	No
Military	No	Yes	No
Economic	No	Yes	No
Israel			
Diplomatic	No	Yes	No
Information	No	Yes	No
Military	No	No	No
Economic	No	No	No
Trend	No	Yes	No

Source: Created by author.

Trend Analysis

Table 6 indicates that there are several trends when summarizing the three case studies. These trends will be analyzed in the context of the subordinate research questions.

Was CW a Strategic Weapon?

None of the case studies justify the classification of CW as a strategic weapon. CW did have some strategic effects, but none that accomplished the likely strategic intent of the attacker. CW did have some use as a tactical weapon, in that it was adept at creating short-term confusion and friction at the tactical and perhaps operational level.

Was CW Employed With the Intent to Achieve a Strategic Political Objective?

In all three case studies there was clear intent to achieve strategic political goals in at least one of the elements of national power. Two of the three case studies saw intent to gain a strategic objective in a nation's diplomatic power, and all three case studies saw intent to gain strategic objectives in the nations' information power. Only one case saw any attempt to gain a strategic objective in military power through CW, and two of three saw an attempt to gain a strategic objective in a nation's economic power.

Did the Targeted Nation Concede a Strategic Objective as a result of CW?

In none of the cases was there sufficient evidence to indicate that the nation under CW attack conceded a strategic objective as a result of the CW attack. There were two cases where strategic concessions were made by the targeted nations, but CW did not appear to play a decisive role in these concessions. Instead, the two case studies with the most prominent concessions were the two which had conventional operations conducted

alongside CW operations. In the Georgia case study, Georgia was forced to give up control of Abkhazia and South Ossetia. This was a result of conventional military action, and not CW. In the Israel case study, Israel was forced to withdraw from Gaza under international pressure and was unable to stop Hamas rocket attacks. Withdrawing from Gaza was an information victory for Hamas against Israel, but this was due to well-executed information operations and not CW. The conventional warfare operations were decisive in accomplishing strategic political goals where CW was indecisive.

The Primary Research Question

This study sought to answer the primary research question: Can Cyber Warfare achieve a strategic political objective? The three case studies examined were three of the most well known cases of CW employed in a strategic context. With these case studies in mind, the answer must be no.

The implications of this answer will be explored and contextualized in Chapter 5. Recommendations will be made for further research, so that the field may continue to grow.

CHAPTER 5

CONCLUSIONS AND RECOMMENDATIONS

Conclusions

Summary

The research conducted in chapter 4 demonstrated that CW is not currently capable of achieving a strategic political objective. There are, however, a few caveats. Strategic objectives were achieved in two of the three case studies, but CW was not the primary reason those objectives were achieved. CW did have a strategic impact in all of the case studies, but it was not a decisive strategic weapon. The answers for the three subordinate research questions will put the answer to the primary question in context.

Was CW a strategic weapon?

In all three cases CW did not display the characteristics expected of a strategic weapon. For CW to be considered a strategic weapon in these cases it needed to decisively achieve a strategic political objective as a clear result of the attack. In all three cases CW failed to achieve that. Whereas a nuclear weapon can immediately cripple a communication node like a city, CW was incapable of generating a lasting and decisive effect when employed. In all three cases the effects of the CW attacks were mitigated and countered by defenders. CW's inability to generate immediate results, and its susceptibility to rapid defense prevents it from being labeled a strategic weapon in the three case studies.

Was CW employed with the intent to achieve a strategic political objective?

In all three cases CW was used with the intent to achieve a strategic political objective. In Estonia that objective may have been the replacement of the Soviet War Memorial, or it may more likely have been the intent to prevent the Estonians from solidifying their relationship with NATO, the EU, and the U.S. The intent may have also been to warn Estonia of the risks it was taking by encouraging the Western aspirations of other former Soviet satellite states like Ukraine, Moldova, and Georgia. In the Russia-Georgia War that intent was clearer.

Russian CW against Georgia was intended to disrupt Georgian strategic level communication with the international community, while conventional forces accomplished their mission. These attacks were is support of Russia's strategic goal to limit NATO's reach in the Caucuses, and prevent Georgia from becoming part of a Western community as opposed to a Central Asian community. CW may have also had operational and tactical level intent, but Russian attempts to control the strategic IO environment through CW had the greatest potential to showcase Russian CW capability and intent. With control of the IO environment, Russia would be able to shape Western support for Georgia and Western ambitions for the region.

In the Gaza War, CW was employed against Israel with the intent to control and influence Israel's ability to employ strategic communication with the West and the International community. Hamas and its supporters would then be able to shape the West's posture towards Israel and its actions in Gaza.

Did the targeted nation concede a strategic political objective as a result of CW?

Estonia conceded no strategic political objective. On the contrary, Estonia strengthened its relations with NATO, the EU, and the U.S. Estonia also continued to support its Baltic neighbors, and Ukraine, Moldova, and Georgia in turning towards the West. Estonia also did not move the Soviet War Memorial back into the center of the capital, Tallinn.

In Georgia, the Russians were able to accomplish their strategic goal of preventing NATO encroachment in the Caucuses, but only in limited fashion. Georgia does not appear to be joining the EU or NATO in the near future, but both organizations have made promises that Georgia will eventually be a member state. It was not CW that gave pause to NATO and the EU. What checked NATO's and the EU's aspirations in the Caucuses, was Russian armed intervention ostensibly in support of Abkhazia and South Ossetia. CW was unable to prevent Georgian strategic communication of their message to the West, and the West remained supportive of Georgia.

In Gaza, the Israelis were also forced to halt their operations, but not due to any CW operations. The Gaza War is interesting in that IO played a decisive role, but IO was not affected by CW. Hamas was much more effective at employing modern IO tools, like social networking sites and YouTube. Hamas also made use of the conventional media more effectively than Israel. The CW campaign to assist in the IO campaign was primitive and ultimately ineffective. Hamas achieved its strategic communication objectives, but not through CW.

With this summary in mind, six conclusions present themselves. These conclusions coupled with the subsequent recommendations seek to refine CW into the strategic weapon that cyberspace's omnipresence in our daily lives implies CW could be.

Conclusions One

CW alone cannot achieve a strategic political objective. In the two cases where strategic political objectives were achieved, CW was an integral part and not the sole player. Beyond the three case studies presented, CW in the future will be reliant on some form of assistance in the physical world. This assistance may be in the form of conventional forces on the ground, but it will more likely come from agents inside organizations that are targeted. These agents will provide the structural knowledge and vulnerabilities of the networks that will allow cyber warriors to plan their attack. This exploitation and planning will be key in allowing CW to generate a decisive and immediate result that cannot be defended against. External hackers will not be able to map the networks vulnerabilities with enough speed and thoroughness to be effective. Effective strategic CW will not happen independently of action on the ground.

Conclusion Two

CW is effective as part of a conventional campaign. CW is effective at shaping the information battle space as conventional forces conduct operations. The Russia-Georgia War demonstrated that CW can disrupt communication, misinform, and gather intelligence. This is the most likely role for CW in the near future. A modern military organization will likely employ some form of cyber attack as part of a CW campaign in support of conventional operations.

Conclusion Three

CW offensive capability is not currently greater than CW defensive capability. CW will have difficulty becoming a strategic level weapon until its offensive capability overwhelms an adversary's strategic defensive capability. Currently, when an exploit is found that allows offensive CW to occur, a patch is almost immediately available which closes the exploit and protects other unaffected systems. The defensive challenge becomes not creating the patch, but making sure the vulnerable systems are constantly updated. In all three case studies, cyber attacks were mitigated and halted by patches being applied to vulnerable systems.

The paths that offensive CW takes to reach its target are also very vulnerable. Like an attacking conventional force that has the bridge in front of it destroyed, a CW attack is neutralized when its path is removed. In all three case studies, attacking domains were refused access to the vulnerable systems. When the attackers sought out other "bridges," those paths were also neutralized.

The offensive challenge is to exploit vulnerability so quickly and completely that the target nation is incapable of mounting a sufficient defense. The attack must also generate results that are of sufficient duration that the connected real world systems begin to collapse from want of rapid, accurate, and secure information connectivity. The three case studies suggest that CW is not currently capable of these requirements when faced with a cyber defense.

Conclusion Four

CW capability cannot be employed against a target without significant CW vulnerability. The Russia-Georgia case study demonstrated that Georgia's vulnerability to

CW was much less than Estonia, because the Internet and information infrastructure were not sufficiently integrated into Georgian government and society. CW cannot disrupt a network that is not connected to anything. Strategic connectivity must exist for CW to be employed strategically. A lack of strategic connectivity results in a lack of strategic vulnerability to CW. This same concept will travel well to the operational and tactical levels. Tactical connectivity creates tactical vulnerability, and operational connectivity creates operational vulnerability. It is likely that nations will be able to control their vulnerability by monitoring and securing the information nodes that allow connectivity between the three levels of war. This prevents a tactical attack from becoming an operational or strategic attack, by controlling vulnerability.

To evaluate a nation's susceptibility to strategic CW attack the framework of the network must be analyzed to demonstrate a strategic vulnerability. If sufficient vulnerability does not exist, then great strategic CW power becomes irrelevant. However, if a nation has its strategic level systems able to communicate with each other via a common network, then a strategic CW vulnerability exists.

Conclusion Five

The three case studies have demonstrated that there has not yet been a Cyber Hiroshima yet. The U.S. dropped its Atomic Bomb on Hiroshima in 1945 and changed world security. Policy makers and security professionals are eager to treat Estonia as a Cyber Hiroshima, but the comparison is inaccurate. The Atomic Bombs at Hiroshima and Nagasaki undeniably forced the Japanese to surrender. The cyber attacks in Estonia did not achieve that type of objective. The attacks in Estonia were effective at generating awareness for cyber threats, but they did not change the military and political landscape.

It is possible that a Cyber Hiroshima may occur in the future. To be a watershed event in strategic warfare, like nuclear weapons, this Cyber Hiroshima would need to clearly create new strategic conditions, and be almost indefensible once it is unleashed. The three case studies suggest that this capability does not yet exist.

Conclusion Six

Nations are not willing to openly generate the CW power necessary to achieve their strategic objectives. In all three case studies, the cyber attacks were coming from civilian controlled botnets, and the attacks were coordinated on civilian hacker forums. The code and exploits given to these armies of civilian hackers may have originated from a state controlled source, but there is no unclassified evidence to support state sponsorship. Nations are unwilling to be openly responsible for CW so far. This brings civilian hackers to the forefront of any CW conflict. In all three case studies, civilians participated on both sides of the conflict. This trait of CW becomes an essential part in a campaign, because many civilian hackers can summon robust botnets to attack a target's networks and systems. A large number of bots lengthens the duration of attack as well.

It takes significant computing power to execute a DoS for a significant length of time. State sponsored organizations may not have access to the botnets and zombies necessary to generate enough CW combat power for effective disruption and corruption. To solve this issue, states can covertly enable sympathetic hackers through hacker forums. States maintain deniability while generating sufficient CW combat power.

Recommendations

1. A classified study needs to be conducted (to include the three case studies in this paper) to compile all data into a more complete picture of what CW is capable of as a strategic weapon.

2. In preparing for defense against CW, the civilian population (along with its latent computing knowledge, variety, and capability) needs to be integrated into all courses of action.

3. A study needs to be conducted to map CW capability and vulnerability throughout the international community. This map would indicate the presence of CW capability and vulnerability at the strategic, operational, and tactical levels for each nation. This map would make it easier to template future CW threats and vulnerabilities that could affect the U.S.

The omnipresence of cyberspace in daily life implies that CW must ultimately become a weapon capable of significant strategic capability. Currently CW is similar to the annual influenza that citizens are exposed to every year. Most people get a little sick then recover as their bodies' defenses get the upper hand on the invading virus. A few very vulnerable people, such as the elderly and the very young are infected with catastrophic results. Their defenses are unable to respond effectively to the virus. Current CW follows a similar model. Network defenses keep improving their anti-bodies to suppress potentially catastrophic cyber attacks, limiting the effects to a few sick days. Only extremely vulnerable systems without updated immune systems have catastrophic failures. Currently CW does not appear capable to deliver on its promise of overwhelming cyber Armageddon.

GLOSSARY

Bot. A computer that runs programs autonomously.

Botnet. A term referring to any network of bots. Botnets are most often associated with malicious software. When the term botnet is used in the context of malicious software it refers to a network of zombie computers that can be activated and employed by a bot herder or bot master for malicious tasks. Malicious task examples are DDoS attacks, spam, and Adware. Botnet software is normally installed on computers by worms, Trojans, and other forms of malicious downloads.

Computer Network Attack. Operations to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves. Electronic attack (EA) can be used against a computer, but it is not computer network attack(CNA). CNA relies on the data stream to execute the attack while EA relies on the electromagnetic spectrum. An example of the two operations is the following: sending a code or instruction to a central processing unit that causes the computer to short out the power supply is CNA. Using an electromagnetic pulse to destroy a computer's electronics and causing the same result is EA.

Denial of Service. An attempt to make a computer resource unavailable to its intended users.

Distributed Denial of Service. When multiple systems attempt to flood the bandwidth or resources of a system in order to make it unavailable to its intended users.

Domain Name System. A naming system for computers, services or any resources connected to the Internet. It translates human friendly names into Internet protocol (IP) addresses that the computers can use. An example is www.example.com translates to 204.678.143 IP address.

Server. A computer that provides client stations with access to files and printers as shared resources to a computer network.

Structured Query Language. A database computer language designed for managing data in relational database management systems.

Structured Query Language Injection. A code injection that exploits a security vulnerability in the database layer of an application.

Zombie. A compromised computer attached to the Internet. Often part of a botnet it will be used to perform malicious tasks under remote direction. Most owners of zombie computers are unaware that their computer has become a zombie in a botnet.

REFERENCE LIST

Books

Cornell, Svante E. and Starr, S. Frederick, eds. 2009. *The guns of August 2008: Russia's war in Georgia.* New York: M.E. Sharpe.

Erickson, Jon. 2008. *Hacking: The art of exploitation.* San Francisco: No Starch Press, Inc.

Goldstein, Emmanuel, ed. 2009. *The best of 2600: A hacker odyssey.* Indianapolis: Wiley Publishing, Inc.

Libicki, Martin C. 2007. *Conquest in cyberspace: National security and information warfare.* New York: Cambridge University Press,

Schneier, Bruce. 2008. *Schneier on security.* Indianapolis: Wiley Publishing, Inc.

Thomas, Timothy L. 2005. *Cyber silhouettes: Shadows over information operations*. Fort Leavenworth: Foreign Military Studies Office.

———. 2004. *Dragon bytes: Chinese information-war theory and practice*. Fort Leavenworth: Foreign Military Studies Office.

———. 2007. *Decoding the virtual dragon: Critical evolutions in the science and philosophy of China's information operations and military strategy*. Fort Leavenworth: Foreign Military Studies Office.

U.S. Department of the Army. 2003. Field Manual (FM) 3-13, *Information operations.* Washington, DC: Government Printing Office.

U.S. Department of Defense. Chairman of the Joint Chiefs of Staff. 2006. Joint Publication (JP) 3-13, *Information operations.* Washington, DC: Government Printing Office.

Verton, Dan. 2003. *Black ice: The invisible threat of cyber-terrorism.* Emeryville: McGraw-Hill/Osborne.

Wozniak, Steve, and Gina Smith. 2006. *iWoz.* New York: W.W. Norton and Company.

Internet References

Al Jazeera. "Israel in 'all-out' war with Hamas." Al Jazeera. http://english.aljazeera.net/news/middleeast/2008/12/200812299414067415 3.html (accessed 13 October 2009).

Associated Press. “Cyber command to create force for future.” *MSNBC*. www.msnbc.msn.com/id/30575707/print/1/displaymode/1098/ (accessed 6 May 2009).

———. “Hackers Attack U.S. naval war college.” *MSNBC*. www.msnbc.msn.com/ id/16057306/print/1/displaymode/1098 (accessed 6 May 2009).

Baltic Security and Defence Review. “Defence policies’ 06 in brief: Estonia, Latvia, Lithuania.” *Baltic Security and Defence Review*. http://14._Defence_Policies_ 2006_in_Brief-Estonia_Latvia_Lithuania(1).pdf (accessed 4 August 2009).

Baltic Times. “Estonia’s economy grows 11.5 percent in 2006.” *The Baltic Times*. http://www.baltictimes.com/news/articles/17329/ (accessed 1 October 2009).

Bar’el, Zvi. “Egypt, Saudis threaten to rescind Arab peace plan.” Haaretz. http://www.haaretz.com/hasen/spages/1091590.html (accessed 13 October 2009).

Ben-Ari, Tomer. “Israel: Information operations threats and countermeasures.” Australian government. http://www.au.af.mil/info-ops/iosphere/ 08special/iosphere_special08_ben-ari.pdf (accessed 13 October 2008).

Benn, Aluf. “Netanyahu convinced Obama seeks clash with Israel to appease Arabs.” *Haaretz*, http://www.haaretz.com/hasen/spages/1091428.html (accessed 13 October 2009).

Brenner, Bill. “Black hot 2007: Lessons of the Estonia attacks.” SearchSecurity.com. http://searchsecurity.techtarget.com/news/interview/0,289202,sid14_gcil265720,0 0.html (accessed 10 June 2009).

Brom, Shlomo. “Operation cast lead, January 2009: An interim assessment.” Strategic Assessment. http://www.inss.org.il/upload/(FILE)1234084380.pdf (accessed 13 October 2009).

Bumgarner, John, and Scott Borg. “Overview by the US-CCU of the cyber campaign against Georgia in August of 2008.” United States Cyber Consequences Unit. http://www.registan.net/wp-content/uploads/2009/08/US-CCU-Georgia-Cyber-Campaign-Overview.pdf (accessed 7 October 2009).

Catignani, Sergio. “Variation on a theme: Israel’s operation cast lead and the Caza strip missile conundrum.” *Small Wars Journal*. http://smallwarsjournal.com/ documents/castlead.pdf (accessed 13 October 2009).

Central Intelligence Agency. “The world factbook: Georgia.” https://www.cia.gov/ library/publications/the-world-factbook/geos/gg.html (accessed 5 October 2009).

———. “The world factbook: Israel.” https://www.cia.gov/library/ publications/the-world-factbook/geos/is.html (accessed 13 October 2009).

Cisco. “MagtiCom launches first mobile WiMAX service in Georgia with Cisco end-to-end solution.” Shareholder.com. http://files.shareholder.com/downloads/CSCO/0x0x271069/9d517546-aed0-45f0-b84b-3fd40ce22e0c/CSCO_News_2009_2_9_Press_Releases.pdf (accessed 7 October 2009).

Coffman, K. G. and A. M. Odlyzko. “The size and growth rate of the Internet.” AT&T Labs Research. http://www.dtc.umn.edu/~odlyzko/doc/internet.size.pdf (accessed 2 August 2009).

Commission of the European Communities. “Communication from the commission to the European Parliament, the council, The European economic and social committee and the committee of the regions on critical information infrastructure protection.” http://ec.europa.eu/information_society/policy/nis/docs/comm_ciip/comm_en.pdf (accessed 19 July 2009).

Council of the European Union. “Declaration by the presidency on behalf of the European union on the situation in Georgia.” Council of the European Union. http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/cfsp/109556.pdf (accessed 7 October 2009).

Cyber Security Strategy Committee. “Cyber security strategy.” Estonian Ministry of Defence. http://mod.gov.ee/static/sisu/files/Estonian_Cyber_Security_Strategy.pdf (accessed 2 October 2009).

Denning, Dorothy E. “A view of cyberterrorism five years later.” Naval Post Graduate School. http://faculty.nps.edu/dedennin/publications/Cyberterror%202006.pdf (accessed 18 July 2009).

Derfner, Larry. “Why the Gaza war between Israel and Hamas broke out now.” *U.S. News and World Report*. http://www.usnews.com/articles/news/world/2008/12/30/why-the-gaza-war-between-israel-and-hamas-broke-out-now.html (accessed 13 October 2009).

Economy Watch. “Israel economic statistics and indicators.” *Economy Watch*. http://www.economywatch.com/economic-statistics/country/Israel/year-2009/ (accessed 13 October 2009).

Erlanger, Steven. “A Gaza war full of traps and trickery.” *The New York Times*. http://www.nytimes.com/2009/01/11/world/middleeast/11hamas.html?_r=1 (accessed 13 October 2009).

Espiner, Tom. “CIA: Cyberattack caused multiple-city blackout.” ZDNet.com. http://news.zdnet.com/2100-1009_22-184416.html (accessed 4 May 2009).

Estonian Embassy, Moscow. “Estonia and Russia.” http://www.estemb.ru/eng/estonia_and_russia (accessed 4 August 2009).

Estonian Foreign Policy Institute. “Estonian foreign policy yearbook 2006.” http://www.evi.ee/english/publi.html (accessed 4 August 2009).

Estonian Ministry of Defense. “Estonian defence policy 2006.” http://mod.gov.ee/?op=body&id=400 (accessed 4 August 2009).

Estonian Ministry of Foreign Affairs. “Estonian economy.” http://web-static.vm.ee/static/failid/420/Economy_April2006.pdf (accessed 1 October 2009).

———. “The Estonian government’s European union policy for 2004-2006.” http://The_Government_s_European_Union_Policy_for_2004_2006_Final(1).pdf (accessed 4 August 2009).

———. “The European security and defence policy.” http://web-static.vm.ee/static/failed/476/EDSP.pdf (accessed 4 August 2009).

———. Website. http://www.vm.ee/eng/nato/kat_359 (accessed 4 August 2009).

European Commission: Information Society ad Media Directorate-General. “Towards a strengthened network and information security policy in Europe.” www.ec.europa.eu/information_society/policy/nis/docs/pub_consult_nis_2009/pc_executive_summary%20v1.pdf (accessed 19 July 2009).

Evron, Gadi. “Internet attacks against Georgian websites.” CircleID.com. www.circleid.com/posts/print/88116_internet_attacks_georgia/ (accessed 10 June 2009).

Fabian-Marks, Johanna. “Energy security position paper.” University of Washington. http://jsis.washington.edu/euc//file/Estonia%20Position%20Paper%20Energy%20Security.pdf (accessed 4 August 2009).

Fischer, Stanley. “Challenges facing the Israeli economy in the globalization era.” The Bank of Israel. http://www.bis.org/review/r080129b.pdf (accessed 13 October 2009).

Foreign Policy. “Seven questions: Georgia’s special relationship.” http://www.foreign policy.com/story/cms.php?story_id=4624 (accessed 7 October 2009).

Francois, Renaud. “Georgia: Assessment of a disastrous military adventure.” European Strategic Intelligence and Security Center. http://www.esisc.org/documents/pdf/en/georgia-assessment-of-a-disastrous-military-adventure-409.pdf (accessed 5 October 2009).

Global Security. “Georgia-army order of battle.” http://www.globalsecurity.org/military/world/georgia/army-orbat.htm (accessed 5 October 2009).

Glorioso, Andrea. “Towards a European union policy on critical information infrastructure protection.” Cooperative Cyber Defence Center of Excellence. www.ccdcoe.org/cyberwarfare/images/244.pdf (accessed 19 July 2008).

Government of Georgia. “Report by the government of Georgia on the aggression by the Russian federation against Georgia.” http://www.civil.ge/files/files/GeorgianGovernmentReportWar.pdf (accessed 8 October 2009).

Haaretz News Service. “Obama proposed plan for peace deal within two years.” *Haaretz*. http://www.haaretz.com/hasen/spages/1091465.html (accessed 13 October 2009).

Hamilton, Robert E. “Georgian military reform--an alternative view.” Center For Strategic and International Studies. http://csis.org/files/media/csis/pubs/090203_hamilton_militaryreform.pdf (accessed 7 October 2009).

Heller, Aron. “Israel rethinks Saudi peace plan.” *The Washington Times*. http://www.washingtontimes.com/news/2008/oct/20/israel-rethinks-saudi-peace-plan/ (accessed 13 October 2009).

Independent. “Social networking sites enter gaza conflict.” *The Independent*. http://license.icopyright.net/user/viewFreeUse.act?fuid=Mzc2MTgyOQ%3D%3d, (accessed 10 June 2009).

Information Warfare Monitor. “Gaza 2.0: The information landscape of war.” http://128.100.171.10/modules.php?op=modload&name=News&file=article&sid-=2130 (accessed 5 June 2009).

———. “Gaza 2.0: The new battleground of Middle Eastern Conflict.” http://128.100.171.10/modules.php?op=modload&name=News&file=article&sid-=2150 (accessed 5 June 2009).

———. “Israel’s accidental youtube war.” http://128.100.171.10/modules.php?op=modload&name=News&file=article&sid-=2142 (accessed 5 June 2009).

Internet World Stats. “Internet usage in Asia.” http://www.internetworldstats.com/stats3.htm (accessed 7 October 2009).

Jones, Garret. “The revolution will be brought to you by text messaging.” *Foreign Policy Research Institute*. http://www.fpri.org/endnotes/200803.jones.revolutiontextmessaging.html (accessed 10 December 2008).

Kaeo, Merike. “Cyber attacks on Estonia: Short synopsis.” Double Shot Security. www.doubleshotsecurity.com/pdf/NANOG_eesti.pdf (accessed 18 July 2009).

Korns, Stephen W., and Joshua E. Kastenberg. “Georgia’s cyber left hook.” *Parameters*. www.carlisle.army.mil/usawc/Parameters/08winter/korns.pdf (accessed 18 July 2009).

Krangel, Eric. “Cyberwar: Israel and Hamas attack each other’s media.” *The Business Insider*. http://www.businessinsider.com/2009/1/cyberwar-israel-and-hamas-attack-each-others-media (accessed 5 June 2009).

LECG Ltd. “Connectivity scorecard 2009: United States.” USIIA.org. http://www.usiia.org/pubs/United_States.pdf (accessed 2 August 2009).

Levine, Mark. “Who will save Israel from itself?” Al Jazeera.net. http://english.aljazeera.net/focus/war_on_gaza/2009/01/200911011272326074l.html (accessed 13 October 2009).

Link, Martin. “Cyber attacks: Estonia.” E-Arsenal. www.bilgitoplumu.gov.tr/yayin/CyberAttacks.pdf (accessed 18 July 2009).

Lobjakas, Ahto. “Estonia: NATO’s brand new center of cyberwarfare excellence.” Wired.com. http://www.wired.com/beyond_the_beyond/2008/04/estonia-natos-b/ (accessed 4 August 2009).

Mahnaimi, Uzi and Baxter, Sarah. “Barack Obama links Israel peace plan to 1967 borders deal.” *The Times*. http://www.timesonline.co.uk/tol/news/world/middle_east/article5162537.ece (accessed 13 October 2009).

Marcus, Jonathan. “The 2009 Israeli election” A bump in the road to peace?” *The Washington Quarterly*. http://docs.google.com/gview?a=v&q=cache:fIhEH0tSaSoJ:www.ciaonet.org/journals/twq/v32i3/f_0017407_14889.pdf+israeli+election+2009+filetype:pdf&hl=en&gl=us&sig=AFQjCNGy7m7WvhXO1QEXDolScXA9iWUjBA (accessed 13 October 2009).

Margolis, Eric S. “Israel’s fait accompli in Gaza.” Al Jazeera. http://english.aljazeera.net/focus/war_on_gaza/2009/01/200914102257130539.html (accessed 13 October 2009).

Markoff, John. “Before the gunfire, cyberattacks.” *The New York Times*. http://www.nytimes.com/2008/08/13/technology/13cyber.html?_r=1 (accessed 5 October 2009).

Matthews, Matt M. “The Israeli defense forces response to the 2006 war with Hezbollah.” *Military Review*. http://usacac.army.mil/CAC2/MilitaryReview/Archives/English/MilitaryReview_20090831_art009.pdf (accessed 13 October 2009).

McGreal, Chris. “Why Israel went to war in Gaza.” *The Guardian*. http://www.guardian.co.uk/world/2009/jan/04/israel-gaza-hamas-hidden-agenda (accessed 13 October 2009).

Ministry of Industry, Trade, and Labor. “Israel: A resilient global economy.” http://www.investinisrael.gov.il/NR/rdonlyres/24B3DDFF-BAF7-4EF5-8395-

07946CAE794B/0/IsraelAResilientGlobalEconomyMarch09.pdf (accessed 13 October 2009).

Morozov, Evgeny. “Cyber-scare.” *Boston Review*. http://bostonreview.net/BR34.4/morozov.php (accessed 2 September 2009).

Morrill, Dan. “Cyber war Israel and Hamas.” Toolbox for IT. http://it.toolbox.com/blogs/managing-infosec/cyber-war-israel-and-hamas-29096 (accessed 5 June 2009).

Nabucco Gas Pipeline International. “Nabucco gas pipeline project.” http://www.nabucco-pipeline.com/cms/upload/press%20and%20public/presentations/Official%20Project%20Description_Q1_2009_v01.pdf (accessed 8 October 2009).

NATO. “NATO opens new centre of excellence on cyber defence.” http://www.nato.int/docu/update/2008/05-may/e0514a.html (accessed 2 October 2009).

———. “NATO’s relations with Georgia.” http://www.nato.int/cps/en/natolive/topics_38988.htm (accessed 7 October 2009).

———. “NATO’s relationship with Georgia.” http://www.nato.int/issues/nato-georgia/index.html (accessed 7 October 2009).

———. “Estonia.” NATO. http://www.nato.int/issues/commitment/docs/080325-estonia.pdf (accessed 2 October 2009).

Odnokolenko, Oleg. “Controversial aspects of new Russian military doctrine questioned.” Open Source Center. https://www.opensource.gov/portal/server.pt/gateway/PTARGS_0_0_246_203_121123_43/content/Display/2083080?highlightQuery=eJxdjEEOgjAQRa%2FSsIJjoI2RhSVpSozLBj7SKK2ZKSbeXmhl42b%2Bm%2Fx5U3Z0h4%2BiVlIYyw9OFMYUcUJKiTee4TXvh3%2B1Xpid9YlPGEA2upDXmmYMuQjUg6vE5W60Wlycdxzps%2FH6d50SIzxjwwOFfloIP63IXiGujTk3ShzbThl9q74IKj3G&fileSize=95902 (accessed 15 October 2009).

O’Loughlin, Toni. “Israel considers reviving Saudi peace plan to resolve conflict.” *The Guardian*. http://www.guardian.co.uk/world/2008/oct/20/middleeast-israel-saudi-peace-plan (accessed 13 October 2009).

Orav, Aivo. “Measuring foreign relations.” Estonian Ministry of Foreign Affairs. http://web-static.vm.ee/static/failid/175/Aivo_Orav.pdf (accessed 4 August 2009).

Project Grey Goose Phase I Report. “Russia/Georgia cyber war-findings and analysis.” Scribd.com. http://www.scribd.com/doc/6967393/Project-Grey-Goose-Phase-I-Report (accessed 18 July 2009).

Project Grey Goose Phase II Report. “Project grey goose phase II report.” Scribd.com. http://www.scribd.com/doc/13442963/Project-Grey-Goose-Phase-II-Report (accessed 13 October 2009).

Radio Free Europe Radio Liberty. “Estonia: New president reflects on Russia, other foreign policy challenges.” http://www.rferl.org/content/article/1071886.html (accessed 4 August 2009).

———. “Russia denies involvement in alleged Georgian military coup.” http://www.rferl.org/content/Russia_Denies_Involvement_In_Alleged_Georgian_Military_Coup_/1622819.html (accessed 7 October 2009).

Reuters. “Georgia’s top general replaced after four months.” Radio Free Europe Radio Liberty. http://www.rferl.org/content/Georgias_Top_General_Replaced_After_Four_Months/1504821.html (accessed 7 October 2009).

Rockefeller, John D., and Olympia Snowe. “Statement on the Obama administration’s cybersecurity review.” U.S. Senate Committee on Commerce, Science, and Transportation. http://commerce.senate.gov/public/index.cfm?FuseACtion=PressReleases.Detail1&PressRelease_1d=e01505d-f7b7 (accessed 2 August 2009).

Saydjari, O. Sami. “Defending cyberspace.” Cyber Defense Agency. http://www.cyberdefenseagency.com/publications/Defending_Cyberspace.pdf (accessed 4 May 2009).

———. “Structuring for strategic cyber defense: A cyber manhattan project blueprint.” Annual Computer Security Applications Conference. http://www.acsac.org/2008/program/keynotes/saydjari.pdf (accessed 18 July 2009).

———. “Weak spots on cyber defense.” GCN. http://www.gcn.com/Articles/2006/09/19/O-Sami-Saydjari--Weak-spots-on-cyberdefense.aspx?Page=2 (accessed 3 August 2009).

Shachtman, Noah. “U.S. cyber command:404 error, mission not (yet) found.” Wired.com. www.wired.com/dangerroom/2009/06/foggy-future-for-militarys-new-cyber-command (accessed 18 July 2009).

Sharp, Jeremy M. “Lebanon: The Israel-Hamas-Hezbollah conflict.” *Congressional Research Service*. http://www.fas.org/sgp/crs/mideast/RL33566.pdf (accessed 13 October 2009).

Shlaim, Avi. “How Israel brought Gaza to the brink of humanitarian catastrophe.” *The Guardian*. http://www.guardian.co.uk/world/2009/jan/07/gaza-israel-palestine (accessed 13 October 2009).

Sydney Morning Herald. “Estonia urges firm EU, NATO response to new form of warfare: Cyber attacks.” *Sydney Morning Herald*. http://www.smh.com.au/news/Technology/Estonia-urges-firm-EU-NATO-response-to-new-form-of-warfarecyberattacks/2007/05/16/1178995207414.html (accessed 4 August 2009).

Tiido, Harri. “The evolution of security 2006-2007: EU and NATO cooperation.” Estonian Ministry of Foreign Affairs. http://web-static.vm.ee/static/faillid/096/Harri_Tiido.pdf (accessed 4 August 2009).

Tinnel, Laura S., Saydjari, O. Sami, and Farrell, Dave. “Cyberwar strategy and tactics: An analysis of cyber goals, strategies, tactics, and techniques.” Cyber Defense Agency. http://www.cyberdefenseagency.com/publications/Cyberwar_Strategy_and_Tactics.pdf, (accessed 18 July 2009).

Toth, Beatrix. “Estonia under cyber attack.” Hungarian National Computer Emergency Response Team. www.cert.hu/dmdocuments/EStoia_attack2.pdf (accessed 18 July 2009).

Transparency International Georgia. “Aid to Georgia: Transparency, accountability, and the JNA.” http://www.transparency.ge/files/215_447_426697_Aid%20to%20Georgia%20ENG.pdf (accessed 8 October 2009).

Traynor, Ian. “Russia accused of unleashing cyber war to disable Estonia.” *The Guardian*. http://www.guardian.co.uk/world/2007/may/17/topstories3.russia (accessed 4 August 2009).

U.S. Congress. House. “Testimony of O. Sami. Saydjari.” House Committee on Homeland Security. http://homeland.house.gov/SiteDocuments/20070425145307-82503.pdf (accessed 15 October 2009).

———. “Witnesses, members discuss how to secure cyberspace.” Committee on Science and Technology, U.S. House of Representatives. http://science.house.gove/press/PRArticle/aspx?NewsID=2517 (accessed 18 July 2009).

United Kingdom Ministry of Defence. “European defence paper no 3.” Ministry of Defence. www.mod.uk/NR/rdonlyres/817B556A-OAAO-4761-804B-211D52F375EF/dpolpaper3_european_def.pdf (accessed 19 July 2009).

United States Cyber Consequences Unit. “US-CCU’s analytic method.” U.S. Cyber Consequences Unit. http://www.usccu.us/#The_US-CCU (accessed 19 August 2009).

Warner, Gary. “Radical Muslim hackers declare cyberwar on Israel.” http://garwarner.blogspot.com/2008/12/muslim-hackers-declare-cyberwar-on.html (accessed 5 June 2009).

White House. “Cyberspace policy review.” www.whitehouse.gove/assets/documents /Cyberspace_Policy_Review_final.pdf (accessed 18 July 2009).

Williams, Rachel. “Global hackers threaten net security in cyber warfare aimed at top targets.” *The Guardian*, www.guardian.co.uk/technology/2007/nov /29/hacking.news?gusrc=rss& (accessed 18 July 2009).

Wilson, Tim. “Study of Russia-Georgia cyber conflict brings warnings to U.S. businesses, citizens.” Dark Reading. http://www.darkreading.com/security/ cybercrime/showArticle.jhtml;jsessionid=TQQPDFSSCYDB1QE1GHOSKH4ATMY32JVN?articleID=219400367 (accessed 19 August 2009).

Woehrel, Steven. “Estonia: Current issues and U.S. policy.” Congressional Research Service. www.fas.org/sgp/crs/row/RS22692.pdf (accessed 4 August 2009).

Wood, Bradley J., O. Sami Saydjari, and Victoria Stavridou. “A proactive holistic approach to strategic cyber defense.” Cyber Defense Agency. http://www.cyberdefenseagency.com/publications/Cyberwar_Strategy_and_Tactics.pdf (accessed 18 July 2009).

Woodcock, Bill. “Lessons learned from the Russian-Estonian cyber-conflict.” Packet Clearing House, www.lacnic.net/documents/ixp/woodcock-caso_estonia.pdf (accessed 19 July 2009).

INITIAL DISTRIBUTION LIST

Combined Arms Research Library
U.S. Army Command and General Staff College
250 Gibbon Ave.
Fort Leavenworth, KS 66027-2314

Defense Technical Information Center/OCA
825 John J. Kingman Rd., Suite 944
Fort Belvoir, VA 22060-6218

Dr. Jack D. Kem
DJIMO
USACGSC
100 Stimson Avenue
Fort Leavenworth, KS 66027-2301

Mr. John A. Schatzel
CTAC
USACGSC
100 Stimson Avenue
Fort Leavenworth, KS 66027-2301

CMDR Christopher R. Vega
DJIMO
USACGSC
100 Stimson Avenue
Fort Leavenworth, KS 66027-2301