STRATEGIC CYBER DETERRENCE

A Thesis
Presented to the Faculty
Of
The Fletcher School of Law and Diplomacy

By

CHRISTOPHER FITZGERALD WRENN

In partial fulfillment of the requirements for the
Degree of Doctor of Philosophy

JULY 2012

Dissertation Committee
Professor Robert L. Pfaltzgraff, Jr., Chair
Professor Antonia H. Chayes
Professor William C. Martel

COLONEL CHRISTOPHER F. WRENN (CHRIS)
26 Pearl Street, Medford, MA, 02155 · 325-864-1515 · cwrenn01@tufts.edu

Education

Tufts University, the Fletcher School **Medford, MA**
PhD Candidate, 2009–present
Pursuing doctoral study in International Relations.
Research topic: Deterrence, cyber deterrence

Tufts University, the Fletcher School **Medford, MA**
National Defense Fellow, 2006–2007
Pursued a course of study in areas central to United States national security: nuclear proliferation, counterproliferation, terrorism, crisis management, homeland security, and intelligence.
Research topic: Global Salafi jihadist insurgency

Air University, Air Command and Staff College **Montgomery, AL**
Master of Military Operational Art and Science, June 2000
Completed a course of study with focus on national security and military studies. Partial curriculum: national and international studies; nature of war; joint operations; future capabilities and concepts; intervention, peacekeeping and the U.S.
Research topic: United Nations peacekeeping operations in Western Sahara

Harvard University, Kennedy School of Government **Cambridge, MA**
Master of Public Administration, June 1995
Completed a course of study in national security, international security, and domestic public policy. Partial curriculum: uses of history in assessing foreign governments; pursuing the national interest; international mediation and conflict resolution; drug control policy.

North Carolina State University **Raleigh, NC**
Bachelor of Arts Economics and Business Management, December 1984

Experience

Division Chief, Nuclear and Homeland Defense Capabilities Based Planning (2007–2009) **Washington, DC**
Headquarters, United States Air Force
Led the development and assessment of Air Force nuclear and homeland defense capabilities, shortfalls, and risk to ensure required U.S. strategic forces were fielded. Conducted quantitative research for the Air Force resulting in an assessment of existing and future force development to help shape the $122B Air Force budget strategy.

Director of Operations, then Commander 7th Operations Support Squadron
(2003–2006) Abilene, TX
Led combat operations in the B-1 bomber over Afghanistan. Commanded 242 Airmen in planning and executing operations for a conventional bomber base and an airlift group. Ensured the readiness and combat training of an expeditionary operations center, intelligence unit, mission planning cell, air traffic control facility, combat communications suite, and weather station.

Assistant to the Commander, then Deputy Chief, Commander Staff Group
(2001–2003) Omaha, NE
United States Strategic Command (USSTRATCOM)
Led staff of eight in formulating courses of action regarding strategy, policy, force structure, arms control, and proliferation. Shaped policy and debate leading to the Presidential decision for USSTRATCOM to develop global strike; missile defense; information operations; and Command and Control capabilities. Commander's speechwriter and action officer for Operations, Logistics, and Intelligence directorates.

Nuclear War Plan Advisor to the Commander USSTRATCOM
(2000–2001) Omaha, NE
Personal advisor to the Commander on the Nation's nuclear war plan. Responsible for assisting the Commander in directing the strategic nuclear triad during wartime and exercise operations. Prepared to formulate war plan recommendations for the President.

B-1B Navigator, Instructor Navigator, Assistant Flight Commander
(1992–1999) Grand Forks, ND and Abilene, TX
Held various positions, including supervising the production of seventy-five B-1B navigators yearly and the recurrent training of seventeen permanent team members. As Wing Battlestaff director, deployed 143 troops, 290 tons of cargo, and two B-1B bombers for Operation DESERT FOX. Served as Strategic Arms Reduction Treaty and Chemical Weapons Convention officer.

United Nations Military Observer (1997–1998) Western Sahara, Africa
Participated in UN Mission for the Referendum in Western Sahara, an African peacekeeping mission that monitors the cease-fire between Moroccan and Frente POLISARIO forces along a 900-mile front. Located two new mine fields, six unknown water wells, and mapped 243 kilometers of uncharted roads. Discovered and then ensured the protection of thirty-one unknown prehistoric cave painting sites. Instrumental in refining UN High Commission for Refugees plan to repatriate 65,000 refugees.

Air Operations Officer, Operation Support Justice IV
(1993) Panama City, Panama
Served at focal point for all U.S. aerial operations in Central and South America. Responsible for theater-wide counter drug missions, airlift support, search-and-

rescue missions, and aerial reconnaissance. Coordinated missions involving U.S. Department of Defense, Coast Guard, Customs Service, Drug Enforcement Agency, Central Intelligence Agency, Federal Bureau of Investigation, and forces from fourteen nations.

B-52 Training, Navigator, and Evaluator/Instructor Navigator
(1988–1992) Sacramento and Merced, CA; and Shreveport, LA
Flew twenty-six combat missions during Operation DESERT STORM. Senior B-52 navigator on the base; assessed training for 400 aviators.

Abstract

The world has witnessed two cyber wars, the first between Estonia and Russia in 2007 and the second between Georgia and Russia in 2008. In both of these wars, the same problem existed and will continue to proliferate as without imposed costs and/or denied benefits, state and non-state actors will further develop and refine capabilities that have the ability to take advantage of cyber vulnerabilities.

The scope of this study is to understand the nature of cyber war and its purpose in order to develop a theory of cyber deterrence. An initial challenge surfaced because of a lack of definitional consistency for terminology in the cyber domain. To address this challenge, I relied upon time-tested Clausewitzian ideals to define cyber war as the continuation of state policy by cyber means.

The principal research question focused on developing requirements for cyber deterrence theory that are applicable to cyber war. The requirements that emerged were grounded in preceding deterrence theories and forged from a vulnerability-based assessment of the existing cases of cyber war. I closely analyzed exploited and unexploited vulnerabilities to help inform the requirements for cyber deterrence by denial. This permitted me to reverse engineer what actually occurred to design a theory that may prove more relevant to deterring cyber war in other cases. In the course of the case studies, I learned that cooperation appears to play a larger role in cyber deterrence than earlier forms of deterrence theory. This inspired a theory of cyber deterrence based upon denial, punishment, and cooperation.

Four hypotheses informed by basic deterrence, criminal justice deterrence, and nuclear deterrence theories were rooted in a critical question regarding the cyber domain: How is cyber deterrence possible if attribution, offensive capabilities, defensive capabilities, or cooperative relationships are either missing from or inadequate to deter a malicious actor?

The hypotheses, structured on the triadic components of denial, punishment, and cooperation, were tested using the two cases of cyber war. What I discovered in the process of analyzing and evaluating the cases and then synthesizing this with the literature left me with neither a full account of what is possible nor an account of what is not possible. Instead, the analysis indicated the presence of a middle ground where cyber deterrence becomes conditional and/or variable in its effectiveness based on attention or inattention to the triadic components.

This means that cyber deterrence requires tailoring for different classes of actors based on their kinetic and non-kinetic capabilities. It also means that the elements, which comprise the triadic components, require constant attention because of the rapid pace of technological developments. Because of these developments, capabilities and vulnerabilities constantly expand and contract, which indicates that the effectiveness of cyber deterrence is perhaps more conditional as a function of time than previous deterrence variants.

Dedication

To Andi Wrenn

My wife's sacrifice on this long journey was greater than that of any other. I am forever indebted to her for the love, encouragement, patience, and kindness that she extended without fail for three years – all of which carried me through many difficult days and long nights.

Acknowledgements

I am grateful to many for the tremendous opportunity I was given to pursue an advanced degree at the Fletcher School. Those who have and continue to lead the United States Air Force recognize the importance of continuous education in maintaining and developing the capabilities that protect our nation and when needed help fight and win our wars. Three Airmen were integral to this process, and over many years, they have been incredibly giving of their time and energy to help me serve to the best of my ability.

General Raymond E. Johns, Jr., recognized a void in our nation's approach to deterrence and asked that I study the subject in-depth. When no immediate avenue was available to pursue a PhD, he created this opportunity out of thin air by helping to secure funding and accepting degradation in his staff manning for three years. Dr. Colonel (Ret.) Stephen Wright was my commander in the mid-1990s and has mentored me for over fifteen years. He assisted General Johns in helping pave a path for this Ph.D. journey, and over the last three years he has spent many hours helping me think through complex theories, which helped shape the structure and outcome of this dissertation. Brigadier General (Ret.) Jonathan George served as my commander on several occasions and has mentored and guided me for over twenty years. More than any other, the opportunities he created for me over two decades gave me the experience and education to make me competitive for Fletcher's demanding program. General George opened many doors for me during my research, all of which helped

confirm the need for this research and shape my perception of the evidence as it unfolded. Men, I am forever indebted to each of you.

I am fortunate to have been able to work with a dissertation committee of world-class scholars. In determining where to pursue a Ph.D., I must confess, I did not choose Fletcher – I chose Professor Robert L. Pfaltzgraff, Jr., who happened to be among the Fletcher faculty. Not only was Professor Pfaltzgraff instrumental in helping me gain admission into the Fletcher School, he has served as my advisor, a teacher in several courses, and chair of my dissertation committee. The impact this man has had on me personally and professionally is profound. His influence on this dissertation extends from cover to cover. Let me simply say that I have few regrets in life – one is that I was not able to study under this man at a younger age so that I could benefit from his instruction longer.

Professor Antonia H. Chayes has broadened my educational horizons, and her investment in me and this dissertation can be seen in the quite proper injection of cooperation into the cyber deterrence equation. Professor William C. Martel was instrumental in this process as he helped me to critically think through the policy and technical issues associated with deterring cyber war in a manner that I believe significantly strengthened this research. I cannot imagine assembling a more ideal committee for this topic. I thank each of you for helping me.

Aside from those who made it possible for me to pursue this opportunity and those who helped me achieve success, many others were always there. I have learned that this journey is one I could not complete alone. Dr. Jenifer Burckett-Picker, director of the Fletcher School Ph.D. program, and her staff were always

supportive and encouraging. There were many trying days in which her words of wisdom helped me to see a ray of hope among dark clouds. I also appreciate the friendship, support, inspiration, and debate from Dr. Alison Russell, Dr. Colonel Tom McCarthy, Dr. Itamara Lochard, and Liz McClintock and other fellow Ph.D. candidates.

Beyond the Fletcher family, my long-standing friends Colonel (Ret.) Harry Foster and Dr. Adam Lowther were of more help than I believe they realize. The weekly debates on issues of the day and feedback on many ideas expressed in this dissertation were extremely helpful. I thank you both.

I am appreciative of the time several others devoted to this research. Of note were Drs. Andrew Bennett and Anna Seleny, who helped me think through my research questions and hypotheses; Drs. Pano Yannakogeorgos and Gregory Rattray, who offered advice on varying aspects of cyber deterrence; and Shawn Carpenter, who helped me better understand the mindset of hackers and the skill sets needed to defend against them. Also, Jess Barnett and James Wrenn read every word of this dissertation; their help with editing was invaluable.

I am thankful that the cyber deterrence literature includes the thoughtful insight of many scholars. Without their weighty contributions, this research would have been impossible for me to pursue.

Lastly, I gratefully acknowledge my family. For three years, I have been less of a husband, father, grandfather, son, and brother to pursue this journey. My family supported me as I learned a foreign language, completed all necessary

coursework, and produced a dissertation that has been accepted by a top-tier international graduate program.

To all of these people and the few others I may have unfortunately missed – thank you. I hope that the outcome of this research justified your investment.

List of Figures

List of Tables

Contents

Chapter 1: Introduction

As long as nations rely on computer networks as a foundation for military and economic power and as long as such computer networks are accessible to the outside, they are at risk.

— Martin C. Libicki[1]

Problem Statement

Attacks frequently occur in cyberspace at both the state and non-state actor levels; however, twice these attacks have risen to the level of cyber war.[2] The first cyber war occurred in 2007 when Russia attacked Estonia and the second in 2008 with the Russia-Georgia war. In both of these cyber wars, the same problem existed and will continue to proliferate as without imposed costs and/or denied benefits, state and non-state actors will further develop and refine capabilities that have the ability to take advantage of cyber vulnerabilities. These vulnerabilities permit those with malicious intent to assess and potentially exploit or attack government and civilian infrastructure.

The scope of this deterrence study is to understand the nature of *cyber war*. This study recognizes the differences between *cyber attacks* (that fall below the threshold of cyber war), *cyber espionage,* and *cybercrime* and that states may wish to deter these activities as well. Cyber war, cyber attacks, cyber espionage, and cybercrime are vastly different yet related phenomena.[3] Attackers initiate

---

[1] Martin C. Libicki and Project Air Force, *Cyberdeterrence and Cyberwar* (Santa Monica, CA:Rand, 2009), xiii.

[2] Viruses, worms, netbots, and phishing are examples of cyber attacks methods used in cyber warfare.

[3] Criminal justice deterrence theory will be introduced in the literature review section as it offers context and perspective leading to the formation of nuclear Cold War deterrence, which, in turn provided concepts early efforts to construct cyber deterrence theory. Cyber espionage, cyber attacks (below the threshold of cyber war), and cybercrime are grave problems and worthy of further study; however, they are beyond the scope of this research, which focuses on how a state may best deter other states or non-state actors that use cyber warfare to achieve vital or important

each of these activities through a networked system that connects computers and, as such, these attackers may be susceptible to deterrence.[4] Cyber war through a series of cyber attacks is possible because there are vulnerabilities in the system(s) that link individual computers or vulnerabilities in the hardware or software of individual computers.[5] This raises a significant concern because a precise set of factors that provide effective deterrence for vulnerabilities in one area may not work in another. For example, a state could successfully deter cyber war but not be able to deter cyber espionage or cybercrime with the same approach.

U.S. policies are based upon analogies to nuclear deterrence that do not respond well to either the technical or political realities of cyber attacks, cyber espionage, cybercrime or the potential for cyber warfare. Reliance upon dated deterrence theory is troublesome, because as Libicki has argued, the principal "system vulnerabilities do not result from immutable physical laws. They occur because of a gap between theory and practice."[6] The "gap" Libicki refers to may be better described as a divide or barrier. The effect of this divide is a mismatch

---

national security interests. The literature indicates that cyber attacks, cyber espionage, and cyber attacks are threats to states. There is growing debate regarding the threat from cyber war; however, recent history has provided two cyber wars (Estonia 2007 and Georgia 2008) with which to research this topic. Current and potential harm to states' security interests is present to bind this research by focusing exclusively on cyber war.

[4] As the use of computer networks is a uniting aspect of these focus areas, vulnerabilities inherent in the network may prove common in cyber attacks, cyber espionage, cybercrime and cyber war. To the extent that vulnerabilities are shared in each of these areas, similar applications of cyber deterrence by punishment and denial imply susceptibility to a common deterrence approach. However, differences remain that may challenge a common or "one size fits all" cyber deterrence approach.

[5] A human element may also serve as a factor. People with access to computers can inject viruses or steal data.

[6] Libicki and Project Air Force, *Cyberdeterrence and Cyberwar*, xiv. Libicki goes on to explain that in theory, "a system should do what its designers and operators want it to do"; however, in practice, "it does exactly what its code tells it to do." Complexity of systems and ever-changing technology make it difficult to contain vulnerabilities, and this makes cyber deterrence more challenging.

between the theories and strategies that are developed to address operational and technical cyber vulnerabilities. This divide magnifies vulnerabilities that invite malicious behavior, which complicates the deterrence equation.

U.S. cyber deterrence policy is at risk because of the disconnect between theory and practice. U.S. declaratory policy regarding cyber deterrence rests upon a strategy of punishment that imposes costs for malicious actions and reliance upon defenses to deny aggressors the capability to achieve their goals.[7] However, as the literature review revealed, some scholars question the value of basing a cyber deterrence strategy on the nuclear-era model as it may invite a conceptual failure.[8]

Defining Key Concepts

The first step in bridging the divide is coming to terms with the lack of definitional clarity in the literature.[9] The inability to agree on key concepts and terms complicates emerging cyber challenges. Without greater clarity and agreement among policy makers and scholars, it is difficult to isolate and examine cyber war, which this research seeks to deter. [10] Cyber attacks (below the

---

[7] U.S. Department of Defense, "Department of Defense Cyberspace Policy Report - A Report to Congress Pursuant to the National Defense Authorization Act for Fiscal Year 2011, Section 9*34*," last modified November 2011, 2, http://www.washingtonpost.com/wp-srv/world/documents/cyberspace-policy-report.html.

[8] Jeffrey R. Cooper, *New Approaches to Cyber-Deterrence: Initial Thoughts on a New Framework* (SAIC: December 29, 2009), 78–79. Cooper referenced Libicki as he noted, "It is also unfortunately common to view specific features of nuclear deterrence doctrine as defining deterrence in general and then attempting to apply these features to cyber-deterrence."

[9] Because the definitional boundaries are not firm regarding *cyber war* and *cyber attacks*, I have organized and presented alternative definitions, which contrast those used in this research. While definitional consistency remains unclear, what is clear is that cyber offers a new form of warfare that must be addressed.

[10] This research will focus on the challenge of cyber war as faced by states from peers and non-state actors. The literature demonstrated that cyber attacks, cyber espionage, and cybercrime are exceptionally challenging but, as of yet, do not rise to the potential of damage we may expect from future cyber wars. Cyber war, if undeterred, erodes a state's capacity to protect important national

threshold of cyber war), cyber espionage, and cybercrime although pressing challenges for states, exceed the scope of this project. However, the literature review will examine criminal justice deterrence theory as it informs the study.[11]

How can state actors, scholars, or this researcher design a framework to deter cyber war without definitional consistency? To deal with this challenge, this research relies upon time-tested Clausewitzian ideals to define cyber war as the continuation of state policy by cyber means.[12] Cyber war is distinguished from cyber attacks as it is a "form of comprehensive warfare, not merely a set of techniques."[13] There exists a willingness by scholars to create definitional consistency for this term (see Table 1.1 for an abbreviated offering of several of the many available definitions). However, there is no public attempt by the U.S. government or its agencies designated with cyber responsibilities to define cyber war. As evidence, consider that the U.S. Department of Defense's Joint Publication (JP) 1-02 defined a range of cyber activities but did not define cyber war.[14]

---

security interests. I recognize that in not concentrating on lesser forms of cyber attack that fall short of cyber war, I have limited myself to cyber attacks capable of bringing a state to its knees, which is in many ways the equivalent of a physical attack by traditional or nontraditional means.

[11] The deterrence of cybercrime exceeds the scope of this research. This challenge is more appropriate for research focusing on domestic and international law enforcement and is recommended as an area for further study. However, criminal justice deterrence theory is important in understanding how to evaluate the requirements helpful in constructing a cyber deterrence theory due to the impact the evolution of criminal deterrence theory has had on the capacity of states to use punishment and denial to obtain desired outcomes.

[12] Carl von Clausewitz in *On War* famously wrote that war "is nothing but the continuation of policy with other means." This research purposely structures the definition of cyber war from a state-centric perspective. This research will argue that non-state actors may conduct cyber attacks and engage in cyber espionage; however, they are, at this time and for the near future, incapable of waging cyber war.

[13] L. Scott Johnson, "Toward a Functional Model of Information Warfare," *Central Intelligence Agency*, June 27, 2008, https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/97unclass/warfare.html.

[14] U.S, Department of Defense, "Joint Publication 1-02, Department of Defense Dictionary of Military and Associated Terms" (September 8, 2010), 68, last modified November 2011,

Table 1.1: Alternative Definitions of Cyber War

Arquilla and Ronfeldt – conducting, and preparing to conduct, military operations according to information-related principles[15]
Billo and Chang – involves units organized along nation-state boundaries, in offensive and defensive operations, using computers to attack other computers or networks through electronic means[16]
Carr – the art and science of fighting without fighting; of defeating an opponent without spilling their blood[17]
Clarke – actions by a nation-state to penetrate another nation's computers or networks for the purposes of causing damage or disruption[18]
Lewis – use of force to cause damage, destruction, or casualties for political effect by states or political groups[19]
Rid – a potentially lethal, instrumental, and political act of force conducted through malicious code[20]

lhttp://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf. JP 1-02 articulated the concept of computer network operations (CNO) as being "comprised of computer network attack, computer network defense, and related computer network exploitation enabling operations."

[15] Timothy L. Thomas, "Nation-state Cyber Strategies: Examples from China and Russia," in *Cyberpower and National Security*, 1st ed. (Washington, DC: National Defense University Press, 2009), 440–441. Timothy L. Thomas is an analyst at the Foreign Military Studies Office at Fort Leavenworth, Kansas and a retired Lieutenant Colonel from the U.S. Army. John Arquilla is a professor at the U.S. Naval Postgraduate School, while David Ronfeldt serves with the Adjunct Research Staff at the RAND Corporation.

[16] Charlies G. Billo and Welton Chang, *Cyber Warfare: An Analysis of the Means and Motivations of Selected Nation States* (Institute for Security Technology Studies at Dartmouth College, December 2004), 3, http://www.ists.dartmouth.edu/docs/cyberwarfare.pdf. Charles Billo is a Senior Research Associate at the Institute for Security Technology Studies at Dartmouth College. Welton Chang is a Research Intern at the Institute for Security Technology Studies.

[17] Jeffrey Carr, *Inside Cyber Warfare*, 1st ed. (Sebastopol, Calif: O'Reilly Media, 2010), 2. Carr wrote that Sun Tzu inspired this definition. Jeffrey Carr is a cybersecurity expert and founder of Taia Global, Inc.

[18] Richard A. Clarke, *Cyber War: The Next Threat to National Security and What to Do About It*, 1st ed. (New York: Ecco, 2010), 8. Richard A. Clarke served in several presidential administrations, which culminated in his service as Special Advisor to the President on cybersecurity during the George W. Bush administration.

[19] J.A. Lewis, *Thresholds for Cyberwar* (Center for Strategic and International Studies, September 2010), 1, http://csis.org/files/publication/101001_ieee_insert.pdf. Lewis noted that force involves violence or intimidation. James A. Lewis is Director and Senior Fellow for the Technology and Public Policy Program at the Center for Strategic & International Studies (CSIS).

[20] Thomas Rid, "Cyber War Will Not Take Place," *Journal of Strategic Studies* (2011): 1. Rid questioned the existence of cyber war, as has Howard Schmidt, cyber security czar for the Obama administration. The presence or absence of cyber war in the current geopolitical environment is interesting, but definitional clarity remains a prerequisite for determining such presence and, more importantly, is central in examining cyber deterrence theory in the scope of this research. Dr. Thomas Rid is a Reader in War Studies at King's College London. He also is a non-resident fellow at the Center for Transatlantic Relations in the School for Advanced International Studies, Johns Hopkins University, in Washington, DC.

This research defines cyber attack as the use of cyber capabilities to cause harm.[21] One may distinguish cyber attacks from cyber war in three ways:

- They consist of techniques, or measures and countermeasures
- They have limited and local goals, and limited scope and orchestration (that is, being restricted to a specific [cyber] operation
- They perform a supporting role for political, economic, or military activities[22, 23]

This study will use this definition to help assess threat calculations and offensive capabilities, which are key factors in an effective punishment strategy to deter cyber war. The alternative definitions in Table 1.2 are largely narrow, which suggests that stepping back from specific definitions may serve two purposes beyond the clarity required to conduct this research. First, less specificity may foster greater consensus between policy makers and scholars. Second, a broader definition may help develop a more inclusive set of offensive cyber actions and thus produce a more precise body of knowledge that has greater relevance in advancing cyber deterrence theory.[24]

---

[21] This definition is adapted from the treatment of "attack" in *Webster's New World College Dictionary* (Foster City, Calif.: IDG Books Worldwide, 2001), 91. This alternative, yet more basic, definition of cyber attack permits a more straightforward attempt in channeling all efforts or attacks by malicious state or non-state group actors to conduct harm through cyber means. Harm is defined as that which "hurts, injures, or damages." See *Webster's New World College Dictionary*, 649.

[22] Johnson, "Toward a Functional Model of Information Warfare." The characteristics that distinguish cyber attacks from cyber war were adapted from Johnson's work, which focused on traditional forms of information attack.

[23] The distinction between concerted cyber attacks and cyber war is blurred. For example, one could argue that Olympic Games, the U.S. cyber action against Iran to derail its nuclear ambitions, might rise to the level of cyber war as the U.S. is continuing state policy by cyber means. I suggest that Olympic Games falls short of cyber war and is more properly referred to as a cyber attack because of the techniques employed, the limited scope of the operation, and the fact that the attacks are performing a supporting role for political and arguably military activities. For insight into Olympic Games, see David E. Sanger, *Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power* (Crown, 2012), 188–225.

[24] An enduring cyber deterrence theory should address the broad range of offensive actions malicious actors may currently undertake as well as those that may be envisioned for the future.

Table 1.2: Alternative Definitions of Cyber Attack

Billo and Chang – intrusions into unprotected networks for the purpose of compromising data tables, degrading communications, interrupting commerce, or impairing critical infrastructures[25]
JP 1-02 – computer network attack is action taken through the use of computer networks to disrupt, deny, degrade, or destroy information resident in computers and computer networks or the computers and networks themselves[26]
Lewis – an individual act intended to cause damage, destruction, or casualties[27]
Libicki – deliberate disruption or corruption by one state of a system of interest to another state[28]
National Research Council – the use of deliberate actions, perhaps over an extended period of time, to alter, disrupt, deceive, degrade, or destroy adversary computer systems or networks or the information and/or programs resident in or transiting these systems or networks[29]
Nye – a wide variety of actions ranging from simple probes to defacing websites, to denial of service, to espionage and destruction[30]
Waxman – efforts to alter, disrupt, or destroy computer systems or networks or the information or programs on them[31]

The Puzzle

Despite the differences between cyber war and nuclear conflict, it is perplexing that U.S. policy makers are recasting elements of deterrence theory from the Cold War and post-Cold War eras and applying it to cyber policy when its relevance is unclear.[32] This research seeks to determine the requirements for

[25] Billo and Chang, *Cyber Warfare: An Analysis of the Means and Motivations of Selected Nation States*, 7.
[26] U.S. Department of Defense, "Joint Publication 1-02, Department of Defense Dictionary of Military and Associated Terms," 67–68.
[27] Lewis, *Thresholds for Cyberwar*, 1.
[28] Libicki and Project Air Force, *Cyberdeterrence and Cyberwar*, 23. Martin Libicki is a senior management specialist at RAND Corporation.
[29] National Research Council (U.S.), *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities* (Washington, DC: National Academies Press, 2009), 10–11.
[30] Joseph S. Nye, Jr., "Nuclear Lessons for Cyber Security," *Strategic Studies Quarterly* 5, no. 4 (2011): 20.
[31] Matthew C. Waxman, "Cyber-Attacks and the Use of Force," *Yale Journal of International Law*, Vol. 36, #2 (summer 2011), http://www.lexisnexis.com.ezproxy.library.tufts.edu/hottopics/lnacademic/?verb=sr&csi=172860. Matthew C. Waxman is a Professor of Law, Columbia Law School.
[32] This researcher is puzzled by the actions of U.S. policy makers who appear to have recast elements of nuclear deterrence theory from the Cold War and post-Cold War eras to apply to cyber

the deterrence of cyber war based upon the vulnerabilities, which permit attacks, and to develop a theory to deal with this challenge. Strategy and policy to address these circumstances, without theoretical merit, will continue to prove woefully inadequate. As of this writing, there is no evidence that the U.S. is deterring state and non-state actors that perpetually assault U.S. security interests with cyber attacks or that it could deter a cyber war should the occasion arise.

In the case of the U.S., either cyber deterrence is not present or is failing repeatedly regarding cyber attacks. The U.S. has not overtly engaged in cyber war and therefore it may be possible that the U.S. has a cyber war deterrence strategy in place, which has been successful; or it may be that the U.S. has not faced a cyber war. As the literature review revealed the latter to be the more likely case, the theoretical requirements that the U.S. needs to execute a strategy of cyber deterrence against a state or non-state actor is undeniably important. The fact that existing vulnerabilities complicate effective cyber deterrence, and present challenges not associated with previous forms of deterrence, reinforce the need for this research.[33]

---

policy, which some (Cooper, Libicki) suggest may be of questionable relevance. The findings of this research may indicate that nuclear deterrence theory served as a foundation for U.S. declaratory policy for cyber deterrence. Alternatively, the facts may yield that only the major precepts, the overarching time-tested components of deterrence theory at large, upon which the nuclear variant relied, informed the cyber iteration. The literature review for this study yielded the perception that some cyber scholars question the efficacy of cyber deterrence based on the nuclear model due primarily to problems in attribution. Absent technological innovation, many deem cyber attribution impossible. Other scholar's suggest that attribution is not as difficult as imagined, while still others argue that attribution is not necessary for cyber deterrence.

[33] Committee on Deterring Cyberattacks: Informing Strategies and Developing Options; National Research Council, "Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy," *National Academies Press*, 2010, 364, http://www.nap.edu/catalog.php?record_id=12997#toc. The National Resource Council (NRC) further supports the need for this study at this time. NRC proceedings presented a broad cyber deterrence research agenda. Regarding their lead category, Theoretical Models for Cyber Deterrence, two of their posed questions – what are the strengths/limitations of applying

Research Questions and Hypotheses

Q_1 - What are the requirements for cyber deterrence theory to deter cyber war against states and non-state actors?[34]

Q_{1A} - What can be learned about the requirements for cyber deterrence theory from criminal justice deterrence, nuclear deterrence, and existing cyber deterrence theories?[35]

Q_2 - How do states and non-state actors in the cyber domain exploit vulnerabilities?[36]

The first question in this study, Q_1, investigates the requirements for cyber deterrence theory to deter cyber war against states and non-state actors. The researcher will answer this question in the analysis phase of the research, which will occur in Chapter 6. Answering this question requires a synthesis of the broader deterrence requirements (learned from addressing Q_1 and Q_{1A}) and a clear understanding of the case-specific vulnerabilities that align to the focus areas (made possible with the application of Q_2 to each case).

---

traditional deterrence theory to cyber conflict and what lessons and strategic concepts from nuclear deterrence are relevant to cyber deterrence – are similar to those posed by this researcher. In addition, the Council desires greater examination of operational considerations in cyber deterrence. Another two of their questions – what can be learned from case studies about the operational history of previous cyber intrusions and what would a technology infrastructure designed to support attribution contribute to deterrence of cyber attacks – are also related to the work undertaken in this study.

[34] Cyber war in its most august form clearly has the potential for greater harm as cyber attacks as well as cyber espionage or cybercrime may be seen as either components inclusive in cyber war or as stand-alone events. The intent is to coax out the requirements to deter malicious actors from engaging in cyber warfare and then construct a cyber deterrence theory from these requirements as informed by the cases studied.

[35] The major components of deterrence theory, punishment and denial are present in the criminal justice, nuclear, and cyber frameworks of deterrence theory. Yet, the requirements for each are different. Understanding these differences will better inform cyber deterrence theory. Further, understanding the evolution of deterrence within each may also prove useful.

[36] This research relies upon the definition of *vulnerability*, a noun, as representing conditions described as "exposed, defenseless, weak, sensitive, unprotected, unguarded, unshielded, helpless, powerless, and insecure." See the *Oxford American Dictionary and Thesaurus* (Oxford University Press, USA, 2003), 1726.

Sub-question Q_{1A}, permits us to learn whether existing deterrence theories and frameworks help provide the basic requirements for cyber deterrence theory. The central components of deterrence have historically been punishment and denial, however, cooperation features prominently in the literature on the cyber domain. Therefore, this study approaches cyber deterrence theory through the lens of a triadic framework that uses each of these concepts. Punishment is examined through two core categories, attribution and offensive capability or retaliatory means. The study examines denial from a defensive perspective with a keen focus on exploited and unexploited vulnerabilities. The answer to Q_{1A} forms a major part of the literature review in Chapters 2 and 3.

The ability to answer the second question, Q_2, relies upon using an historical perspective to examine vulnerabilities across various cases. This process permits an evaluation of the attacks used by malicious actors, which in turn helps develop the requirements for cyber deterrence theory. In sum, it is the combination of findings gleaned about broader deterrence requirements learned from examining Q_{1A} and findings from the case studies regarding vulnerabilities, Q_2, that help foster the design of a cyber deterrence theory.[37]

This research offers four hypotheses, structured as follows. Informed by basic deterrence theory, a critical question in the cyber realm is how deterrence is

[37] The researcher purposely uses the phrase "design of a cyber deterrence theory" in describing the desired goal of this study. The researcher believes that there is no widely accepted theory of cyber deterrence; there are only numerous ideas and frameworks for what may or may not constitute such a theory. The scholarly work on cyber deterrence that precedes this study has given us robust frameworks and various policy options, yet no theory. For example, Jeffrey Cooper offers a framework for cyber deterrence that serves as a foundation for this research; however, frameworks of this nature are theories in the making, not theory. Theory in this sense is the uniting of ideas into a system that seeks to explain phenomena.

possible if attribution, offensive capabilities, defensive capabilities, or cooperative relationships are either missing from or inadequate to deter a malicious actor.[38]

> H_1 - If attribution is present in cyber deterrence strategy, then credible deterrence of states and/or non-state actors through a punishment strategy is possible. (IV - attribution; DV - credible cyber deterrence by punishment)[39]
>
> H_2 - If the offensive capability to hold at risk what an actor values is present in cyber deterrence strategy, then credible deterrence of states and/or non-state actors through a punishment regime is possible. (IV – offensive capability; DV - credible cyber deterrence by punishment)[40]
>
> H_3 - If a state's cyber vulnerabilities are protected by defensive capabilities from cyber aggression by states and/or non-state actors, then credible cyber deterrence by denial is possible. (IV – cyber defensive capability; DV – credible cyber deterrence by denial)[41]
>
> H_4 - If a state's cyber infrastructure is protected by cooperative relationships between non-adversaries and adversaries, then credible cyber

---

[38] It is conceivable that the analysis, evaluation, and synthesis undertaken in this research may not indicate the extremes of what is possible or not possible; rather, they may indicate a middle ground where deterrence becomes conditional and/or variable in its effectiveness. It would be highly valuable to understand some of these nuances as well when developing policy options for decision makers.

[39] See Richard L. Kugler, "Deterrence of Cyber Attacks," in *Cyberpower and National Security*, 1st ed. (Washington, DC: National Defense University Press, 2009), 309–310. Kugler rejected the view that the attribution problem "paralyzes" thinking about cyber deterrence. He offered a core argument with three components: "cyber attacks should not be seen in isolation"; offensive and defensive capabilities are required to deter cyber attacks; and deterrence contains psychological and cognitive aspects, as it is necessary to understand an attackers motives.

[40] See Kenneth Geers, *Strategic Cyber Security* (CCD COE Publication: NATO Cooperative Cyber Defence Centre of Excellence, 2011), 111, http://www.ccdcoe.org/publications/books/Strategic_Cyber_Security_K_Geers.PDF. Geers conducted a thorough examination of denial and punishment. He closely looked at the three requirements to execute deterrence by these means: capability, communication, and credibility. He noted that both denial and punishment lack credibility. Geers suggested that finding success in a denial approach is unlikely as actors obtain cyber attack technology easily, international legal frameworks are insufficiently developed, there is no cyber inspection regime, and a prevailing perception exists that cyber attacks do not warrant a deterrence response because they do not constitute a substantive threat. He concluded that punishment offers the only "real" option, but this deterrence strategy also lacks credibility due to concerns associate with attribution and asymmetry.

[41] See Ryan J. Moore, "Prospects for Cyber Deterrence" (2008). Moore captured the elements needed to deter state and non-state actors in cyberspace. These are denial, punishment, thresholds, and articulated national policy. He admitted there are challenges such as "technological limitations, policy and regulation issues, and the ripple effect of poorly understood changes" that make cyber deterrence a "wicked problem." Moore concluded that until these and other challenges are resolved, the U.S. will "likely have to emphasize denial deterrence, because the veil of anonymity makes punitive deterrence extremely difficult to accomplish."

deterrence by cooperation is possible. (IV – cooperative relationships; DV – credible cyber deterrence by cooperation)[42]

Methodology

Theory is the "systematic reflection on phenomena," which explains and demonstrates how phenomena are linked in a coherent relationship.[43] To examine what is taking place within deterrence theory and construct an approach to cyber deterrence, this study will employ deductive and inductive reasoning. The inductive method permits the researcher to "investigate physical and social phenomena by observing a number of instances in the same class and by describing in detail both the research procedures followed and the substantive results."[44] Subsequently, the study relies upon the deductive approach to begin with a concept and from applicable definitions and assumptions proceed by "plausible, logical steps to deduce (draw out) subordinate propositions and necessary conclusions."[45]

The first step in this study is to conduct a literature review of criminal justice, nuclear, and existing material related to cyber deterrence theory and policy.[46] This examination yielded a comprehensive understanding of the

---

[42] Cooper, *New Approaches to Cyber-Deterrence: Initial Thoughts On A New Framework*, 4. Cooper argued that the international system has evolved to include a wider range of actors. Because of this evolution, he recommended adoption of a concept he called the "three Cs – cooperation, competition, and conflict." He defined cooperation as the "relationship in which the objective is a positive-sum outcome for participants as a whole"; competition occurs when the "objective is an improved relative position, but one that can often produce an increase in overall welfare"; and conflict occurs when the "objective is an improved relative position, not an overall improvement in welfare." See page 123.

[43] James E. Dougherty and Robert L. Pfaltzgraff, *Contending Theories of International Relations: A Comprehensive Survey* (New York: Longman, 2001), 17.

[44] Ibid., 27. Dougherty and Pfaltzgraff observed that a "fruitful combination" of deductive and inductive reasoning is required in theory building.

[45] Ibid., 26.

[46] Criminal justice deterrence theory will be reviewed. The principle features, which include those that may have helped shape the early theoretical underpinnings of nuclear deterrence theory, will

theoretical foundation that is required for effective deterrence and the researcher learned that there are fundamental principles that characterize each of these three areas. The literature demonstrated that aspects of punishment and denial are at the core of criminal justice deterrence, nuclear deterrence, and discussions on approaches to cyber deterrence theories. However, cooperation featured prominently in the literature, particularly in the cyber literature. Yet, differences remain that have resulted in debates among scholars and practitioners in each theory. As such, it is critical for this exercise in theory building to understand those aspects of deterrence theory that have worked and those that have not. Further, the literature review considered the evolution of governmental policies in these differing areas, which added context to variations in the theories under study.[47]

From the core components of deterrence theory, punishment and denial, this research will use a typology for examining the case studies. In addition, each case will consider the utility of cooperation as it may profoundly inform cyber deterrence theory. This study, rather than using a threat-based analysis common in the literature, will conduct a vulnerability-based examination of the proposed two cases. This approach will allow the gathering of the requirements with which to form a cyber deterrence theory based upon the inherent vulnerabilities that exist in the cyber domain.

---

be presented. The focus of the study is state-centric, and the individual nature of the majority of criminal justice deterrence literature places this area beyond the study's bounds.

[47] This researcher is puzzled by the actions of U.S. policy makers who appear to have recast elements of nuclear deterrence theory from the Cold War and post-Cold War eras to apply to cyber policy, which some (Cooper, Libicki) suggest may be of questionable relevance. The findings of this research may indicate that nuclear deterrence theory served as a basis for U.S. declaratory policy for cyber deterrence. Alternatively, the facts may yield that time-tested components of deterrence theory at large, upon which the nuclear variant relied, informed the cyber iteration.

Dependent/Independent Variable (DV/IV) Framework

This research relies upon several independent variables: attribution, offensive capabilities, defensive capabilities, and cooperative relationships for which the dependent variable is credible cyber deterrence.[48] The literature review, which examined basic deterrence theory, criminal justice deterrence theory, nuclear deterrence theory, and cyber deterrence theory, indicated that deterrence by punishment, denial, and/or cooperation form the main requirements for a theory of cyber deterrence theory.

A fundamental problem is that the capacity to punish cannot be present in deterrence theory if attribution is absent. During the Cold War, there was an "expectation that the United States would recognize if an attack had occurred, by whom, and with what."[49] However, in the cyber domain, this is not the case. Further, if attribution is uncertain, states cannot rely upon offensive capabilities, which are also required for punishment. If a state is unable to determine who committed a cyber act or determines the actor but cannot punish the attacker because it lacks offensive capabilities, then the greater the need becomes for denial capabilities.

This study uses portions of an established taxonomy, Fleury et al's attack-vulnerability-damage (AVD) model (see Annex A), to help assess the independent variables – attribution, offensive capabilities, and defensive

[48] Transparency, will, uncertainty, barriers to entry, discrimination of cost, and other factors do not rise to the threshold that equates to the role that punishment, denial, and cooperation serve in deterrence theory. Cooperative relationships rise to the level of an independent variable worthy of study as the literature revealed that it may provide greater utility in cyber deterrence theory than in prior theories.

[49] Keith B. Payne, *The Great American Gamble: Deterrence Theory and Practice from the Cold War to the Twenty-first Century* (Fairfax, Va.: National Institute Press, 2008), 361.

capabilities and their top-level analytical components across the cases (see Table 1.3). The research will use the attack and vulnerability aspects of the model, as damage considerations are beyond the scope of the study.

Table 1.3: Comparison of Independent Variables Across Cases

Triadic Components	Independent Variables	Elements	Estonia	Georgia
Denial	Defensive Capabilities	*Exploited Vulnerabilities*		
		Targets		
		Defensive Actions		
		Unexploited Vulnerabilities		
Punishment	Attribution	*Origin*		
	Offensive Capabilities	*Retaliatory Means*		
Cooperation	Cooperative Relationships	*Non-adversaries*		
		Adversaries		

The Fleury model's attack component is helpful because it includes three categories supportive of our analysis: origin, action (defensive and offensive/retaliatory), and target. The capacity to determine the origin or source of the attack is the essence of attribution. The action undertaken and the target categories of the attack component combine with the model's vulnerability component to permit examination of offensive and defensive independent variables.[50] The nature of offensive and defensive actions in the cyber domain is such that they are often indistinguishable. When distinguishable, an action-reaction interplay exists; therefore, it is best to examine these IVs in tandem.

[50] Terry Fleury, Himanshu Khurana, and Von Welch, "Towards A Taxonomy of Attacks Against Energy Control Systems," in *Proceedings of the IFIP International Congerence on Critical Infrastructure Protection*, 2003, 7–13, http://www.ncsa.illinois.edu/People/hkhurana/IFIP_CIP_08.pdf. Fleury et al's AVD model has been adopted as the taxonomy through which the IV's will be assessed across the cases. The terms and definitions used in this model are presented in Annex A.

Using this methodology will yield insight into vulnerabilities present in each case.[51] Collectively, these vulnerabilities will be merged and analyzed in conjunction with what we learn from examining cooperative relationships in the cases to influence the requirements for cyber deterrence theory.[52]

Case Study Framework[53]

This research uses John Stuart Mill's method of difference to guide the case selection process.[54] Since the differences across these cases should lead to consideration of alternative effects, it becomes even more obvious that "the more similar the cases, the fewer the candidate causes."[55] This makes it easier to determine the real cause(s) of the activity under examination. Additionally, this study will use process tracing to explore "the chain of events" through which "case conditions" are translated into "case outcomes."[56] This offers the potential for revealing alternative causes that in their own right contribute to theory development and modification.

---

[51] Some categories in this model may not on the surface represent a direct vulnerability; however, they may lead to the discovery of underlying conditions that indirectly contributed to vulnerabilities.

[52] The researcher is aware that this taxonomy will only yield technological vulnerabilities. It is possible that there are vulnerabilities in non-technical areas, which may be revealed in the case studies. This potential drove an examination of criminal justice, nuclear, and cyber deterrence theory beyond understanding the requirements of each to learn how these theories evolved to close technical and non-technical vulnerabilities as they emerged.

[53] Case selection bias is not an issue as there are only two known cases of cyber war to choose from in the public domain and both of these, Estonia in 2007 and Georgia in 2008 are included in this research.

[54] See Stephen Van Evera, *Guide to Methods for Students of Political Science* (Ithaca: Cornell University Press, 1997), 57. When employing the method of difference, an "investigator chooses cases with similar general characteristics and different values on the study variable (the variable whose causes or effects we seek to establish)."

[55] Ibid., 69. This further reinforces the decision to adopt the method of difference as it is "preferred when the characteristics of available cases are homogenous (most things about most cases are quite similar)."

[56] Ibid., 64.

This researcher must acknowledge a significant research challenge, which is the difficulty of locating any cases that demonstrated the success or failure of cyber deterrence. The question is how would one know whether a case represented an absence or failure of deterrence or the success of deterrence?[57] As the researcher stays mindful of various methodological pitfalls, this research pursues a different path by determining the vulnerabilities exploited by actors in the case studies. Based upon these vulnerabilities, this study compares how and, ideally, why attacks occurred. This approach will permit a determination of what the requirement for deterrence might have been in each case. The researcher will use these requirements to build a theory to deter cyber war.[58]

The selected cases highlight the vulnerabilities faced by a diverse range of actors and their organizational capacity, size, and capabilities, which combine with other relevant factors to indicate that a hybrid deterrence construct may satisfy the purpose of deterring cyber war. This research will yield a theory from the requirements that are determined to be necessary to counter vulnerabilities in each case.

Assumptions and Limitations

This research includes several assumptions. First, when a cyber operator believes that he is employing cyber deterrence, the use of defensive or offensive capabilities to exploit or punish cyber offenders indicates that these actors sought

[57] See Paul Huth and Bruce Russett, "Testing Deterrence Theory: Rigor Makes a Difference," *World Politics* 42, no. 4 (July 1, 1990): 466-501. Lebow and Stein's critique of Huth and Russett's study on extended deterrence serves as a caution for any researcher embarking upon a study of deterrence.

[58] The idea to use a vulnerabilities-based study to determine the requirements for cyber deterrence emerged in several conversations between the researcher and Professor Robert L. Pfaltzgraff, Jr. in September and October 2011. Professor Pfaltzgraff was the originator for this novel approach to avoid the classic pitfall of trying to "prove a negative" common in deterrence case study research.

at some measure a deterrent effect with their actions. Second, deterrence theory pertaining to cyber war should prove consistent; however, policy prescriptions may be significantly different.[59] Third, the use of non-state actors in this research refers to non-state actor groups that have posed or may pose a threat to states through cyber attacks.

There is sufficient literature to study the deterrence theories and frameworks under review, and U.S. policies relevant to cyber deterrence are readily obtainable. The most critical and perhaps difficult source of information pertains to gathering a precise understanding of the technical and other vulnerabilities exploited in each case due to the security classification of these events by various governments. This difficulty presents a limitation, although one that should not undermine the quest for a theoretical breakthrough. While respective countries generally do not reveal such vulnerabilities, there are open-source ways to evaluate who did what, to whom, and how.

Contribution and Significance

The main contribution of this research is the development of a theory of cyber deterrence. Additional contributions to scholarly and policy making debate will occur on several levels. First, through examining vulnerabilities, particularly those of a technical nature, it will be possible to define the requirements for a cyber deterrence theory. This alone contributes to scholarship and existing U.S. cyber deterrence declaratory policy. Second, there is a divide between the cyber

[59] The primary theoretical components of deterrence, punishment and denial have consistent utility in cyber deterrence theory just as in criminal justice and nuclear deterrence theory. However, analysis revealed there are additional components, such as cooperation, which features prominently in some cyber deterrence frameworks that may be merged with punishment and denial to form a theory.

technical and policy communities that this research may help to bridge. While the complex nature of the technical aspects of cyber is partly to blame, this study embraces these complexities as it seeks to use technical vulnerabilities to help establish requirements for a breakthrough theory.

Last, this approach may help to develop a different mindset across the cyber community. A cyber security dilemma appears to be growing. Perhaps cyber is the popular concept of this decade, as was terrorism in the last and peacekeeping in the one before. That an "industrial complex" is forming around cyber suggests that analysis based on careful research is essential for guiding policy.

This research seeks to make an original contribution to the literature on cyber deterrence. First, this study offers a theory of cyber deterrence whereas previously others have proposed frameworks or done little more than critique cyber deterrence through the lens of nuclear deterrence concepts. Second, this research offers a vulnerability-based approach to study deterrence in contrast to other approaches in the literature. Third, this study redefines cyber war, which may help foster more agreement on the subject. Fourth, for a policy-centric study, this research helps to close the divide between cyber technicians, scholars, and policy makers.

Dissertation Overview

Chapters 2-3 contain the literature review for this dissertation, which includes an examination of four theories. Basic deterrence theory, criminal justice deterrence theory, and nuclear deterrence theory, reviewed in Chapter 2,

provide the historical context with which to frame a theory of cyber deterrence. Chapter 3 examines the literature to understand existing scholarship and policy movement toward a theory of cyber deterrence. The historical evolution of the latter three theories offers insight into the core requirements of deterrence in each theory. These requirements when analyzed with findings from the vulnerability assessments undertaken in the case studies will help inform a cyber deterrence theory.

Chapters 4-5 present two case studies. The purpose of these case studies is to help understand the requirements for deterring cyber war. To accomplish this goal, each case begins a brief overview, which precedes an assessment of the targets attacked and the vulnerabilities exploited. Then the study explores the basis for deterring cyber war in each case by considering what a deterrence relationship would look like driven by the key concepts gleaned from the literature review: punishment, denial, and cooperation.

Chapter 4 is the Russia-Estonia case, which features state and private sector actors from both parties. In 2007, Estonia experienced crippling cyber attacks against its government and several corporations in the world's first cyber war. There is plausible evidence that the Russian government in concert with other actors committed the attacks. The Estonian cyber attack was a large distributed denial of service attack (DDoS) as attackers used more than 1 million computers from around the world to attack the Estonian cyber system.

Chapter 5 is the Russia-Georgia case. This case features Georgia and internal private sector actors opposed to Russia and that country's internal private

sector actors. Cyber attackers conducted this second state-level cyber war in 2008. As in the Estonia case, the major type of attack against Georgia was also a DDoS.[60] Western experts were able to determine that websites used to launch the attacks had links to the Russian intelligence system. The Russian government denied this and placed blame on citizen "populists" outside of the government's sphere of influence. What is different in this case is that an attack on Georgian cyber capabilities preceded a physical attack.

Chapter 6 includes analysis of the requirements for a theory of cyber deterrence and provides the study's conclusions. This chapter begins with sections that review the research problem, questions, and hypotheses. Next key definitions and theoretical concepts are reviews prior to an analysis of the Estonia and Georgia cyber war case studies. Next, these findings were compared and contrasted with what we have learned from the historical requirements of deterrence theories from the literature review. This helped form the genesis for a new set of cyber deterrence requirements – requirements that shaped a theory of cyber deterrence. The chapter closes with implications for the future, recommendations for future research, and research conclusions.

[60] TechTerms.com, "The Tech Terms Computer Dictionary," n.d., http://www.techterms.com/. A DDoS is an attack to overwhelm a computer system(s) to make it unavailable for use. A DDoS "attack tells all coordinated systems to send a stream of requests to a specific server at the same time." This results in a backlog of requests, which may lead to limited or no response.

Chapter 2: Exploring Deterrence Theory

As long as the problem of preventing the use of force by aggressors remains central to international relations, the need for theories upon which effective policies can be based will be apparent.

— James E. Dougherty and Robert L. Pfaltzgraff, Jr.[1]

Introduction

This chapter introduces the deterrence literature that establishes a foundation for cyber deterrence theory. Basic deterrence theory, criminal justice deterrence theory, and nuclear deterrence theory offer explanatory value, which helps establish the bases for cyber deterrence. Basic deterrence theory provides an overview of many of the concepts that will appear in the latter three theories. The sections on criminal justice deterrence theory and nuclear deterrence theory provide the intellectual foundation for this research. The examination of these theories incorporates an historical analysis for two reasons.[2] First, this approach permits an in-depth study, which assists in mining each theory for its core requirements. Second, the perspective gained by analyzing key aspects of each theory's evolution adds perspective that will be invaluable in Chapter 6, the analysis chapter of this research.

---

[1] James E. Dougherty and Robert L. Pfaltzgraff, *Contending Theories of International Relations: A Comprehensive Survey* (New York: Longman, 2001), 397.

[2] The researcher believes that an in-depth analysis of the historical evolution of criminal justice deterrence and nuclear deterrence theories will prove invaluable in the analysis chapter. Developing a theory of cyber deterrence requires more than mining existing theories for requirements and then using these requirements, in conjunction with existing cyber vulnerabilities to inform that alternative. The history, the experiences, the debates among the scholars and policy makers of the great theories, must factor into the undertaking at hand. Therefore, care and deliberation has preceded the inclusion of each scholar as well as the exclusion of the many that were studied but not included for the practical reason of keeping the length of this chapter to a manageable size.

This approach, while complex, permits the researcher and reader to face the immense challenge of cyber deterrence armed with the knowledge gained from an analysis of the works of deterrence scholars representing diverse fields across great spans of time. Additionally, the realization one takes away from analyzing the historical evolutions of criminal justice and nuclear deterrence theories is that they each took time to mature – and so, too, it is reasonable to expect that cyber deterrence theory should be no different in that it took time for a theory to coalesce.

Basic Deterrence Theory

Central to this dissertation is deterrence theory. In its simplest expression, actors achieve effective deterrence when they credibly communicate a threat that deters the targeted actor against whom the threat is directed in the form intended by the communicator. A credible threat is a product of capability and will that proscribes an action. A targeted actor must clearly receive the communicated threat. The targeted actor, in response, decides to acquiesce and refrain from taking action in the prohibited venue, i.e., maintains the status quo. Therein, traditional deterrence theory works as follows: Actor A proscribes a potential action by Actor B for which Actor A is willing to threaten Actor B with consequences that prevent, or deter, Actor B from taking the proscribed action. Actors can be nation-states, groups other than states, or single individuals.

Credible deterrence requires Actor A's threat to Actor B to be both credible and overtly communicated. This is problematic as overt communication is not always perfect or present. Actor A must exhibit both capability and will for

the threat to be considered credible. Additionally, Actor A's capability must be transparent as Actor B must know the capability exists in order to believe the threat is credible in the language of deterrence. However, this is not necessarily the case in the real world. The capabilities of Actor A may be offensive in that they inflict cost and/or defensive in that benefits are denied to Actor B. Further, attribution is a constant value. This entails conditions where a credible threat is attributable to a known Actor A and the "targeted action" is attributable to a known Actor B.[3]

Requirements of Basic Deterrence Theory

The core components of basic deterrence theory are punishment and denial. The causal mechanisms of punishment are offensive in nature, and those of denial are defensive. See Table 2.1 for a summary of the requirements for basic deterrence to occur in theory.

There are seven requirements to deter by punishment in basic deterrence theory. These requirements are attribution, threat, communication, credibility, capability, will, and transparency. First, an actor must have a known adversary to punish or threaten to punish. Without attribution, an actor does not have the capacity to identify whom it will punish or threaten. Only if an actor knows the identity of the adversary it wishes to deter can it issue a threat to deter the adversary from engaging in unwanted activity.

For a threat to have merit, an adversary must receive and understand the threat. Therefore, communication of the threat must be clear and credible. A

[3] This description of basic deterrence emerged from multiple conversations between the researcher and Dr. Stephen Wright in April–May 2010 and was further shaped by numerous conversations with Professor Robert L. Pfaltzgraff, Jr., in May and October 2011.

credible threat requires that the adversary understand that the deterring actor has the offensive capability to fulfill the promise of a threat or to retaliate if deterrence fails. It is insufficient that the actor possesses the capability to punish offensively but lacks the will to act. An adversary must realize that the deterring actor will act in retaliation or on the promise of a threat.[4] However, one additional requirement is necessary. Transparency of capabilities must exist for an adversary to know that the deterring actor possesses the capacity to act as promised.

Table 2.1: Requirements of Basic Deterrence Theory

Core Components	**Causal Mechanisms**	**Purpose**	**Requirements**	**Rationale**
Punishment	Offensive	Inflict cost/threaten to inflict cost	Attribution	Must know who to threaten or hold accountable
			Threat	Must be issued and received
			Communication (of threat)	Must be clear and understood by receiving party
			Credibility (of threat)	Must be believable, which requires capability and will
			Capability (offensive)	Adversary must know the capacity exists to make good on a threat or promise of retribution
			Will	Adversary must know that the promise of a threat or retaliation will be acted upon
			Transparency	Adversary must know that the capability exists to fulfill the promise of a threat or retaliation

[4] It may be equally argued that uncertainty surrounding a deterrer's intentions coupled with capacity is enough to deter; however, absent uncertainty the lack of will is a death nail to credible deterrence.

Denial	Defensive	Deny benefits	Capability (Defensive)	Must have capacity to defend or deny access to protected entity

Basic deterrence theory instructs that an actor may deter by denial for which the causal mechanisms are defensive. The capacity to deny benefits to an adversary requires that the deterring actor use defensive capabilities to defend or deny access to protected entities. Such capabilities generally represent barriers to entry and are typically passive in nature. A defense is passive in that once in place, it remains static. However, active defenses may be employed that exhibit characteristics of offensive capabilities in the form of an automatic response in reply to an adversary's action.[5]

Criminal Justice Deterrence Theory

Introduction

This section reviews criminal justice deterrence theory because it represents the intellectual foundation for nuclear and cyber deterrence theory.[6] Criminal justice deterrence theory differs from basic, nuclear, and cyber deterrence theory in one major aspect. Criminal deterrence considers punishment the principal means to accomplish deterrence, while denial through defensive means is a branch of crime prevention.[7] This section presents an overview of the evolution of criminal deterrence and a description of situational crime prevention

[5] Transparency is as important for active defenses as it is for offensive capabilities under the punishment rubric.
[6] Professor Antonia Chayes noted in an office conversation with the researcher on April 27, 2012 that criminal justice deterrence theory has "probably shaped these other deterrence theories without contextual differentiation," which further increases the importance of this effort.
[7] Professor Antonia Chayes noted in correspondence with the researcher on June 29, 2012 that "increasingly, through analysis of crime-prone areas prevention is theorized." She observed that the "thinking is there but not the corresponding action."

and concludes with a presentation of the requirements of criminal deterrence and situational crime prevention theory.

The historical evolution of criminal deterrence will take the reader through four historical periods: the classical enlightenment scholars, the rise of criminology and the Italian School, the re-emergence of criminal deterrence theory, and the revival of criminal deterrence theory. Next follows a section that explains the relationship between deterrence and crime prevention. Lastly, a section on situational crime prevention investigates the usefulness of this concept as a component of criminal justice deterrence.

Criminal deterrence is "the omission of a criminal act because of the fear of sanctions or punishment."[8] This approach relies upon the threat or fear of sanctions to induce in a potential offender the inclination to refrain from committing a criminal act.[9] Situational crime prevention is "doing things in a particular place that make it impossible or inconvenient to offend."[10] This concept relies upon a defensive posture to prevent or deny opportunities to a potential offender by locking one's doors or storing valuables in a safe.

The use of punishment has received far greater attention as a means to control the criminal urges of man than has forms of denial in the literature. This

---

[8] Raymond Paternoster, "How Much Do We Really Know About Criminal Deterrence?" *Journal of Criminal Law and Criminology* 100, no. 3 (2010): 1.

[9] See Jeremy Bentham, *An Introduction to the Principles of Morals and Legislation* (Oxford: Clarendon Press, 1996), 34, http://www.questia.com/CitationHandler.qst;jsessionid=F765A4A3B2E1F32F022F1A9A2B1A70C6.inst3_2a&WebLogicSession=F765A4A3B2E1F32F022F1A9A2B1A70C6.inst3_2a. Bentham defined a sanction as "a source of obligatory powers or motives: that is, of pains."

[10] Daniel Nagin, "Deterrence: Scaring Offenders Straight," in *Correctional Theory: Context and Consequences* (SAGE, 2011), 77, http://books.google.com/books?id=_dkMQVFmOFgC&pg=PA67&lpg=PA67&dq=nagin+deterrence%22scaring+offenders+straight%22&source=bl&ots=63AZMq2uhe&sig=lLh587P49j2hGFvGWiW0N35Snec&hl=en&sa=X&ei=BC8IT6XpDMHY0QHVm6XHAg&ved=0CDwQ6AEwBA#v=onepage&q=nagin%20deterrence%22scaring%20offenders%20straight%22&f=false.

is the case because in large measure, the possibilities for denial were limited, making vulnerabilities unavoidable and leaving society with deterrence through the threat of punishment as the best recourse.[11] When the threat of deterrence failed, society needed the capacity to follow through with the threat of sanctions, which required arrest and then trial, followed by a fine or imprisonment. The effects of these actions, in theory, then deterred other potential offenders. Historically, along with deterrence (by punishment), there have been four other purposes for punishment: retribution (eye for an eye), expiation (atoning for one's actions), reformation (reforming an individual so he or she will no longer commit crimes), and social defense (protecting society by jailing or incapacitating offenders).[12]

This research traces the evolution of criminal deterrence theory because it adds context to the study and helps develop an understanding of the enduring requirements to execute this theory. Further, in studying the evolution of the criminal deterrence, the enduring theoretical nature of punishment, which has changed little over several hundred years, becomes more apparent. The foundation of criminal deterrence theory begins with Cesare Beccaria in the classical enlightenment period.[13]

---

[11] Lawrence Freedman, *Deterrence* (Malden, MA: Polity Press, 2004), 60.
[12] Marvin E. Wolfgang, "The Just Deserts vs. the Medical Model," in *Contemporary Masters in Criminology*, edited by Joan McCord and John H. Laub, Plenum Series in Crime and Justice (New York: Plenum Press, 1995), 279–280. The reader may note that some purposes for punishment, such as reformation or rehabilitation sharply distinguish criminal justice from cyber deterrence theory.
[13] John Lewis Gillin, *Criminology and Penology* (New York London: The Century Co,, 1926), 323. The classical enlightenment period occurred in the eighteenth century and represented an "outgrowth of general intellectual development" in a variety of fields.

Historical Evolution of Criminal Deterrence

Classical Enlightenment Scholars

By the middle of the eighteenth century, punishment for criminal offenders was brutal. Forms of torture were commonplace, yet as horrendous as sanctions were, the risk of punishment deterred some but not all criminal activity. In that era and to the present, the threat of punishment required the capacity to attribute criminal acts, in which the targeted actor must believe that his or her transgressions can be determined. Uncertainty surrounding the belief that authorities would not detect one's criminal behavior and emotions that cloud one's judgment are some reasons why criminal justice deterrence fails. Because this lack of realism is characteristic of some criminals, the impact of deterrence is weakened.[14]

In this early period, one finds that deterrence theory did not "seek to explain criminal behavior, (but) merely to prevent it from occurring through law and punishment."[15] Enlightenment scholars, beginning with Italian Cesare Beccaria (1738–1794) and continuing with Englishman Jeremy Bentham (1748–1832), sought to move society from the senseless use of brutality to instill fear to a more reasoned use of punishment tailored to the nature and severity of the crime.

---

[14] The utility of the role of uncertainty as a causal factor in the failure of criminal deterrence theory emerged in a conversation between the researcher and Professor Antonia Chayes on April 27, 2012 and in correspondence from June 29, 2012.

[15] Morgan Summerfield, "Evolution of Deterrence Crime Theory," *Associated Content*, May 18, 2006, 4, http://www.associatedcontent.com/article/32600/evolution_of_deterrence_crime_theory.html?cat=37.

Beccaria was one of the first to write extensively about the use of criminal deterrence to reduce crime. His book, *On Crimes and Punishments,* published in 1764, is a "protest against the abuses which had risen in a despotic and autocratic society, callous to the sufferings brought about by its laws."[16] He argued for the necessity to punish criminals because of the fear it instilled in others, which deterred the commission of similar acts.[17] However, he observed that "abuses" masquerading as punishments undermined authorities. He advocated for a more rational approach to punishment, seeing this as a means to increase effectiveness. Beccaria was also an ardent believer in crime prevention. He realized that the keys to prevention were simple and clear laws, societal reward for virtuous behavior, and education.[18]

Beccaria introduced certainty and celerity as key deterrence requirements, because it was important to link the crime with the corresponding punishment. Certainty is the "probability that a criminal act will be followed by punishment,"[19] while celerity is "how quickly a punishment follows a criminal act."[20] He reasoned that "the more promptly and more closely punishment follows upon the commission of a crime, the more just and useful it will be."[21]

In conjunction with certainty and celerity, Beccaria suggested that the duration and nature of the punishment must be appropriate to the offense. He noted, "It is not the intensity of punishment that has the greatest effect on the

---

[16] Gillin, *Criminology and Penology*, 324.
[17] Cesare Beccaria, *On Crimes and Punishments*, trans. Henry Paolucci (The Bobbs-Merrill Company, Inc., 1963), 35, http://www.questia.com/PM.qst?a=o&d=9061406#. Beccaria wrote that punishment must be prompt, public, and proportional to the act, 99.
[18] Ibid., 93–98.
[19] Nagin, "Deterrence: Scaring Offenders Straight," 71.
[20] Ibid.
[21] Beccaria, *On Crimes and Punishments*, 55.

human spirit, but its duration."[22] He suggested that in linking the punishment with the crime, it was crucial that the punishment conform to the nature of the crime.[23] Therefore, the goal should be to locate the "proper proportion between crimes and punishments."[24]

Beccaria's contribution humanized the penal system. Instead of barbarity, he suggested moderation in which "the pain threatened by the punishment just exceeded the anticipated pleasure from the commission of the act."[25] Thus, Beccaria's introduction of proportionality fundamentally reshaped the use of punishment to deter crimes. However, he was clear that in the grand scheme of confronting offenders and potential offenders, "it is better to prevent crimes than to punish them."[26]

Beccaria redefined how society used punishment to address crime; however, he did not provide a theory of criminal deterrence or prevention.[27] Beccaria's classical approach relied upon the threat of punishment, not its actual use, and was therefore largely symbolic. This was not the case for Jeremy Bentham, an Englishman, whom Beccaria heavily influenced even though they differed on penal policy.[28]

Jeremy Bentham (1748–1832) provided a theory of criminal deterrence using human conduct as a model. He developed a "notion of utility," which he

---

[22] Ibid., 46–47.
[23] Ibid., 57.
[24] Ibid., 62.
[25] Daniel Gilling, *Crime Prevention: Theory, Policy, and Politics* (London: UCL Press, 1997), 26.
[26] Beccaria, *On Crimes and Punishments*, 93.
[27] Although Beccaria did not introduce a formal theory of criminal justice or crime prevention theory, he introduced requirements central to formation of these theories: certainty, celerity, severity, etc.
[28] Gilling, *Crime Prevention*, 28–29.

expressed as the "weighted balance between two opposing considerations – pleasure (benefits) and pain (costs)."[29] Bentham explained this balance in the first paragraph of chapter 1 in *An Introduction to the Principles of Morals and Legislation*, which he published in 1789:[30]

> Nature has placed mankind under the governance of two sovereign masters, pain and pleasure. It is for them alone to point out what we ought to do, as well as to determine what we shall do. On the one hand, the standard of right and wrong, on the other the chain of causes and effects, are fastened to their throne. They govern us in all we do, in all we say, in all we think; every effort we can make to throw off our subjection, will serve to but to demonstrate and confirm it.

From Bentham's notion of utility emerged what later scholars called rational choice theory. Utility, as he described it, is the difference between benefits and costs after considering available options from which one chooses a course of action that offers the greatest benefit at the least cost.[31] Bentham identified four sources of pleasure (benefit) and pain (cost) from which one would navigate to obtain the greatest utility: "the physical, the political, the moral, and the religious."[32]

An understanding of these four sources of pleasure and pain help in forming an appreciation of how Bentham's requirements for deterrence, introduced in the following paragraph, helped build an enduring foundation for criminal justice deterrence theory. An example of physical pleasure that an offender might derive from crime is the euphoria from using illegal narcotics, while physical pain would be the cost of suffering a stab wound from the victim

[29] Paternoster, "How Much Do We Really Know About Criminal Deterrence?" 3.
[30] Bentham, *An Introduction to the Principles of Morals and Legislation*, 11.
[31] Paternoster, "How Much Do We Really Know About Criminal Deterrence?" 3.
[32] Bentham, *An Introduction to the Principles of Morals and Legislation*, 34.

in a botched robbery. Examples of political sanctions are those issued by authorities according to the laws of society. The pain of a political sanction is evident in the death penalty or lengthy prison sentences. The source of pleasure from moral aspects come from the prestige among the community of thieves for one's commission of a crime, while the same criminal act can also serve as a source of pain to arouse condemnation among the law-abiding citizens in one's community. Religious pleasure from the belief in the afterlife is common among many faiths, while the fear of one's soul being "damned to hell" can serve as a source of religious pain.[33]

Bentham moved beyond an introduction of the sources of pain and pleasure to describe critical elements that will be "greater or less" depending upon the following circumstances:[34]

1. Its *intensity*
2. Its *duration*
3. Its *certainty* or *uncertainty*
4. Its *propinquity* (proximity) or *remoteness*
5. Its *fecundity*, or the chance it has of being followed by sensations of the same kind: that is, pleasures, if it be a pleasure; pains, if it be a pain
6. Its *purity*, or the chance it has of not being followed by sensations of the opposite kind: that is, pains, if it be a pleasure; pleasures, if it be a pain

The first four of these six elements serve as requirements in criminal deterrence theory. This is the case because these are the essential factors in assessing pleasure or pain, and therefore authorities can manipulate each in isolation or in combination to achieve the desired deterrent effect. For example, to achieve

[33] Paternoster, "How Much Do We Really Know About Criminal Deterrence?" 3.
[34] Bentham, *An Introduction to the Principles of Morals and Legislation*, 38. Bentham specified that fecundity and purity should not be taken into account in evaluating the values of pleasure or pain. For that reason, this researcher does not classify these as requirements for criminal deterrence theory.

effective crime deterrence, the intensity of pain and its duration must be appropriate to the offense. In addition, the certainty of punishment and meting it out should occur in close proximity to the commission of the offense. Both of these examples capture points of agreement between Bentham and Beccaria.

Bentham observed that the tendency for an offender to commit a crime depended upon the offender's capacity to achieve pleasure and avoid the pain of punishment.[35] He described the kinds of "simple pleasures" as sense, wealth, skill, good name, power, and piety and "simple pains" as privation, senses, awkwardness, ill name, piety, and benevolence.[36] However, Bentham noted that "pain and pleasure are produced in men's minds by the action of certain causes. But the quantity of pleasure and pain runs not uniformly in proportion to the cause; in other words, to the quantity of force exerted by such cause."[37] This meant that his "notion of utility," which is the balance between benefits (pleasure) and costs (pain), drives behavior based upon an individual's perception of self-interest.

Bentham's treatment of punishment, particularly his approach to proportionality, which called for the lowering of the severity of punishment as an incentive to potential offenders to commit lesser crimes, introduced a more humane legal system than was the norm of his day.[38] In this regard, Bentham saw punishment as being in the best interest of the offender and a societal necessity,

[35] Ibid., 49.
[36] Ibid., 42.
[37] Ibid., 51.
[38] Ibid., cv.

which was a novel approach. In short, he rejected a retributive-centric deterrence theory by removing the "anger" from punishment.[39]

Freedman commented that Bentham influenced "would-be offenders through creating the impression of pain without actually having to inflict it."[40] To accomplish this, Bentham introduced prevention schemes that relied upon education and employment; however, for the truly delinquent, he suggested the panopticon. The panopticon, a precursor of modern penitentiaries, was a circular prison in which a guard could watch inmates at all times from a central well. Bentham believed that the panopticon served to deter crime and reform criminals who spent time inside this facility.[41]

The works of Beccaria and Bentham and their conception of deterrence did not lay the foundation for early criminologists. Instead, criminologists relied upon biological and psychological models based on the work of psychiatrists and others who believed that criminal behavior resulted from a "pathological mind" more than other factors and thus affected only a small number of people.[42] The next section begins with an examination of the work of Italian Cesare Lombroso (1835–1909), a critic of the classical school, before transitioning to prominent American criminologist, Edwin Southerland (1883–1950).

Criminology and the Italian School

Italian Cesare Lombroso (1835–1909) rejected the classical school, which posited that crime occurs because of the human nature of the individual. He

[39] Gordon Hughes, *Understanding Crime Prevention: Social Control, Risk, and Later Modernity* (Buckingham: Open University Press, 1998), 30.
[40] Freedman, *Deterrence*, 61.
[41] Gilling, *Crime Prevention*, 28–29.
[42] Paternoster, "How Much Do We Really Know About Criminal Deterrence?," 4.

offered an alternative theory: Offenders inherit factors that lead them to commit crimes.[43] In the latter part of the nineteenth century, Lombroso's work led to three core assumptions of the Italian School that were significantly different from those of rational choice theory:[44]

> 1. Crime is not a rational choice but is caused.
> 2. Crime is caused by biological, psychological, and/or sociological factors.
> 3. Offenders are different from non-offenders; there is something special about them or their social situation that makes them commit crimes.

Lombroso appreciated the deterrent value in preventive methods. He believed that educating children and assisting adults at critical junctures diminished crime.[45] Like Beccaria, he saw value in the role that threats played in the deterrent calculus. Unlike Beccaria and Bentham, who opposed the death penalty, Lombroso supported the death penalty in some cases. Regarding the fear of capital punishment, he wrote that it "would serve as a check to the murderous proclivities displayed by some criminals when they are condemned to perpetual imprisonment."[46] Thus, the nature of the threat was effective on the most hardened criminal, which, aside from crimes of passion, implied a greater deterrent effectiveness among the general population. In circumstances where individuals "make repeated attempts on the lives of others … the only remedy is the application of the extreme penalty – death."[47]

---

[43] Gillin, *Criminology and Penology*, 332.
[44] Francis T. Cullen, *Correctional Theory: Context and Consequences* (Thousand Oaks, CA: SAGE, 2012), 73.
[45] Cesare Lombroso, "Criminal Man," 1911, 175, http://www.gutenberg.org/files/29895/29895-h/29895-h.htm.
[46] Ibid., 209.
[47] Ibid.

According to Lombroso's research, inherited biological traits resulted in the "born criminal." Born criminals possessed physical anomalies such as skulls that tend to exaggerate the "ethnical type prevalent in their native countries," handle-shaped ears, shifty eyes, and long arms compared to the lower limbs.[48] Psychological characteristics included "natural affections" for animals and strangers but hatred for one's family, a lack of "repentance and remorse," cynicism, treachery, vanity, impulsiveness, cruelty, and idleness.[49] Sociological issues included population density, previous prison life, professions that "encourage inebriety" (cooks, innkeepers, servants, bricklayers, attorneys, and military men), gender (primarily men), and age (most crimes are committed between ages 15 and 30).[50]

Critics of Lombroso's physical, psychological, and social theories emerged before his death to challenge his findings. While these critics and others later discredited much of his work, he remains important in the field of criminology because scholars credit him with shifting emphasis from the crime to the criminal.[51] American Edwin Sutherland (1883–1950) capitalized on this change in emphasis with great impact.

Sutherland authored *Criminology,* which offered the thesis: "Crime is learned through interaction with others and is repeated when reinforced."[52] The prominence of his work allowed him to become one of the more influential

---

[48] Ibid., 1–20. Lombroso was a phrenologist, one who bases an "assumption that an analysis of character can be made by a study of the shape and protuberances of the skull," see *Webster's New World College Dictionary*, Fourth, 1086.
[49] Lombroso, "Criminal Man," 28–42.
[50] Ibid., 144–152.
[51] "Cesare Lombroso," *Jewish Virtual Library*, 2008, http://www.jewishvirtuallibrary.org/jsource/judaica/ejud_0002_0013_0_12733.html.
[52] Cullen, *Correctional Theory*, 193.

criminologists of the twentieth century. His views further displaced the value of deterrence through punishment theoretically and in practice.

Sutherland cautioned, "Punishment does have some deterrent value, but it also fails dismally as a means of keeping persons from crime."[53] He noted that there was no direct linkage between the frequency of crimes and the severity of punishment. Sutherland did concede a closer proximity between certainty of punishment and frequency of criminal acts but noted that this lacked sufficient evidence. His critique helped reduce modern society's reliance upon punishment to deter crime.[54] The majority of criminologists continued to discredit deterrence until its revival in the mid-twentieth century.

The next section begins with an examination of the work of criminologists who held anti-deterrence views: Hans von Hentig, Jackson Toby, James Appel, and Neil Peterson. In the mid-1950s, Johannes Andenaes countered these anti-deterrence views. The research of John Ball and C. Ray Jeffery followed Andenaes' to help criminal deterrence theory re-emerge.

Criminal Deterrence Theory Debate Re-emerges

Criminology turned its back on deterrence theory for nearly two centuries. This rejection included an aversion to Bentham's notion of utility, which insisted that all individuals possessed the self-interested motivation to commit a crime.[55] Hans von Hentig offered insight into the criminologist's negative perspective on

[53] Edwin H. Sutherland, "Criminology", 1924, 618–619, http://www.questia.com/PM.qst?a=o&d=27947981.
[54] Ibid. Beccaria urged that penalties should be just sufficiently severe enough to deter others.
[55] Paternoster, "How Much Do We Really Know About Criminal Deterrence?" 4.

deterrence in his 1938 article. His guiding assumptions of the "usual methods of deterrence" were:[56]

1. Men know in every case what is harmful to them.
2. Men are in every case frightened by danger.
3. Men realize in every case the correct steps to avoid peril.

From these assumptions, von Hentig argued that Bentham's views on the "pain of the punishment" were "unreal and simple-minded."[57] Von Hentig elaborated, "The principle of deterrence has its limits, because human nature is not under all circumstances and at all events responsive to the menace of punishment."[58] To substantiate his position, he offered four complications of deterrence theory: [59]

1. One should not expect state-sanctioned punishment to cause fear in experienced criminals.
2. The frightened criminal or threatened individual has many reactions, most include the improvement of techniques, not folding to state pressure or retreating.
3. Excessive deterrence creates protective aggression (a robber kills the victim, a rapist strangles the victim).
4. Deterrent-centric laws, courts, and police cause more brutal criminals.

Von Hentig was convinced that deterrence was destined to fail because the pain (cost) of punishment was a distant danger while the pleasure (benefit) was immediate and therefore the immediate advantage of committing a crime was such an advantage to a potential offender that deterrence would not work.[60] Decades later, two additional works captured the criminologists' continued rejection of deterrence theory.

---

[56] Hans Von Hentig, "Limits of Deterrence," *Journal of the American Institute of Criminal Law and Criminology* 29, no. 4 (1938): 556.
[57] Ibid., 559–560.
[58] Ibid., 560.
[59] Ibid., 560–561.
[60] Paternoster, "How Much Do We Really Know About Criminal Deterrence?" 4–5.

Jackson Toby, in a fashion similar to von Hentig questioned the deterrent value of punishment for society. Toby argued that those who have adopted the norms of society are not able to commit criminal offenses as their "self-concept" inhibits such activity. Toby suggested that the criminological model of controlling one's action through pain and pleasure calculations could deter only an unsocialized (amoral) person.[61]

James Appel and Neil Peterson conducted research on the effects of punishment on animal behavior and concluded similarly as Toby and many other criminologists that punishment is "essentially an ineffective way to control or eliminate the behavior of the punished organism."[62] During their research, they observed that "punishment suppresses concurrently rewarded behavior only as long as it continues to follow each response."[63] They determined that even when a "very severe shock is used, punishment is an unfortunate choice" because "behavior can be inhibited to such an extent that the organism might well perish or be (permanently) damaged."[64] Therefore, similar efforts to replicate deterrence through punishment, particularly severe punishment, in humans are as likely to be counterproductive as they were in animal subjects.

Several scholars emerged to counter the overwhelming anti-deterrence sentiment among criminologists in the 1950s. The first of these, Johannes Andenaes, published an influential article in 1952 that would later serve as the

[61] Jackson Toby, "Is Punishment Necessary," *Journal of Criminal Law, Criminology and Police Science* 55 (1964): 333.
[62] James B. Appel and Neil J. Peterson, "Whats Wrong with Punishment," *Journal of Criminal Law, Criminology and Police Science* 56 (1965): 453.
[63] Ibid., 452.
[64] Ibid.

core of his book *Punishment and Deterrence*. John Ball and C. Ray Jeffery followed Andenaes in helping reignite the debate surrounding the value of criminal deterrence theory.

Andenaes noted a trend toward specific or special prevention (individual prevention), with which he found fault. In contrast to popular sentiment of the day, he introduced and advocated general prevention, or "the ability of criminal law and its enforcement to make citizens law-abiding." To accomplish this required reliance upon the "frightening or deterrent effect of punishment" because the risk associated with being arrested, convicted, and punished exceeded the benefit of committing the offense."[65] Twenty years after introducing this concept, he refined his definition of general prevention as "restraining influences emanating from the criminal law and the legal machinery."[66] He distinguished general prevention from deterrence because the former includes a moral aspect regarding the influence of punishment. His restriction of deterrence in a manner that distinguished it from general prevention is different from some scholars, who combined the two.[67]

Andenaes rejected criticism that questioned the value of deterrence through punishment and focused his efforts on the conditions and effects of using punishment to ensure deterrence.[68] He reinvigorated the ideas of Beccaria and Bentham, which had been buried for centuries, such as "deterrence depends not

---

[65] Johannes Andenaes, "General Prevention – Illusion of Reality," *Journal of Criminal Law, Criminology and Police Science* 43 (1952): 179.
[66] Johannes Andenæs, *Punishment and Deterrence* (Ann Arbor: University of Michigan Press, 1974), 34.
[67] Ibid., 35–36.
[68] Ibid., 84.

simply on the risk of being punished, but also on the nature and magnitude of punishment."[69]

Andenaes distinguished general deterrence (the threat of punishment drives deterrence) from special deterrence (the act of punishment yields deterrence) as he did with general and specific/special prevention.[70] Andenaes' concept of general prevention included general deterrence and, as previously alluded, the effect that punishment may have on morals that cause individuals to follow societal norms.[71]

What made Andenaes distinct from his contemporaries was his view that individuals would conform to societal norms if faced with punishment for nonconformance.[72] He conceded that psychology had demonstrated that the pleasure-pain principle was not as valid as broadly assumed in Bentham's penal theory; however, he argued that regardless of a lack of empirical data, it is a "fundamental fact of social life" that the risk of pain or other undesirable consequences serve to motivate most people.[73]

Following Andenaes, John Ball challenged the prevailing negative view of punishment and deterrence by most criminologists.[74] He observed that the concept of deterrence had been "evident through the ages in Western thought concerning crime and punishment."[75] Ball echoed Andenaes in noting the

---

[69] Ibid., 24.
[70] Ibid., 84.
[71] Paternoster, "How Much Do We Really Know About Criminal Deterrence?" 5.
[72] Ibid.
[73] Andenæs, *Punishment and Deterrence*, 147.
[74] John C. Ball, "The Deterrence Concept in Criminology and Law," *Journal of Criminal Law, Criminology and Police Science* 46 (1955): 347. He defined deterrence as "the preventive effect which actual or threatened punishment of offenders has upon potential offenders."
[75] Ibid.

absence of empirical data on deterrence, but instead of rejecting the theory for lack of evidence, he suggested a formal research approach. To pursue this research agenda, Ball offered six factors to determine the deterrent effect of punishment. These factors, particularly certainty and individual knowledge of the law, helped form deterrence theory:[76]

1. Social structure and value system under consideration
2. Particular population in question
3. Type of law being upheld
4. Form and magnitude of the prescribed penalty
5. Certainty of apprehension and punishment
6. Individual's knowledge of the law as well as the prescribed punishment, and his or her definition of the situation relevant to those factors

In 1965, C. Ray Jeffery published an article on deterrence that built upon the work of Andenaes and Ball to rejuvenate criminal deterrence by punishment.[77] He argued that if authorities issue a punishment, but then stop the punishment, an offender will return to a pattern of committing offenses.[78] Jeffery's work in studying the learning theory of criminals led him to conclude that the certainty of punishment was an important factor in deterring crime.

Jeffery, influenced by Bentham and Beccaria, considered certainty a more important factor than severity in successful deterrence. Regarding statistical evidence (using capital punishment data), he cited two factors that limited the deterrent value of this form of punishment: uncertainty and the time element. Jeffery observed that the lesson to learn from capital punishment was that the improper use of punishment does not deter. As a result, he further concluded that

---

[76] Ibid., 348.
[77] C. Ray Jeffery, "Criminal Behavior and Learning Theory," *Journal of Criminal Law, Criminology and Police Science* 56 (1965): 298. Jeffery defined punishment as, "the withdrawal of a reinforcing stimulus or the presentation of an aversive stimulus."
[78] Ibid.

avoidance and escape behaviors were likely to be the result of severe punishment.[79]

The next section traces the revival of criminal deterrence theory. Three scholars featured prominently in this revival: economist Gary Becker, sociologist Jack Gibbs, and philosopher Michel Foucault.

Revival of Criminal Deterrence Theory

Several works emerged in the late 1960s and 1970s to help remove criminal deterrence theory from life support to face a revival in popularity among scholars. Paternoster noted that the long-standing rejection of the use of punishment to deter crime resulted more from ideology than empirical evidence. Gary Becker, an economist, and Jack Gibbs, a sociologist, fostered interest in empirically testing hypotheses of deterrence theory, while Michel Foucault, a philosopher, provided an account of the capacity of authorities to punish offenders and the role of prisons in this process.[80]

Becker's empirical study concluded that criminal behavior theory should disregard a lack of social standards and psychological impediments and instead concentrate on the factors that drive potential offenders to act rationally in their self-interest.[81] He advanced ideas similar to Bentham's, arguing for an approach that pursued the widely accepted economic notion of utility, which predicts that an offender will commit a crime if the "expected utility" is greater than the utility gained from conducting some other activity. Becker observed that some people

[79] Ibid., 299. Jeffery cited examples of avoidance and escape, such as: not leaving fingerprints, hiring a good lawyer, bribing police, and pleading to a reduced charge
[80] Paternoster, "How Much Do We Really Know About Criminal Deterrence?" 6.
[81] Gary S. Becker, "Crime and Punishment: An Economic Approach," *Journal of Political Economy* 76, no. 2 (March 1, 1968): 170.

adopt a life of crime because benefits exceed costs, not because they possess motivation that inherently differs from their peers.[82]

Gibbs' study focused principally on punishment as he pursued a more specific theory over the general approach of Bentham, Andenaes, and Becker. Gibbs pursued an empirical approach to determine whether actual punishment had a deterrent effect on crime. The timeless idea that "in some situations some individuals are deterred from some crimes by some punishments" was insufficient to advance deterrence theory without proof.[83]

Gibbs argued two hundred years after Beccaria and Bentham that scholars have been unable to move deterrence beyond an "unsystematic theory," which assumes that the "doctrine reduces to a simple proposition, such as: certain, swift, and severe punishments deter crime."[84] Propositions like this distort the concept because the deterrence doctrine consists of two independent parts, specific deterrence and general deterrence.[85]

Specific deterrence, also known as special deterrence, as the term implies, "is specific to the person being punished."[86] When authorities punish a criminal, the criminal's fear of future risk of punishment is increased, which reduces the offender's tendency to commit additional crimes.[87] General deterrence, on the other hand, results in an impact on non-offenders from the mere threat of

[82] Ibid., 176.
[83] Jack P Gibbs, *Crime, Punishment, and Deterrence* (New York: Elsevier, 1975), 11.
[84] J. P. Gibbs, "Assessing the Deterrence Doctrine: A Challenge for the Social and Behavioral Sciences," *American Behavioral Scientist* 22, no. 6 (July 1, 1979): 653.
[85] Ibid., 653–654.
[86] Nagin, "Deterrence: Scaring Offenders Straight," 70.
[87] Gibbs, "Assessing the Deterrence Doctrine," 668.

punishment based upon that given an offender.[88] Gibbs introduced two variants of general deterrence, absolute general deterrence and restrictive general deterrence.[89]

Gibbs described absolute general deterrence as occurring when a person refrains from a criminal act because of a perceived risk of punishment.[90] Restrictive general deterrence occurs when an offender reduces the tendency to commit a criminal act for some period because the offender believes that the curtailment will reduce the risk of punishment.[91] Gibbs concluded that there was no "systemic evidence" of specific deterrence; however, findings regarding general deterrence are not "totally negative."[92] His empirical research found that "perhaps punishment is effective in generating compliance with the laws" because if the doctrine of deterrence is valid, "then states where the certainty and severity of punishment were higher would have lower homicide rates," which is what his research confirmed.[93] Gibbs' empirical study confirmed the validity of general deterrence and subsequently encouraged a generation of scholars.

Michel Foucault joined Becker and Gibbs in furthering the debate on the value of punishment. In his classic book, *Discipline and Punish: The Birth of the Prison*, he examined the history of punishment since the eighteenth century with a

---

[88] Ibid., 654.
[89] Ibid., 660–661.
[90] Gibbs, *Crime, Punishment, and Deterrence*, 32. In this form of deterrence, it is the punishment or rather the threat of punishment that serves as the impetus through which an individual's or a group of individuals' risk calculation is influenced so as not to engage in the activity in question.
[91] Ibid., 33. An example of restrictive deterrence may be found in the risk calculus associated with automobile parking in a metropolitan area. In most cities, the chance of receiving a ticket for parking in an unauthorized area or exceeding for a few minutes the paid time on a meter is quite low. However, the risk of a fine or boot being placed on one's automobile offers sufficient punishment such that many among the population seek to avoid the slightest infraction. Such individuals fear that their repetition of the offense will eventually result in punishment.
[92] Gibbs, "Assessing the Deterrence Doctrine," 674.
[93] Paternoster, "How Much Do We Really Know About Criminal Deterrence?" 7.

precise treatment of the evolution of the various means and methods used to torture, punish, and discipline the wayward among polite societies. Foucault instructed that "instead of taking revenge, criminal justice should simply punish."[94] He noted that it is the act of punishment that "robs forever the idea of a crime of any attraction."[95] The means and techniques upon which he reported have changed significantly; however, the central thesis in criminal justice that punishment or the threat of punishment deters potential offenders remains unchanged from the beginning of recorded history.

The next section considers the relationship between deterrence and crime prevention. The purpose of this section is to understand the value that prevention efforts can bring to the deterrence calculus.

Deterrence and Crime Prevention

If one wishes to determine the important factors in criminal deterrence, then it is necessary to understand what matters most to offenders.[96] The literature is clear that costs and benefits as perceived by the criminal are a crucial component. However, David Kennedy noted that when criminal deterrence failed, academics and policy makers focused on objective reasons such as reporting rates, effectiveness of police in apprehending suspects, and rates of prosecution that result in sanctions.

---

[94] Michel Foucault, *Discipline and Punish: The Birth of the Prison*, 1st American ed. (New York: Pantheon Books, 1977), 74. Foucault begins by examining the role of torture in the criminal justice process. At this time, prior to the eighteenth century, executions in public and corporal punishment were central features. He then examines the reform of punishment in the eighteenth century with the advent of the prison system.

[95] Ibid., 104.

[96] David M. Kennedy, *Deterrence and Crime Prevention: Reconsidering the Prospect of Sanction*, Routledge Studies in Crime and Economics ; V. 2. (London: Routledge, 2009), 23.

Instead, Kennedy argued that subjective matters were more important. Subjective matters are those factors that specifically make a potential crime appear appealing – or unappealing – to a potential offender. These factors include a potential offender's knowledge of the law, lack of an ability to receive information communicated by authorities, and failure to appreciate formal and informal sanctions.[97]

Kennedy's consideration of subjective matters is in keeping with the ideas of classical deterrence theory; however, when one considers deterrence in a crime prevention construct, a slight nuance emerges. Deterrence and prevention both hold that potential offenders must be rational and thus act in a self-interested manner. The difference arises in that deterrence provides individuals reasons to choose to refrain from committing offenses, while prevention offers potential offenders opportunities to avoid committing crimes.[98]

Classical theorists appreciated the value prevention added to deterrence theory. For example, Beccaria referred to prevention as an effort that requires simple laws that are widely supported. He argued that laws should be clear so that no interpretation is required. Beccaria also added that education is a requirement and then asked, "Do you want to prevent crimes? See to it that enlightenment accompanies liberty."[99]

[97] Ibid., 23–39. Formal sanctions are those imposed according to law, while informal sanctions are those levied by a culture or community, such as shame or embarrassment.
[98] Hughes, *Understanding Crime Prevention: Social Control, Risk, and Later Modernity*, 30.
[99] Beccaria, *On Crimes and Punishments*, 95.

Bentham was the most "influential 'apostle' of the utilitarian discourse on prevention and deterrence."[100] Bentham's work, as presented previously, argued for an "efficient preventive system." He and others afterward wondered "whether crime could be viewed in the old way as a simple function of depravity."[101] These classical views went beyond reframing criminal deterrence by punishment to serving as the intellectual foundation for crime prevention theory.[102]

Glaser offered three preventive approaches to reduce crime: primary crime prevention, secondary crime prevention, and tertiary crime prevention. Primary crime prevention focuses on the causes of crime, while secondary crime prevention seeks to reform offenders. Tertiary crime prevention centers on physically stopping criminals, which leads one to consider the impact of situational crime prevention.[103]

The next section examines the work of Jan J. M. van Dijk and Jaap de Waard, Maurice Cusson, and particularly Ronald Clarke, who focus on situational crime prevention. The researcher believes that this "tertiary" form of crime prevention, although it targets individuals, will prove useful in constructing a state-centric theory of cyber deterrence.

---

[100] Hughes, *Understanding Crime Prevention: Social Control, Risk, and Later Modernity*, 30.
[101] Ibid., 30–31.
[102] Michael H. Tonry, *The Handbook of Crime & Punishment* (New York: Oxford University Press, 1998), 372–380. Crime prevention theory may be classified into three areas: situational crime prevention (crime event focused), community crime prevention (community or neighborhood focused with attention to community organization and development) and criminality prevention (offender-focused and based upon family policy, education policy, and youth policy). The purposes of this research are informed with a focus on situational crime prevention theory. The others, while interesting, offer information that is beyond the scope and purpose of this study.
[103] "Science and Politics as Criminologists' Vocations," in *Contemporary Masters in Criminology*, edited by Joan McCord and John H. Laub, Plenum Series in Crime and Justice (New York: Plenum Press, 1995), 293–300. It is this tertiary mode, which refers to situational crime prevention that best merges with classical criminal deterrence theory to inform this research.

Situational Crime Prevention

Dijk and Waard described crime prevention as "the total of all private initiatives and state policies, other than the enforcement of criminal law, aimed at the reduction of damage caused by acts defined as criminal by the state."[104] Stated simply, crime prevention depends upon the use of locks, alarms, cameras, fences, safes, security guards, and the like that affect potential offenders in two ways. First, the threat of detection leads to punishment, and second, the costs of conducting a crime are immediately greater. The value of immediacy and certainty are as effective in prevention as in deterrence.

Deterrence and situational crime prevention share commonalities, but as Cusson pointed out there is also a point of departure, which centers on the capacity to instill fear.[105] It is the fear of sanction in the deterrence construct, which has an "inhibiting influence" on the potential offender.[106] With situational crime prevention, fear is "generated by specific situational risks that have an immediate impact on an offender's decisions."[107] A key goal of situational crime prevention is to "instill fear in any individual contemplating a crime by increasing the risks."[108]

Ronald Clarke built upon the idea of increasing risk in defining situational crime prevention as:

---

[104] Jan J. M. van Dijk and Jaap de Waard, "A Two-Dimensional Typology of Crime Prevention Projects; With a Bibliography," *Criminal Justice Abstracts* 23, no. 3 (September 1991): 483.
[105] Maurice Cusson, "Situational Deterrence: Fear During the Criminal Event," *Crime Prevention Studies* 1 (1993): 55.
[106] Ibid., 56.
[107] Ibid., 65.
[108] Ibid., 55. Cusson drew upon the work of Clarke in "Situational Crime Prevention: Theory and Practice" in the *British Journal of Criminology* 20:136-147, 1983, and the "Introduction" from *Situational Crime Prevention: Successful Case Studies*, 1992, for this insight.

> Compromising measures directed at highly specific forms of crime that involve the management, design, or manipulation of the immediate environment in as systematic and permanent a way as possible so as to reduce the opportunities for crime and increase its risks as perceived by a wide range of offenders.[109]

He noted that every crime requires a motivated offender and the opportunity to commit a crime. Therefore, one cannot solely explain crime by examining the dispositions of criminals to various aspects of deterrence theory as criminologists suggest.

Clarke observed two mistakes that criminologists have historically made in this regard. First, criminologists seek to explain the criminal and disregard the crime. Second, he argued that modern criminologists confuse efforts to bring crime under control with those of reigning in the criminal. In short, he questioned a long-standing assumption that to reduce crime the focus should lie on the criminal.[110]

Historically, criminological literature relies upon formal and informal social control measures to curtail crime. Formal control includes the institution of law, which authorities use to sanction, confine, and thus deter a population. Informal control is the effort by a society to ensure conformity by socializing norms. Clarke argued that these two approaches have ignored an important third category, which is the precautions that people and organizations take every day to prevent crime. Examples of these precautions include locking doors, installing

---

[109] Ronald V. Clarke, "Situational Crime Prevention," in *Building a Safer Society: Strategic Approaches to Crime Prevention*, Crime and Justice v. 19 (Chicago: University of Chicago Press, 1995), 91. Clarke previously introduced this definition in his 1983 article "Situational Crime Prevention: Theory and Practice," appearing in *Crime and Justice: An Annual Review*, vol. 4.
[110] Ronald V. Clarke, *Situational Crime Prevention: Successful Case Studies*, 2nd ed. (Criminal Justice Press, 1997), 2. Clarke drew upon the work of Gottfredson and Hirschi (1990) and Wilkins (1990) for his assessment on the mistakes of modern criminologists.

burglar alarms, living in safe neighborhoods, teaching children to avoid strangers, and similar defensive measures. Situational crime control fits into this third category.

Clarke introduced twelve "opportunity-reducing" techniques of situational prevention under three distinct categories (see Table 2.2). First, to increase the effort for potential criminals, he proposed hardening targets, establishing access control, deflecting offenders, and controlling facilitators.[111] To harden a target means using a physical barrier to deny criminals access to things they may steal or destroy by relying upon locks, safes, and bars. In controlling access, Clarke uses physical means to deny criminals access to places, which may be individual buildings or building complexes. Historically, a moat surrounding a castle captured this type of response. From a modern perspective, installing a perimeter fence and requiring access through a guarded entry point accomplish this.

To deflect an offender, Clarke referred to examples where municipalities or corporations control large crowds of people through conscious efforts to reduce the effects of congestion. For example, Britain uses clever scheduling of soccer events to avoid long waiting periods, and Disney uses signs, pavement markings, and friendly hosts to reduce crime and frustration among large crowds.

Controlling facilitators includes a wide range of actions to hinder some catalysts of criminal behavior. Such actions include restricting patrons from carrying guns into businesses that sell alcoholic beverages, bars refusing to serve

[111] Clarke, "Situational Crime Prevention," 109.

patrons that appear to be approaching intoxication, and the use of caller-ID systems to block obscene or unwanted telephone calls.[112]

Table 2.2: Opportunity-reducing Techniques[113]

Increasing the Effort	Increasing the Risks	Reducing the Reward
1. *Target hardening*	5. *Entry/exit screening*	9. *Target removal*
Steering locks	Baggage screening	Removable car radio
Bandit screens	Automatic ticket gates	Exact change fares
Slug (fake coin) rejector	Merchandise tags	Phonecard
2. *Access control*	6. *Formal surveillance*	10. *Identifying property*
Fenced yards	Security guards	Property marking
Entry phones	Burglar alarms	Vehicle licensing
ID badges	Speed cameras	ID numbers for car radios
3. *Deflecting offenders*	7. *Employee surveillance*	11. *Removing inducements*
Tavern location	Park attendants	Graffiti cleaning
Street closures	Pay phone location	Rapid repair
Graffiti board	Closed-circuit TV	Vagrant-proof bench
4. *Controlling facilitators*	8. *Natural surveillance*	12. *Rule setting*
Gun controls	Street lighting	Customs declaration
Credit card photo	Defensible space	Income tax returns
Caller-ID	Neighborhood watch	Hotel registration

Second, Clarke introduced the importance of increasing the risk of authorities catching potential offenders. To increase risk, he advocated four activities: entry/exit screening, formal surveillance, employee surveillance, and natural surveillance. Entry and exit screening is different from controlling access as the purpose, in this case, is not to deny access, but to elevate the risk of arrest for potential criminals. Examples of this type of screening are baggage and passenger security checks at airports, the door scanning systems that alert librarians that patrons have not properly checked out, and the automatic ticket gates found in modern subway systems.

Formal surveillance is security provided by professionals hired to deter and apprehend criminals such as security guards, store detectives, and local law

[112] Ibid., 110–112.
[113] Ibid., 109. Clarke adapted his twelve techniques of situational prevention from his 1992 book *Situational Crime Prevention: Successful Case Studies*.

enforcement. Employee surveillance refers to reliance upon employees, not hired for criminal deterrence purposes, to surveil customers in a secondary capacity to their normal duties. Here, one expects a watchful clerk to detect an act of shoplifting or a cash register attendant to identify a stolen credit card. Natural surveillance includes activities that property owners undertake to make it more difficult for criminals to gain entry undetected. This includes trimming or removing trees and bushes and adding or enhancing lighting.[114]

Lastly, Clarke suggested that reducing the reward for criminal activity offers the potential for large prevention dividends. Here he relies upon actions, which include removing the target (that which the criminal covets), identifying or marking one's property, removing inducements, and setting rules. Examples of removing the target for a criminal are replacing coin parking meters with electronic systems and the use of safes with timers by banks and other businesses.

Identifying or marking property can be as benign as engraving one's name on a tool or using a system of registering vehicles, which is common in most nations. Removing inducements to criminal activity involves activities such as painting murals on vacant walls to deter graffiti or installing vagrant-proof benches at bus stops and parks. Lastly, examples of rule setting are private companies using regulations to govern an employee's use of company time and equipment to read personal email or the installation of procedures regarding cash register accounting. Rule setting may occur in the public domain – for example, a

[114] Ibid., 113–116.

town may deny citizens to legally consume alcohol in public or institute a curfew for minors.[115]

Summary

Crime prevention theory offers a denial component in situational crime prevention, which, when combined with punishment to deter a potential offender, results in robust criminal deterrence theory. This section traced the historical evolution of criminal deterrence by investigating the origin and revival of deterrence theory and concluded with the importance of the role of both deterrence and prevention.

In concluding this section on criminal justice deterrence, it is important to pause and note that deterrence through punishment occurs in response to criminal laws. Criminal law serves as a "system of deterrent threats," a system that always works well in that no one questions the problem of threats that fail to work.[116] The fact that threats did not deter offenders is not crucial because laws to deter criminals also target potential offenders.[117] Therefore, in contrast to nuclear deterrence, successful criminal deterrence is not an "all-or-nothing matter" as the "system can still be viewed as succeeding despite the failures of threatened sanctions."[118]

Next, this study presents the requirements for criminal justice deterrence theory. The requirements to deter potential offenders have been adopted from this overview of the works of classical and modern scholars. These requirements

---

[115] Ibid., 116–118.
[116] R. Wasserstrom, "War, Nuclear War, and Nuclear Deterrence: Some Conceptual and Moral Issues," *Ethics* 95, no. 3 (1985): 436.
[117] Ibid.
[118] Ibid., 443.

represent the factors that are essential for authorities to consider in using punishment to deter potential offenders. Additionally, as punishment does not deter all potential offenders, presentation of the key requirements of situational crime prevention offers a deterrence by denial component to criminal justice deterrence theory.

Requirements of Criminal Justice Deterrence Theory

The core components of criminal justice deterrence theory are punishment and prevention. The causal mechanisms of punishment are offensive as they are actions taken by authorities to ensure a desired response or necessary conditions that are required for effective punishment to take place. The causal mechanisms for prevention are defensive in nature. See Table 2.3 for a summary of the requirements for criminal deterrence to occur in theory.

There are ten requirements to deter by punishment in criminal deterrence theory. These requirements are rationality, social structure/value system, threat, communication, sanctions, certainty, celerity, severity, proportionality, and knowledge. Rationality predicts that an offender will commit a crime if the "expected utility" is greater than the utility gained from conducting some other activity and is a necessary condition for authorities to deter a potential offender from criminal activity.[119]

The existence of a social structure and value system is necessary, particularly in Western societies, as this helps determine "people's respect for legal ideology and its administration."[120] If authorities are to deter its population,

[119] Becker, "Crime and Punishment," 176.
[120] Ball, "The Deterrence Concept in Criminology and Law," 349.

then the capacity to abide by the law must be present among a population that includes potential offenders. Authorities must rely upon the threat or fear of sanctions to induce in a potential offender the inclination to refrain from committing a criminal act.

Sanctions may be formal or informal. Formal sanctions are those imposed according to law, such as imprisonment or fines, while a culture or community levies informal sanctions, such as shame or embarrassment.[121] Authorities' use of a threat of sanction to deter requires communication of the threat and sanction to potential offenders. For communication to be effective, authorities must clearly deliver the message, and potential offenders must receive and understand that message.

Certainty and celerity are key deterrence requirements because it is important to link the crime with the corresponding punishment. Certainty is the "probability that a criminal act will be followed by punishment,"[122] while celerity is "how quickly a punishment follows a criminal act."[123] Beccaria reasoned, and Bentham and others have held since similar views, that "the more promptly and more closely punishment follows upon the commission of a crime, the more just and useful it will be."[124]

[121] Kennedy, *Deterrence and Crime Prevention*, 31-34.
[122] Nagin, "Deterrence: Scaring Offenders Straight," 71.
[123] Ibid.
[124] Beccaria, *On Crimes and Punishments*, 55.

Table 2.3: Requirements of Criminal Justice Deterrence Theory[125]

Core Components	Causal Mechanisms	Purpose	Requirements	Rationale
Punishment	Offensive actions taken by authorities or conditions necessary for effective offensive actions	Inflict cost	Rationality	Capacity to assess benefits and cost is a necessary condition
			Social structure and value system	Capacity to abide by the law must be present
			Threat	Threats must be issued and received
			Sanctions	A source of pain is necessary to increase cost calculations of potential offenders
			Communication (of threat/sanctions)	Must be clear and understood by receiving party
			Certainty	Criminal acts must be followed by punishment to be of most use
			Celerity	The more quickly a punishment follows a crime, the more just and useful
			Severity	Reducing the level of punishment is an incentive to commit lesser crimes
			Proportionality	Punish the crimes that cause the most damage more severely
			Knowledge (of the law and risks)	A law that a potential offender is not aware of cannot deter
Prevention (Denial)	Defensive actions taken by any actor	Deny benefits	Increase the effort	Deny access to things someone wants to steal
			Increase Risks	Make it more likely that an offender will be detected
			Reduce Rewards	If costs exceed benefits, a potential offender has been deterred

[125] The requirements for punishment were subjectively derived from the evolution of criminal deterrence theory. The researcher believes that the literature provides sufficient evidence that each of these factors meets the standard for inclusion as a requirement. A requirement is defined as a "something obligatory or demanded, as a condition" or "something needed" see *Webster's New World College Dictionary*, 1218. The requirements for prevention/denial were adopted from Clarke, "Situational Crime Prevention," 109.

Severity refers to the level of punishment authorities give to offenders.[126] The lowering of the severity of punishment is an incentive to potential offenders to commit lesser crimes.[127] Proportionality has a slightly different meaning as it refers to authorities' efforts to conform punishment to the nature of the crime.[128] The idea behind proportionality is to punish the most damaging crimes more severely than lesser offenses. Lastly, for authorities to deter a potential offender, that individual must have knowledge of the law and the likely punishment for violating that law.[129] A law of which he is not aware cannot deter a potential offender.[130]

Criminal deterrence theory incorporates the capacity to prevent an actor from engaging in criminal activity by denial for which the causal mechanisms are defensive. The capacity for authorities or individual actors to deny benefits to a potential offender requires that the deterring actor use capabilities to defend or deny access to protected entities. Situational crime prevention includes defensive precautions that organizations and people use every day to prevent crime.

Ronald Clarke captured the requirements for situational crime prevention with his typology (see Table 2.2), which included three categories: increasing the effort, increasing the risks, and reducing the reward for potential offenders. To increase the effort for potential criminals, he proposed hardening targets, establishing access control, deflecting offenders, and controlling facilitators. To increase risk, he advocated four activities: entry/exit screening, formal

[126] The level of punishment includes the intensity and duration of the sanction.
[127] Bentham, *An Introduction to the Principles of Morals and Legislation*, cv.
[128] Beccaria, *On Crimes and Punishments*, 57.
[129] Ball, "The Deterrence Concept in Criminology and Law," 348.
[130] Ibid., 351.

surveillance, employee surveillance, and natural surveillance. Clarke suggested that reducing the reward for criminal activity offered the potential for large prevention dividends. Here he relied upon actions that include removing the target (that which the criminal covets), identifying or marking one's property, removing inducements, and setting rules.[131]

Crime prevention theory offers a denial component in situational crime prevention, which, when combined with punishment to deter a potential offender results in robust criminal deterrence theory. The concepts of criminal deterrence and the ebb and flow of debate among scholars are similar to the core concepts and evolution of strategic nuclear studies, yet, as Freedman observed, "how little they draw upon each other's work."[132]

Nuclear Deterrence Theory

Introduction

Deterrence by punishment and denial by defense are central features of nuclear deterrence theory. The desire to punish, which made attribution necessary, held sway over denial in the earlier years of the theory's evolution. Attribution for a nuclear attack required accuracy in identifying the attacker and timeliness in responding.[133]

[131] Clarke, "Situational Crime Prevention," 109–118. Clarke's taxonomy was explained in detail in an earlier section of this study, *Situational Crime Prevention*.
[132] Freedman, *Deterrence*, 60.
[133] The capability and will to communicate a credible threat to the target of a deterrence strategy or policy must be present if deterrence through punishment is the intent.

During the Cold War, there was an "expectation that the United States would recognize if an attack had occurred, by whom, and with what."[134] The Union of Soviet Socialist Republics (USSR) was the only actor capable of a nuclear attack on the U.S. for many years; therefore, deterrence through the threat of retaliation had a predictable effect.[135] Regarding the capacity to punish, which was necessary for a threat to be credible, it was presumed that the only two nuclear capable actors, the U.S. and USSR, had "comparable intentions and comparable financial, military, and technological resources – at least to the extent that each (was) suspected to seek, establish, and sustain secure offensive retaliatory nuclear capabilities for mutual deterrence purposes."[136] However, in the post-Cold War era, the value of deterrence by denial has gained favor. This is in part due to the increased number of nuclear actors and the potential difficulty of attributing an attack to a non-state actor that may acquire a nuclear device.

Nuclear deterrence theory is in part based on criminal justice and differs little from cyber deterrence theory except in one major aspect. Given the lethality of one nuclear warhead used in anger, a single failure of nuclear deterrence would be catastrophic. This is not the case with these other theories. The differences are apparent as one reads the following overview of the evolution of nuclear deterrence through three distinct waves during the Cold War and one afterward. The review of these four waves of nuclear deterrence theory traces both the

---

[134] Payne, *The Great American Gamble: Deterrence Theory and Practice from the Cold War to the Twenty-first Century*, 361. Attribution became more difficult with the proliferation of actors capable of WMD attacks in the post-Cold War era. Efforts to enhance nuclear forensics have aided the nuclear attribution challenge.
[135] Ibid. Payne noted the difficulty in relying upon an indiscriminant "generic threat" if the U.S. were unable to identify potential attackers.
[136] Ibid., 336.

evolution of punishment and denial strategies and the evolution of various manifestations of the theory. This section concludes with a presentation of the major requirements for nuclear deterrence theory, which have endured through the pre- and post-Cold War era.

Historical Evolution of Nuclear Deterrence

First Wave of Nuclear Deterrence Theory

Jervis noted that the initial wave of deterrence theory, which occurred in the first few years immediately after World War II, resulted in very little impact.[137] The impact that did arise emerged from the early work of men such as Bernard Brodie, George Kennan, and Paul Nitze. Bernard Brodie's 1946 book *The Absolute Weapon* introduced the first use of a form of the word *deterrence* in the nuclear age.

Brodie observed that the "bomb may act as a powerful deterrent to direct aggression against great powers without preventing the crisis out of which wars generally develop."[138] He further explained that for this deterrent effect to be present the "aggressor state must fear retaliation."[139] The necessity to instill fear in a potential adversary required a threat – or, more specifically, a threat of retaliation.

Brodie argued that a threat of retaliation does not have to be wholly certain, as it is sufficient that an adversary believe that a "good chance" of a

---

[137] Robert Jervis, "Review: Deterrence Theory Revisited; Deterrence in American Foreign Policy: Theory and Practice," *World Politics* 31, no. 2 (January 1979): 291. Jervis in the 1970s identified three waves of deterrence theory that have come to be used since their inception as a means though which many scholars examine the evolution of Cold War deterrence theory.
[138] Bernard Brodie, *The Absolute Weapon* (New York: Harcourt, Brace and Company, 1946), 85.
[139] Ibid., 74.

threat's validity exists.[140] To impress upon an adversary that the U.S. could retaliate if attacked, Brodie suggested that the "first and most vital" action should be to guarantee "retaliation in kind." While the phrase "second-strike capability" would emerge later, the concept Brodie introduced at the outset of the nuclear age required the U.S. to reduce vulnerabilities to an atomic attack and to establish the capability to fight back after such an attack.[141] Brodie believed that the more horrible the potential outcome of an attack, the greater the U.S.' capacity to deter an adversary "by even a marginal chance at retaliation."[142]

With this early work in *The Absolute Weapon*, Brodie described the first three requirements for what would eventually become nuclear deterrence theory: An adversary must be present (which requires attribution), an actor must issue a threat to instill fear of retaliation in that adversary, and to fulfill an expectation of retaliation, the capacity to respond in-kind after an attack is necessary.

Nuclear deterrence at this early stage was in its infancy.[143] However, ideas that would form the foundation of U.S. nuclear policy began to emerge. Of note, also in 1946, is George Kennan's "Long Telegram," which he followed in 1947 with his article "The Sources of Soviet Conduct." In the telegram and article, he advocated a policy of containment regarding the Soviets. The intent of a policy of containment was to limit the USSR in its ambitions to encroach on areas vital to U.S. security interests. Kennan did not use the word *deterrence* in either work; however, his ideas were in harmony with the central idea and

---

[140] Ibid.
[141] Ibid., 76–88.
[142] Ibid., 107.
[143] Concept, in this sense is a "central or unifying idea or theme." See *Webster's New World College Dictionary*, Fourth: 301.

unifying theme of deterrence that would shortly emerge.[144]

In 1948, the now declassified Top Secret National Security Council report NSC 20/3 laid out U.S. objectives to counter Soviet threats. Specifically, this report called for developing "a level of military readiness which (could) be maintained as long as necessary as a deterrent to Soviet aggression."[145] The policy established in NSC 20/3 helped to prepare the U.S. for the dramatic change that emerged on August 29, 1949, when the Soviet Union exploded its first atomic bomb.

Like Kennan, Paul Nitze was highly influential during this period. Nitze argued that the U.S. strategy should be "graduated deterrence" because a declaratory policy that deviates too far from an action policy is weakened.[146] He was in an ideal position as Director of the State Departments Policy Planning Office to advocate for graduated deterrence in response to potential Soviet aggression. Nitze was instrumental in developing National Security Council Paper Number 68 (NSC-68), the first comprehensive national strategy for the U.S. in the Cold War.

On April 14, 1950, within eight months of the USSR's entry into the "nuclear club," NSC-68 was completed. *NSC-68: U.S. Objectives and Programs for National Security* precisely laid out a policy of containment for the Soviet

---

[144] X., "The Sources of Soviet Conduct," *Foreign Affairs* 25, no. 4 (July 1947): 581. http://www.jstor.org/stable/20030065. Kennan wrote that a policy of containment should be "designed to confront the Russians with unalterable counter-force at every point where they show signs of encroaching upon the interests of a peaceful and stable world."
[145] "U.S. Objectives With Respect to the USSR to Counter Soviet Threats to U.S. Security," n.d.
[146] Paul H. Nitze, "Atoms, Strategy and Policy," *Foreign Affairs* 34, no. 2 (January 1, 1956): 187–188. Nitze drew upon a definition of "graduated deterrence" that defined the policy as one that limited "wars (in weapons, targets, area, and time) to the minimum force necessary to repel aggression.

Union. As a result of rapidly developing Soviet Union capabilities, the authors of NSC-68 concluded and President Truman agreed that the "U.S. must have substantially increased general air, ground, and sea strength, atomic capabilities, and air and civilian defenses to deter war."[147] This document refined the ideas for first strike and second strike as well as the policy of graduated deterrence. As a result of actions stemming from NSC-68, there was an increase in U.S. nuclear capability and associated planning.[148]

In the second wave, nuclear deterrence theory began to coalesce into a form that would serve as a foundation for U.S. strategy and policy throughout the Cold War. Yet, as the second wave emerged into a classical zero-sum game there were already examples of cooperation – the 1953 and 1954 Geneva conferences and the Austrian State Treaty of 1955.[149] These cooperative efforts were exceptions to the norm of first wave interaction between the U.S. and USSR. These efforts were discounted at the time; however, cooperation between the nuclear superpowers, despite their vast differences, came to exist during the 1960s from "shared, or at least similar, general ideas of world order and of its survival."[150]

Second Wave of Nuclear Deterrence Theory

The second wave began in the mid-1950s after many ideas from the early nuclear period lay dormant for roughly ten years. It was during this second wave

---

[147] Ernest R. May and National Security Council, *American Cold War Strategy: Interpreting NSC 68* (Boston: Bedford Books of St. Martin's Press, 1993), 76.
[148] Strategy is "the science of planning and directing large-scale military operations" or a "stratagem or artful means to some end." See *Webster's New World College Dictionary*, Fourth: 1416.
[149] Roger E. Kanet and Edward A. Kolodziej, eds., *The Cold War as Cooperation* (Baltimore: Johns Hopkins University Press, 1991), 31.
[150] Ibid., 34.

that scholars first theoretically elaborated upon the idea of deterrence.[151] Deterrence theory in the early part of the second wave was like the game of Chicken.[152] In this game, circumstances occur whereby each party "tries to prevail by making the other think it is going to stand firm."[153] It is from this idea that massive retaliation was born in NSC-162/2 in October 1953.

A central tenet of massive retaliation was the dependence upon the capacity to retaliate instantly and massively.[154] George and Smoke identified three major interrelated factors that further underscored the rationale for massive retaliation. These combined factors are the U.S.' experience in Korea, the question of economic costs of military forces during peacetime, and technological advancements.[155] Given the significant U.S. lead in nuclear capability over the Soviet Union, massive retaliation, the first systematic theory of deterrence, remained the guiding strategy for the U.S. for most of the 1950s.[156]

The mutual relationship between the U.S. and the Soviet Union became the basis for deterrence theory and served to focus the effort. In 1954, Kauffman presented three requirements that were necessary for the U.S. to deter its nuclear

---

[151] *Webster's New World College Dictionary*, Fourth: 1485. Theory is "a formulation of apparent relationships or underlying principles of certain observed phenomena, which has been verified to some degree."
[152] Jervis, "Review: Deterrence Theory Revisited; Deterrence in American Foreign Policy: Theory and Practice," 291. Jervis described this game as "situations in which the first choice of both sides is to stand firm, but in which both prefer retreating and letting the other side win to a mutually disastrous confrontation."
[153] Ibid., 292. This implication of the model enables scholars to understand many of the bargaining tactics actors adopt.
[154] Alexander L. George and Richard Smoke, *Deterrence in American Foreign Policy: Theory and Practice* (New York: Columbia University Press, 1974), 27.
[155] Ibid., 27–28. In essence, the U.S. sought to avoid wars like Korea by threatening nuclear strikes. In addition, nuclear weapons were cheaper than large conventional forces and thus technological advancements in nuclear capabilities made it possible to avoid large conventional wars.
[156] Ibid., 27.

adversary:[157]

1. Having an effective military capability
2. Its ability to impose unacceptable costs on the adversary
3. Using that capacity if attacked

The requirement for an "effective military capability" was necessary because for a U.S. threat of retaliation to be credible, it must possess the capacity to "inflict an 'unacceptable level of damage,' coupled with a clear intention and political will to use it punitively."[158] The requirement for political will was important as deterrence must be "conclusive" in that inherent in the U.S. threat of retaliation and the Soviet Union's perception of U.S. will, the "certainty of destructive retaliation" must never been in doubt.[159]

Despite U.S. efforts to fulfill these requirements, by the late 1950s, two criticisms of massive retaliation surfaced. First, the U.S. was vulnerable to a surprise attack.[160] Second, the Soviet Union's expanding nuclear capability demanded a response.[161] Graduated deterrence found new life as some scholars and practitioners reconceived it to counter the criticisms of massive retaliation.

---

[157] Patrick M. Morgan, *Deterrence Now* (Cambridge, UK: Cambridge University Press, 2003), 4. Morgan draws upon William Kaufmann's 1954 work, *The Requirements of Deterrence*, Center of International Studies Memorandum no. 7, Princeton University.

[158] Dougherty and Pfaltzgraff, *Contending Theories of International Relations: A Comprehensive Survey*, 352.

[159] Keith B. Payne, *Deterrence in the Second Nuclear Age* (Lexington: University Press of Kentucky, 1996), 80.

[160] Many perceived the numerically disadvantaged Soviet Union might calculate to strike first.

[161] Lawrence Freedman, *The Evolution of Nuclear Strategy*, vol. 3 (Basingstoke, Hampshire England; New York: Palgrave Macmillan, 2003), 342–344. From the Soviet's nuclear test in 1949 through the mid-1950s, "there had been an anticipation of effective parity." In the early 1960s, the U.S. gained numerical superiority. Khrushchev took three steps to improve the Soviet position: emphasis on threats to NATO members that could be attacked more readily, increase the explosive capacity of each warhead, and place medium and intermediate range missiles in Cuba. This third action "back-fired dramatically" as the outcome of the resulting crisis confirmed publicly the "comparative weakness of the Soviet Union." This led Khrushchev to pursue detente to "hold down American military strength through arms control, obviating the need for large-scale" weapons procurement programs," see 250-254. Under Brezhnev, the Soviets in the late 1960s embarked on a build-up of nuclear forces to gain parity with U.S. nuclear missile capabilities. By the end of the 1960s, the Soviet's were equal in raw numbers with the U.S., see 254-255.

Nitze, a proponent of graduated deterrence, suggested that it was in "the interest of the West that the means employed in warfare and the area of engagement" be "restricted to the minimum level which still permits us to achieve our objectives."[162] Specifically, this meant that the U.S. would meet small Soviet attacks with tactical nuclear weapons restricted to the local theater instead of a massive intercontinental nuclear exchange.[163]

Henry Kissinger agreed and argued in favor of developing limited nuclear weapons capability advocated by the doctrine of graduated deterrence. He postulated that stalemates were a feature of wars throughout history and introduced the idea of the "nuclear stalemate." To counter a potential nuclear stalemate, he suggested that U.S. military doctrine should be one in which limited wars could be fought.[164]

Kissinger observed that the deterrence aspects of a nuclear stalemate deter "not only aggression, but resistance to it; and it deters not war as such, but all-out war. The side which can present its challenges in less than all-out form may be able to use the 'nuclear stalemate' to its advantage."[165] He believed that failure to take such an advantage benefitted the Soviet Union because the U.S. would leave the Soviets with an opening to push for geopolitical gains with the knowledge that the U.S. would not risk total war. Graduated deterrence was somewhat short-lived as critics noted that the Soviets would soon have tactical nuclear

[162] Nitze, "Atoms, Strategy and Policy," 188.
[163] George and Smoke, *Deterrence in American Foreign Policy*, 30.
[164] Henry A. Kissinger, "Force and Diplomacy in the Nuclear Age," *Foreign Affairs* 34, no. 3 (April 1, 1956): 349–366.
[165] Ibid., 353.

weapons.[166] Those critics came to power with the election of President John Kennedy.

These "critics" were fortunate to have great counsel in the foundational works of Thomas Schelling and Herman Kahn as sources for policy options in what had become a "delicate balance of terror." Albert Wohlstetter wrote at that time a "stable balance" did not exist – in fact, the balance had become precarious, and this condition held critical implications for policy. Further, he observed, "Deterrence in the 1960s [was] neither assured nor impossible but [would] be the product of sustained intelligent effort and hard choices."[167] Schelling and Kahn were dominant figures in the "intelligent effort" and helped decision makers navigate the hard choices.

Thomas Schelling provided a "strategy of conflict" that considered rationality, game theory, and arms control among many other factors. Schelling observed that nuclear weapons changed the equation such that it was no longer necessary to defeat an adversary's military. The possibility existed to coerce an adversary by holding its citizens at risk.[168] His threat-centric argument in which the populations remained vulnerable served as the preferred policy of choice by decision makers for most of the Cold War.

A threat works "because of what the other players expect us to do in response to his choice of moves, and we can afford to make the threat only

---

[166] George and Smoke, *Deterrence in American Foreign Policy*, 30–31.
[167] Albert Wohlstetter, "The Delicate Balance of Terror," *Foreign Affairs* 37, no. 2 (January 1, 1959): 213. He argued that deterrence was not "automatic" but required work and that "to deter an attack means being able to strike back in spite of it."
[168] Thomas C. Schelling, *The Strategy of Conflict* (Cambridge: Harvard University Press, 1960).

because we expect it to have an influence on his choice."[169] A calculus of this nature suggests that the "rationality of the adversary is pertinent to the efficacy of the threat." This means that an adversary must have awareness of his value system and the capacity to understand available alternatives and determine risk.[170] An assumption resulting from the concept of rationality was that the U.S. and Soviet Union could avoid nuclear war if both parties made "correct choices."[171]

Rationality is a requirement for deterrence; nevertheless, there are those who question this requirement.[172] The leading criticism for the assumption of rationality by U.S. policy makers in deterrence theory came from Robert Jervis. Jervis found fault with scholars who concentrated on deductive logic while disregarding the perceptions of policy makers.[173] He theorized that this led to missed signals and misperceptions; however, he conceded, "the fact that people are not completely rational does not automatically vitiate this approach."[174]

As previously pointed out, Schelling accepted an assumption of rationality in deterrence theory; however, he recognized that decision makers could depart from rationality. He noted that irrationality could arise from a variety of factors, such as "a disorderly and inconsistent value system, faulty calculation, (or) an inability to receive messages or to communicate efficiently."[175] Further, he suggested that it may be "rational for a rational player to destroy his own

---

[169] Ibid., 10.
[170] Ibid., 6–13.
[171] Philip Green, *Deadly Logic: The Theory of Nuclear Deterrence* (Columbus: Ohio State University Press, 1966), 158.
[172] Dougherty and Pfaltzgraff, *Contending Theories of International Relations: A Comprehensive Survey*, 383.
[173] Ibid., 357.
[174] Robert Jervis, Richard Ned Lebow, and Janice Gross Stein, *Psychology and Deterrence* (Baltimore, Md.: Johns Hopkins University Press, 1985), 5.
[175] Schelling, *The Strategy of Conflict*, 16.

rationality" in certain situations. Thus, a player could feign irrationality to deter a threat based on the presumption of his rationality or to add credibility to a threat he would not make under other circumstances.[176]

In either circumstance, the deterrer must communicate the threat to an adversary. Schelling defined *threat* as "communication of one's own incentives, designed to impress on the other side the automatic consequences of his act."[177] For deterrence to occur, an adversary must receive and clearly understand the threat communicated by the deterrer. Schelling's purposeful use of the word *communication* is instructive because in the process of transmitting a threat and associated resolve, an adversary could deter that threat by purposeful efforts to avoid receiving the communication.[178] Likewise, it is possible that inadvertent communication miscues can hinder deterrence.

The requirements for effective deterrence extend beyond the act of communicating a well-designed threat to a rational adversary. Jones noted that "one cannot fear something which one knows will never happen."[179] Therefore, threats must be credible, which means that the capability and political will must exist to carry out the threat. Further, this means that transparency is a prerequisite because the threatened party must have visibility into the deterrer's capacity to fulfill the commitment inherent in the threat.[180] To achieve effective deterrence, the deterrer cannot keep capability or the political will that lends credibility to the

---

[176] Ibid., 143.
[177] Ibid., 35.
[178] Ibid., 39. An adversary could avoid receiving communications by simply avoiding messages or destroying communication channels.
[179] Roy E. Jones, *Nuclear Deterrence: A Short Political Analysis* (London: Routledge & K. Paul, 1968), 20.
[180] Schelling, *The Strategy of Conflict*, 40.

threat a secret.[181]

This does not mean that uncertainty did not play a role in Cold War nuclear deterrence. Uncertainty existed because:[182]

> Not all the frontiers and thresholds are precisely defined, fully reliable, and known to be so beyond the least temptation to test them out, to explore for loopholes, or to take a chance that they may be disconnected this time. Violence, especially war, is a confused and uncertain activity, highly unpredictable, depending on decisions made by fallible human beings organized into imperfect governments, depending of fallible communications and warning systems and on the untested performance of people and equipment. It is furthermore a hotheaded activity, in which commitments and reputations can develop a momentum of their own.

The existence of uncertainty inserted an "inherent sense of risk," which had the potential to rapidly get out of control should a crisis escalate into war.[183] Schelling captured this idea with his "threat that leaves something to chance" approach to deterrence.[184] In practice, this meant that the U.S. relied upon the Soviet's fear of uncertainty regarding U.S. potential actions, which created the impression that a crisis could escalate against either side's wishes.[185]

To prevent an escalation that could result in general war, Schelling argued that it was the "threat of pain," not the "threat of military defeat," upon which the usefulness of deterrence theory resided. This was possible because the "power to

---

[181] Dougherty and Pfaltzgraff, *Contending Theories of International Relations: A Comprehensive Survey*, 352.
[182] Thomas C. Schelling, *Arms and Influence* (New Haven: Yale University Press, 1966), 93.
[183] Freedman, *The Evolution of Nuclear Strategy*, 3:207.
[184] Schelling, *The Strategy of Conflict*, 187–188. Schelling noted that general war might be initiated accidentally through some kind of accident, false alarm, panic, or mischief.
[185] Payne, *The Great American Gamble: Deterrence Theory and Practice from the Cold War to the Twenty-first Century*, 32. Regarding uncertainty, Jervis offered the salient idea that even though both the U.S. and USSR believed the other would not want to destroy the world in a suicidal attack; creating uncertainty was deterrence enough given the destructive power in the hands of each.

hurt" or, rather, impose costs on civilians had become dominant in military affairs as nuclear-enabled states could now bypass military on military applications of force to impose extreme damage on civilian populations.[186]

This approach required the preservation of the inherent vulnerabilities of the respective populations and industries of the U.S. and former Soviet Union. Schelling explained why preserving vulnerabilities was important in the context of a surprise attack:[187]

> The special significance of surprise attack thus lies in the possible vulnerability of retaliatory forces. If these forces were themselves invulnerable – if each side were confident that its own forces could survive an attack, but also that it could not destroy the other's power to strike back – there would be no powerful temptation to strike first. And there would be less need to react quickly to what might prove to be a false alarm.

His argument for the U.S. to protect its ability to respond to Soviet nuclear aggression with nuclear weapons instead of the U.S. population was the central idea that bolstered the deterrence concept of mutually assured destruction.[188] It was also necessary, as previous scholars have noted, to ensure a second strike capability. This meant that the U.S. "must have massive reserves deployed in invulnerable positions."[189] The U.S. maintained a second-strike capability through the Cold War and beyond.

Herman Kahn, on the other hand, saw the necessity to develop defensive capabilities, to which Schelling vehemently objected. Kahn believed that "unless the United States was capable of limiting damage to itself in a nuclear war, it

---

[186] Schelling, *Arms and Influence*, 1–34.
[187] Schelling, *The Strategy of Conflict*, 233.
[188] Ibid.
[189] Jones, *Nuclear Deterrence*, 21.

could not credibly threaten nuclear escalation."[190] The threat of nuclear escalation was necessary because the Soviets would only see U.S. deterrence threats as credible if an "expectation of a deliberate U.S. decision to escalate" were evident.[191] However, Kahn was just as concerned about war starting by miscalculation as by accident and noted that a miscalculation would be more likely to occur from escalation than from any other factor. He conceded that efforts to limit escalation elevated the likelihood of the actors using limited amounts of violence, but this was worth the risk.[192]

Kahn, in arguing for the value of defense in the deterrence calculus, wrote, "The threat of mutual suicide is a very uninspiring concept."[193] He articulated an alternative idea to pursue development of defensive capabilities, particularly aerial defenses. The value of a defensive approach to nuclear deterrence would later gain favor in the early 1980s as the Reagan-era Strategic Defense Initiative (SDI) was debated.[194] However, a contemporary scholar of Kahn, Glenn Snyder, articulated the case for deterrence that relies upon defense.

Glenn Snyder's book *Deterrence and Defense*, published in 1961, observed that the "central problem" in U.S. security policy was differentiating

---

[190] Payne, *The Great American Gamble: Deterrence Theory and Practice from the Cold War to the Twenty-first Century*, 29.
[191] Ibid., 255.
[192] Herman Kahn, *On Thermonuclear War* (Princeton, N.J.: Princeton University Press, 1960), 229. Kahn defined escalation as "the unpremeditated increase or spread of a limited operation."
[193] Ibid., 96. Kahn offered four reasons that made it "feasible" to pursue this course of action. First, aerial defenses would prevent the Soviets from getting a "free ride" were they to conduct a first strike against U.S. industries or cities. Second, these defenses would offer a "usable warning" that a strike by Soviet bombers of missiles was imminent. Third, by stopping "small strikes" that might take place after an initial exchange, the U.S. would enhance its position regarding the attrition of enemy forces. Lastly, aerial defenses would prove beneficial in "reorganization and recuperation" efforts to include reconstituting strategic forces.
[194] Strategic missile defense, as a deterrence calculation, was realized with the fielding of missile defense architecture in the beginning of the twenty-first century. Vulnerability to attack from rogue actors fueled this effort.

deterrence and defense. He accomplished this by defining deterrence as a process of convincing an adversary to refrain from offensive action by presenting a decision in which the costs outweighed the benefits, while defense simply meant reducing costs in case deterrence fails. In essence, deterrence focuses on the intentions of an adversary, and the purpose of defense is to limit or remove an adversary's capacity to cause damage.[195]

The differentiation Snyder made between defense and denial is also important in understanding the range of defensive capabilities needed to deter by defensive measures. He postulated that the value of defense is a combination of the capability to deny and the ability to lessen war damage. This expanded the requirements for deterrence by defense beyond the mere establishment of barriers and protective measures. This perspective was what allowed him to argue that deterrence is a peacetime concern, while defense is a wartime matter given that the "ability to lessen war damage" aspect is a key component of denial.[196]

Snyder also noted the characteristics that distinguish denial and punishment. Denial capabilities deter because they affect an adversary's "probability of gaining his objective." Examples of these types of capabilities are conventional Army, Navy, and air military forces. Punishment capabilities rely upon strategic nuclear weapons, which affect an adversary's "estimate of possible costs."[197] Snyder admitted that these distinctions were not "sharp"; however, the

---

[195] Glenn Herald Snyder, *Deterrence and Defense* (Princeton, NJ: Princeton University Press, 1961), 3.
[196] Ibid., 4. Snyder pointed out that "after the enemy's attack takes place, (U.S.) military forces perform different functions and yield wholly different values than they did as deterrents prior to the attack."
[197] Ibid., 14.

inherent nuances impact the deterrer's credibility. He reasoned that a threat of punishment with a nuclear response is credible when faced with a nuclear attack. Yet, this same threat in response to a conventional attack is "less credible than a threat to fight a 'denial' action."[198]

Reliance upon deterrence, which requires an offensive capability, and defense are necessary because one's "security is a function of both of these elements."[199] These elements depend upon nuclear weapons for different purposes, yet nuclear weapons have both an offensive and defensive component. For example, the threat of retaliation is a deterrent to an adversary's potential first strike, while the actual use of a nuclear weapon to strike back after an adversary has attacked first is a defensive action. Snyder introduced "qualitative requirements" to counter both of these circumstances.[200]

To deter a direct attack, it is necessary to reduce vulnerability. The requirements to accomplish this rely upon "hardening, dispersal, mobility, and concealment" of U.S. nuclear capability. Snyder believed that the capacity to protect forces to deter a first strike is unnecessary "except for those forces which are held back from the first strike for bargaining purposes."[201]

Preserving the survivability of retaliatory force is necessary to deter a surprise attack. The U.S. nuclear triad is clearly the major element of assuring retaliation, examples of these forces comprise a fleet of intercontinental ballistic missiles (ICBM) with nuclear warheads, long-range nuclear capable bombers, and

[198] Ibid., 15.
[199] Ibid., 31.
[200] Ibid., 85.
[201] Ibid.

submarines equipped with the Polaris intermediate range ballistic missiles (IRBM). ICBMs are land-based, and while their position is fixed, they are dispersed and hardened – therefore, survivable at that time given the limited accuracy of Soviet long-range missiles.

While bomber bases were vulnerable, aircraft on ground alert, ready to take off within minutes, and those on airborne alert were survivable. Bombers were vulnerable to enemy air defenses, which was not the case for ICBMs. However, bombers offered the president the capability to recall an attack once under way, which was not possible with ICBMs or submarine-launched missiles. Submarines equipped with the Polaris IRBMs offered "elements of invulnerability," and while vulnerable in port, submarines at sea had the advantage of "mobility, concealment, and protection provided by the sea itself."[202]

Because of these capabilities, Snyder considered that the U.S. might deter the Soviets from deliberately starting World War III because their loss of twenty million lives in World War II remained a fresh memory.[203] An accident or miscalculation could lead to an escalation neither side intended, which fueled the logic of a defensive, damage-limiting posture centered on preparedness. Yet, at that time, the justification to invest in greater defensive capability depended upon the likelihood of a Soviet first strike. Regarding this likelihood, Snyder commented:[204]

---

[202] Ibid., 86–90. Snyder offered an in-depth discussion of each of these systems and links these capabilities to the "qualitative requirements" he suggests are necessary for deterrence and defense.
[203] Ibid., 57.
[204] Ibid., 117.

> The value of all preparedness measures intended to reduce our losses or to make positive gains in all-out war tends to decline as the probability of war declines. If we had the high-confidence deterrence we have been discussing, substantially insuring against all possible Soviet incentives for a first strike, the chances of war would be very low. In view of this, it seems doubtful that the defense benefits from having forces well beyond those necessary for high-confidence deterrence would justify their peacetime costs.

The debate surrounding Schelling's deterrence through a threat of punishment and Kahn's advocacy for the value of deterrence by defense formed two distinct camps to which scholars such as Brodie, Wohlstetter, and Snyder offered significant contributions. These scholars built upon the earlier theoretical work in the first wave to solidify the enduring requirements for nuclear deterrence in the second wave. This theoretical work guided and informed U.S. decision makers as nuclear deterrence strategies and policies were developed and refined.[205] The Kennedy administration adopted an approach toward the Soviet Union that reflected the impact of this scholarly debate.

The Kennedy administration's answer to graduated deterrence came in the form of flexible response in 1961. Flexible response incorporated capability and doctrine for making highly controlled, limited, and selective strategic strikes.[206] This represented a policy product of a few ideas suggesting, with only moderate confidence, the usefulness of precise and careful application of limited force.[207] On its heels, scholars and practitioners formulated assured destruction or mutual assured destruction in 1962. Flexible response never represented a strategy in the

[205] While there were differences in deterrence theory approaches between the Schelling and Kahn camps, there were also policy differences within and between administrations. It is not inconsistent to have to have these differing elements in public policy matters.
[206] George and Smoke, *Deterrence in American Foreign Policy*, 40.
[207] Ibid., 42.

same sense as deterrence by assured destruction.[208]

Assured destruction or mutual assured destruction (MAD) centered on the capacity to deter by inflicting unacceptable levels of destruction on the adversary.[209] The massive nuclear arsenals of the superpowers drove this idea. Further, assured destruction offered precise criteria for contingency planning of operations and for decisions on force structure and procurement.[210] This approach was the most enduring of the Cold War as it served as a policy product, which directly flowed from a systematic theory of strategic deterrence that a number of presidents supported with high confidence.[211]

As the second wave transitioned to the third, so too did the continuation of ongoing cooperative efforts between the U.S. and USSR, which had begun during this period. Although keen adversaries, possession of these powerful weapons served to often unite the interests of both parties. For example, after the October 1962 Cuban Missile Crisis there was the "Hot Line Agreement, the Partial Test Ban Treaty (PTBT), and discussion of the non-proliferation of nuclear arms."[212] Another important example was the 1967 Glassboro meeting in which President Johnson and Prime Minister Alexei Kosygin discussed "bilateral relations,

---

[208] Ibid.
[209] Dougherty and Pfaltzgraff, *Contending Theories of International Relations: A Comprehensive Survey*, 382. The concept of mutual assured destruction was based in Schelling's arguments regarding the utility of the threat of punishment, the power to hurt, and the necessity for mutual vulnerability of civilian populations previous discussed in this chapter.
[210] George and Smoke, *Deterrence in American Foreign Policy*, 42.
[211] Ibid.
[212] Roger E. Kanet and Edward A. Kolodziej, eds., *The Cold War as Cooperation* (Baltimore: Johns Hopkins University Press, 1991), 43. Kanet and Kolodziej note that "one of the main results of the Cuban missile crisis was an evident acceleration of the process of cooperative learning between the U.S. and USSR," see page 45.

scientific cooperation, and prospects for arms control and disarmament."[213] Although the immediate relevance of this meeting was "overshadowed by the events in Czechoslovakia in 1968," its importance stemmed from the fact that "it placed on the agenda of both sides such issues as the discussions of anti-ballistic missiles (later developed into the ABM Treaty 1972), strategic arms limitation (later also developed into the Strategic Arms Limitations Talks (SALT) 1 and SALT 2 treaties, 1972 and 1979)."[214] The relevance of these arms control efforts has emerged during the third wave because of their role in increasing transparency, which is an important component of deterrence.

Third Wave of Deterrence Theory

The third wave began in the 1970s and was characterized by the realization that there was a "lack of a search for supporting evidence" regarding deterrence theory by earlier scholars.[215] This is somewhat remarkable given that the 1960s witnessed a U.S. investment that mounted into the trillions of dollars, leading to the buildup of an arsenal that would surpass 70,000 nuclear warheads during the Cold War. Unfazed by their predecessors or the investment in this buildup, scholars in the early 1970s considered no tenet of deterrence sacrosanct as they set about to systematically examine the deterrence doctrine with great rigor.

Academics questioned the rational actor model and other central

[213] Ibid., 46. The initiation of these cooperative efforts occurred during the escalation of the Vietnam War. While the U.S. was mired in Vietnam, "Soviet strategic forces were enlarged by several orders of magnitude."
[214] Ibid., 47.
[215] Jervis, "Review: Deterrence Theory Revisited; Deterrence in American Foreign Policy: Theory and Practice.," 301.

propositions upon which deterrence theory depended. At the core of this challenge of the rational actor model was the work of Irving Janis on groupthink, Allison on bureaucratic models[216], and Jervis on perception and misperception.[217] This scrutiny gave rise to the notion that U.S. reliance on the rationality of the Soviet Union and its leaders may be faulty.[218]

Because of the empirical work of the period, an examination of other propositions and assumptions resulted in challenges to nuclear deterrence theory. Some academics, anxious to undercut nuclear deterrence, began to argue that the U.S. should base foreign policy on positive inducements and nuanced diplomacy rather than what had become a predictable and dangerous regime of military threats. They suggested that U.S. and Soviet antagonism had significantly lessened with the result of what were previously first-order security interests that now appeared secondary in nature.[219]

George and Smoke, with their 1974 book *Deterrence in America Foreign Policy*, ushered in the third wave.[220] They "claimed that deterrence had led to an exaggerated role for the military dimension in U.S. foreign policy and had

---

[216] Graham T. Allison, *Essence of Decision: Explaining the Cuban Missile Crisis*, 2nd. ed. (New York: Longman, 1999), 4–7. Using the Cuban missile crisis, Allison directly challenged the rational actor model of Schelling. Allison's Rational Actor Model (RAM or Model I) posited that "most analysts explain (and predict) behavior of national governments in terms of [this] one basic conceptual model." He offered two alternative models, which he called the "Organizational Behavior Model (Model II) and a Governmental Politics Model (Model III) that he argued provided a basis for "improved explanations and predictions."

[217] Freedman, *Deterrence*, 22.

[218] It is worthy to note that rationality as an underlying assumption of deterrence weathered this criticism to remain in the post-Cold War era an enduring assumption of the doctrine.

[219] Freedman, *Deterrence*, 22.

[220] George and Smoke, *Deterrence in American Foreign Policy*, 591. George and Smoke's study resulted in three findings: Deterrence is better viewed as part of a broader influence process than a self-contained strategy, a broader theory that encompasses deterrence, is needed to influence conflict processes, and decision makers need to recapture classical diplomacy to influence adversaries.

discouraged attempts to transcend the cold war."[221] Scholars continued to develop this line of reasoning through the third wave.[222] These efforts challenged the idea of using the vast U.S. military nuclear arsenal as the central tool for demonstrating resolve.

The result of third wave criticisms was not an invalidation of the concept of issuing a threat to the deterrence calculus. The value of the threat of punishment, much like rationality and other requirements for deterrence theory established in the second wave, remained an enduring assumption of deterrence. However, many political and military decision makers, by this point, had become uncomfortable with the status quo. This resulted in a significantly new look for deterrence theory.

In the early 1970s, "strategic parity had become one of the major factors shaping the superpowers interactions."[223] Aside from parity, other factors such as the Vietnam experience, a "troubled partnership" with the Atlantic Alliance, and rethinking of the U.S. approach to China resulted in a new conceptual framework known as the Nixon Doctrine. The doctrine's three main elements: power, partnership, and negotiation had "clear implications for U.S.-Soviet rivalry and cooperation."[224] The element of negotiation sought to transition these states from "unwritten, tacit rules" to explicit rules guiding their interaction. This effort took

[221] Freedman, *Deterrence*, 23.
[222] Ibid. Much later, shortly after the end of the Cold War and well beyond the intense academic scrutiny on deterrence during the third wave, Lebow and Stein elaborated on George and Smoke's point far more emphatically. Lebow and Stein argued the U.S. had "overdosed on deterrence." They suggested that an "exaggerated view of the importance of demonstrating resolve" in less than important situations combined with an unprecedented arms race and a needless degree of antagonism drove a "distorted strategy."
[223] Kanet and Kolodziej, *The Cold War as Cooperation*, 47.
[224] Ibid.

the form of the May 1972 Basic Principles Agreement (BPA).[225]

The BPA codified the "main rules of existence" between the U.S. and USSR and served as a "charter for détente."[226] There were several main points that elaborated the degree of cooperation:[227]

- Peaceful coexistence should be the main principle on which to base U.S.-Soviet relations
- Ideological and social differences were not to be obstacles to the bilateral development of normal relations
- Importance was given to preventing the development of situations capable of causing a dangerous exacerbation of their relations
- Both parties pledged to exercise restraint in their mutual relations and to negotiate and settle differences by peaceful means

The BPA provided "some important rules for the conduct of nuclear warfare." However, even though the agreement was "little more than a statement of intent" it is important because it "marked a shift from an atmosphere of confrontation."[228]

Signed during this same period, the Anti-Ballistic Missile (ABM) Treaty (May 1972) and SALT I (July 1972) were "guided by the goals of preserving the balance of terror and codifying the equilibrium point in armaments thought to exist when both sides were confident and satisfied with their assured destruction deterrents."[229] SALT I linked mutual offensive nuclear force limits to mutual limits on BMD." BMD was viewed for it potential to protect ICBMs and preserve stable deterrence; therefore, if SALT I limited the "Soviet ICBM threat to U.S. ICBMs, then BMD was regarded as largely unnecessary and could be

---

[225] Ibid., 48.
[226] Raymond L. Garthoff, *Détente and Confrontation: American-Soviet Relations from Nixon to Reagan* (Brookings Institution Press, 1985), 290.
[227] Kanet and Kolodziej, *The Cold War as Cooperation*, 49–50.
[228] Steve Phillips, *Heinemann Advanced History: Cold War in Europe and Asia* (Heinemann Secondary Education, 2001), 178.
[229] Payne, *The Great American Gamble: Deterrence Theory and Practice From the Cold War to the Twenty-first Century*, 155.

limited strictly or banned." [230]

Within two years, Secretary of Defense James Schlesinger argued in 1974 that increased Soviet ICBM capability undercut assured destruction. He wrote that U.S. options lay between the two extremes of doing nothing and thus surrendering or launching a large second strike, which would be suicidal. Finding this circumstance strategically unacceptable, he ushered in a new deterrence theory: selective targeting or limited options. Selective targeting was highly controversial as many critics argued that nuclear war had become "thinkable." Others suggested an alternative view by arguing that Schlesinger strengthened deterrence as he made the threat of a U.S. response more credible.[231]

Over a decade after these changes unfolded, Payne observed, "the labels occasionally changed, but the basic differences upon which positions were based did not."[232] Given the benefit of hindsight, Payne's claim was an indictment of some third wave scholars who sought to find their "supporting evidence" within the confines of those existing positions. Payne, as a disciple of Kahn, relished the rise of the value of defense in nuclear deterrence that re-emerged with great flourish in the 1980s during the Reagan Administration to counter the long-standing preeminence of Schelling's offensive-oriented argument.[233]

---

[230] Ibid., 154.
[231] James R. Schlesinger, "Schlesinger's Limited Nuclear Options," *Air Force-Magazine.com* 89, no. 2 (February 2006): 3 Nov 2009. Selective targeting provided the president a wider set of options in two regards. First, it limited the chance of uncontrolled escalation. Second, the strategy emanating from the theory resulted in plans to strike only meaningful targets with an appropriate combination of accuracy and yield to hold at risk only the desired target.
[232] Payne, *Deterrence in the Second Nuclear Age*, 7.
[233] Payne is correct that labels did change, and certainly he is on the mark that the positions were static, i.e., the afore-mentioned Schelling and Kahn camps. Nevertheless, his observation does not question the changes that occurred during and arguably leading up to the third wave particularly within the offensive camp as underscored in the new deterrence theory of the Schlesinger era.

The SDI emerged under President Reagan's leadership in the 1980s. During this period, decision makers and some scholars "began to embrace the concept of defense against nuclear weapons as a basis for deterring the use of nuclear weapons."[234] Nitze pointed out that to achieve this goal, SDI had to fulfill two criteria. First, defense had to be cost-effective, which meant that it had to be less expensive for the U.S. to build a defense than for the USSR to build more ICBMs. Second, defensive capabilities had to be able to withstand a first strike, which meant they had to be survivable.[235] Critics argued this was too difficult and that because no "defensive system can be foolproof," the U.S. still had to have its traditional deterrent structure, which made the argument for deterrence through defensive capabilities "baseless."[236]

Throughout the majority of the Cold War, decision makers and most deterrence scholars cast aside the value of defensive military capabilities to counter intercontinental ballistic missiles. This happened because decision makers were convinced that defensive capabilities would disrupt the stable deterrence balance that was firmly entrenched in the idea of mutual vulnerability to nuclear retaliation by the U.S. and Soviet Union.[237] With events leading to the

---

[234] Dougherty and Pfaltzgraff, *Contending Theories of International Relations: A Comprehensive Survey*, 382–383. SDI was the second of three great debates on ballistic missile defense in the U.S. The first debate occurred over a seven-year period from 1965 to 1972 and concluded with the anti-ballistic missile, or ABM, treaty. The third debate emerged after the end of the Cold War in the late 1990s. This third debate proposed national missile defense (NMD) as the best means to field limited capability to defend the U.S. against rogue actors.

[235] Michael Charlton, *From Deterrence to Defence: The Inside Story of Strategic Policy* (Cambridge, MA: Harvard University Press, 1987), 101. By cost effective Nitze meant that a "defense must be cheap enough that an opponent would have "no incentive to add additional offensive capability to overcome the defense," see Paul Vorbeck Lettow, *Ronald Reagan and His Quest to Abolish Nuclear Weapons*, 1st ed. (New York: Random House, 2005), 155.

[236] Charlton, *From Deterrence to Defence*, 142.

[237] Dougherty and Pfaltzgraff, *Contending Theories of International Relations: A Comprehensive Survey*, 382–383. Vulnerability was also addressed by mobile systems. The U.S. pursued the MX

fall of the Berlin Wall in November 1989, support for these ideas began to unravel.

Until this point, the U.S. deterred the Soviet Union by a threat of punishment, which potentially required the defeat and destruction of the USSR. The rubric of assured destruction, which had long dominated U.S. western deterrence thought, had begun to change as policy makers wanted both offensive and defensive-centric deterrence as robust as possible. Although decision makers reduced the large defensive shield imagined by proponents of the SDI to a small-scale system designed to counter a few long-range missiles from a rogue actor, the value of defense in the deterrence calculus had become a mainstay in U.S. nuclear deterrence theory.[238]

The fall of the Berlin Wall and collapse of the Soviet Union in 1991 resulted in many scholars arguing there was no further value in deterrence theory. This view proved shortsighted as the shift from a long-standing bipolar world resulted in international structural changes with implications for most every state actor. These changes ensured a prominent role for nuclear deterrence theory, albeit in revised form, for a wider cast of state and non-state actors – a theory that now relied upon both the "combination of punitive threats and denial measures" to influence the decision calculus of potential adversaries.[239]

Peacekeeper land-based mobile missile to assure second strike capabilities. The U.S. did not field the MX; however, the Soviets embraced mobile missiles systems as a hedge against the vulnerability of fixed sites.

[238] Ibid., 378. The U.S. announced in 1999 that it would deploy a limited missile shield to counter the growing threat from North Korea as soon as the technologies were available.

[239] Payne, *The Great American Gamble: Deterrence Theory and Practice from the Cold War to the Twenty-first Century*, 371.

Post-Cold War Deterrence Theory

The U.S. and Soviet Union have dramatically drawn down the number of nuclear weapons in their arsenals since the end of the Cold War. However, these weapons will remain fixtures in their arsenals, and those of other nuclear capable actors, for decades to come, if not forever. If Iran should soon develop nuclear weapons capability, there will be ten states in the "nuclear club."[240] It is in this context that Colin Gray coined the label "second nuclear age" by which he suggested "that so many features of the emerging security environment are sufficiently different from that of the Cold War that the post-Cold War period deserves to be considered a new, yet still nuclear age."[241]

Gray argued that in the second nuclear age, there is a "contemporary inclination to marginalize deterrence."[242] He substantiated this contention with five points:[243]

> 1. Deterrence had become "inherently unreliable."
> 2. U.S. Cold War strategic behavior was not as "magisterial as was believed at the time."
> 3. U.S. deterrence theorists confused "rationality with reasonableness."
> 4. Deterrence had become marginalized because post-Cold War "adversaries appear to be undeterrable."
> 5. Deterrence theory had been developed by those who were generally not "historians or close students of Clausewitz."

Payne concurred by noting, "Lingering Cold War expectations that deterrence can

---

[240] The U.S., Russia, United Kingdom, China, France, India, Pakistan, and North Korea have declared nuclear weapons capability while Israel is believed to have nuclear capability.
[241] Payne, *Deterrence in the Second Nuclear Age*, 8–9. The second nuclear age contains readily visible trends such as the rise of regional powers and the proliferation of weapons of mass destruction.
[242] Colin S. Gray, *Maintaining Effective Deterrence* (Carlisle Barracks, PA: Strategic Studies Institute, U.S. Army War College, 2003), vi.
[243] Ibid., vii.

be orchestrated to perform predictably and reliably should at last be discarded."[244] By that, he meant the vestiges of Cold War deterrence theory are inadequate to the task of deterring a rising breed of actors in the twenty-first century.

Despite the inadequacies, Payne recognized that "U.S. deterrence policies of the second nuclear age will be called on to prevent rogue challengers from initiating or escalating an attack against the U.S."[245] However, this new challenge facing the U.S. was different and in many ways far more complex than that of the Cold War. The difficulty of positively identifying an attacker, the origin of weapons, the nature of an attack, or the fact that an attack had taken place now proved more difficult.[246]

Under these conditions, what actor(s) should the U.S. threaten with punitive action? In this new era, there are many potential adversaries and limited confidence in attribution. The balance of terror construct, which required attribution, functioned well in the Cold War but now no longer applies. In this circumstance, the value of cooperation between the U.S. and other states is greater; therefore, the U.S. must be careful not to issue a "punitive retaliatory threat" against a state whose cooperation may be needed.[247] These factors caused scholars to wonder how the U.S. could effectively structure deterrence, as "it seems unlikely that U.S. leaders could confidently rely on policies of deterrence to convince a regional challenger to accept the possibility of military defeat on its

[244] Payne, *The Great American Gamble: Deterrence Theory and Practice from the Cold War to the Twenty-first Century*, 324.
[245] Payne, *Deterrence in the Second Nuclear Age*, 32–33.
[246] Payne, *The Great American Gamble: Deterrence Theory and Practice from the Cold War to the Twenty-first Century*, 361. Payne noted that relying upon the "indiscriminate broadcast of a generic threat to a generic audience of 'usual suspects'" lacked credibility and undermined confidence in deterrence.
[247] Ibid.

home soil and its own demise without resorting to its WMD."[248]

The debate that followed relied upon familiar scenarios and traditional responses re-emerged. For example, Dougherty and Pfaltzgraff suggested that "just as Cold War nuclear deterrence has rested upon the prospect of retaliation in response to aggression, post-Cold War deterrence could include denial."[249] This recommendation was theoretically on solid footing, yet it is prudent to recall, "The bipolar superpower deterrence relationship of the Cold War has been replaced by a group of states, and possibly eventually non-state actors."[250] This diverse range and larger number of state and non-state actors significantly changed the deterrence by denial calculus; however, this added complexity is insufficient to reject Dougherty and Pfaltzgraff's assertion.

The wide range of state and non-state actors is made up of those in which the U.S., in many cases, had less information than was available on the Soviet Union during the Cold War. Payne noted that a new priority question, "How much do you know" about an actor, replaced the old priority question "How much force is enough?"[251] The potential of new, possibly irrational actors about which the U.S. knows little undermined nuclear deterrence theory. Martel highlighted this challenge as he observed that some societies, "in particular revolutionary societies or leaderships, may be more likely to use nuclear weapons as we enter

[248] Payne, *Deterrence in the Second Nuclear Age*, 34.
[249] Dougherty and Pfaltzgraff, *Contending Theories of International Relations: A Comprehensive Survey*, 378.
[250] Ibid., 384.
[251] Payne, *The Great American Gamble: Deterrence Theory and Practice from the Cold War to the Twenty-first Century*, 305.

the twenty-first century."[252]

Deterrence remained a basis for stability, but its reliability was in question. This was particularly true given the U.S.' unfamiliarity with the leaders of both countries and non-state actors that it considered potential adversaries. With few shared assumptions or guaranteed communication channels, the U.S. is wise to anticipate "complex challenges and potential failure of deterrence in the post-Cold War environment."[253] From this challenge, the argument for the value of defense capabilities as a component of deterrence theory garnered much sway.

In the Cold War period, defensive systems "were criticized as destabilizing because they would allegedly lead the Soviet Union to build larger offensive forces."[254] In the second nuclear age, the opposite was true as limited U.S. defensive capabilities, to the extent they did not threaten Russia or China, deterred rogue actors with only a few nuclear weapons.[255] Stephen Cimbala's explanation, based upon the ideas of Clausewitz, that "the defensive form of warfare is intrinsically stronger than the offensive" may offer insight into why rogue state and non-state actors remain deterred from using nuclear weapons or weapons with radiological effects against the U.S.[256]

Cimbala argued that many scholars have been "misguided" to reverse Clausewitz's assertion on the supremacy of the defense. He noted that those who

---

[252] William C. Martel, "Deterrence and Alternative Images of Nuclear Possession," in *The Absolute Weapon Revisited: Nuclear Arms and the Emerging International Order* (Ann Arbor: University of Michigan Press, 1998), 227.
[253] Dougherty and Pfaltzgraff, *Contending Theories of International Relations: A Comprehensive Survey*, 384.
[254] Ibid., 385.
[255] However, in response to the Bush Administrations 2001 withdrawal from the ABM Treaty, Russia maintained a legacy position that U.S. missile defenses threaten their nuclear capabilities. This concern led the Russians to sign the 1972 ABM Treaty in the first place.
[256] Stephen J. Cimbala, *Strategy After Deterrence* (New York: Praeger, 1991), 179.

believe that "offense pays and defense is feckless" are wrong. Instead, he countered that because "offensive technologies are preeminent," then "defensive strategy pays dividends."[257] Further, Cimbala reasoned that if both sides have similar capabilities, then defense is easier than offense because its objectives, preservation and protection, are easier.[258] By extension, this assertion means that if both sides have dissimilar capabilities, then defense is even more inviting.

Aside from the implications of the renewed debate on defense, deterrence theory significantly shifted in response to the nature of the threat the U.S. faced in 2006. The 2006 Quadrennial Defense Review (QDR) introduced the concept of tailored deterrence. This theory moved the U.S. from a one-size-fits-all approach toward developing tailorable capabilities to deter advanced military powers, regional weapons of mass destruction (WMD) states, or non-state terrorists.[259] This theory capitalized on the implementation of the New Triad, which relied on nuclear and non-nuclear strike capabilities; a defensive leg comprised of active and passive defenses; and a responsive industrial infrastructure.[260] Yet, Elaine Bunn argued that capabilities beyond the New Triad were required to tailor

---

[257] Ibid., 207. Cimbala based this on the idea that "there is no bonus for preemption compared to awaiting attack and then retaliating." While referring to U.S./USSR calculus, this logic equally transfers to rogue state and non-state actors because the U.S. capacity for retaliation (assuming attribution is possible) makes the "hasty choice for war less likely." Cimbala offered two weaknesses of a defensive strategy: The promise of retaliation cannot limit the consequences of war should deterrence fail, and it does not offer flexible responses to anything short of war.

[258] Ibid., 211.

[259] David S. McDonough, "Tailored Deterrence: The 'New Triad' and the Tailoring of Nuclear Superiority" (Canadian International Council, March 2009), http://www.canadianinternationalcouncil.org/download/resourcece/archives/strategicd~2/sd_no8_200.

[260] IFPA-Fletcher Conference and Fletcher School of Law and Diplomacy, *Nuclear & Non-Nuclear Forces in Twenty-First-Century Deterrence: Final Report* (Cambridge, Mass: Institute for Foreign Policy Analysis, 2006), vi.

deterrence to an increasing number of diverse actors and circumstances.[261]

Incorporating conventional capabilities into nuclear deterrence strategy and policy occurred because of a revolution in military affairs realized by the advancement of conventional precision-guided weapons capabilities. This renewed a long-standing debate on the efficacy of conventional deterrence as the consensus began to emerge on the utility of deterrence by denial. All the while, these technological advancements evolved as the international structure continued a transformation that began with the end of the Cold War.

As the Cold War concluded, the assumptions that superpowers relied upon no longer provided stability in the post-Cold War world. As such, conventional deterrence emerged, which did little to undermine the value of deterrence theory. The literature – or rather seams in the literature – suggest additional work is required in the field to explain and address the demands stemming from the proliferation of new capabilities, such as those envisioned in cyber war and cyber attack. Of particular concern is how to deter state actors and non-state actor groups from employing malicious cyber capabilities to take advantage of vulnerabilities in target states.

Summary

Nuclear deterrence theory combines elements of punishment and denial to deter a potential adversary from initiating an attack with nuclear weapons. This

[261] M. Elaine Bunn, "Can Deterrence Be Tailored?" *Strategic Forum*, no. 225 (January 2007): 1. Bunn argued that "detailed knowledge of the society and leadership that we seek to influence" must be acquired. This required more than the New Triad; a tailored approach needed the "full range of military capabilities, presence, and cooperation, as well as diplomatic, informational, and economic instruments." Elaine Bunn is a Senior Research Fellow in the Institute for National Strategic Studies at the National Defense University.

section traced the historical evolution of nuclear deterrence by investigating the origin of the theory in the first wave and examining how it evolved through three subsequent waves. While many of the elements of this theory are consistent with those of criminal deterrence, the application is different for several reasons. The more prominent among these are the number of actors and the destructive potential of nuclear weapons.

The pool of actors with criminal justice deterrence encompasses at most the entirety of the population and at least that lesser subset of the population that is inclined to commit crimes. The pool of actors in nuclear deterrence is limited to those with nuclear weapons; initially there were two, and by the end of the Cold War, nine state actors possessed nuclear capabilities. Second, the destructive capacity of nuclear weapons created an imperative whereby every potential aggressor must be deterred, whereas in the criminal realm the stakes are far less as the "system can still be viewed as succeeding despite the failures of threatened sanctions."[262]

Next, this study presents the requirements for nuclear deterrence theory. The requirements to deter potential attackers, adopted from the overview of the four waves of nuclear deterrence theory, will add value in discovering clues that inform how to deter actors that use the cyber realm for malicious purposes. Because of the potentially devastating outcome, the requirements for nuclear deterrence are essential for states to use in a punishment approach to deter potential attackers. Additionally, as the threat of punishment may not deter all

[262] Wasserstrom, "War, Nuclear War, and Nuclear Deterrence," 443.

adversaries, the incorporation of the key requirements to deter by a denial component adds credibility to the theory.[263]

Requirements of Nuclear Deterrence Theory

The core components of nuclear deterrence theory are punishment and denial. The causal mechanisms of punishment are offensive, and they are actions taken by a state to ensure a desired response or necessary conditions that are required for the threat of effective punishment to take place. The causal mechanisms for denial are defensive in nature. See Table 2.4 for a summary of the requirements for nuclear deterrence to occur in theory.

There are nine requirements to deter by punishment in nuclear deterrence theory. These requirements are rationality, attribution, threat, communication, credibility, capability, will, transparency, and second strike. Rationality is a requirement because, for a threat to work, an adversary must have awareness of his value system and the capacity to understand available alternatives and determine risk.[264] An assumption resulting from the concept of rationality was that the U.S. and Soviet Union could avoid nuclear war if both parties made "correct choices."[265]

Attribution is necessary to identify whom to threaten to deter a nuclear attack or punish if deterrence fails. The threat itself is critically important and worked during the Cold War because it informed the USSR of what to expect in

[263] This is particularly the case in circumstances where non-state actors may acquire WMD as they may be less susceptible to be deterred by threats of retaliation.
[264] Schelling, *The Strategy of Conflict*, 6–13.
[265] Green, *Deadly Logic: The Theory of Nuclear Deterrence*, 158.

response to their choices from the U.S.[266] The U.S. relied upon the threat of punishment to induce in the Soviet Union the inclination to refrain from initiating a nuclear attack. The use of a threat of punishment had value for two reasons. First, the threat had the potential to ensure deterrence; however, if deterrence failed, the threat made it clear that the U.S. had the capacity to carry out the retaliation that it promised.

For the threat to work, additional conditions were necessary. These conditions are sufficiently important that they meet the threshold as requirements for nuclear deterrence theory.[267] First, the U.S. threat of punishment required communication of its threat of punishment to the USSR. For this communication to be effective, the U.S. had to deliver the threat and the USSR had to receive and understand the message inherent in that threat.

The requirements for effective deterrence went beyond the act of communicating a well-designed threat to a rational adversary. Jones noted that "one cannot fear something which one knows will never happen."[268] Therefore, the U.S. threat had to be credible, which meant that the Soviet Union had to believe the U.S. would follow through. For this to happen, effective deterrence required that the U.S. possess the capability and political will to carry out its threat. Further, this required transparency of U.S. capabilities because the Soviet Union had to have visibility into the U.S. capacity to fulfill the commitment

[266] Schelling, *The Strategy of Conflict*, 10.
[267] The researcher considered conditions to meet the criteria as requirements if their omission would result in an outright failure of nuclear deterrence theory. Subjectivity was involved in process; however, the literature in each case supports inclusion of these conditions as requirements.
[268] Jones, *Nuclear Deterrence*, 20.

inherent in the threat.[269]

Last, second strike capability was a requirement to impress upon the Soviet Union that the U.S. could retaliate if attacked. Early scholars determined that this was the "first and most vital" action the U.S. should pursue to guarantee retaliation.[270] Schelling's argument for the U.S. to protect its ability to conduct a second strike to respond to Soviet nuclear aggression with nuclear weapons instead of protecting the U.S. population was the central idea that bolstered the deterrence concept of mutually assured destruction.[271]

Later nuclear deterrence theory evolved to incorporate denial by defensive means to prevent a rogue actor from attacking the U.S. and/or allies with a limited nuclear attack. The value of defense resulted from a combination of the capability to deny and the ability to lessen war damage.[272] The capability to deny an adversary an unobstructed avenue results by reducing vulnerabilities though hardening, dispersing, and concealing U.S. capabilities. However, the requirements for deterrence by defense extend beyond the establishment of barriers and protective measures. Because nuclear weapons have both an offensive and defensive component, the threat of retaliation is a deterrent to a potential adversary's first strike, while the actual use of a nuclear weapon to strike back after an adversary has attacked first is a defensive action.[273] The capacity to strike back requires a lessening of anticipated war damage to preserve the survivability of the retaliatory force.

---

[269] Schelling, *The Strategy of Conflict*, 40.
[270] Brodie, *The Absolute Weapon*, 107.
[271] Schelling, *The Strategy of Conflict*, 233.
[272] Snyder, *Deterrence and Defense*, 4–5.
[273] Ibid., 85.

Table 2.4: Requirements of Nuclear Deterrence Theory[274]

Core Components	Causal Mechanisms	Purpose	Requirements	Rationale
Punishment	Offensive	Threat of punishment increases adversary's costs	Rationality	Adversary must have awareness of his value system and the capacity to understand available alternatives and determine risk
			Attribution	Necessary to identify whom to threaten or punish if deterrence fails
			Threat	Must be issued and received
			Communication (of threat)	Must be clear and understood by receiving party
			Credibility (of threat)	Must be believable, which requires capability and will
			Capability (offensive)	Adversary must know the capacity exists to make good on a threat or promise of retribution
			Will	Adversary must know that the promise of a threat or retaliation will be acted upon
			Transparency	Adversary must know that the capability exists to fulfill the promise of a threat or retaliation
			Second Strike	Adversary believes retaliation in-kind is possible after an attack
Denial	Defensive	Deny benefits	Capability to deny	Reduce vulnerability by hardening,

[274] The requirements for punishment were subjectively derived from the evolution of nuclear deterrence theory. The researcher believes that the literature provides sufficient evidence that each of these factors meet the standard for inclusion as a requirement. A requirement is defined as a "something obligatory or demanded, as a condition" or "something needed." See *Webster's New World College Dictionary*, 1218.

Core Components	Causal Mechanisms	Purpose	Requirements	Rationale
				dispersal, mobility and concealment
			Ability to lessen war damage	Preserves survivability of retaliatory force

Chapter Summary

This chapter introduced deterrence literature that establishes a foundation for cyber deterrence. It highlighted the predominance of deterrence by punishment, which requires a threat, attribution, and an offensive capability. Deterrence by denial, which relies upon defensive capabilities, also featured prominently. The perspective gained from studying the historical evolution of each theory took the researcher beyond the task of solely gathering requirements to gain a deeper level of insight into these theories that will prove invaluable in determining the bases for cyber deterrence theory.

Chapter 3: Cyber Deterrence Theory

Deterrence in this field is different from any other. It will not function as it did during the Cold War ...

– General Keith B. Alexander[1]

Introduction[2]

This chapter builds upon basic deterrence theory, criminal justice deterrence theory, and nuclear deterrence theory presented in the previous chapter to help us understand the requirements for a theory of cyber deterrence. Just as nuclear deterrence theory was shaped by the preceding centuries of criminal justice deterrence theory, so too is cyber deterrence shaped by these theoretical predecessors. In cyber deterrence theory, deterrence by cooperation emerges as a core theoretical component. Cooperation requires interdependency between

[1] *Statement of General Keith B. Alexander* (Washington, D.C.: House Committee on Armed Services, n.d.), 5.

[2] This section examined the works of scholars who use different terminology to explain similar phenomena, which may invite criticism that this study is comparing "apples with oranges." While definitions are important, focusing attention on the differences between cyber war, strategic information warfare, information warfare, and information operations does not matter in this study's approach to examining the literature to better understand the requirements of deterring cyber war. This researcher believes that cyber war, strategic information warfare, and information warfare have similar meanings, with the exception that cyber war is a more encompassing term than the other two, which is a view that reverses the commonly held position that cyber is a subset of information operations. As presented in the introduction, cyber war is the continuation of state policy by cyber means. Strategic information warfare is the "means for state and nonstate actors to achieve objectives thought digital attacks on an adversary's center of gravity"; see Gregory J. Rattray, *Strategic Warfare in Cyberspace* (Cambridge, MA: MIT Press, 2001), 14. Information warfare has a range of definitions "from those narrowly focusing on the improved used of electronic means to achieve advantage on conventional battlefields to very broad definitions conceptualizing information warfare as any effort to affect information systems in peacetime"; see Rattray, *Strategic Warfare in Cyberspace*, 9. Information operations consist of a subset of capabilities that an actor may use in cyber, strategic information, or information warfare. Information operations (IO) are "the integrated employment of electronic warfare (EW), computer network operations (CNO), psychological operations (PSYOP), military deception (MILDEC), and operations security (OPSEC), in concert with specified supporting and related capabilities, to influence, disrupt, corrupt, or usurp adversarial human and automated decision making while protecting our own"; see Joint Chiefs of Staff, *Joint Publication 3-13: Information Operations* (Washington, DC: Joint Chiefs of Staff, 2006), ix.

actors and norm creation to foster international agreements in a triadic construct with punishment and denial.[3] The combination of the evolution of punishment and denial as central features of these theories, the perspective gained from studying the historical evolution of each theory, and the new ideas that emerged in establishing a basis for cyber deterrence results in a core set of requirements that help forge a theory of cyber deterrence.

The characteristics of cyber and nuclear capabilities are distinguishable for five reasons. First, the nature of the weapons and their effects are vastly different. Second, there are differences in the spatial scale in which actors employ these capabilities. Third, there are temporal differences in the duration of attacks and the lingering effects. Fourth, exhibitions of heroism and bravery are not likely a factor in the cyber domain. Lastly, a diffusion of decision making is more prevalent in cyber operations.[4] Despite these differences, the theoretical underpinning of cyber deterrence, as with nuclear deterrence, rests upon the

[3] Amit Sharma, "Cyber Wars: A Paradigm Shift from Means to Ends," in *The Virtual Battlefield: Perspectives on Cyber Warfare* (Amsterdam: Ios Press, 2009), 14–15. Sharma uses the phrase "cyber triad" and identifies the three components as "regular defence/military assets and networks," an "isolated conglomerate of air-gapped networks situated across the friendly nations as part of cooperative defence," and a "loosely connected network of cyber militia involving patriotic hackers, commercial white hats and private contractors." Amit Sharma is Deputy Director/Scientist C in the Institute for System Studies and Analysis, Defence Research and Development Organization, Ministry of Defence, Government of India. Retired U.S. Air Force Lt. Gen. Harry Raduege also describes a cyber triad consisting of resilience, attribution, and offensive capabilities, see Andrew Nagorski, ed., *Global Cyber Deterrence: Views from China, the U.S., Russia, India, and Norway* (EastWest Institute, 2010), 4, http://www.ewi.info/system/files/CyberDeterrenceWeb.pdf.

[4] Wasserstrom, "War, Nuclear War, and Nuclear Deterrence," 426–427. This list was adapted from Wasserstrom's essay on ethics in which he compared criminal and nuclear deterrence.

capability to deter by punishment and denial, although enhancing international cooperation and the formation of new norms may add value.[5]

It is possible that cyber deterrence theory holds greater promise than nuclear deterrence theory. This may be the case given the paradox of nuclear deterrence in which "carrying out of the threatened response, when the threat has been unsuccessful as a deterrent, lacks sense as well as justification."[6] In the case of cyber, fulfilling a threat of retaliation may be justified and make perfect sense. Wasserstrom's indictment aside, early cyber scholars debated and came to differing conclusions on the utility of cyber deterrence based largely upon the Cold War nuclear experience.

An initial wave of cyber deterrence scholarship formed after the Cold War and continued until a second wave emerged after the 2007 Russia – Estonia cyber war. The next section examines this first wave by considering the views of scholars who relied upon the nuclear experience to inform early approaches to cyber deterrence. Subsequently, the study evaluates the positions of those who determined cyber deterrence to be problematic or irrelevant. Before transitioning to the second wave theorists, an introduction of early U.S. cyber deterrence policy provides context for second wave policy, which included the first declaration of cyber deterrence as U.S. policy. Cooperation in cyber war is then considered prior to concluding this chapter with a presentation of the major requirements that serve as a basis for cyber deterrence theory, which have emerged from criminal

[5] As we saw in the previous chapter, cooperation took place between the U.S. and USSR. The cooperation between these nuclear adversaries was essential to the range of treaties and agreements that were essential to deterrence during and after the Cold War.
[6] Wasserstrom, "War, Nuclear War, and Nuclear Deterrence," 438.

justice deterrence theory, nuclear deterrence theory, and the work of scholars in the initial and second waves of the Digital War era.[7]

The Initial Wave of Cyber Deterrence

The initial wave began when the term *cyber deterrence* first appeared in a 1994 article of *Wired Magazine* by Professor James Der Derian.[8] The first wave continued until 2007, when the cyber war between Russia and Estonia brought greater awareness to the cyber challenge, thus initiating a second wave of scholarship and policy that laid a foundation for cyber deterrence theory. In the initial wave, cyber deterrence literature did not move beyond a formative stage. This is not unlike the first wave of scholarship in the Cold War that paved the way for the following waves of theorists that refined Cold War nuclear deterrence theory.

The purpose of this first section is to understand how cyber deterrence evolved in the first wave and to draw upon this scholarship to help form a concise list of cyber deterrence requirements to aid in the research objective of developing a theory of cyber deterrence. The next section examines the work of scholars who drew upon nuclear deterrence to shape their position on cyber deterrence.

---

[7] The Digital War era refers to the period encompassing the initial and second wave of cyber deterrence theory, which began in the mid-1990s and continues to the date of this study. A continuum of cyber activities at the state-level have existed such that the traditional terms *peace* and *war* fall short in capturing the interaction between states in the cyber domain. During this period, major powers have either prepared for cyber war or engaged in overt or covert cyber attacks that have culminated in cyber war or the realization of state objectives without engaging in cyber war. This definition does not suggest that alternative periods of armed aggression, such as the U.S. post-9/11 "terrorism wars," do not also warrant separate distinction.

[8] Will Goodman, "Cyber Deterrence: Tougher in Theory Than in Practice?" *Strategic Studies Quarterly* 5, no. 4 (Fall 2010): 103. In 2010, Will Goodman served as an "adviser on defense and veterans issues to Senator Patrick Leahy." Previously, as the "assistant for plans to the assistant secretary of defense for homeland defense and America's security affairs, he oversaw operational and contingency plans, participated in national-level exercises, and managed several counterterrorism portfolios."

Immediately following is a section that contrasts these views with scholars who concluded that the concept of cyber deterrence is problematic. In reviewing this literature, the reader is asked to consider that the prospects of cyber war and major cyber attacks were not figments of overactive imaginations but manifestations of legitimate international and domestic concerns that emerged in the mid-1990s. In the ensuing years, debate continued with no resolution regarding the value of using nuclear deterrence theory as a model for cyber deterrence to counter these threats.

Cyber Deterrence Shaped by the Nuclear Experience

Wheatley and Hayes concluded, "Some information warfare attacks on the United States are deterred by the same policy that deters other types of attack"; however, they conceded that an information warfare capability is unlikely to form a credible deterrent on its own.[9] Yet, as with nuclear deterrence, the cyber iteration requires an actor who seeks to deter a targeted actor. Similarly, a range of requirements exists that are strikingly similar to many of the conditions necessary for nuclear and criminal justice deterrence. Wheatley and Hayes offered the following requirements for cyber deterrence.[10]

- A threat to something of value that exceeds the perceived gain of non-compliance
- A clear statement of the behavior to be avoided or performed

[9] Richard E. Hayes and Gary F. Wheatley, *Information Warfare and Deterrence* (National Defense University, 1996), https://www-hsdl-org.ezproxy.library.tufts.edu/?abstract&doc=14452&coll=documents&url=https://www-hsdl-org.ezproxy.library.tufts.edu/homesec/docs/dod/nps08-100603-06.pdf. Wheatley and Hayes noted that IW has grown to become a "catch-all" term that encompasses many activities long associated with competition, conflict, and warfare, such as propaganda (including Media War), Deception, C2W, EW, and PSYOPs. Dr. Hayes is President, Evidence Based Research, Inc. Rear Admiral Wheatley, USN (Ret.) was a Program Manager at Evidence Based Research, Inc.

[10] Ibid.

- Clear and unambiguous communication of the threat and the desired or proscribed behavior to the target
- Credible threat, meaning that the target believes the actor has the will and capability to execute the threat
- Situational constraints that make it impossible for the target to avoid punishment
- Controllability of the threat and its implications by the actor

Wheatley and Hayes' first requirement described rationality, and the second suggested a partial definition of a threat. Communication and credibility share a commonality with nuclear deterrence, while situational constraints and controllability are more appropriate solely for cyber deterrence.

Wheatley and Hayes were concerned that over time some Cold War-era scholars may "bring extraneous concepts or baggage" to the debate.[11] This was due in part to the fact that there were no simple solutions and thus some scholars may be tempted to rely upon what they know irrespective of the demands of this new domain. For example, an over reliance on punishment may be detrimental to cyber deterrence theory as U.S. cyber offensive capabilities have major limitations when compared with the offensive potential of nuclear weapons. In addition, detractors of nuclear deterrence by denial may confer the same sympathies upon cyber deterrence by denial. Such "baggage" could undermine the promising aspects of denying an adversary access to critical U.S. systems by defensive means.

While defensive measures only gained favor late in the Cold War and afterward, their value in cyber deterrence was considerable from the start. Nuclear deterrence-inspired defensive requirements are equally valid in cyber deterrence as the "beginning point for deterring attacks on important computer

[11] Ibid.

systems" came from a "visible set of defenses." Wheatley and Hayes proposed seven defensive measures that should be at the core of a cyber deterrence by denial approach:[12]

1. Systems Vulnerability Analysis
2. Systems Hardening
3. Security Training
4. Redundancy and Backup
5. Aggressive Law Enforcement
6. Tagging Hardware and Software with Electronic ID
7. Embracing (Systems Interdependency with Potential Attackers)[13]

Timothy Thomas adopted an approach to cyber deterrence similar to that of Wheatley and Hayes in that he believed that information technologies and nuclear technologies were comparable; however, he moved beyond punishment and denial approaches to consider the value of cooperation between states. Thomas focused his effort on the threats to information systems and offered several means to deter information assaults. Deterring these assaults was important because attacks against "information technologies and capabilities

[12] Ibid.
[13] Ibid., 13. Embracing means to engage "potential attackers by including them as stakeholders." The authors argue that adversaries that have been embraced and educated are "less likely to consider attacks." Because of the interdependency of the global information system, embracing potential attackers and convincing them avoid self-harm could help deter cyber attacks that unleash cascading effects.

could prove to be as destructive to state sovereignty and the well-being of the citizens of any state as the kind of armed assault feared during the Cold War."[14]

Thomas characterized the main threat to information systems as an "adversary's ability to alter, replace, or delete the information stored or generated by these systems and to influence the processes by which it is managed."[15] He identified five elements of this threat.[16]

1. Advanced information technologies are required if one is to disrupt the integrity of information systems
2. The absence of legal mechanisms
3. The emergence of new methods to manipulate perceptions, emotions, interests, and choices
4. The speed with which information assaults can be conducted
5. The availability of masses of information to anyone who wants it

These elements help to distinguish vulnerabilities associated with the threats that exist in the cyber domain, which are less a factor in nuclear and criminal justice. By understanding these vulnerabilities and others, the requirements for cyber deterrence theory are best determined.

Thomas observed that unlike during the Cold War, when the U.S. and Russia maintained strong control over nuclear weapons, there is a vast range of actors with the means to spread computer viruses and exploit computer systems.

---

[14] T.L. Thomas, "Deterring Information Warfare: A New Strategic Challenge," *Parameters* 26, no. 4 (1996): 9–10. Thomas offered a definition of deterrence to counter information assault: "The ability through international law, specific applications of information technologies, or the monitoring of 'perception management' to deter an information assault on the territory of a sovereign state"; see page 6. Thomas drew upon an National Defense University definition of information warfare: "actions taken to preserve the integrity of one's own information systems from exploitation, corruption, or destruction while at the same time exploiting, corrupting, or destroying an adversary's information systems and in the process achieving an information advantage in the application of force," see page 2. Tim Thomas, LTC (Ret.) serves in the Foreign Military Studies Office at Fort Leavenworth, Kansas.

[15] Ibid., 3–4.

[16] Ibid., 4–5. Thomas expanded on the first point to include the requirement to "defeat an opposing force or damage a state infrastructure through information warfare (satellite surveillance systems, global navigation systems, commercial communications, and satellite systems)."

Control is not centralized, and there is no government with a monopoly on cyber capabilities; therefore, the "means to detect, control, and respond to such intrusions need to be developed far beyond those required by the nuclear threat."[17] Thomas offered four means to deter information assaults:[18]

1. International legal aspects need to be negotiated to avoid the potential of escalation.
2. Agreements must be brokered that limit technological advancements (digitalization, miniaturization).
3. States need to establish a crisis management early warning system to address attacks after they are detected.
4. States must nurture the "growing business of transnational relations."

All of these require cooperation between states. Thomas' ideas bolster the inclusion of cooperation with punishment and denial as the core components of a triadic approach to cyber deterrence theory.

Roger Barnett elaborated on punishment and denial, filling in some of the theoretical gaps left by Wheatley and Hayes. He focused on the role of will in the punishment calculus and the necessity of deterrence by denial. Regarding deterrence by both punishment and denial, he suggested that the U.S. needed to articulate a deterrence policy that communicated the "willingness of the United States to play an active role in information operations across the board."[19]

Barnett, in considering U.S. will, observed that an adversary had to be rational because "For deterrence to be effective, it suffices that an adversary believe that he will be worse off – perhaps much worse off – for undertaking a

[17] Ibid., 7.
[18] Ibid., 8.
[19] Roger W. Barnett, "Information Operations, Deterrence, and the Use of Force," *Naval War College Review* 50, no. 2 (1998): 7. Roger Barnett is a professor of naval warfare studies at the Naval War College.

particular action than for not attempting it."[20] This meant that an adversary has to have the capacity to weigh benefits and costs and then make a decision based on the risk associated with the available options. An important aspect of this calculation for a potential cyber miscreant revolves around U.S. willingness to respond to an attack.

A state can communicate will by a declaration of policy or a demonstration of capability. The U.S. at this point (1998) in the initial wave had exhibited neither publicly. Barnett took exception with this because U.S. information operations capabilities were not the issue. The problem was lack of a perception of U.S. will by adversaries, as without will, there is no certainty of retaliation and the latter is what deters with a deterrence by punishment approach.[21]

If an adversary does not fear punishment because will is lacking, then a state must deter by denial. This requires strong defenses to deny adversaries the opportunity to reach their objectives with a first strike. Barnett recommended four requirements to defend against an information attack:[22]

1. Identification and authentication mechanisms
2. Well-trained and disciplined systems operators
3. High assurance firewalls
4. Auditing and trace-back methods

Problems for deterrence arise when one considers that U.S. defenses against information operations are weak. The nation's "vulnerability to the information

[20] Ibid., 4.
[21] Ibid., 4–5.
[22] Ibid., 3.

operations of others [is] considerable" because the U.S. "will to act" and "defenses [are] weak, or perceived as weak."[23]

Howard Lipson recognized the weakness of the defense and advocated a deterrence by punishment approach. He believed that only through a threat of retaliation or some other punishment could a deterrent effect take place.[24] Lipson isolated attribution as a precondition to punish an attacker; however, determining the origin of an attack is a difficult requirement to achieve. In spite of the difficulty, he noted that a nation's capability to "track and trace" the origin of any cyber attack was key to effective deterrence and a "nation's long-term survival and prosperity."[25]

The challenge in identifying a specific actor for the deterring state to punish is extremely difficult because "track and trace capabilities are primitive compared with the capabilities of attackers."[26] Well-designed attacks are nearly impossible to trace, with certainty, to a point of origin. While there have been gains and the research is promising, the capability to attribute offered "accountability, redress, and deterrence" but was neither a panacea nor a "substitute for robust, well-engineered, secure, and survivable systems."[27]

---

[23] Ibid., 4.
[24] Howard F. Lipson, *Tracking and Tracing Cyber-Attacks: Technical Challenges and Global Policy Issues* (CERT Coordination Center, November 2002), 20, http://www.sei.cmu.edu/reports/02sr009.pdf. Howard F. Lipson is a "senior member of the technical staff in the CERT Program in the Software Engineering Institute at Carnegie Mellon University. Lipson has been a computer security researcher at CERT for 18 years."
[25] Ibid., 3. The purpose for tracing attacks is to deter future attacks by punishing the actors that originated them. "To accomplish this, a direct link must be drawn between the IP address of the machine that originated the attack and the individual or entity that set the attack in motion." However, it is difficult to link IP addresses of machines to actors; see pages 18-19. The link between an IP address and an actor can be nearly obscured by using mobile devices and services; see page 20.
[26] Ibid., 63.
[27] Ibid., 64.

Geoffrey French concurred with his predecessors that cyber deterrence could be effective even though difficult challenges remained. He argued that the U.S. could mitigate some of these challenges by tailoring cyber deterrence. His work moved the debate forward and was a significant development as previously most scholars took a punishment or denial approach with no distinction between types of actors.

French believed that the U.S. could deter strategic information warfare (SIW) attacks by countering the capabilities and motivations of adversaries with strategies tailored specifically for that class of actor (see Table 3.1).[28] His logic depended upon an acceptance of the position that the U.S. had to rely on deterring cyber attacks instead of detecting and then defeating attacks to protect critical information infrastructure. However, with this approach, the U.S. faced a "conundrum of deterring an ability that an adversary developed to counter U.S. strength."[29] French's idea of a aligning a "specific type" of deterrence tailored to capabilities of potential adversaries meant that the U.S. had to better understand a diverse range of actors, the essence of strategic cyber attacks, and the capabilities needed to deter these attacks.[30]

French identified the forms of deterrence and the tools needed to tailor deterrence for a range of actors with diverse capabilities. He accounted for the

[28] G.S. French, *Building a Deterrence Policy Against Strategic Information Warfare* (DTIC Document, 2002), 13, http://www.dodccrp.org/events/2002_CCRTS/Tracks/pdf/061.PDF. French defined strategic information warfare attacks as those against the information technology base of a nation's critical infrastructure; see page 1. Geoffrey S. French is a "Program Manager for CENTRA Technology, Inc. who has supported the Federal Bureau of Investigation, the Department of Defense, and the Department of Homeland Security in counterintelligence, infrastructure protection, and risk analysis since 1999."
[29] Ibid., 4.
[30] Ibid.

potential adversaries that the U.S. is likely to face in the cyber domain from state and non-state actors. For each of these, he identified whether punishment, denial, or some combination would be effective. He recommended that a powerful state in deterring a peer had to remove the incentive to attack, while deterring lesser states required an emphasis on escalation under the deterrence by punishment approach. French identified "components of need" that informed requirements for cyber deterrence; examples of these are communication, credibility, and intelligence.

Table 3.1: Strategies Most Likely to Deter SIW Attacks[31]

Adversary	Form	Tool	Component of Need
Major power	Removing incentive	High-level policy discussions and exchanges	Communication
Minor power	Punishment	Emphasis of escalation	Credibility
Rogue state	Denial	Improved security of select civilian infrastructures	Intelligence
Terrorist group	Denial and punishment	Improved security of select civilian infrastructures Emphasis of willingness and ability to pursue and punish	Applicability

French recognized that this tailored approach would not be easy because the Internet and the U.S. information infrastructure were not built with security in mind. Nevertheless, it required a high priority. The U.S. government, particularly the U.S. Department of Defense (DoD), recognized this need and began to transform to address these challenges in the early part of the twenty-first century.

[31] Ibid., 13.

In 2002, Secretary of Defense Donald Rumsfeld assigned to U.S. Strategic Command (USSTRATCOM) a wide range of responsibilities beyond its traditional nuclear deterrence mission. The command's new missions were global strike; global missile defense; global command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR); and integrated information operations (for DoD only). Admiral James Ellis, Commander USSTRATCOM, in addressing his responsibility for global information operations, noted that this could include "everything that we can bring to bear as a nation." [32] Ellis postulated that eventually military commanders might write annexes to plans that support IO. Ellis saw the same potential for deterrence in the cyber realm as the first wave scholars who were sympathetic to this approach. He said that these new threats, which include information operations, can be deterred and that the "concepts of deterrence still apply." Because Ellis served as the commander for all U.S. nuclear forces, it is reasonable to assume that he meant that some concepts of nuclear deterrence are applicable to cyber deterrence.[33]

USSTRATCOM's early effort in cyber deterrence was not without criticism. Worden and Correll identified several barriers that were impediments to change, which where inherent in USSTRATCOM's early cyber culture: lack of strategic analysis, lack of necessary capabilities, and organizational inertia

[32] Jason Ma, "Information Operations to Play a Major Role in Deterrence Posture," *Inside Missile Defense*, December 10, 2003, http://www.lexisnexis.com.ezproxy.library.tufts.edu/hottopics/lnacademic/?verb=sr&csi=285572.
[33] Ibid.

oriented more toward warfighting than prevention.[34] Because of this entrenched culture, Worden and Correll advocated for a distinct "Information Corps" to train, organize, and equip cyber operators.[35]

USSTRATCOM provided an operational focus, while a new strategic approach was needed, an approach that sought to "create effects in the minds of [U.S.] adversaries" beyond network attack and defense.[36] One key feature of an alternative approach was to increase cooperation as a means to prevent attacks. Historically, the U.S. avoided cooperation in the information realm because the capabilities of U.S. intelligence collection were too "sensitive to share." [37]

The authors in the first wave who supported cyber deterrence drew from the requirements of nuclear deterrence to make their respective cases for the value of punishment and denial. Some concluded that deterrence by prevention and cooperation added value. In the initial wave there were also leading scholars who considered cyber deterrence problematic or irrelevant. The following section surveys the literature that captured these views.

The Problem with Cyber Deterrence

Martin Libicki argued that deterrence of attacks against U.S. information systems is problematic. He suggested that a deterrence policy that included specifics would offer little gain given the cost. Libicki explained that it was already the case that any actor harming the U.S. expected retaliation. Further, because the U.S. has not declared the amount of retaliation that an act of harm

[34] S.P. Worden and R.R Correll, *Responsive Space and Strategic Information* (National Defense University: DTIC Document, 2004), 1–2.
[35] Ibid., 8.
[36] Ibid., 1.
[37] Ibid., 3.

warranted, a specific cyber deterrence policy may result in retaliation followed by escalation against an actor that could prove imprudent. In short, an attacker's identity mattered, and blindly committing to a policy of retaliation invited greater harm. Retaliating against the wrong party "weakens the logic of deterrence" and "makes a new enemy.[38]

Libicki hedged in that he did not cite cyber deterrence as irrelevant. Instead, he suggested that if information warfare "comes into its own," the deterrence calculus will "have to be rethought, not simply ported from familiar but misleading terrain."[39] He explained that aside from deterrence, the U.S. can use denial and detection (with prosecution) to defend its critical information systems. However, denial and detection are "less than satisfactory" as the former merely "frustrates attacks by preventing them" and the latter when combined with prosecution only takes the "attacker out of circulation" for an indeterminable amount of time. Libicki concluded that defenses are good only to a certain extent because they are unable to stand up to a full-scale attack by a determined nation.[40]

Libicki outlined five elements of deterrence that he used to isolate the problems a state would encounter in trying to deter information attacks. Libicki critiqued these elements in sequence by highlighting the challenges posed by

---

[38] Martin C. Libicki, *Defending Cyberspace and Other Metaphors* (National Defense University, 1997), 41-43, http://www.hsdl.org/?view&did=446854. Martin Libicki is a senior management scientist at the RAND Corporation.

[39] Ibid., 63. Libicki called deterrence and graduated response Cold War "leftovers." He said, "If information warfare is regarded as an aspect of strategic warfare, they may well be (leftovers)." See page 42.

[40] Ibid., 41.

cyber deterrence. The first three elements pertain to explicit deterrence and the remaining two are applicable to deterrence in kind.[41]

1. The incident must be well defined
2. The identity of the perpetrator must be clear
3. The will and ability to carry out punishment must be believed
4. The perpetrator must have something of value at stake
5. The punishment must be controllable

Regarding a state's effort to define an incident, Libicki noted that a nuclear event would be obvious and a response clearly actionable, while hacker attacks are numerous and generally more of a nuisance and thus trivial.[42] Next, attribution or determining the perpetrator in an information attack is difficult. Rarely can a state trace back an attack with certainty, and if a suspect is determined, linking that suspect with a sponsoring government is "hardly guaranteed."[43] If the U.S. retaliated without proof, it then appears to be the aggressor.

Third, the will and capability to carry out punishment, which reflects on the certainty of response in deterrent policy, "presumes incident and response are tightly linked."[44] This is a difficult process, made more so because the U.S. does not immediately recognize all attacks. Even when an incident is evident, the lack of timely attrition or failure to attribute lengthens the time between the incident and response, which reduces the credibility of the deterrer's threat of retaliation.

[41] Ibid., 44. Libicki borrowed these five elements from Richard Hayes. *Explicit* means that the deterrence policy is communicated to the potential attacker. *In kind* refers to a tit-for-tat approach using similar means to retaliate with a similar effect.
[42] Ibid., 46.
[43] Ibid., 49.
[44] Ibid., 51.

On the latter two elements, Libicki questioned the value of a retaliatory policy that promised a response. He argued that the U.S., or any state, that does not build flexibility into its deterrent posture makes a serious mistake because the identity of the attacker matters. Unlike the circumstances of the Cold War, in information warfare, "there is no canonical foe and no lesser case."[45] As noted earlier, this risks a confrontation that may be unwanted.

The final element, controllability, tends to support not retaliating in kind. Controllability, the ability to predict the scope of a response, is difficult. Because it is impossible to gauge the effect of potential retaliatory action, "graduated response is almost meaningless," thus calling into question the capacity to control escalation.[46] Libicki's assessment that IO deterrence is problematic contained a hedge; in the future circumstances may warrant a "rethinking" of the subject. Richard Harknett was far more critical in his evaluation of cyber deterrence.

Harknett concluded that Cold War deterrence provided "poor guidance" for deterring information warfare. He argued that information warfare is better "understood in the context of offense and defense."[47] During the Cold War, deterrence became prominent, and offense and defense provided support. The idea of conflict between great powers evolved to become something to avoid because of nuclear weapons. Prior to the Cold War, powerful states avoided war by having a robust offense and the capacity to defend. In this earlier era, offense and defense dominated, with deterrence relegated to the role of a by-product at best.

---

[45] Ibid.
[46] Ibid., 45–46.
[47] Richard J. Harknett, "Information Warfare and Deterrence," *Parameters* (1996): 93.

There are two types of information warfare: net war and cyber war. Harknett argued that net war and cyber war are better suited to offense-defense models than deterrence. This is because efforts to incorporate information warfare into the deterrence framework "miss what is distinctive about these new form of conflict – the contestability of connectivity."[48] In cyber war, connectivity is a key because "deterrence strategy will have to overcome the problem of contestability." This means that in cyber war, the upper hand will go to the party that controls the electromagnetic spectrum as this provides an "enhanced ability to see, decide, and move at a pace that should overwhelm adversaries."[49] Harknett believed that this new form of conflict requires an offense and defense rather than a deterrence approach because networked military operations will depend on connectivity and therefore adversaries will attack that connectivity.[50]

Regarding, net war, the utility of deterrence is more limited than cyber war. This is partly due to the focus net war places on societal connectivity, which is susceptible to personal, institutional, and national-level attacks.[51] Harknett reasoned that an attack on any of these levels that destroyed only information was not susceptible to retaliation in kind.

---

[48] Ibid., 104. Harknett relied on John Arquilla and David Ronfeldt to define *net war* as "information-related conflict at a grand level between nations or societies. It means trying to disrupt, damage, or modify what a target population knows or thinks about itself and the world around it." They define *cyber war* as "conducting, and preparing to conduct, military operations according to information-related principles. It means turning the 'balance of information and knowledge' in one's favor." Harknett describes connectivity in regards to the information technology network as the seamless joining of its parts in a manner that creates shared situational awareness throughout an organization. See pages 93-95. Professor Harknett is the Faculty Chair at The Charles Phelps Taft Research Center, University of Cincinnati.

[49] Libicki, *Defending Cyberspace and Other Metaphors*, 99–100.

[50] Harknett, "Information Warfare and Deterrence," 100. Harknett argued that deterrence is not suited to net war because deterrence theory depends upon retaliation in kind.

[51] Ibid., 101.

A state cannot without great difficulty deter or dissuade a potential adversary when there is little the deterring state can hold at risk.[52] Harknett postulated that connectivity may provide an answer to this dilemma, but there are three problems. First, this assumes that there is a similar dependence and societal value placed on connectivity by the deterring and deterred state. Second, there is the potential for adverse effects on the deterrer due to the lack of geographical boundaries in net war. Lastly, there is a tremendous problem in relying upon a deterrence by punishment approach directed toward state actors because an attack may come from non-state actors.[53]

Harknett's criticism of deterrence rested on the "contestability of connectivity." He argued that scholars who attempt to use nuclear deterrence or other strategic approaches miss this distinctive feature of information warfare.[54] Stephen Blank followed Harknett's path as he also failed to see the usefulness of deterring information warfare.

Blank concurred with Libicki and Harknett that deterring IW is impossible with existing capabilities and deterrence concepts.[55] He expanded upon Harknett's critique with a series of arguments that Harknett either ignored or overlooked. Blank's summation of the debate was:[56]

1. Because IW counters C4ISR, this causes a state to use or lose deterrence capabilities as command and control may be lost.

---

[52] Ibid., 102.
[53] Ibid., 102–103.
[54] Ibid., 104.
[55] Stephen Blank, "Can Information Warfare Be Deterred?" *Defense Analysis* 17, no. 2 (August 2001): 121. Blank defined information warfare as "attacks against information networks and against the informational component of weapons systems"; see page 131. Stephen Blank is Professor of Russian National Security Studies at the Strategic Studies Institute of the U.S. Army War College.
[56] Ibid., 125–126.

2. Because attribution is difficult, the threat of retaliation is diminished.
3. IW occurs in peace and war, and as IW is ongoing, there is no distinction between peace and war, which is necessary to deterrence.
4. IW is a peacetime occurrence; it is impossible to determine if a peer state or individual hacker initiated an attack, thus complicating a proper response.
5. U.S. efforts to develop cooperative security arrangements require transparency and confidence building measures. Because information often becomes corrupted, the whole process is compromised and then both sides will likely relapse into worst-case scenarios and unyielding mutual suspicion. These negative perceptions and suspicions may hasten rather than prevent conflict.
6. Information has transformed the battlefield to a point where the distinction between the military and civilian populations is moot.

Blank acknowledged that IW attacks might have strategic effects (excluding the physical aspects) of nuclear attacks; however, he found Harknett's thesis compelling except in cases where a state is willing to pre-emptively use WMD to deter an IW attack.[57] Blank concluded that neither "models of conventional nor nuclear deterrence can deter an IW attack except where one opponent has a usable WMD capability."[58] Therefore, WMD proliferation may prevent states from escaping an IW arms race.[59]

The Birth of U.S. Cyber Deterrence Policy

As first wave scholars debated the usefulness of cyber deterrence, U.S. cyber policy began to emerge. There are two purposes for surveying U.S. national security cyber policy in this research. First, it demonstrates the extent to which senior U.S. policy makers came to rely on cyber deterrence. Second, such a survey reveals additional evidence that the U.S. lacked an acceptable cyber deterrence theory.

[57] Ibid., 133.
[58] Ibid., 134.
[59] Ibid.

Key U.S. strategy documents began to highlight challenges posed by the cyber domain at the beginning of the first wave in the mid-1990s. By 1997, most White House cyber documents suggested that deterrence offered a way ahead. Lacking in these documents was an explanation of the requirements for cyber deterrence strategy and direction to implement those requirements. Mindful of the evolution of cyber deterrence scholarship in the first wave, a review of the documents presented in this section should leave readers with the realization that there was a disconnect between policy, strategy, and theory. This section examined applicable presidential national security strategies (NSS) and major cyber-related security documents to reach this conclusion.

Presidential strategic guidance from NSSs drives the strategy and policy of all governmental civilian and military organizations. Two presidential administrations produced nine NSSs during the first wave: Bill Clinton's (8) and George W. Bush's (1). Clinton's 1995 and 1996 NSS were the first to cite the threat to U.S. information systems as a "significant risk to national security," with the 1996 iteration adding that these risks are "being addressed."[60] The next year, 1997 was a watershed year for U.S. cyber policy.

Three 1997 U.S. policy documents demonstrated a change in the U.S. mindset and exhibited a sense of urgency regarding the threat from information/cyber attacks: the May 1997 NSS; the October 1997 report *Critical*

[60] The White House, *A National Security Strategy of Engagement and Enlargement* (Washington, DC: The White House, February 1995), 8. Also, see The White House, *A National Security Strategy of Engagement and Enlargement* (Washington, DC: The White House, February 1996). The Clinton Administration published eight NSSs (1993–2000); the first, in 1993, continued the theme from the previous administration's 1991 and 1993 strategies in which the flow of information was briefly mentioned. In these three strategies, the protection of critical infrastructure and the word *cyber* in any form were not present.

Foundations Protecting America's Infrastructures; and the 1997 report *Toward Deterrence in the Cyber Dimension*. The 1997 NSS highlighted the U.S.' dependence on information infrastructures and noted that the country faced serious challenges with vulnerabilities to critical systems and the exploitation of information. The strategy proposed improving domestic and international cooperation to counter these threats.[61]

The October 1997 report of the President's Commission on Critical Infrastructure Protection, *Critical Foundations Protecting America's Infrastructures*, proceeded from an assumption that deterring and defending the nation from state and non-state actors was not possible given the technological challenges. The Commission recommended that policy makers consider all cyber attacks acts of crime regardless of the attacker. If a criminal investigation revealed that a state attacker was responsible, then "other leadership will be assigned."[62] The Commission observed that domestic and international legal frameworks do not "reflect current technology." These frameworks need modifications to "increase deterrence against computer crimes domestically and internationally."[63]

The 1997 report *Toward Deterrence in the Cyber Dimension*, concluded that the U.S. neither has the capability to preempt a cyber attack by dissuasion,

---

[61] The White House, *A National Security Strategy for A New Century* (Washington, DC: The White House, May 1997).
[62] The White House, *Critical Foundations: Protecting America's Infrastructures, The Report of the President's Commission on Critical Infrastructure Protection* (Washington, DC, October 1997), 80, http://www.fas.org/sgp/library/pccip.pdf. Critical infrastructures are those that are so "vital that their incapacitation or destruction would have a debilitating impact on defense or economic security"; see page B-1.
[63] Ibid., 23. The Commission recognized that deterrence has an "important preventive role against attacks on critical infrastructure"; see page 83.

nor does it have the capabilities or politics that are required to deter cyber attackers.[64] The Commission recommended a national policy that defined the nation's response to a cyber attack on critical information infrastructure. They believed that "certain knowledge that the U.S. is committed to an aggressive policy of responding to cyber attacks" was the best deterrent until defensive technologies mature. A credible national cyber deterrence policy required several components: offensive information warfare capabilities to retaliate in kind; defensive capabilities to surveil, assess, and warn of an attack; and a retaliatory physical strike capability to respond to egregious acts of destruction.[65]

The increase in national-level attention to rising cyber threats in 1997 continued into the next year. In May 1998, Presidential Decision Directive (PDD)/NSC-63 directed development of a plan to ensure by 2000, the U.S. had the capability to "swiftly eliminate any significant vulnerability to both physical and cyber attacks on critical infrastructures, including especially our cyber systems."[66] The ratcheting upwards of an imperative to act in response to the cyber challenge continued in the 1998, 1999, and 2000 NSSs.[67]

---

[64] The White House, *Toward Deterrence in the Cyber Dimension: Report to the President's Commission on Critical Infrastructure Protection* (The White House, 1997), 4.
[65] Ibid., 8. The foundations for these three components of a U.S. cyber deterrence policy are: 1. Offensive IO capabilities need to be improved; the nation can build upon capabilities demonstrated in Operation DESERT STORM (1991) where the U.S. assumed control over Iraqi computerized networks. 2. Defensive systems must improve to protect capabilities for retaliation (second strike) and to identify attackers (attribution). Cooperation must be improved in order to trace attacks. U.S. policy should state that refusal to assist in response to IO attack against U.S. critical infrastructure may indicate that party is aiding the attacker, which may result in a counterstrike. 3. U.S. needs a declaration that IW resulting in the loss of life or major property destruction will face a devastating response. See pages 8-9.
[66] The White House, "Presidential Decision Directive/NSC-63" (The White House, May 22, 1998), http://www.fas.org/irp/offdocs/pdd/pdd-63.htm.
[67] The White House, *A National Security Strategy for a New Century* (Washington, DC: The White House, October 1998). The NSS referred to "a dangerous new threat" and described "threats to the national information infrastructure, ranging from cyber-crime to a strategic

The 2000 NSS commented on the need to build upon the initiatives of the "first-ever national strategy for cybersecurity."[68] The strategy the NSS referred to was the 2000 *National Plan for Information Systems Protection: An Invitation to a Dialogue*, directed by the 1998 PDD/NSC-63. Richard Clarke and his team designed the plan solely to defend cyberspace; it did not mention deterrence.[69] In hindsight, the strategy underlying the plan has been judged ineffective, as Clarke observed in 2010 that "people have tried to create a cyber war defense" but "obviously they have not succeeded."[70] The 2000 defensive-based approach identified three objectives:[71]

1. *Prepare and Prevent*: those steps necessary to minimize the possibility of a significant and successful attack on our critical information networks and build an infrastructure that remains effective in the face of such attacks
2. *Detect and Respond*: those actions required for identifying and assessing an attack in a timely way and then containing the attack, quickly recovering from it, and reconstituting affected systems
3. *Build Strong Foundations*: the things the U.S. must do as a nation to create and nourish the people, organizations, laws, and traditions that will make it better able to Prepare and Prevent, Detect and Respond to attacks on its critical information networks

---

information attack on the United States via the global information network. The 1999 NSS identified foreign governments and terrorist groups as perpetrators of "sophisticated, well-organized capabilities to launch cyber-attacks against critical American networks"; see The White House, *A National Security Strategy for A New Century* (Washington, DC: The White House, December 1999), 17.

[68] The White House, *A National Security Strategy for a Global Age* (Washington, DC: The White House, December 2000).

[69] The White House, *National Plan for Information Systems Protection: An Invitation to a Dialogue* (Washington, DC, 2000), v. Richard Clarke served as the National Coordinator for Security, Infrastructure Protection, and Counter-Terrorism.

[70] Clarke, *Cyber War*, 103.

[71] The White House, *National Plan for Information Systems Protection: An Invitation To A Dialogue*, xi–xii. The plan assumed that the objectives of potential adversaries in attacking U.S. critical infrastructures were for one of three reasons: Assist government-sponsored companies in acquiring an advantage over U.S. competitors; damage the economic stability of the U.S. by targeting financial or industrial resources; or damage U.S. national security by conducting military or intelligence operations. See page 6.

George W. Bush assumed the presidency in January 2001, within a month of the release of the 2000 NSS. Less than nine months later, the terrorist attack of September 11, 2001 set the administration on a new course. In September 2002, the Bush administration released its first NSS. There was no reference to cyber and only brief mention of the need for the capability to conduct information operations, and this was in the context of the nation's response to the 9/11 attacks.

Shortly before the release of the 2002 NSS, the *National Strategy for Homeland Security* identified cyberspace as one of eight major security initiatives. However, this strategy did not mention deterrence and paid scant attention to cyberspace. The strategy directed readers to its implementing component, the *National Strategy to Secure Cyberspace*, for more details on the administration's cyber initiatives.[72]

The February 2003 *National Strategy to Secure Cyberspace* established three strategic goals: Prevent cyber attacks to critical infrastructure, reduce vulnerability to cyber attacks, and minimize damage from cyber attacks.[73] The plan did not offer specifics to deter cyber attacks; however, it concluded that there

---

[72] Office of Homeland Security, *National Strategy For Homeland Security* (Washington, DC: The White House, July 2002), x–9. The 2002 Homeland Security Act created the Department of Homeland Security. This new department "became the lead agency for several industry sectors, including information and telecommunications." The *National Strategy for Homeland Security* directed the Office of Homeland Security and the President's Critical Infrastructure Protection Board to "complete cyber and physical infrastructure protection plans, which would serve as the baseline for later developing a comprehensive national infrastructure protection plan." This strategy did not mandate a completion date – on February 14, 2003, the Bush Administration released the *National Strategy to Secure Cyberspace* and the complementary *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*; see the *Critical Infrastructure Protection: Challenges for Selected Agencies and Industry Sectors*, Report to the Committee on Energy and Commerce, House of Representatives (Washington, D.C.: General Accounting Office, February 2003), 17-18, http://www.gao.gov/new.items/d03233.pdf.

[73] The White House, *The National Strategy to Secure Cyberspace* (The White House, February 2003), viii, https://www-hsdl-org.ezproxy.library.tufts.edu/?abstract&doc=3288&coll=documents&url=https://www-hsdl-org.ezproxy.library.tufts.edu/homesec/docs/whitehouse/cyberspace_strategy.pdf.

was a need to develop "robust capabilities where they do not exist today if [the U.S. is] to reduce vulnerabilities and deter those with capabilities and intent to harm [the] U.S.' critical infrastructures."[74]

This strategy identified five national priorities, which included developing a national cyber response system, reducing vulnerability to cyber threats, increasing awareness with cybersecurity training, securing cyberspace that the government uses, and improving international cooperation.[75] These priorities would help protect infrastructure from cyber attacks but would do little to deter cyber threats. A complement to this strategy was the *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets* released in February 2003. This approach also focused on protecting the U.S.' "critical infrastructures and key assets from physical attack," again with little regard for cyber deterrence.[76] Building upon these strategic documents, in December 2003, President Bush issued *Homeland Security Presidential Directive* (HSPD)-7 to all federal departments to protect U.S. critical infrastructure from terrorist attacks.[77]

The impact of 9/11 on the U.S. effort to counter cyber aggression was evident in HSPD-7 as the nation's focus had become transfixed on terrorism. This was clearly evident in the 2004 *National Military Strategy* as its first priority

[74] Ibid., ix.
[75] Ibid., x–xii.
[76] The White House, *The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets* (Washington, DC: The White House, February 2003), vii.
[77] The White House, *Homeland Security Presidential Directive-7* (Washington, DC: The White House, December 17, 2003), http://www.dhs.gov/xabout/laws/gc_1214597989952.shtm#1. This directive included physical and cyber critical infrastructures and spanned the entirety of the U.S. economy.

was to win the war on terrorism.[78] Terrorism was the central focus of this strategy; however, this NMS profoundly elevated the importance of cyber. The chairman formally incorporated cyberspace as a domain in directing that U.S. military forces "must have the ability to operate across the air, land, sea, space and cyberspace domains."[79] Additionally, although the details were absent, the NMS stated that U.S. joint military forces needed a "comprehensive concept of deterrence" to deter state and non-state actors from threatening "networks and data critical to U.S. information-enabled systems."[80]

In the security climate that existed between late 2003 through early 2006, with few exceptions, an unexplained gap emerged in cyber policy and cyber deterrence literature.[81] Anecdotally, the March 2003 invasion of Iraq, in combination with the ongoing war in Afghanistan, may prove to be an explanatory factor. Regardless, the majority of the nation's policy makers were asleep with regard to the cyber threat as attacks and exploitations continued with no credible response for nearly three years.

A series of cyber-related policy documents emerged in 2006, which indicated a renewed emphasis toward the threats from cyber attacks and espionage.[82] There were four of note in 2006; the first was the March 2006 NSS.

---

[78] Chairman of the Joint Chiefs of Staff, *The National Military Strategy of the United States of America* (Washington, DC: Joint Chiefs of Staff, 2004), iv, http://www.defense.gov/news/Mar2005/d20050318nms.pdf. The NMS is the Chairman of the Joint Chief of Staff's guidance to U.S. military forces. It is based on direction from the President's NSS and Secretary of Defense's National Defense Strategy (NDS); see page 1.
[79] Ibid., 18.
[80] Ibid.
[81] This researcher finds this gap intriguing and worthy of additional study; however, it is beyond the scope of the study.
[82] Again, while puzzling, it is beyond the scope of this research to explain the renewed interest in the cyber threat in late 2005 and early 2006. Perhaps the after-effects of Titan Rain may have

The NSS highlighted the "disruptive challenges from state and non-state actors who employ technologies and capabilities," such as cyber, "in new ways to counter military advantages."[83] The NSS referenced the 2006 QDR to note that the DoD will continue to "adapt and build" a force that is capable of deterring state and non-state actors through a tailored approach.[84] How the DoD was to accomplish this remained unclear.

The 2006 QDR recognized China's investment in capabilities to conduct cyber warfare, but primarily it focused on efforts to deter rogue states' and terrorists' use of WMD.[85] The report highlighted the need to develop capabilities to "shape and defend cyberspace."[86] To satisfy this need, the DoD made four cyber-relevant decisions:[87]

1. Make additional investments in information assurance capabilities to protect information and the Department's computer networks.
2. Strengthen coordination of defensive and offensive cyber missions.
3. Leverage lessons learned from computer network attack and exploitation activities to improve network defense and adopt a defense-in-depth planning approach to protect information.
4. Improve the Department's information sharing with other agencies and with international allies and partners by developing information protection policies and exploiting the latest commercial technologies.

Third, the December 2006 *Deterrence Operations Joint Operating Concept* (JOC) addressed a general approach to tailored deterrence of state and non-state actors. This approach relied upon three components: denying benefits,

---

merged with other attacks to begin an awakening that was not fully realized until the 2007 Russia-Estonia cyber war.

[83] The White House, *National Security Strategy of the United States* (Washington, DC: United States White House Office, March 2006), 44.

[84] Ibid., 43.

[85] Department of Defense, *Quadrennial Defense Review Report* (Washington, DC: Department of Defense, February 6, 2006), 29, 49.

[86] Ibid., 32.

[87] Ibid., 50–51.

imposing cost, and encouraging adversary restraint. The JOC focused primarily on deterring WMD; however, it did consider cyber deterrence within its general framework.[88]

Lastly, the December 2006 *National Military Strategy for Cyberspace Operations*, formerly a secret document, introduced a strategic framework that focused on offensive and defensive cyber operations to achieve the desired strategic goal. To achieve the goal of ensuring "U.S. military strategic superiority in cyberspace," the framework's design relied upon three interwoven components: ends, ways, and means.[89] The "end," the desired outcome, of this strategy required the military to create an environment, which deterred potential adversaries from creating or using offensive cyber capabilities against the nation's interests.[90] This document drew heavily from the 2006 Deterrence JOC as it similarly envisioned deterring potential adversaries by "imposing political, economic, or military costs; denying the benefits of their actions; and inducing adversary restraint based on demonstrated U.S. capabilities."[91]

The framework depended upon five core ways to achieve this end. These were network operations; information operations; kinetic actions; law

---

[88] Department of Defense, *Deterrence Operations Joint Operating Concept* (Washington, DC: Department of Defense, December 2006), 28–42. This framework included eight distinct categories of capabilities as attributes. These categories were global situational awareness; command and control; forward presence; security cooperation, military integration, and interoperability; force projection; active and passive defenses; global strike; and strategic communication. The JOC concluded that "joint information operations," a subset of global strike, strategic communications, to include information operations, as of this report did not meet U.S. cyberspace warfare requirements; see pages74-76.

[89] Chairman of the Joint Chiefs of Staff, *The National Military Strategy for Cyberspace Operations* (Washington, DC: Joint Chiefs of Staff, December 2006), 13, https://www-hsdl-org.ezproxy.library.tufts.edu/?abstract&doc=111189&coll=documents&url=https://www-hsdl-org.ezproxy.library.tufts.edu/homesec/docs/dod/nps37-062409-03.pdf. Ends are described as the "steady state DoD must establish as the comprehensive military contributions"; see pg ix-x.

[90] Ibid., 13.

[91] Ibid.

enforcement and counterintelligence; and themes and messages. Combined, these capabilities formed a set of "proficiencies" that the military had to design, nurture, and operationalize.[92] The document did not specify the means, or resources, needed to sustain the capabilities described in the above core ways.[93]

During the first wave, cyber deterrence was a strategy that the U.S. government seriously contemplated, but did not pursue publicly, in both the Clinton and Bush administrations. The literature captures a long-running debate among scholars regarding the utility of deterrence theory for the cyber domain. A review of major policy documents indicated that deterring potential cyber adversaries was a prominent fixture of U.S. strategy, irrespective of detractors. However, lacking in the open- source literature was a precise description of the requirements for cyber deterrence or a public declaration, without which the conclusion is clear: The U.S. had neither a publicly executable policy of cyber deterrence nor consensus among strategists of the theoretical foundation for such a policy.[94]

---

[92] Ibid., 14. Network operations, as defined in JP 1-02, are "activities conducted to operate and defend the Global Information Grid"; see page GL-2. IO, as defined by DODI 3600.02, is the "integrated employment of the core capabilities of electronic warfare, computer network operations, psychological operations, military deception, and operations security in concert with specified supporting and related capabilities, to influence, disrupt, corrupt, or usurp adversarial human and automated decision making while protecting our own," see page GL-2. Counterintelligence (CI), as defined in JP 1-02, is "information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted by or on behalf of foreign governments or elements thereof, foreign organizations, or foreign persons, or international terrorist activities"; see page GL-1. Themes and messages were not well defined in the document. This core way was described as the capacity for the DoD to rapidly and effectively reach broad target audiences using the Internet and wireless networks with a coordinated and integrated message best tailored to support U.S. objectives; see page 15.

[93] Ibid., 18. There was a brief description of the agencies that contained the means, but no specifics on the precise capabilities or requirements to deter potential cyber adversaries. The researcher was unable to determine if the lack of specificity was purposely vague, which could be a function of security classification issues.

[94] This assessment is based on scholarly literature and governmental documents in the public domain. It is conceivable that in the public domain the existence of cyber deterrence appeared

The Second Wave

The second wave of cyber deterrence began with increased attention to the topic by the U.S. government and scholars because of the April–May 2007 cyber war between Russia and Estonia. Other events followed in quick succession to further fuel a renewal of scholarly debate and public policy focus after a gap of several years in which cyber deterrence received little attention.[95] During this new wave, the debate on cyber deterrence rapidly progressed as a review of the literature yielded three distinct groups of scholars. There were scholars who continued to reflect upon cyber deterrence primarily using the elements of Cold War nuclear theory; those who loosely held to nuclear theory but introduced new ideas to further cyber deterrence frameworks; and a group of detractors who saw cyber deterrence as problematic or irrelevant.

In the second wave, cyber war and major cyber attacks moved beyond mere concerns to become serious challenges to national security. The requirement to respond to these challenges was clear; however, a consensus on how to deter state and non-state cyber aggressors was not forthcoming. Value emerged from the debate as the need to combine some elements of nuclear deterrence theory with new ideas to form a framework for cyber deterrence where

---

lacking while actions were taking place in the classified domain that elicited deterrence effects. Determining these effects is impossible without unfettered access to relevant classified material.

[95] Examples include the August 2008 war between Russia and Georgia and a continuous stream of cyber attacks and exploitations, which include espionage against the Obama and McCain presidential campaigns in 2008; the U.S. military computer breach using an infected flash drive in 2008; and Operation Aurora – an attack by China against Google, Northrop Grumman, and others in 2009. See Daniel Finnegan's PowerPoint presentation, "Cyber Attacks: History and Scenarios" (United States Naval Academy, 2011). The gap in U.S. focus between late 2003 and the beginning of the second wave may be, in part, due to the USG's focus on wars in Iraq and Afghanistan. Additionally, Richard Clarke, the Bush administration's first cyber "czar" resigned in February 2003, allegedly in opposition to the Iraqi war, which began in March 2003. This research recommends a study to understand this gap and why it occurred.

helpful. There was a general acceptance that more work is needed on alternatives to fulfill the confidence the U.S. government placed in the concept with its declaratory policy on cyber deterrence in November 2011.[96]

Cyber Deterrence – A Reflection of Cold War Theory

Ryan Moore argued that the "fundamentals of deterrence" are constant; therefore, they do not change as technology matures and the nature of warfare morphs to absorb these changes. However, the "stratagems used to employ the methodology" to maintain a credible deterrent posture must change.[97] Moore lamented that the "practice of deterrence" remained too familiar with Cold War mentality because the timeless fundamentals have not been properly adapted for the cyber domain.[98]

Moore captured some of the elements needed to deter state and non-state actors in cyberspace. These are denial, punishment, establishment of thresholds, and articulated national policy, all of which closely align with the requirements of nuclear deterrence. The stratagems that must change are associated with challenges such as "technological limitations, policy and regulation issues, and the ripple effect of poorly understood changes" that made cyber deterrence a

---

[96] Department of Defense, *Department of Defense Cyberspace Policy Report - A Report to Congress Pursuant to the National Defense Authorization Act for Fiscal Year 2011, Section 934*, 2. In the report, for the first time, the U.S. issued a declaratory policy regarding cyber deterrence that rested upon a strategy of punishment to impose costs for malicious actions and reliance upon defenses to deny aggressors the capacity to achieve their goals.

[97] Moore, "Prospects for Cyber Deterrence," 46. Moore relied upon Mearsheimer, Morgan and others to define cyber deterrence as "influencing an actor, either by denying the potential gains of the actor or by threatening punishment through the use of retaliation, in order to prevent the actor from utilizing cyberspace as a means to degrade, disrupt, manipulate, deny, or destroy any portion of the critical national infrastructure," see page 46. As of the writing of this thesis, U.S. Air Force Captain Ryan Moore was a graduate student at the Naval Postgraduate School. His thesis advisor was John Arquilla, Professor of Defense Analysis at the U.S. Naval Postgraduate School.

[98] Ibid.

"wicked problem."[99] Moore concluded that until these and other challenges are resolved, the U.S. will "likely have to emphasize denial deterrence, because the veil of anonymity makes punitive deterrence extremely difficult to accomplish."[100]

The U.S. was capable of increasing defenses; however, achieving effective cyber deterrence through this approach required additional developmental work. Moore offered four areas where the nation needed improvements:[101]

1. The U.S. must determine what it considers a cyber attack.
2. The U.S. needs a declaratory cyber deterrence policy.
3. The defense of national critical infrastructure requires strengthening.
4. The U.S. requires more retaliatory threat options.

The U.S. must identify its threshold for an attack because without this, there is no foundation on which to make decisions to retaliate. However, thresholds must remain a secret once determined, otherwise adversaries could design attacks slightly below U.S. redlines. Regarding the second point, if the U.S. does not publicly declare a cyber deterrence policy, then there is no possibility for deterrence because the U.S. will not have a "clear means of communicating that it will respond to cyber attacks."[102]

On Moore's third point, there was concern that the U.S. relied too heavily on a perimeter defense of the nation's critical cyber infrastructure and more in-

[99] Moore, "Prospects for Cyber Deterrence," 61. Moore borrowed deterrence requirements from Morgan's *Deterrence: A Conceptual Analysis*, 1977, p. 32. Requirements for successful deterrence include a credible threat that is recognized by an adversary that has the capacity to make a rational decision. The deterring state must have the capability and will to fulfill the promise of a retaliatory threat; see page 47.
[100] Ibid., 75. Moore also noted that while the 2003 U.S. National Strategy to Secure Cyberspace did not "discuss the creation of a deterrence policy in cyberspace, the strategic objectives within the document (were) consistent with strengthening the denial aspect of a cyber deterrence strategy"; see page 69.
[101] Ibid., 71–75.
[102] Ibid., 71–72.

depth approaches were necessary to enhance deterrence by denial. Lastly, as did Geoffrey French in the first wave, Moore believed that the U.S. should tailor retaliatory threats such that a U.S. response to a cyber attack by a peer state warrants a different approach than a response to a non-state actor. Moore, in recommending these areas for improvement at the cusp of the second wave, captured some of the strategic sentiments that a number of dominant participants in the U.S. cyber policy debate would articulate as cyber deterrence began to receive a greater level of attention.[103]

Joseph Nye sustained Moore's argument that cyber deterrence reflected Cold War nuclear theory in concluding that inter-state deterrence and offensive capabilities are suitable to manage cyber war. Although cyber attacks lack the physical destruction compared to that of nuclear weapons and the challenge of attributing attacks is more complex, the capacity for states to deter each other is still possible.[104] Moore argued that cyber deterrence by denial should be favored because the lack of the attribution made punishment difficult. Nye agreed with Moore's view on denial, for similar reasons.

The capacity to deter a peer state by "entanglement and denial" remains possible even in cases where there is "inadequate attribution." Nye noted that it was "too simple" to suggest that cyber deterrence is invalid because of the difficulty to attribute attacks.[105] There are two reasons why this is the case. First,

---

[103] Ibid., 74–75. Moore cited Elaine Bunn's 2007 article, *Can Deterrence Be Tailored*; however, as the idea of tailored deterrence applies to cyber, Geoffrey French introduced the concept in 2002; both articles have been referenced previously.
[104] Joseph S. Nye, Jr., *Cyber Power* (Harvard Kennedy School: Belfer Center for Science and International Affairs, May 2010), 16, http://belfercenter.ksg.harvard.edu/files/cyber-power.pdf.
[105] Joseph S. Nye, Jr., "Nuclear Lessons for Cyber Security," 33.

even if a state can conceal an attack, the level of interdependency that exists between most states suggests that a large cyber attack would be damaging to the attacker. Nye used a non-cyber example to make this point – the "reluctance of the Chinese government to dump dollars to punish the U.S. after it sold arms to Taiwan in 2010." In contrast to the Cold War relationship between the U.S. and USSR, the U.S., China, and others are "entangled in multiple networks."[106] Because of this degree of interdependency, cyber deterrence remains valid, as attribution may be less relevant in some circumstances.

Second, denial capabilities may be sufficient to deter an anonymous attacker. The use of active defenses in a denial approach or a strong firewall may make an attack less inviting; thus, deterrence takes place when the identity of an attacker is unknown. These reasons lead Nye to observe that "attribution does not have to be perfect" for effective cyber deterrence, and other second wave scholars shared this position.[107]

Dmitri Alperovitch concluded that effective deterrence is conceivable "even without accurate and timely attribution" because a state's retaliatory strike only requires a "sufficient mix of suspicion and evidence" to satisfy an acceptable portion of a state's domestic population and international partners.[108] Likewise, Will Goodman concluded that attribution is possible in some cases, and in others,

---

[106] Ibid.
[107] Ibid., 33–34.
[108] Dmitri Alperovitch, "Towards Establishment of Cyberspace Deterrence Strategy," in *3rd International Conference on Cyber Conflict* (Tallinn, Estonia, 2011), 91, http://www.ccdcoe.org/publications/2011proceedings/TowardsEstablishmentOfCyberstapeDeterrenceStrategy-Alperovitch.pdf. Alperovitch conceded that using automated defenses in response to the attribution problem is too high a risk because of the possibility of injuring an innocent actor. Dmitri Alperovitch is President of Asymmetric Cyber Operations and former VP of Threat Research at McAfee.

it "may not even be necessary for deterrence."[109] He cited U.S. capabilities to identify the originators of some attacks as evidence that attribution is possible. Regarding the necessity of attribution, the 2007 Russian cyber attack on Estonia demonstrated that attribution is not always required because third parties, in shielding a state sponsor, become a viable target for retaliation.[110]

Charles Glaser also acknowledged the attribution challenge, but observed that conventional wisdom on the subject may be mistaken. His reasoning, similar to Nye's, was that the attribution challenge might be less difficult because states bound by "political motives" will choose to avoid cyber attacks out of fear of revealing their identity. He reasoned that states intent on attacking the U.S. probably have political purposes in mind. For example, if an actor is intent on compelling the U.S. to "make political concessions during a crisis before a war starts – the communication required to issue such a compelling threat eliminates the attribution problem.[111]

Regarding other aspects of cyber deterrence, Glaser argued, as did Moore, that the U.S. needed a declaratory cyber policy. Glaser recommended that a declaration must include transparency for its plan of attack, as a potential attacker must believe that the country has the capability to respond. Additionally, if the U.S. intends to use conventional kinetic capabilities to deter cyber attacks, then it

---

[109] Goodman, "Cyber Deterrence: Tougher in Theory Than in Practice?" 124.
[110] Ibid., 125. Goodman continued his reasoning, if a state that has been attacked assigns blame to a third party, then the state sponsor of the third party may be deterred from protecting the third party attacker. In turn, this third party actor may be deterred from attacking again and others watching may be deterred from attacking in the first place.
[111] Charles L. Glaser, *Deterrence of Cyber Attacks and US National Security* (The George Washington University, 2011), 3, http://www.cspri.seas.gwu.edu/Seminar%20Abstracts%20and%20Papers/2011-5%20Cyber%20Deterrence%20and%20Security%20Glaser.pdf.

should make this statement publicly so that potential attackers understand the comprehensive nature of U.S. cyber deterrence policy. Further, Glaser advocated that a U.S. cyber deterrence policy should include both defensive measures and the capacity to reconstitute cyber capabilities. This is consistent with his view that a balanced approach of punishment and denial is required to influence an attacker's decision calculus.[112]

Richard Kugler also rejected the view that the attribution problem "paralyzes" thinking about cyber deterrence. Although there are some attacks in which the identity of the perpetrator is unknown, this does not comprise the entire set of attacks or potentially the most important attacks. Kugler predicted that in the future some powerful states would use the threat of cyber attacks to achieve political ends. These states will want their identities known; therefore, the U.S. needs the capacity to deter these "attributable attackers."[113]

Kugler's core argument advanced three ideas, the latter two mimic significant components of nuclear deterrence theory: "Cyber attacks should not be seen in isolation;" offensive and defensive capabilities are required to deter cyber attacks; and deterrence contains psychological and cognitive aspects, because it is necessary to understand an attacker's motives. Based on these ideas, Kugler

---

[112] Ibid., 1–8. Glaser specified four components in an attacker's deterrence calculus: the benefits of taking the action, the probability of achieving the benefits, the costs the defender will impose, and the adversary's probability assessment that the defender will inflict those costs; see page 1. Glaser's advocacy of a policy that relied upon conventional kinetic operations to deter some types of cyber attacks is implied in the *Department of Defense Strategy for Operating in Cyberspace*, released in July 2011, which will be examined later in this chapter. Charles Glaser is Professor of Political Science and Director of the Institute for Security and Conflict Studies, George Washington University.

[113] Kugler, "Deterrence of Cyber Attacks," 309–310. Kugler considered the standards of proof for attribution to be less demanding in peacetime although in a crisis he suggested that the U.S. required concrete proof; see page 318. Richard Kugler is a senior consultant at the Center for Technology and National Security Policy at the National Defense University.

suggested that cyber deterrence required a "proper combination of motivational instruments and physical capabilities," and further, he noted that a "one-size-fits-all" approach would not succeed. This led him to advocate for a tailored approach, expounding on the ideas of French from the first wave that best suits the challenge of deterring the diversity of actors and their wide range of capabilities to conduct an attack.[114]

Kugler's concept of tailored cyber deterrence was heavily adapted from the 2006 DoD Deterrence JOC. The goal he established to "influence [an] adversary's decision-making calculus" relied upon three key aspects: denying benefits, imposing costs, and offering incentives to garner adversary restraint.[115] To satisfy the requirements of tailored cyber deterrence, Kugler recommended that the following elements were essential:[116]

- A clear and firm declaratory policy spelling out the U.S. intention to deter cyber attacks
- High global situational awareness that is attuned to the full spectrum of potential cyber threats and the circumstances in which they might arise
- Good command and control systems that permit coordinated multiregional and homeland responses to cyber threats
- Effective cyber defenses that protect both U.S. military forces and the U.S. homeland with a high priority for defending key infrastructure
- A wide spectrum of counter-cyber offensive capabilities, including cyber attack and other instruments for asserting U.S. power in order to enforce deterrence before, during, and after crises
- Well-developed U.S. interagency cooperation and collaboration with allies and partners including those in Europe, Asia, and elsewhere
- Cyber deterrence methodologies, metrics, and experiments that can help guide the planning process

Kugler noted that the U.S. has three options for cyber deterrence. The

[114] Ibid.
[115] Ibid., 327.
[116] Ibid., 332.

least demanding was a limited strategy that would "rely mainly on security and defensive measures to achieve its goals, seeking only a gradual, evolutionary improvement in offensive capabilities."[117] The second, more ambitious option required the robust use of offensive and defensive capabilities, which he suggested would yield better results. The final option, the most demanding, called for combining option two with improved collaborative planning with friends and allies. The alternative for not choosing any of these, or other alternative strategic approaches, risks a "growing vulnerability of America's vital information networks."[118]

New Ideas Emerge

Jeffrey Cooper introduced a new approach to cyber deterrence that characterized relationships between states and others similar to those that occur in the financial services industry.[119] Cooper supported his framework with two justifications. First, the Cold War realist model no longer adequately describes the international system because power emanating from networked relationships has supplanted the traditional sources of power (land, labor, capital). Second, the cyber domain possesses unique characteristics that must be considered. Cyber consists of two types of networks that describe the cyber domain's unique properties: networks that are physically connected and networks defined by their linkage to a community of interest.[120]

---

[117] Ibid., 339.
[118] Ibid., 339–340.
[119] Cooper, *New Approaches to Cyber-Deterrence: Initial Thoughts On A New Framework*, 100. Jeffrey Cooper is an SAIC Technical Fellow, Vice President for Technology, and Chief Science Officer of SAIC Strategies, Simulation & Training Business Unit at Science Applications International Corporation (SAIC).
[120] Ibid., 125–128.

Cooper argued that the international system has "evolved away from the Realist model" to "now include a wide range of actors."[121] Because of this evolution, he recommended two concepts to "reformulate deterrence" for the new geopolitical climate. The first new concept is a framework Cooper called the "three Cs – cooperation, competition, and conflict."[122] This framework allowed actors to preserve their interests while also pursuing "mutually beneficial cooperation within multiple sets of relationships."[123] The second concept is networked deterrence, which argued that networks constitute the "real source of value" because they have become the foundation for international power.[124]

These justifications and concepts support Cooper's alternative deterrence framework, which seeks to use the financial services sector approach to "adapt and deter attacks by exerting influence on potential attackers through their networks of relationships."[125] Because of the "complex matrix" created by these relationships between parties with shared interests – "the impacts of these networked relationships can be exploited to shape motivations and behaviors of participants."[126]

The financial services sector is made up of complex relationships and faces a broad range of threats to critical cyber systems. Examples of threats

---

[121] Ibid., 125.
[122] Ibid., 4. Cooper defined cooperation as the "relationship in which the objective is a positive-sum outcome for participants as a whole"; competition occurs when the "objective is an improved relative position, but one that can often produce an increase in overall welfare"; and conflict occurs when the "objective is an improved relative position, not an overall improvement in welfare." See page 123.
[123] Ibid., 121.
[124] Ibid., 5.
[125] Ibid., 133.
[126] Ibid., 132.

include:[127]

- Unauthorized and illicit access to and misuse of sensitive information to protect both client and firm confidentiality,
- Unauthorized information sharing,
- Theft and embezzlement,
- Theft of intellectual property and other unique process data,
- Access to sensitive financial information,
- Illicit credentialing and violation of employee privacy,
- Disruption of communications,
- Disruption of systems, and
- Corruption of data.

Cooper's deterrence framework adapts the model "effectively employed by some members of the financial service sector," to address these threats.

The five core elements of Cooper's framework are "penalty, futility, dependency, counter-productivity, and intolerance." Penalty and futility are characteristics of classic deterrence. Penalty is an element of punishment, while futility is a type of denial effort. Penalty relates to "traditional imposition of potential costs, either by affecting loss value that might be imposed on an attacker or increasing the loss probability." Futility means that a defender has undertaken efforts to "make cyber attacks more difficult, more costly to the attacker, more sporadic, or less effective."[128]

Dependency and counter-productivity, historically not a part of traditional deterrence, pertain to various aspects of relationships in which interdependency between and within networks create a dynamic that a state or non-state actor can exploit to influence cost/benefit calculations. The value of dependency is that it

[127] Ibid., 133–134.
[128] Ibid., 134. Cooper's deterrence framework adds to the financial sector approach by introducing a fifth element, intolerance. He argued that extending the financial services model to state-level cyber deterrence is appropriate because "they are similar enough in character and source, even if the targets and scale might be considerably different," see page 136.

"creates a direct relationship between the potential attacker and the target that creates value for the attack, which could be put at risk." Although similar to dependency, counter-productivity "operates indirectly by affecting a wider set of relationships, including those of the party attacked but also those in which the attacker participates."[129] Intolerance is akin to fostering new norms as Cooper's idea is to create a more "mindful attitude" toward unacceptable behavior in the cyber domain.[130]

Cooper concluded that the U.S. has to create circumstances whereby all state actors appreciate the significance of reciprocity. This implies that cooperation is essential, although relationships between states do not have to be "friendly."[131] He concluded, "Cooperation leads to integration, and integration to the complexity we see in modern life" – with cooperation (good communication and ability to share information), "integration feeds on itself to create even more interconnections."[132] Patrick Morgan equally shared the necessity to incorporate cooperation into cyber deterrence theory.

Morgan drew a parallel between cooperation required for arms control during the Cold War and cooperation needed to secure cyberspace. He noted that

---

[129] Ibid., 135–136.

[130] Ibid., 134–141. Cooper offers an example of dependency within the financial community in which a state may be a client whose continued ability to conduct financial transition could be held at risk by cyber attacks. In that setting, regardless of attribution, a state could retaliate by severing relationships and this potential will affect the attackers cost/benefit calculations. An example of counter-productivity would be the public outrage that could occur after a cyber attack or an attack that a wider audience perceives to deviate from accepted norms. This dynamic can work in a more precise manner in the attacker's own network. For example, if the attacker's network experiences costs from an attack and perceives that norms have been violated, then members of the attacker's network may be less helpful to the attacker. In turn, this affects the attackers cost/benefit calculations in planning future attacks.

[131] Ibid., 161.

[132] Ibid., 61. Cooper observed that cooperation is "one form of effective social relationship among self-interested entities not mediated by higher authority" and is therefore "consistent with an international system in the absence of a Leviathan," see page 111.

"arms control was aimed at making deterrence stable" and that it made reliance on nuclear deterrence "more successful and less burdensome." He argued that this concept is "directly relevant to cybersecurity because the capacity to do harm to and via cyberspace cannot be eliminated." Therefore, cooperation structured to achieve that which Cold War arms control sought can reduce vulnerabilities to harm from cyber attacks, enhance cyber deterrence by defense, and increase possibilities for cyber retaliation.[133]

From his examination of cyber deterrence, Morgan concluded that the "most important lesson" from the Cold War era is that cooperation between states should be adopted and implemented in cyber security strategy because of the "scale and interpenetration" of global interdependence between states is now far greater.[134] Aside from cooperation, Morgan concluded that the U.S. would have to pursue defensive and offensive retaliatory capabilities to deter cyber attacks. He argued that the present era demands a reversal from U.S. deterrence posture of the Cold War because deterrence of cyber attacks must focus on defense to compensate for the "limits of deterrence based on retaliation."[135]

Several additional scholars advocated for the necessity to incorporate cooperation into cyber deterrence theory. Murat Dogrul et al concluded that cooperation to forge an "international legal framework under the UN that

---

[133] Patrick M. Morgan, "Applicability of Traditional Deterrence Concepts and Theory to the Cyber Realm," in *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy* (Washington, D.C: National Academy of Sciences, 2010), 73, http://www.nap.edu/catalog.php?record_id=12997#toc. Professor Morgan is the Tierney Chair, Peace and Conflict, Political Science School of Social Sciences, University of California, Irvine.
[134] Ibid., 75.
[135] Ibid., 58–59. Morgan assessed that deterrence by defense is an important factor in countering the challenge of attribution because with effective defenses, it will be easier to "detail the nature of the severest, most threatening attacks," which helps in deterring the attacker.

addresses cyber aggression is the most critical component" of a comprehensive deterrence approach. They argued that in concert with efforts to develop new international law, it is essential to pursue the formation of new norms, as states must share a "common standard for the conduct of international transactions" in the cyber domain.[136] Jeff McNeil argued that international cooperation is necessary because the "lack of technical detection capability" to solve the attribution challenge moves cyber deterrence efforts toward a legal solution.[137] Joseph Nye also recognized that international cooperation is a concern in the global cyber domain because states have already asked for treaties and negotiations to control cyber aggression. Nye shared Dogrul's recognition that differing norms complicated the process of achieving consensus.[138]

Scott Biedleman argued that the lack of norms did more than "complicate" the process of coordination. The absence of international cyber laws and norms has resulted in a "gray area" that some actors exploit because of the "imprecise thresholds" in the UN charter and other international agreements. This lack of

---

[136] Murat Dogrul, Adil Aslan, and Eyyup Celik, "Developing an International Cooperation on Cyber Defense and Deterrence Against Cyber Terrorism," in *3rd International Conference on Cyber Conflict*, 2011, 38. Dogrul et al determined that an international legal framework is more critical to cyber deterrence than offensive and defensive capabilities. Murat Dogrul is Captain in the Turkish Air Force, and a student officer at the Turkish Air War College in Istanbul. Air War College in Istanbul.

[137] Jeff J. McNeil, "Maturing International Cooperation to Address the Cyberspace Attack Attribution Problem," *ProQuest Dissertation & Theses*, May 2010, 2, http://search.proquest.com.ezproxy.library.tufts.edu/pqdtft/docview/365828910/fulltextPDF/13274145B103A1BC15F/1?accountid=14434. McNeil noted that the absence of appropriate "domestic and international cyberspace legislation makes the problem one of international cooperation." Jeff McNeil completed this dissertation as a graduation requirement of Old Dominion University.

[138] Joseph S. Nye, Jr., "Power and National Security in Cyberspace," in *America's Cyber Future: Security and Prosperity in the Information Age*, vol. II (Center for a New American Security, 2011), 19. Finnemore defined norms as "shared expectations of proper behavior." See "Cultivating International Cyber Norms," in *America's Cyber Future*, 90.

norms and laws has "intensified the dangers of cyber aggressors."[139] Martha Finnemore countered that there is not an absence of an effort to create new cyber norms as some actors have begun the negotiation process to move toward norm creation.[140] She conceded that more work is needed and concluded that successful efforts to create new cyber norms that have the potential to succeed should include the following:[141]

- Norms that are simple and clear, as an overly complex approach will likely not reach the broad audience needed to secure cyberspace
- Grafting cyber norms onto an existing normative framework like human rights or the laws of war may help new norms seem intuitive and enhance compliance
- Multipronged efforts to create and disseminate new norms among diverse audiences will likely yield more rapid progress than focusing on a sole norm-building effort such as single treaty negotiation.
- Treating norms and laws as complementary tools because a judicious use of both will provide the best results
- Technical assistance and funding to help key actors "do the right thing" in cyberspace will greatly increase compliance.

New ideas, such as cooperation and norms, build upon some concepts that have migrated from nuclear deterrence theory to shape alternative visions for cyber deterrence theory.[142] In the midst of this debate, some scholars continued to advocate the irrelevance of cyber deterrence.

---

[139] Scott W. Beidleman, *Defining and Deterring Cyber War* (Carlisle Barracks, PA: U.S. Army War College, June 1, 2009), 20–22, http://www.hsdl.org/?view&did=28659. U.S. Air Force Lt. Col. Beidleman submitted this thesis as a graduate student at the U.S. Army War College, Carlisle Barracks, PA. Beidleman's use of the phrase "imprecise threshold" refers to Article 2(4) and Article 51 of the UN Charter, see Tikk et al., *Cyber Attacks Against Georgia: Legal Lessons Identified* (Tallinn, Estonia: CCDCOE, November 2008), 22, http://www.carlisle.army.mil/DIME/documents/Georgia%201%200.pdf.

[140] Martha Finnemore, "Cultivating International Cyber Norms," in *America's Cyber Future* (Center for a New American Security, 2011), 95. Finnemore offered NATO as an example of an organization that is actively providing a forum for cyber norm discussion among its members.

[141] Ibid., 89–90.

[142] The ideas and frameworks of the cyber scholars referenced in this chapter provided a basis for the theory of cyber deterrence that emerges from the case studies, which is offered later in this study. The effort of this research to migrate concepts that exist in the body of this literature from an assortment of ideas and frameworks to theory fully acknowledges the work of these early cyber deterrence pioneers.

The Continuing Irrelevance of Cyber Deterrence

Martin Libicki, in *Cyberdeterrence and Cyberwar*, offered a straightforward message with a conclusion that was unchanged from his first wave study. Libicki, in re-examining the cyber domain, used the major tenets of nuclear deterrence as a template. He observed that cyber deterrence "seems like it would be a good idea," "game theory supports the belief that it might work," and the Cold War "provides the historical basis for believing cyberdeterrence should work."[143] Libicki acknowledged, "It may well work" but then he laid out a series of questions that differentiated nuclear deterrence from cyberdeterrence, which he concluded works, "to the detriment of cyberdeterrence as a policy." See Table 3.2.[144]

Table 3.2: Factors That Make Cyber Deterrence Problematic[145]

Question	Effect on Cyber Deterrence
1. Do we know who did it?	Cannot know whom to retaliate against
2. Can we hold their assets at risk?	Do not know whether retaliation will have desired effect and thereby deter
3. Can we do so repeatedly?	Cannot know whether retaliation is repeatable
4. If retaliation does not deter, can it disarm?	No second prize for failure to deter
5. Will third parties join the fight?	Will interfere with signaling
6. Does retaliation send the right message to our side?	Deterrence policy may create moral hazard
7. Do we have a threshold for response?	Will interfere with signaling
8. Can we avoid escalation?	Risks of counterretaliation may reduce credibility of retaliation
9. What if the attacker has little worth hitting?	Retaliation could be an exercise in futility

Libicki's first three questions are critical, and the latter six are ancillary.

[143] Libicki and Project Air Force, *Cyberdeterrence and Cyberwar*, 39.
[144] Ibid.
[145] Ibid., 120. Table 2.6 is adapted from Libicki's Table 6.1 "Not All Factors That Make Cyberdeterrence Problematic Make Cyberwar Problematic." To examine Libicki's expanded comment on these questions, see pages 41-74.

Observers can trace each of these nine questions to the requirements for nuclear deterrence. The first question is about attribution, in which he assessed the difficulty in assigning blame for attacks. He observed that without an adversary, a deterring state has no one to punish.[146] As previously addressed, there is disagreement among scholars regarding attribution. Offering a view that attribution may not matter at all, Panayotis Yannakogeorgos concluded that it is a "myth" that cyber deterrence requires attribution.[147] David Clark and Susan Landau offer yet another theme as they argued that the technical challenges of attribution are not an "issue at all." What matters with attribution is that states see the challenge as a "policy concern with multiple solutions depending on the type of technical issue."[148]

Libicki's second, third, and ninth questions relate to the capacity to

---

[146] It is conceivable that Libicki's objection may prove less challenging for states than non-state actors. If so, recommendations by other scholars to pursue tailored cyber deterrence might yield results.

[147] Panayotis Yannakogeorgos, "Thought Leader Perspective: Dr. Panayotis Yannakogeorgos", August 25, 2011, http://www.nsci-va.org/SeniorLeaderPerspectives/2011-08-25-CyberPro-Pano%20Yannakogeorgos.pdf. Yannakogeorgos said that cyber attacks "exploit poor international cooperation resulting from a lack of harmonized cyber security action plans at the national level." He argued that this lack of international cooperation "is a root cause of the cyber attribution challenge." If states are held accountable for "bringing to justice any individual, group, or entity committing any malicious acts within their cyberspace," then "voluntary norms of behavior developed within United Nations over the past decade could guide a doctrine of state responsibility." Dr. Panayotis Yannakogeorgos is a cyber defense analyst with the U.S. Air Force Research Institute.

[148] David D. Clark and Susan Landau, "Untangling Attribution," in *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy* (Washington, DC: The National Academies Press, 2010), 39, http://www.nap.edu/catalog.php?record_id=12997#toc. Examples of technical issues may include a DDoS attack or data exfiltration. The forms of attack and the vulnerabilities that allow them will be examined in the forthcoming case studies. W. Earl Boebert sustained Clark and Landau's conclusion as he noted that the obstacles to alternatives for forensic-based attribution such as sustained covert intelligence and hack back are primarily nontechnical and are of a policy or legal nature. See pages 49, 52 in W. Earl Boebert's, "A Survey of Challenges in Attribution," in *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy* (Washington, DC: The National Academies Press, 2010). David Clark is a Senior Research Scientist at the MIT Computer Science and Artificial Intelligence Laboratory. Susan Landau is a visiting scholar at Harvard's Computer Science Department, formerly a Distinguished Engineer at Sun Microsystems.

punish. He reasoned that if an adversary has nothing to hold at risk, then a threat is empty and retaliation impossible. Libicki is susceptible to criticism with this position. While it may be true that the cyber capabilities of some actors are difficult to hold at risk, it appears far-fetched, perhaps naïve, to limit state responses to an in-kind attack. Why should a state only respond to a cyber attack with cyber capabilities? With robust intelligence, time, and an array of kinetic and nonkinetic capabilities, the valued object of any actor can be determined and held at risk.[149]

Regarding the ability to deter follow-on attacks, Libicki observed that once a state exploits cyber vulnerability by a retaliatory attack, an adversary would make every effort to close that vulnerability. Libicki's assumption limited the deterrer to an in-kind response, which suits the purpose for his argument but may fall short in describing how a state executes its cyber policy. Additionally, Libicki determined that the use of an active cyber defense would suffer from a similar limitation. The deterrer's "cyberattack capability is more likely to lose its punch by being used than by being attacked" because the attacker will close those aspects of the attack profile that were vulnerable to active defenses.[150] In this circumstance, Libicki argued that retaliation would fail on two counts because a potential attacker is neither deterred nor disarmed.

Libicki's fifth, sixth, and seventh points focused on signaling. If a cyber exchange incites a third-party hacker, then signaling is likely to become muddled

[149] This does not suggest that a deterring actor can avoid moral decisions in determining what of value to an adversary it holds at risk.
[150] Libicki and Project Air Force, *Cyberdeterrence and Cyberwar*, 61.

between states.[151] States must also worry about sending the wrong signal domestically. A state can unintentionally undermine deterrence if it enacts policy that "immunize(s) infrastructure owners against risk." This can result in private companies evading their cyber security obligations by conferring responsibility to the state.[152] In addition, establishing a threshold for response causes a problem with signaling as difficulties arise when deciding to retaliate because the stakes become higher and the proportionality of the response is often unclear.

Although Libicki did not believe that cyber deterrence "worked as a policy," he conceded that the role of escalation, impact of will on credibility, and value of defense in enhancing credibility in cyber deterrence are important theoretical considerations. Escalation is a concern for cyber strategists because it is not difficult to imagine that deterring actors will fail to incorporate its uncertainty into the threat equation. It is uncertain because a state can never be sure if an attacker would escalate in response to a retaliatory attack. Further, an attacker could escalate with capabilities that dramatically increase the level of violence to include nuclear weapons. An attacker is likely to escalate if it:[153]

1. Does not believe cyberretaliation is merited
2. Faces internal pressures to respond in an obviously painful way
3. Believes it will lose in a cyber tit-for-tat but can counter in domains where it enjoys superiority

Libicki also examined the role of will and credibility in cyber deterrence theory. He argued that will is less important in cyber than nuclear deterrence because what matters in cyber deterrence is whether a deterring state has

[151] Ibid., 62–63.
[152] Ibid., 63–65.
[153] Ibid., 69.

retaliated. This means that a state's will to retaliate for a cyber attack has the potential for greater impact on the credibility of the deterring state. Regarding credibility, he concluded that the robustness of a state's cyber defenses enhanced credibility for three reasons:[154]

1. The better one's defenses, the less likely an attack will succeed and the less often a cyber deterrence policy will be tested.
2. A good defense adds credibility to the threat to retaliate.
3. Good defenses have a way of filtering out third-party attacks, which facilitates attribution by elimination.

Richard Harknett in re-examining cyber deterrence joined John Callaghan and Rudi Kauffman to reach the same conclusion as that from his first wave research: "What has worked in the nuclear realm ... will not work in cyberspace." The trio used a similar approach from Harknett's earlier effort that led them to argue that the U.S. must "set aside deterrence" and adopt an "offense-defense strategic framework."[155]

Attacks occur constantly in the cyber domain; therefore, the U.S. needs cyber "warfighting capabilities," instead of "war avoidance postures." The defensive features of these warfighting capabilities must be able to "actively blunt attacks" as opposed to dissuading or deterring them. And offensive capabilities must be able to degrade a potential attacker's "capacity to sustain attacks" to protect U.S. security interests.[156]

Harknett et al argued that adopting an offense-defense approach

---

[154] Ibid., 73–74.
[155] Richard J. Harknett, John P. Callaghan, and Rudi Kauffman, "Leaving Deterrence Behind: War-Fighting and National Cybersecurity," *Journal of Homeland Security and Emergency Management* 7, no. 1 (January 1, 2010): 1–2, https://www-hsdl-org.ezproxy.library.tufts.edu/?abstract&doc=120294&coll=documents&url=http://www.bepress.com.ezproxy.library.tufts.edu/cgi/viewcontent.cgi?article=1636%26context=jhsem.
[156] Ibid., 20.

reinvigorates the "historical posture of traditional warfare," thus allowing the U.S. to assume a warfighting demeanor and move beyond the "fifty-plus-year comfort zone of deterrence." Such an approach would permit the U.S. to manage "cyber-leveraged war" to reduce potential harm from cyber aggression. With the nation's effort organized around preparing and fighting wars rather than the "hope of avoidance," the goal of achieving cyber security will be easier to reach.[157]

Kenneth Geers was not as harsh as Harknett et al in condemning cyber deterrence, but he was close. He concluded that cyber deterrence "will take time" because without attribution, it is impossible for an attacker to "feel deterred."[158] To reach this conclusion, he conducted a thorough examination of denial and punishment. This included a review of three requirements to execute deterrence: capability, communication, and credibility.[159]

Geers determined that both denial and punishment lacked credibility. A denial approach was unlikely to work because actors easily obtained cyber attack technology, international legal frameworks were insufficiently developed, there was no cyber inspection regime, and a prevailing perception existed that cyber attacks did not warrant a deterrence response because they did not constitute a substantial threat. Geers reasoned that punishment offered the only "real" option, but this component of deterrence strategy also lacked credibility because of

---

[157] Ibid. Harknett et al do not refer to specific cyber offensive capabilities in their analysis.
[158] Geers, *Strategic Cyber Security*, 121. Dr. Geers is the U.S. Naval Criminal Investigative Service (NCIS) Cyber Subject Matter Expert and was the first U.S. Representative to the Cooperative Cyber Defence Centre of Excellence in Tallinn, Estonia
[159] Ibid., 111. Geers concluded that nations with "robust military, law enforcement, and/or diplomatic might" have the capability (theoretically) to punish an attacker (assuming attribution is possible) either in cyberspace or in a physical domain; see pages 117-118. Regarding communication, for cyber deterrence to be successful, "cyber deterrence should be clearly written," and "an adversary should have no doubt what the consequences will be if the red lines are crossed." See pages 119-120.

attribution and asymmetry.[160]

Lastly, James Lewis stringently discouraged pursuing cyber deterrence as U.S. national policy. He cautioned that the "notion of cyber deterrence was appealing because it was unilateral and it justified building offensive capabilities." Lewis observed that the U.S. possesses advanced offensive cyber capabilities, perhaps the best in the world, but has failed to achieve any measure of deterrence. Lewis concluded that this was clear evidence that cyber-offensive weapons do not deter.[161] As an alternative, Lewis proposed that the U.S. emphasize defensive capabilities and multilateral agreements because with this approach a state could achieve "real security."[162]

Cooperation in the Cyber Warfare Era

An opportunity for states to deter malicious state and non-state actors may rest in part upon deterrence through cooperative measures. Although much work remains, this section provides an overview of cooperation that already exists between adversarial and non-adversarial states pertaining to cyber war. These efforts include the law of war as it pertains to cyber war and international legal regimes that directly and indirectly govern cyber attacks.

---

[160] Ibid., 121. Geers recommended that aside from solving the attribution problem, legal foundation, defenses, and deterrence strategies were needed as quickly as possible, but achieving all of this would take time. Geers did not elaborate on which actors held a "prevailing perception" that cyber attacks did not warrant a deterrence response.

[161] James Andrew Lewis, *Fog of Cyberwar: Discouraging Deterrence* (Switzerland: International Relations and Security Network, 2009), http://www.isn.ethz.ch/isn/Current-Affairs/Special-Reports/The-Fog-of-Cyberwar/Deterrence/. James Lewis is a senior fellow and director of the CSIS Technology and Public Policy program.

[162] Ibid. Lewis stressed the predominance of the defensive over the offensive, but also observed that there is value in both. It may be that in the cyber realm, as was the case with nuclear deterrence, offense and defense are often indistinguishable. Clearly, in the current iteration of cyber conflict, at least publicly, the defense dominates, but technological advances, particularly in attribution, may see this balance shift.

Law of War and Cyber War

The law of war, established in customary international law, encompasses the global community of nations' recognition of *jus ad bellum* and *jus in bello*. Jus ad bellum "lays out when states may lawfully resort to armed conflict." While jus in bello (law of armed conflict) "governs the actual use of force during war."[163]

The UN Charter in Article 51 provides the legal foundation for the use of force in self-defense under jus ad bellum.[164] For states to invoke self-defense under the Charter, it is necessary to "decide if a cyber exploit constitutes an armed attack."[165] Much ambiguity exists regarding Article 51 and cyber attack/war.

Uncertainty is also fueled by a "general consensus" among some scholars that the UN Charter's Article 2(4) merely "prohibits only physical armed force" in the historic kinetic sense. Coincidentally, others argue that cyber attacks "may violate the customary international law norm of nonintervention."[166] Ambiguity extending from these factors existed during the both the Estonia and Georgia cyber wars and will be explored in each case study.

---

[163] Carr, *Inside Cyber Warfare*, 48.

[164] James A. Lewis, *A Note of the Laws of War in Cyberspace* (Center for Strategic and International Studies, April 2010), 1-2, http://csis.org/files/publication/100425_Laws%20of%20War%20Applicable%20to%20Cyber%20Conflict.pdf. Article 51 states, "Nothing in the present Charter shall impair the inherent right of individual or collective self-defence if an armed attack occurs against a Member of the United Nations, until the Security Council has taken measures necessary to maintain international peace and security." Article 2, paragraph 4 of the UN Charter states that "All members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations" and serves with Article 51 to "provide provide the legal framework for 'Jus ad bellum' and decisions on the use of force in self-defense."

[165] Ibid., 2.

[166] Oona A. Hathaway et al., "The Law of Cyber-Attack," *California Law Review* (2012): 28–29. The customary international law norm of nonintervention, "prohibits states from interfering in the internal affairs of other states," see page 27.

In considering an application of jus ad bellum, there are three prevailing views regarding when a cyber attack constitutes an armed attack. These are instrument-based approaches, target-based approaches, and effects-based approaches.[167] The effects-based approach, which "classifies a cyber-attack as an armed attack based on the gravity of its effects" is the most widely accepted. However, a major problem exists with this approach, that remains unresolved – when to respond?

The laws of war, as they currently exist, do "not regulate the vast majority of cyber-attacks."[168] Insight into the following legal regimes offers some evidence of movement to adapt to the challenges of cyber attacks and cyber war. However, the traditional notions of warfare do not accommodate the technological developments that permit destruction of a different order in cyber war. While the scale remains smaller than traditional kinetic war at present, non-kinetic wars have the potential for lethality, which means that they should be treated as war as a matter of policy.

International Legal Regimes Directly Applicable to Cyber War

With exception of Council of Europe's Convention on Cybercrime, "most international agreements have not proceeded beyond the stage of discussing future strategies."[169] The UN, NATO, and the Shanghai Cooperation Organization

[167] Ibid., 32-33. The instrument-based is the classical approach, which stipulates that a cyber attack is not an armed attack under Article 51, because it does not use "traditional military weapons." The target-based approach "broadly sanctions forceful self-defense" to protect critical systems. In this approach, a conventional kinetic response is justified in response to a cyber attack.
[168] Ibid., 44.
[169] Ibid., 54.

International have made some efforts, albeit non-encompassing, to directly regulate cyber attacks.

Council of Europe

The Council of Europe's 2001 Convention on Cybercrime remains the most significant international cooperative effort in the cyber domain. The treaty identified criminal offenses that address several categories of cyber crime, which include offenses against the confidentiality, integrity, and availability of computer data and systems (illegal access, interception, data interruption, system interference); computer-related offenses (forgery and fraud); content-related offenses (child pornography); and copyright infringements.[170]

Cooperation featured prominently in this treaty, particularly the mutual assistance and extradition clauses. However, the treaty was limited in that it "addressed only a portion of the overall challenge." Further, the treaty has failed in the broader sense because its membership is regional in nature and it has done nothing to "regulate most attacks by state parties."[171]

United Nations

The role of the UN has been "largely limited to discussions and informational sharing." The UN's limited cyber security actions have included several vague resolutions, which "have not required any specific action by U.N. members." Although these recommendations were of minimal consequence, they

[170] Council of Europe, "Convention on Cybercrime", November 23, 2001, http://conventions.coe.int/Treaty/en/Treaties/html/185.htm.
[171] Hathaway et al., "The Law of Cyber-Attack," 52.

may eventually prove useful in brokering differences between Russia and the U.S.[172]

North Atlantic Treaty Organization

With the 2007 Estonia and 2008 Georgia cyber war experiences as catalysts, NATO moved towards articulating strategies and taking actions to counter cyber attacks on member states. In 2008, NATO member states ratified the NATO Cyber Defense Policy, created the Cyber Defense Management Authority, and established the Cooperative Cyber Defense Center of Excellence (CCD COE).[173] Of these efforts, the CCD COE or "Center," which became operational in Tallinn, Estonia in October 2008, has significantly enhanced member cooperation around its goal of increasing cyber security.[174]

The CCD COE has used a series of conferences and various publications to educate members. Aside from the CCD COE, NATO has made significant strides in its cyber defense posture, but much more is needed. Despite this progress, it appears that NATO did not fully appreciate the harsh lessons learned by Estonia and Georgia during their cyber wars.

With the exception of the limited role of the CCD COE, NATO is basically useless to help countries deter or respond to cyber attacks as in these circumstances it will "only activate Article 4 of the NATO treaty, which calls upon members to "consult together" in cases of cyber-attacks." Under Article 4,

[172] Ibid., 48–50.
[173] Laasme, "Estonia: Cyber Window into the Future of NATO," 61.
[174] "Cyber Defense," CCD COE, n.d., http://www.ccdcoe.org/.

members are not bound to "assist each other, as would be required under Article 5."[175]

Shanghai Cooperation Organization

The Shanghai Cooperation Organization with the June 2009 Yekaterinburg Declaration emphasized that international information security was "one of the key elements of the common system of international security." The organization adopted an "expansive vision of cyber-attacks to include the use of cyber-technology to undermine political stability." This means that member states including China and Russia are positioned to "be at odds with that of Europe and the United States, which have sought to avoid regulations of cyber-activities that may interfere with the expression of political dissent."[176]

International Legal Regimes Indirectly Applicable to Cyber Attacks

International legal regimes that indirectly regulate cyber attacks include International Telecommunications Law, Aviation Law, Law of Space, and Law of the Sea. These regimes regulate portions of the cyber domain that may be used in cyber attacks. They pre-date the emergence of cyber attacks and therefore, do not "expressly regulate or prohibit cyber-attacks"[177]

International Telecommunications Law

International Telecommunications Law is regulated by a UN agency, the International Telecommunications Union. This law is applicable in circumstances where cyber attacks use international wire or radio frequency communications. The law "cautions against harmful interference, but it allows for military

[175] Hathaway et al., "The Law of Cyber-Attack," 51.
[176] Ibid., 54.
[177] Ibid.

transgressions," which include cyber attacks. Because there are no limits on military use or a mandatory reporting requirement, there are no "teeth" to this law regarding cyber attacks.[178]

International Aviation Law

Cyber attacks that disrupt air traffic control, modify airline passenger lists, or modify no-fly lists are examples of acts covered by aviation law. There are three significant aviation laws that have implications for cyber attacks.[179]

- 1944 Chicago Convention on International Civil Aviation (Chicago Convention)
- 1971 Montreal Convention on the Suppression of Unlawful Acts Against Civil Aviation (Montreal Convention)
- 1988 Protocol for the Suppression of Unlawful Acts of Violence at Airports Serving Civil Aviation (Montreal Protocol)

The Chicago Convention could be invoked if a state uses cyber attacks to target civilian flights. However, an exception permits member states to "disregard the Convention during war or state emergencies."[180] The Montreal Convention covers cyber attacks that would "jeopardize the safety of civil aviation." However, this convention is limited in that it does not apply to any cyber attack unless it "renders an aircraft unable to fly."[181] The Montreal Protocol moved beyond airborne civil aviation to address airport safety. Under this law, prohibited acts related to cyber attacks must endanger airport safety. Examples include "tampering with no-fly lists, passenger manifests, or an airport's computer network system."[182]

---

[178] Ibid., 55–57.
[179] Ibid., 57.
[180] Ibid., 57–58.
[181] Ibid., 58–59.
[182] Ibid., 59.

International Space Law

Computers control satellites that are critical components in military operations and international telecommunications. Cyber attacks are prohibited by the 1967 Outer Space Treaty, which forbids the use of space for "particular destructive purposes."[183] Two follow-on agreements, the Agreement Relating to the 1971 International Telecommunications Satellite Organization (Telecommunications Satellite Organization) and the Convention of the 1979 International Maritime Satellite Organization (Maritime Satellite Organization), "have little impact on cyber attacks." The controlling organizations for these agreements are not positioned to "promulgate public regulations related to cyber attacks."[184]

Law of the Sea

Articles 19, 109, and 113 of the 1982 United Nations Convention on the Law of the Sea (UNCLOS) are applicable to cyber attacks if one interprets these articles as applying to "the use of computer systems on vessels that are at sea." Article 19 addresses a state's "right of innocent passage." The Article prohibits a threat or the use of force against a state and lists collecting information or engaging in acts of propaganda harmful to a state's defense and interfering with a state's communications systems as egregious acts.[185]

Article 109 suggests that states "should cooperate in suppressing unauthorized broadcasting from the high seas." Article 113 "requires states to put in place domestic criminal legislation to punish willful damage to submarine

[183] Ibid., 60.
[184] Ibid., 60–61.
[185] Ibid., 62–63.

cables." To the extent these articles address cyber attacks originating from or transiting the seas, "some minimal legal protections" are in place.[186]

An Evolution in U.S. Cyber Deterrence Policy?

In addressing the thirty-eighth Institute for Foreign Policy Analysis (IFPA)-Fletcher Conference, former Deputy Secretary of Defense William Lynn said, "Cyber security issues are driving a reevaluation of traditional security concepts and strategies."[187] An examination of U.S. policy documents from the second wave demonstrated that this "reevaluation" was well under way – of which cyber deterrence was a prominent fixture. Senior U.S. political and military leaders lent credibility to the theory of cyber deterrence because of its inclusion in nearly every national strategic-level document from the Obama and former Bush presidential administrations. Unfortunately, consensus on the requirements for theory or strategy to deter state and non-state actors from engaging in cyber war remained unclear.

The 2007 Estonia and 2008 Georgia crises provided a wake-up call in the U.S. In 2009, early in his administration, President Barack Obama directed a comprehensive, sixty-day assessment of U.S. cyber security policies. The May 2009 Cyberspace Policy Review's assessment incorporated a different twist from previous government documents. The review identified an end-state goal to achieve a trusted information infrastructure that the nation can depend upon for its

[186] Ibid., 63.
[187] *Air, Space, & Cyberspace Power in the 21st-Century* (Cambridge, MA: Institute for Foreign Policy Analysis, Inc., 2010), 15.

security and commerce.[188] A trusted information infrastructure constructed by a national partnership between public and private organizations would have four outcomes:[189]

1. Enhance economic prosperity and facilitate U.S. market leadership in the information and communications industry;
2. Enable the United States to deter, prevent, detect, defend against, respond to, and remediate interruptions and damage to U.S. information and communications infrastructure;
3. Ensure U.S. capabilities to operate in cyberspace in support of national goals; while at the same time;
4. Protect privacy rights and preserving civil liberties.

This document may prove seminal as it considered cyber deterrence necessary for a successful outcome of a new infrastructure. Additionally, for the first time, the extent of the cyber threat had a U.S. president's attention.[190] In quick succession, through 2010 and 2011, a series of U.S. policy documents prominently addressed the threat of cyber attacks and espionage.

The February 2010 QDR advocated a defensive cyber posture built upon training U.S. forces, adapting organizational structures, and improving international cooperation.[191] The report emphasized pursuing a tailored approach to deterrence and observed, "Such tailoring requires an in-depth understanding of

---

[188] The White House, *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure* (The White House, May 2009), 1.
[189] Ibid., B–1.
[190] The White House, "Remarks by the President on Securing Our Nation's Cyber Infrastructure," May 29, 2009, http://www.whitehouse.gov/the-press-office/remarks-president-securing-our-nations-cyber-infrastructure. President Obama noted that he directed the four-month Cyberspace Policy Review shortly after entering office. He recounted recent cyber threats to the U.S., including his personal experience of being the target of hackers to demonstrate the imperative he placed on the challenge. He observed that the cyber threat is one of the "most serious and economic and national security challenges we face as a nation."
[191] Department of Defense, *Quadrennial Defense Review Report* (Washington, DC: Department of Defense, February 2010), 38-39. The QDR did not elaborate on training U.S. cyber forces beyond stating a goal of improving "efforts to imbue its personnel with a greater appreciation for the threats and vulnerabilities in the cyber domain and to give them the skills to counter those threats and reduce those vulnerabilities at the user and system administrator levels."

the capabilities, values, intent, and decision making of potential adversaries, whether they are individuals, networks, or states."[192] To strengthen U.S. deterrence capacity, the report identified the need to improve attribution in cyberspace, develop better capabilities to conduct cyberspace operations, and "foster" international cyber norms.[193]

In March 2010, the Obama administration publicly released components of the Comprehensive National Cybersecurity Initiative (CNCI),[194] while updating the CNCI to incorporate recommendations from the 2009 Cyberspace Policy Review. These recommendations included establishing a defensive line against cyber threats and efforts to strengthen the future cybersecurity environment.[195]

Within two months of the public release of the updated CNCI, President Obama published the 2010 NSS. The NSS made it clear that the U.S. will continue to field forces to deter both state and non-state actors in the cyber

---

[192] Ibid., 14. Elsewhere, the reported stated that the U.S. "deterrent remains grounded in land, air, and naval forces." See page v. This implies that cyberdeterrence is not "grounded" in the U.S. deterrence posture and that more work is required on the policy and theory, which serves as its foundation.

[193] Ibid., 14–15. The QDR did not elaborate on how to achieve the goal of fostering international cyber norms. The report was limited to broad language that expressed an objective to "collaborate with other U.S. departments and agencies and international partners both to support their efforts and to ensure our ability to operate in cyberspace," see page 39.

[194] The Bush administration developed the CNCI in 2008, and the prominent details had remained in secrecy since that time. The CNCI strategy was "codified in NSPD-54/HSPD-23 and initiated programs focused primarily on the security of Executive Branch networks, which represent only a fraction of the global information and communications infrastructure on which the United States depends." See page 4, The White House, *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure*.

[195] The White House, *The Comprehensive National Cybersecurity Initiative* (Washington, DC: The White House, March 2010), 1–2, https://www-hsdl-org.ezproxy.library.tufts.edu/?view&doc=118707&coll=limited. Efforts to strengthen the future cybersecurity environment included "expanding cyber education; coordinating and redirecting research and development efforts across the Federal Government; and working to define and develop strategies to deter hostile or malicious activity in cyberspace." See page 2. As mentioned earlier in reference to other government documents, the language in the CNCI seemed vague, presumably due to security classification issues.

domain. The strategy highlighted the cyber threats from criminal hackers, organized crime, terrorist networks, and states.[196]

The 2010 NSS continued a theme that was common in other U.S. strategy documents as the specifics remained unclear as to how the U.S. was to accomplish cyber deterrence. The level of detail did not go much further than a declaration that the U.S. will "deter, prevent, detect, defend against, and quickly recover from cyber intrusions and attacks" through several avenues.[197] The strategy broadly proposed to counter these attacks with additional investment in people and technology and increasing cooperation by expanding domestic and international partnerships.

The NSS, in conjunction with the CNCI, linked the theory of deterrence to the physical world of the cyber infrastructure. The integrating agent came in the form of the National Cyber Incident Response Plan Interim Version (NCIRP). The September 2010 NCIRP incorporated aspects of the strategy, recommendations, and findings from many of the documents reviewed previously in the first and second waves. The NCIRP addressed how the U.S. will respond to a cyber attack by presenting the actions of the incident response cycle and the roles and responsibilities of mission partners.[198]

---

[196] The White House, *National Security Strategy* (Washington, DC: The White House, May 2010), 27, http://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf.
[197] Ibid., 27–28.
[198] Department of Homeland Security, *National Cyber Incident Response Plan - Interim Version* (Washington, DC: Department of Homeland Security, September 2010), 24–29, http://www.federalnewsradio.com/pdfs/NCIRP_Interim_Version_September_2010.pdf. When prevention and protection efforts fail, coordination between mission partners using a common operational picture proceeds through four sequential steps to complete the cyber incident response cycle. These steps are first to detect the incident, then the incident is analyzed to determine if the act was an attack or an accident. Third, if needed, response activities are coordinated and conducted by the mission partners. Lastly, resolve means that the intended outcomes are

Building upon the initiatives of 2010, the following year saw a marked increase in attention to U.S. cyber policy, beginning with an update to the NMS in February 2011.[199] The strategy recognized that deterrence principles had to be adapted because several factors made it more difficult to deter cyber aggressors. The NMS highlighted these factors as "lack of international norms, difficulties of attribution, low barriers to entry, and the relative ease of developing potent capabilities."[200] The strategy did not provide specific details on the U.S. military's approach to countering these factors other than to note that the U.S. Strategic Command and U.S. Cyber Command will coordinate with domestic and international partners to "develop new cyber norms, capabilities, organizations, and skills."[201]

In May 2011, the Obama administration published the *International Strategy for Cyberspace*, which presented an approach rooted in deterrence and

---

examined to determine if the appropriate response has been employed or it additional coordination is required. Universal roles and responsibilities are designed to ensure all participating agencies (mission partners) are prepared to respond as needed. Preparedness activities include engaging with other organizations, planning responses, organizing and equipping, training and exercising, and constant evaluation to improve the incident response cycle.

[199] Chairman of the Joint Chiefs of Staff, *The National Military Strategy of the United States of America* (Washington, DC: Joint Chiefs of Staff, February 2011), https://www-hsdl-org.ezproxy.library.tufts.edu/?view&did=10755. The purpose of the NMS is to provide the ways and means by which the U.S. military accomplishes the objectives of the 2010 NSS; see CJCS cover letter.

[200] Ibid., 3–8.

[201] Ibid., 10. U.S. Strategic Command (USSTRATCOM) is one of nine U.S. combatant commands, and its mission is to detect, deter, and prevent nuclear, space, and cyber attacks against the U.S. and allies; see "United States Strategic Command," *United States Strategic Command*, n.d., http://www.stratcom.mil/. U.S. Cyber Command (USCYBERCOM) is a component of USSTRATCOM and was established by the Secretary of Defense on June 23, 2009. The command reached full operating capacity (FOC) on October 31, 2010. USCYBERCOM is responsible for a broad range of cyberspace operation to ensure the U.S. and allies have "freedom of action in cyberspace, while denying the same to adversaries"; see "United States Cyber Command," *United States Strategic Command*, n.d., http://www.stratcom.mil/. The commander of USCYBERCOM serves in a dual capacity as director of the U.S. National Security Agency (NSA). The NSA "leads the U.S. Government in cryptology that encompasses both Signals Intelligence (SIGINT) and Information Assurance (IA), and enables Computer Network Operations (CNO)," see "National Security Agency/Central Security Service", n.d., http://www.nsa.gov/.

dissuasion but was also heavily dependent upon enhancing cyber defenses, norm creation, and domestic and international cooperation. The strategy firmly stipulated that the cost of attacking or exploiting U.S. cyber infrastructure will "vastly outweigh" the reward. The strategy declared that the U.S. "reserves the right to use all necessary means" to defend its interests and those of allies from state and non-state "hostile acts in cyberspace."[202] This implied, for the first time, that the U.S. could consider a kinetic response to retaliate for a nonkinetic cyber attack. In response to this presidential strategic guidance, the DoD published the *Strategy for Operating in Cyberspace* in July 2011.

The *Strategy for Operating in Cyberspace* aggressively embraced a new position in declaring that cyberspace is an "operational domain" in which forces will be included with the other domains of land, sea, air, and space.[203] To deter internal and external "malicious actors" the strategy advocated four new defensive initiatives: Enhance cyber hygiene, strengthen internal information management capabilities, employ active cyber defenses, and develop new computing architectures.[204] Additional initiatives embraced expanding domestic and

---

[202] The White House, *International Strategy for Cyberspace - Prosperity, Security, and Openness in a Networked World* (Washington, DC: The White House, May 2011), 12-13, http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf. The strategy treated deterrence, defense, norm creation, and cooperation as distinct components.

[203] Department of Defense, *Department of Defense Strategy for Operating in Cyberspace* (Washington, DC: Department of Defense, July 2011), 5, http://www.defense.gov/home/features/2011/0411_cyberstrategy/docs/DoD_Strategy_for_Operating_in_Cyberspace_July_2011.pdf.

[204] Ibid., 6–7. Cyber hygiene is "taking simple precautions to reduce the cyber risks to national and economic security." Examples include installing anti-virus protection, using firewalls, and updating operating system and program software; see "National Cybersecurity Awareness Month Advocates Good 'Cyber Hygiene,'" *CIO.gov*.

international cyber coordination, training an "exceptional" cyber workforce, and improving the capacity to take advantage of rapid technological innovations.[205]

While these 2010 and 2011 policy documents represented significant movement in cyber policy, their usefulness was expressed by General Keith Alexander, Commander USCYBERCOM, who said in September 2011 that U.S. "cyber strategy is 'broken' and needs to be repaired."[206] In November 2011, within two months of these remarks, the U.S. issued declaratory policy for deterring cyber attacks in the DoD's *Cyberspace Policy Report.*

The *Cyberspace Policy Report* underscored that deterrence in cyberspace relies upon "denying an adversary's objectives" and "imposing costs" for aggression. The report stressed the familiar themes for the need to establish international "norms of behavior" and to enhance attribution capabilities. Of note, the report reiterated the right of the U.S. to use "all necessary means" to defend its interests in cyberspace.[207] In the short time between General Alexander's observation about U.S. cyber strategy and the release of the *Cyberspace Policy Report*, there was no indication in other policy documents or scholarly literature that the criticism leveled by General Alexander had become moot. This indicated that the U.S. issued declaratory cyber policy based on the foundation of a "broken" strategy.

---

[205] Ibid., 8–12. The strategy noted that international cooperation to build situational awareness and warning capabilities enabled collective deterrence.
[206] "Nation's Cyber Strategy Is 'Broken,' USCYBERCOM Commander Says," *Defense Systems*, September 14, 2011, http://www.defensesystems.com/Articles/2011/09/14/AGG-USCYBERCOM-Alexander-cyber-strategy-broken.aspx.
[207] Department of Defense, *Department of Defense Cyberspace Policy Report - A Report to Congress Pursuant to the National Defense Authorization Act for Fiscal Year 2011, Section 934*, 2–4.

Summary

There is no evidence that a widely accepted cyber deterrence theory exists or that the U.S. has a credible comprehensive cyber deterrence strategy. Cyber deterrence literature is exhaustive in contemplating the pros and cons of the various elements, some from nuclear deterrence and others from new ideas such as cooperation and norm formation. In the final analysis, that which exists in the scholarly community is a range of ideas and frameworks that have not coalesced to form an overarching theory upon which to base national policy. In U.S. policy, cyber deterrence exists, but only as a slogan because there is minimal, if any, operational impact on state and non-state actors that continue to attack and exploit the country.[208]

Existing notions of cyber deterrence combine elements of punishment, denial, and cooperation into a triadic concept to deter a potential adversary from initiating a cyber attack. This chapter traced the historical evolution of cyber deterrence by investigating its origin in the first wave and examining how it evolved through the second wave. While many of the elements that comprise cyber deterrence are similar to those of nuclear deterrence, they are also consistent with some aspects of criminal justice deterrence.

The large number of actors a state must deter suggests that some concepts of criminal justice prevention may augment cyber deterrence by denial more

[208] This observation excludes individuals as deterrence of cyber crime is beyond the scope of the study.

effectively than that of the nuclear model.[209] The pool of actors in criminal justice deterrence encompasses at most the entirety of the population and at the least a lesser subset of the population that is inclined to commit crimes. The pool of actors in nuclear deterrence is limited to those with nuclear weapons, initially two, but by the end of the Cold War far more states possessed nuclear capabilities.

The U.S. does not have to deter every malicious cyber actor; it only needs to deter state and non-state actors that cause the most harm. The potential of destruction from cyber war, while less than that from a nuclear attack, suggests that the nuclear approach to punishment may better inform an effort to deter cyber aggression from states; however, care should be taken to avoid escalation between peer states. The destructive capacity of nuclear weapons created an imperative whereby a state had to deter every potential nuclear-capable aggressor. In the criminal realm, the stakes are far less as the "system can still be viewed as succeeding despite the failures of threatened sanctions."[210] An approach that accepts the repetitive failure and subsequent resetting of deterrence may not be ideal given the stakes, but perhaps it could prove sufficient.

Requirements of Cyber Deterrence Theory

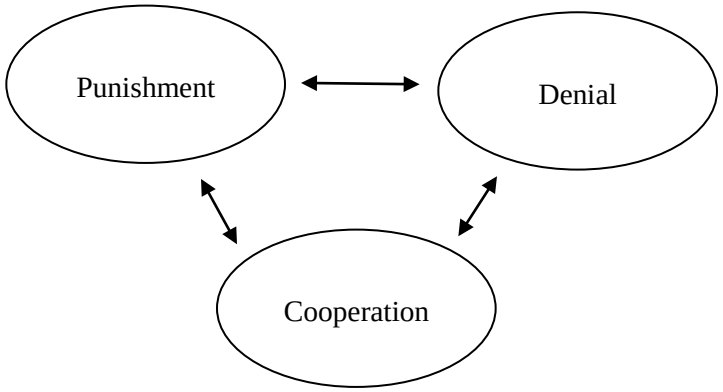
This section, drawing upon criminal justice, nuclear, and emerging cyber deterrence literature presents a theoretical concept for cyber deterrence that suggests how an actor may deter an attack on its information infrastructure. To raise the cost of malicious cyber attacks to a prohibitive point, actors may use a

[209] The analysis chapter of this study, based upon the findings from the case studies, will consider if there are additional aspects of nuclear deterrence by denial and criminal justice deterrence by prevention that inform alternative constructs for cyber deterrence.
[210] Wasserstrom, "War, Nuclear War, and Nuclear Deterrence," 443.

triadic approach for cyber deterrence, which has three core components: punishment, denial, and cooperation.

Each of these components may singly deter; however, when combined they interact to provide a sturdy theoretical foundation for cyber deterrence (see Figure 3.1). The causal mechanisms of punishment are offensive actions taken by a state to ensure a desired response or necessary conditions that are required for the threat of effective punishment to occur. The purpose of punishment or the threat of punishment is to increase a potential adversary's cost beyond the desired benefit – to escalate the cost such that it exceeds the benefits to be derived from the exploitation of a targeted state's cyber vulnerabilities.

Figure 3.1: Triadic Components of Cyber Deterrence



The causal mechanisms for denial are defensive, while the causal mechanisms for cooperation are preventive. The purpose of denial and cooperation is the same – to deny benefits. This occurs when a state on its own or in cooperation with others eliminates or reduces vulnerabilities, thus preventing cyber attacks and an ensuing cyber war. See Table 3.3 for a summary of the requirements for cyber deterrence to occur in theory.

There are eleven requirements to deter cyber war by punishment: rationality, social structure and value systems, attribution, threat, sanctions, communication, credibility, capability, will, transparency, and retaliation. Rationality is a requirement because for a threat to work, an adversary must have awareness of a social structure and value system and the capacity to understand available alternatives to determine risk.[211] The existence of a social structure and value system is necessary because this helps determine "people's respect for legal ideology and its administration."[212] If one state is to deter another in the cyber domain, then authorities must have the capacity to deter their respective populations; therefore, the capacity to abide by the law must be present among a population that includes potential offenders. Authorities must rely upon the threat or fear of sanctions between and within states to induce in potential offenders the inclination to refrain from committing malicious cyber acts. If the cost associated with a threat to that which a potential cyber attacker values is greater than the expected benefits, then that actor will not attack. [213]

Attribution is necessary to identify an actor to threaten or punish should deterrence fail.[214] However, some scholars argue that attribution is less relevant because of interdependency and entanglement.[215] This research has reconfirmed that attribution is necessary for cyber deterrence by punishment just as it is necessary in criminal justice and nuclear deterrence theory.

---

[211] Schelling, *The Strategy of Conflict*, 6–13.
[212] Ball, "The Deterrence Concept in Criminology and Law," 349.
[213] Hayes and Wheatley, *Information Warfare and Deterrence*.
[214] Libicki and Project Air Force, *Cyberdeterrence and Cyberwar*, 41.
[215] Joseph S. Nye, Jr., *Cyber Power*, 16.

The issuance of a threat is critically important and only works when the deterring state informs the potential aggressors what to expect in response to attacks.[216] Several factors influence the success of a threat. First, states should tailor threats to the class of actor because a cyber attack by a peer state warrants a different approach than a response to a non-state actor.[217] Second, the potential attacker must have something of value that the deterring state can threaten.[218] Third, there must be a clear statement of the activity a potential actor is to avoid.[219] Fourth, the deterring state needs to establish a threshold because, without this determination, there is no foundation from which to issue a threat or carry it out.[220] Lastly, controllability is a factor because of the uncertainty of escalation. Planning and executing a threat should take into account the potential for retaliatory action and resilience.[221]

In the cyber domain, formal sanctions should exist and accompany the issuance of a threat. States or groups of states may impose sanctions according to law or agreements.[222] Authorities' use of a threat of sanction to deter requires communication of the threat and sanction to potential offenders. For this communication to be effective, a state has to deliver a "clear and unambiguous" message that the potential attacker has to receive and understand.[223]

The requirements for effective cyber deterrence exceed the act of communicating a well-designed threat to a rational adversary. The threat must be

---

[216] Schelling, *The Strategy of Conflict*, 10.
[217] French, *Building a Deterrence Policy Against Strategic Information Warfare*, 1.
[218] Libicki, *Defending Cyberspace and Other Metaphors*, 44.
[219] Hayes and Wheatley, *Information Warfare and Deterrence*.
[220] Moore, "Prospects for Cyber Deterrence," 71–72.
[221] Libicki, *Defending Cyberspace and Other Metaphors*, 45–46.
[222] Kennedy, *Deterrence and Crime Prevention*, 31-34.
[223] Hayes and Wheatley, *Information Warfare and Deterrence*.

credible, which means that the potential attacker has to believe that the deterring state has the "will and capability" to follow through.[224] Additionally, cyber deterrence requires transparency of a state's potential capabilities because attackers must have a sense of a state's capacity to fulfill a promise to retaliate.[225]

The capacity to retaliate impresses upon a potential adversary that a state could respond if attacked. A response could be in kind, which requires the ability to reconstitute cyber forces. A response could be general in that a state could use kinetic capabilities to retaliate for a cyber attack.[226]

Denial is the second core component of cyber deterrence. A state employs denial by defensive means to prevent a malicious actor from attacking its critical information infrastructure. Capabilities that deny an adversary an unobstructed approach to sensitive information systems center on reducing cyber vulnerabilities through hardening, redundancy, training, and continuous vulnerability analysis.[227] The capacity for states to deny benefits to potential offenders requires that the deterring actor use these capabilities to defend or deny access to protected entities. Further, there are three defensive precautions that states can use to prevent cyber attacks and thus deter cyber war.

States can increase the level of effort required to attack their cyber infrastructure, increase the risks to potential attacks for undertaking cyber attacks, and reduce the reward for potential offenders to initiate a cyber war. To increase

---

[224] Ibid.
[225] Transparency is required in cyber deterrence to the point where a potential attacker appreciates the potential of a state's response. It would not be prudent to expose precise cyber capabilities as once a capability is revealed, it is possible for the vulnerabilities targeted by that capability to be closed.
[226] The White House, *Toward Deterrence in the Cyber Dimension: Report to the President's Commission on Critical Infrastructure Protection*, 8.
[227] Hayes and Wheatley, *Information Warfare and Deterrence*.

the effort for potential attackers, states should harden anticipated cyber targets and establish rigid network and systems access controls. To increase the risk for attackers, enhancing cyber surveillance is critical for early warning and detection of attacks as well as developing an understanding of a potential attacker's cyber vulnerabilities, which may be exploited in retaliation. Reducing the reward for initiating cyber war offers potential for large prevention dividends. These actions include removing or isolating the target that a potential attack covets, removing inducements for cyber attacks by eliminating and reducing vulnerabilities, and establishing rules among the community of nations that punish states for engaging in cyber warfare.[228]

Cooperation is the final core component of cyber deterrence. The causal mechanisms for cooperation are preventive and consist of four requirements: interdependency, norm creation, international law, and international agreements. Interdependency between states, particularly within and between networks, creates a dynamic that a state can exploit to influence the cost and benefit calculations of a potential attacker.[229] The development of norms is critical to the long-term success of cooperative efforts, as states must share a "common standard for the conduct of international transactions."[230] The formation of new norms helps to develop international law and agreements that have not kept pace with

[228] Clarke, "Situational Crime Prevention," 109–118. Clarke's taxonomy was explained in detail in an earlier section of this study, *Situational Crime Prevention*.
[229] Cooper, *New Approaches to Cyber-Deterrence: Initial Thoughts on a New Framework*, 134–141.
[230] Dogrul, Aslan, and Celik, "Developing an International Cooperation on Cyber Defense and Deterrence Against Cyber Terrorism," 38.

technological challenges.[231] International agreements are critical as they allow states to regulate cyber matters in accordance with the law of treaties. International agreements are not treaties, but they are executive in nature and generally easier to negotiate.[232]

Table 3.3: Core Components of Cyber Deterrence Theory[233]

Core Components	Causal Mechanisms	Purpose	Requirements	Rationale
Punishment	Offensive	Threat of punishment increases adversary's costs	Rationality	Adversary must have the capacity to weigh perceived gains against the risk of noncompliance
			Social structure and value system	Capacity to abide by the law must be present
			Attribution	- It is necessary to identify whom to threaten or punish if deterrence fails - Attribution is made less challenging by holding states accountable for the actions of those under state control.
			Threat	Clear statement of the behavior to be avoided is essential

[231] Ibid. Dogrul et al determined that an international legal framework is more critical to cyber deterrence than offensive and defensive capabilities.
[232] Mark Engsberg, "An Introduction to Sources for Treaty Research," *Hauser Global Law Program*, March 2006, http://www.nyulawglobal.org/Globalex/Treaty_Research.htm#_B._Treaties_and_International Agree. A treaty is a "formally signed and ratified agreement between two nations or sovereigns."
[233] These components for cyber deterrence were subjectively derived from the literature of criminal justice, nuclear, and cyber deterrence theory. The researcher believes that the literature provided sufficient evidence that each of these factors meet the standard for inclusion as a core component and supporting requirement.

Core Components	Causal Mechanisms	Purpose	Requirements	Rationale
			Sanctions	A source of pain is necessary to increase cost calculations of potential offenders
			Communication	Must be clear and unambiguous
			Credibility	Target believes the deterring actor has the will and capability to execute the threat
			Capability	Adversary must know the capacity exists to fulfill a threat
			Will	Adversary must be certain of an actor's fortitude to retaliate in response to an attack
			Transparency	Adversary must know that the (potential) capability exists to fulfill a threat.
			Second strike/resilience	Adversary must believe that a deterrer's capability to retaliate will remain following an attack.
Denial	Defensive	Deny benefits	Capability to deny	Reduce vulnerability by hardening, redundancy, and training.
			Increase the effort	Deny access to things someone wants to steal.
			Increase risks	Make it more likely that an

Core Components	Causal Mechanisms	Purpose	Requirements	Rationale
				offender will be detected
			Reduce rewards	If costs exceed benefits, a potential offender has been deterred
Cooperation	Preventive	Deny benefits	Interdependency	Creates a dynamic that can be exploited to influence an adversary's cost/benefit calculus
			Norm creation	Need a common standard for the conduct of international cyber transactions
			International law	New law helps account for technological changes to deter malicious cyber actors.
			International agreements	Allows states to regulate cyber matters in accordance with the law of treaties

Chapter 4: Russia vs. Estonia

What government needs to do is pay attention to industry experts that keep telling them where their holes are and then do the obvious – fix the holes.

– Clint Stewart[1]

Introduction

The world's first cyber war, ignited by the removal of a WWII-era Soviet memorial statue, took place between Russia and Estonia. It lasted for twenty-three days, beginning on April 26 and ending on May 18, 2007. The war consisted of two phases (see Figure 4.1 for an overview of the main events of the crisis). Phase I began on April 26 and ended on April 29, 2007. During this short period, the attacks were simple and targeted government web servers, news portals, and select websites for defacement.[2]

The main attack, Phase II, occurred between April 30 and May 18, 2007. The attacks in this phase were sophisticated, massive, and well coordinated. The principal offensive actions were distributed denial-of-service (DDoS) attacks against Estonia's critical information infrastructure, which included targeting the backbone routers of the data communications network and Domain Name System (DNS) servers. Many attacks were successful for only a short period, as the interruptions in the data communications backbone network lasted for less than five minutes (see Appendix B for additional information).

---

[1] "Security Experts Admit China Stole Secret Fighter Jet Plans | The Australian," *CYBER SECURITY Forum Initiative - CSFI*, March 12, 2012, http://www.linkedin.com/groupItem?view=&srchtype=discussedNews&gid=1836487&item=100388036&type=member&trk=eml-anet_dig-b_pd-ttl-cn&ut=2rNyMBCY1tFR81.

[2] Toomas Viira, "Cyber Attacks Against Estonia - Overview and Conclusions," in *Information Technology in Public Administration of Estonia - Yearbook 2007* (Tallinn, Estonia: Ministry of Economic Affairs and Communications, 2008), 71, http://www.riso.ee/en/files/IT_yearbook_2007_final.pdf. The Estonian Prime Minister's website was defaced in Phase I.

This war was the first cyber war. In conducting the war, Russia's offensive cyber attacks were politically motivated.[3] Their goal was to overload, with the intent of damaging, Estonia's cyber network.[4] Attackers primarily used variations of DDoS flood attacks, although efforts to modify some target's websites through defacement met with brief success.[5]

We cannot know whether deterrence based on an approach centered on a triadic relationship between denial, punishment, and cooperation would have prevented the cyber attack against Estonia. However, we can determine the extent

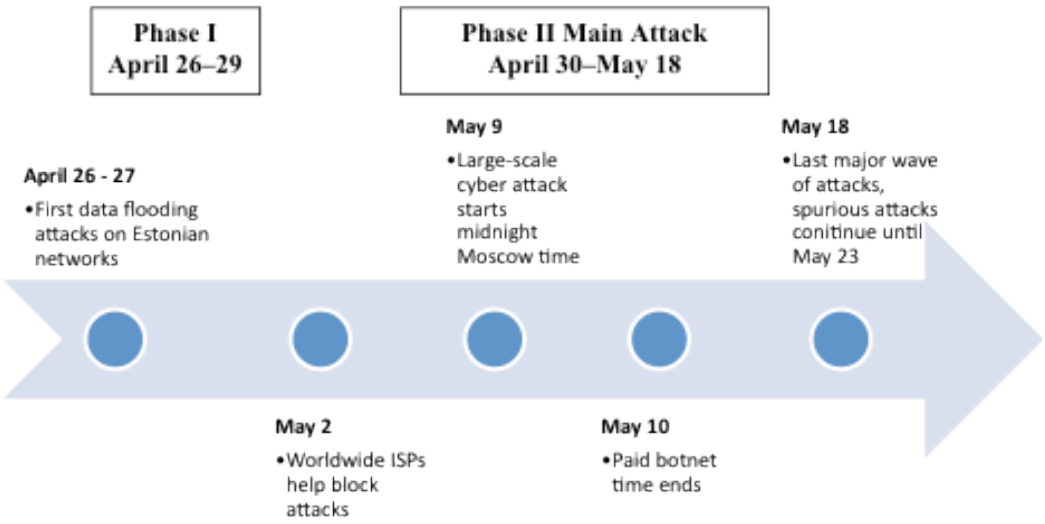
[3] The researcher felt it necessary to assert that this case represents the first cyber war because the literature includes arguments to the contrary, see Thomas Rid, "Think Again: Cyberwar," *Foreign Policy*, April 2012. The attacks in Estonia meet the threshold of Rid's definition of cyber war because it was violent, purposeful, and political. Because electric force is "one of the basic physical forces," this research concluded that Estonia's attackers used a form of physical force to "damage," thus meeting an established definition of violence and satisfying Rid's first requirement; see "Coulomb Force," *Britannica Online Encyclopedia*, n.d., http://www.britannica.com/EBchecked/topic/140084/Coulomb-force. In the Estonian case, elements of Russia's Nashe youth group were identified as attackers. This group had the capabilities – or access to them – and a desired goal. They wanted to teach "the Estonian regime the lesson that if they act illegally," a response will be forthcoming. See "2007 Cyber Attack on Estonia Launched by Kremlin-backed Youth Group," *Homeland Security News Wire*, March 13, 2009, http://www.homelandsecuritynewswire.com/2007-cyber-attack-estonia-launched-kremlin-backed-youth-group. Therefore, because there was a means and an end, this was a purposeful war. Third, war must be political. The Estonian crisis was a political attack. Attackers targeted the Estonian government, banking, and media cyber systems, see Rain Ottis, "A Systematic Approach to Offensive Volunteer Cyber Militia" (Tallinn Technical University, n.d.), 184, http://digi.lib.ttu.ee/i/?585. This was the "first time in history when such attacks were aimed at an entire country and involved a variety of instruments, techniques, and strategies in the service of a political battle." See Reet Oorn, "'Cyber War' and Estonia: Legal Aspects," in *Information Technology in Public Administration of Estonia - Yearbook 2007* (Tallinn, Estonia: Ministry of Economic Affairs and Communications, 2008), 74, http://www.riso.ee/en/files/IT_yearbook_2007_final.pdf.

[4] Viira, "Cyber Attacks Against Estonia - Overview and Conclusions," 72.

[5] Terry Fleury, Himanshu Khurana, and Von Welch, "Towards A Taxonomy of Attacks Against Energy Control Systems," in *Proceedings of the IFIP International Congerence on Critical Infrastructure Protection*, 2003, 7–9, http://www.ncsa.illinois.edu/People/hkhurana/IFIP_CIP_08.pdf. A flood occurs when an attacker "repeatedly accesses or overloads the target's capacity, possibly disabling the target." Modify means to "change the contents of the target." This research examines the offensive cyber actions taken against the Estonians. It does not include the actions taken that established the preconditions for DDoS attacks via botnets. To locate vulnerable computers in which to insert a malicious bot, one would likely need to probe potential targets. To probe means to "determine characteristics of a system." Scanning, which is attempting to "access targets sequentially to determine specific characteristics," may also prove useful. Lastly, a hacker may spoof an intended victim; this requires assuming the "appearance of a different entity in the system to access the target."

of vulnerability as well as the actual vulnerabilities that formed the basis for the cyber attacks against Estonia. We can also assess the capabilities possessed by Estonia to exploit the vulnerabilities of the attackers. What would Estonia have had to protect in order to deny the attackers the targets that were attacked? What capabilities would Estonia have had to possess to punish the attackers, assuming of course that attribution could be established? It is unknown if this triadic arrangement would have elevated the costs to deter the cyber war in this circumstance. However, the case study assesses this deterrence concept by reference to what was attacked.

Figure 4.1: 2007 Estonia Cyber War Timeline[6]



Denial – Defensive Action as a Basis for Cyber Deterrence

An opportunity for Estonia to deter Russia and Nashe may have rested upon deterrence by denial through defensive measures. However, before moving forward, it is useful to explain the significance of Nashe. The Kremlin's chief

[6] Merike Kaeo, "Cyber Attacks on Estonia Short Synopsis", n.d., http://www.doubleshotsecurity.com/pdf/NANOG-eesti.pdf. See Landler and Markoff, "Digital Fears Emerge After Data Siege in Estonia," for information that was merged with an adaptation of Kaeo's timeline.

ideologist, Vladislav Surkov, conceived the idea for Nashe, a Russian youth movement that receives its funding from private sources.[7] Later in the chapter, Nashe will be linked to the cyber attacks against Estonia.

This section examines the weaknesses and vulnerabilities that Russia exploited to attack Estonian cyber targets as well as unexploited vulnerabilities that either party could have used but did not. By studying these vulnerabilities in combination with the targets and means of attack Russia used, it is possible to isolate requirements, which may provide a basis for cyber deterrence by denial.

Vulnerability – Due to Internet Dependence

An important basis for Estonia's vulnerability to cyber attack stemmed from the government's, private sector's, and general population's heavy reliance on the Internet. More than "two-thirds of Estonia's population have access to broadband."[8] In 2006, 86 percent completed income taxes online. At the time of the attack, the government accomplished 100 percent of its business on the Internet, while businesses and private citizens conducted 99 percent of their banking online.[9]

Estonian dependence on the Internet started in 2001 with its incorporation of an infrastructure and e-infrastructure named X-Road.[10] X-Road is "a technical and organizational environment that enables secure data transfer between digital state databases" and "enables secure data transfer between individuals and state

[7] "2007 Cyber Attack on Estonia Launched by Kremlin-backed Youth Group." Nashe is also referenced as Nashi in some sources, which means "ours" in Russian.
[8] Christopher Rhoads, "Cyber Attack Vexes Estonia, Poses Debate," *The Wall Street Journal*, May 18, 2007, http://online.wsj.com/article/SB117944513189906904-__3K97ags67ztibp8vLGPd70WXE_20070616.html.
[9] Kaeo, "Cyber Attacks on Estonia Short Synopsis," 4.
[10] Thilek, "Estonia Cyber Attacks 2007," December 28, 2009, http://meeting.afrinic.net/afrinic-11/slides/aaf/Estonia_cyber_attacks_2007_latest.pdf.

institutions."[11] In 2007, Estonia was the "most 'wired' country in Europe, with more than 355 government agencies online."[12]

Estonia's Internet dependency and systems weaknesses combined with vulnerabilities inherent in the cyber domain to expose the country to cyber attack. For example, with DDoS attacks, it is a matter of "pure mathematics" as "no security appliance or anti-DDoS solution can help against a coordinated and focused series of attacks."[13]

> If you have a 100 Mbits/s (100 Million) pipeline and your attacker sends you 1 Gbits/sec (1 Billion) of junk data, your security appliances might prevent the junk traffic reaching your network plug, but the incoming pipeline will still be filled by ten times the amount of data it can handle, virtually disconnecting the target from the rest of the Internet.[14]

Vulnerability – A Function of System Weaknesses

Vulnerability, for our purpose, "describes why an attack can be successful." It does not "specify the actual target that is vulnerable, but rather the weakness in the system that can be exploited." The extent of the problem Estonia encountered was significant as attackers exploited the configuration of Estonia's cyber network to conduct DDoS attacks and web defacements.[15]

---

[11] Lembe Käärman, *X-Road Regulations* (mandator, December 19, 2006), 4, http://ftp.ria.ee/pub/x-tee/doc/X-Road_regulations.pdf.
[12] Thilek, "Estonia Cyber Attacks 2007."
[13] Roberto Preatoni, "The Lessons We Are NOT Going to Learn," mi2g, *The Digital Bending of Estonia on Its Physical Knees - The Lessons We Are NOT Going to Learn*, June 2, 2007, http://www.mi2g.com/cgi/mi2g/frameset.php?pageid=http%3A//www.mi2g.com/cgi/mi2g/media.php. Preatoni quipped that any 13-year-old "cracker" could "build a DDoS network capable of several gigabytes-per-second firepower in a matter of a few days."
[14] Ibid.
[15] Fleury, Khurana, and Welch, "Towards a Taxonomy of Attacks Against Energy Control Systems," 9–10. When a system is not properly configured, "a hacker can gain improper access." Examples include "poor account management where certain unused accounts and/or services have (possibly high-level) access to the system; components with known flaws that are not correctly patched; weak or non-existent authentication (including unchanged passwords); and misconfigured perimeter protection and/or access control policy."

Because of these weaknesses, Estonia was susceptible to offensive cyber attacks exploiting vulnerabilities that created a "national security situation." Jaak Aaviksoo, Estonia's defense minister, said that the situation "compared to when your ports are shut to the sea,"[16] which is tantamount to a cyber blockade. Estonia's systems weaknesses and resident vulnerabilities were exploitable due to its "dependence on computer networks" and the Internet.[17] Further, Estonia's "lack of defensive protocols" or pre-planned actions in advance of an attack made it an easier target for exploitation.[18]

Estonia could have reduced the weaknesses in its networks and closed vulnerabilities by hardening its systems. This would have increased Russia's level of effort and helped reduce inducements for cyber attack by eliminating or reducing vulnerabilities. However, the effectiveness of defensive efforts can be difficult to sustain due to the rapidly changing nature of cyber technology; therefore, engineering resilience into one's computer networks may inject an added sense of futility into an attacker's decision calculus that could enhance deterrence.

Estonia had some of these mechanisms in place; for example, Estonia's X-Road information technology (IT) architecture was a "completely distributed, resilient system with distributed management" that did not centralize or "change

[16] Landler and Markoff, "Digital Fears Emerge After Data Siege in Estonia."
[17] Alex Michael, *Cyber Probing: The Politicisation of Virtual Attack* (Defence Academy of the United Kingdom, December 2010), 14, http://www.voltairenet.org/IMG/pdf/Cyber_Probing.pdf.
[18] Richards, "Denial-of-Service: The Estonian Cyberwar and Its Implications for U.S. National Security." Defensive protocols are pre-planned actions, at the ready, to rapidly respond to an attack.

the ownership of data."[19] X-Road did "not have a single point of failure," as all systems components could "be doubled for resilience against failures and attacks." Because of the technical resilience engineered in X-Road, the damage from the 2007 cyber attacks was far less. However, the pace of technological changes combined with the ingenuity of attackers makes it difficult to stay ahead of emerging vulnerabilities. Despite claims of Estonia's resilience due to X-Road, Russian attackers managed to create havoc at the time and place of their choosing because of the inherent weaknesses in Estonia's networks.

Denial by defensive means requires a constant process of assessing and updating hardware and software to keep pace with the speed of innovation. In addition, those tasked with computer security must continuously adapt training programs to account for this dynamic. Rapid hardware and software innovations and the continuous training needed to remain abreast of these advancements help form technical requirements that make cyber deterrence unique from other variants of deterrence theory. Technical experts must help develop these requirements, and a bridge must exist between the cyber technical and policy communities to design effective cyber deterrence policy. In the Estonia case, the weaknesses that made the attackers' offensive actions possible were susceptible to denial by defensive measures.

[19] "X-Road e-Government Interoperability Framework" (Tallinn, Estonia, 2011), http://www.cyber.ee/home/information-systems/X-Road_factsheet_2011.pdf. Resilience is "the ability of a system to recover from adversity and either revert to its original state or assume an adjusted state based on new requirements"; see Myriam Dunn Cavelty, "Critical Information Infrastructure Vulnerabilities, Threats and Responses," *ICTs and International Security* Three (2007): 19.

Russian Exploitation of Estonia's Cyber Vulnerabilities

Cyber attacks against Estonian targets were possible because Russian attackers identified and exploited hardware and software vulnerabilities. The exploitation of these vulnerabilities posed a significant problem; however, had Estonia mitigated its cyber vulnerabilities, cyber war may not have been possible. Recognizing and then closing vulnerabilities is a requirement for deterrence by denial.

How Cyber Exploitations May Take Place

To understand vulnerabilities inherent in DDoS attacks, it is necessary to understand more about these attacks. DDoS is a variant of denial-of-service (DoS) attacks. DoS attacks first appeared in the mid-1980s as a method to target networks and websites by blocking user access. This can be accomplished in a couple of ways: Repetitive requests clog the server, which means that users cannot access the site, or hackers can block the communication links between servers and networks, which means that users cannot send or receive information.[20]

Hackers use malware (malicious software) in cyber attacks to destroy computer hardware and software and to turn computers into zombies. A bot is a form of malware that turns the computer into a zombie, which means that a bot herder or someone who has rented his or her botnet can command it to participate in future attacks while the owners of the zombies remain unaware.[21] There are

[20] Richards, "Denial-of-Service: The Estonian Cyberwar and Its Implications for U.S. National Security."
[21] Ibid. A botnet is a collection of zombies. A bot herder is a hacker who gathers or herds this collection.

many forms of DoS attacks: flood attacks, logic/software attacks, mail bombing, permanent denial-of-service (PDoS) attacks, accidental denial-of-service attacks, and DDoS attacks.[22] DDoS attacks were brutal in the Estonian cyber war because they overwhelmed targets by overloading servers and quickly depleting resources from widely dispersed locations.[23] Russian hacker sites offered easy access to tools for novices to initiate these DDoS attacks (see Figure 4.2).

Figure 4.2: Russian Hacker Site Offers DDoS Tools on the Internet[24]

Those who attacked Estonia's networks and servers used more than one million zombies. Aside from controlling users' computers without their knowledge, two additional problems arose. First, hackers relied on intermediaries, which formed a "cloaking device" that concealed the hacker, thus making attribution extremely difficult. Second, because they used intermediaries

[22] Ibid. Mail bombing is the purposeful transmission of massive amounts of unwanted email to a targeted actor's account.
[23] Jose Nazario, "Political DDoS: Estonia and Beyond," 2008, 3, http://static.usenix.org/events/sec08/tech/slides/nazario-slides.pdf.
[24] Thilek, "Estonia Cyber Attacks 2007."

and rented botnets online, hackers created a "large-scale attack with little or no effort."[25]

How Cyber Exploitations May Be Conducted by Overloading Servers

Using DDoS Attacks to Exploit Hardware Vulnerabilities

Hackers used two variants of flood attacks to overwhelm Estonia's networks, Internet Control Message Protocol (ICMP) and Transmission Control Protocol (TCP) flooding. ICMP flooding ties up the "server so that legitimate user requests go unfulfilled." It works by "sending the victim's IP [Internet Protocol] network address to broadcasting computers, which in turn 'broadcast' the IP address to other computers, beginning a chain reaction." These responses, in the form of information packets, overload the victim's IP address when returned.[26]

Using DDoS Attacks to Exploit Software Vulnerabilities

TCP SYN floods use a different approach. This type of attack "overloads a victim's server by exploiting communication protocols." This occurs when an attack transmits "information requests with a false 'return address' to a server, which unsuccessfully attempts to return contact until it times out." This process "clogs the system" such that it "renders the server unavailable to respond to other legitimate requests."[27]

---

[25] Richards, "Denial-of-Service: The Estonian Cyberwar and Its Implications for U.S. National Security." DDoS attacks surfaced in 1999; "the first documented case involved a hacker who used a network of 227 zombie computers to overload a single computer at the University of Minnesota."

[26] Richards, "Denial-of-Service: The Estonian Cyberwar and Its Implications for U.S. National Security." ICMP flooding is also known as "smurfing."

[27] Ibid.

Using Ping Attacks to Exploit Software Vulnerabilities

Ping attacks, also used in Estonia, are different from flood attacks, which designers have engineered to overload targets. Ping attacks, also known as the "Ping of Death," are logic/software attacks that break communication protocols by forcing errors. When an attacker sends a "group of pings (packets of information) that exceed the maximum size allowed by the system," the system crashes because it is unable to "reassemble the packets."[28]

Exploiting Software Vulnerabilities in Back-end Databases – The Main Culprit

Estonian websites failed rapidly after DDoS and ping attacks "because the back-end databases were not designed to respond to repeated floods of requests."[29] DDoS flood and ping attacks were successful because they took advantage of vulnerabilities in Estonia's cyber infrastructure. The fundamental problem was how the government web servers were configured. The industry standard has created a norm whereby webpages are quickly constructed and fielded with content management systems (CMS). CMSs are application servers that "build every webpage from a database of elements including pictures, video, and text content."[30]

---

[28] Ibid. Teardrop attacks, another form of logic/software attacks, "work much the same way, sending malformed pings to the target server. The hacker manipulates these packets of information so that they cannot be reassembled, and when the target system attempts to do so, it forces a fatal error and crashes the system."

[29] Richard Stiennon, *Surviving Cyberwar* (Lanham, Md: Government Institutes, 2010), 89–90. CMS systems "include the popular WordPress for blogs or the open source Joomla and Drupal for more sophisticated websites. Each uses PHP scripts to pull information from a SQL database such as MySQL or MicrosoftSQL. (PHP is high-level programming language; SQL stands for Structured Query Language.)"

[30] Ibid.

A database is a system for collecting information to "organize, sort, and retrieve large amounts of data efficiently." Databases have two sections, a front and a back end. The front end contains the "application objects, such as the queries, forms, reports, macros, and modules" and is "used on the user's desktop." The front end is linked to the back end, which "stores the tables with the data" on a server because it is a "location shared by many users."[31] Estonia's principal vulnerability, within its control, was a lack of proper systems configuration in the back-end component of its database systems.[32]

This same configuration vulnerability likely aided hackers conducting website defacements.[33] SQL injection is the most common method for website defacement. The SQL injection technique "exploits a security vulnerability occurring in the database layer of an application."[34]

The SQL injection uses data that have not been properly validated as part of a command (or query). These "specially crafted" data "trick the application into executing unintended commands or changing data." This allows the attacker

---

[31] "What Is a Database," *Database Designs*, n.d., http://www.database-designs.com/DatabaseDefinition.html. The computer language or programming that retrieves information from databases is SQL.

[32] Fleury, Khurana, and Welch, "Towards a Taxonomy of Attacks Against Energy Control Systems," 9. "When a resource is improperly configured, a hacker can gain improper access," which creates a vulnerability. The case did not yield publicly available evidence of attacker's use of front-end exploits against Estonia.

[33] Ibid. A specification vulnerability occurs "when a process or component has design flaws, these flaws can be used in unintended ways to gain access to the system."

[34] Eneken Tikk, Kadri Kaska, and Liis Vihul, *International Cyber Incidents: Legal Considerations* (Tallinn, Estonia: Cooperative Cyber Defence Centre of Excellence (CCD COE, 2010), 114, http://www.ccdcoe.org/publications/books/legalconsiderations.pdf. The vulnerability is "present when user input is either incorrectly filtered for string literal escape characters embedded in SQL statements or user input is not strongly typed and thereby unexpectedly executed." SQL is a "database computer language designed for the retrieval and management of data in relational database management systems (RDBMS), database schema creation and modification, and database object access control management."

to "create, read, update, alter, or delete data stored in the back-end database."[35] Because this type of website defacement affects the back-end database rather than the front-end static web application files, efforts to track changes would not have detected the attack while in progress.[36]

Cyber Targets: Estonia's Networks a Focus of Russian Hackers[37]

Estonia experienced crippling cyber attacks against its government, financial sector, media, and several corporations. To hold these targets at risk, attackers principally focused on the country's networks and, to a lesser extent, individual users.[38] Within Estonia's critical network infrastructure, they targeted "web servers, e-mail servers, DNS servers, and routers.[39]

Attackers targeted wide-ranging entities, including the "government, the president, the parliament, police, banks, Internet service providers (ISP), online media, as well as many small businesses and local government sites."[40] Of these, attackers favored "government web and e-mail servers, on-line banking services,

---

[35] "SQL Injection Tutorial: Learn About SQL Injection Vulnerabilities and Prevention," *Veracode*, n.d., http://www.veracode.com/security/sql-injection.
[36] "SQL Injection 2.0," *Computerdoctors*, n.d., http://www.mauskar.com/index.php/browse-news/11-news/40-sql-injection-20.
[37] Fleury, Khurana, and Welch, "Towards A Taxonomy of Attacks Against Energy Control Systems," 8-9. The target is "the resource that is being attacked."
[38] Ibid., 9. A network "consists of computers, switches, hubs, etc., connected via wires or wirelessly." A user is "someone with authorized access to a system." The researcher determined that individual systems (computers and peripheral devices) were not targeted in the attacks; however, such attacks would have been necessary to build the botnets that were used against Estonia. There was no evidence that attackers manipulated data for monetary or other gain. Data consist of "information suitable for processing by humans or machines" or can be a "single resource such as a file stored on a hard drive or the transmission of such data across a communications network."
[39] Rain Ottis, "Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective," in *Proceedings of the 7th European Conference on Information Warfare and Security* (Plymouth: Academic Publishing Limited, 2008), 163–168. Most visible to the public were the attacks against web servers.
[40] Ibid.

and on-line news services."[41] While not encompassing of all of these categories, Jose Nazario, Senior Security Engineer for Arbor Networks, provided a list of major government agencies targeted in Phase II (see Table 4.1). Government sites, including those of the prime minister, state police, and Ministry of Finance, received a greater number of attacks than other agencies. As Phase II progressed, "targeted websites grew to number in the hundreds."[42]

Table 4.1: Analysis of Phase II Targets – May 2007[43]

Attacks	Destination	Address	Target
35	195.80.105.107/32	pol.ee	Estonian Police
7	195.80.106.72/32	www.riigikogu.ee	Estonian Parliament
36	195.80.109.158/32	www.riik.ee www.peaminister.ee www.valitsus.ee	Official State Web Center Prime Minister Estonian Government
2	195.80.124.53/32	m53.envir.ee	Ministry of the Environment
2	213.184.49.171/32	www.sm.ee	Ministry of Social Affairs
6	213.184.49.194/32	www.agri.ee	Ministry of Agriculture
4	213.184.50.6/32		Estonian CERT
35	213.184.50.69/32	www.fin.ee	Ministry of Finance
1	62.65.192.24/32	starman.ee	Private telecom provider

Russia Attacks Estonia

One needs to understand how cyber attacks are carried out in order to develop requirements for cyber deterrence. First, as will be detailed in a following section, the researcher states up-front that in this case attribution was possible and that this is how we can assert that Russia attacked Estonia. The

[41] Ottis, "A Systematic Approach to Offensive Volunteer Cyber Militia," 184.
[42] Richards, "Denial-of-Service: The Estonian Cyberwar and Its Implications for U.S. National Security."
[43] Jose Nazario, *Estonian DDoS Attacks – A Summary to Date*, DDoS and Security Reports (Arbor Networks Security, May 17, 2007), http://ddos.arbornetworks.com/2007/05/estonian-ddos-attacks-a-summary-to-date/.

relationship between identified and alleged perpetrators and the links that connected them left no doubt of Russian involvement in these attacks.

Combining a thorough understanding of the facts and circumstances of the attacks with previous analysis on the vulnerabilities that were exploited and those available for exploitation helps create a stronger basis for deterrence by denial in this case. In examining the cyber attacks against Estonia, the case study used various components of the Fleury et al taxonomy. Particularly useful were the model's attack components of origin and action to conduct this analysis (see Annex A).[44]

The attacks began at 10 p.m. on April 26, 2007, but were not discovered until April 27, when Jaak Aaviksoo, Estonian Minister of Defense, was unable to access the prime minister's Reform Party website.[45] The attacks, as previously noted, came in two distinct waves, on April 26–29 and April 30–May 18, 2007.[46] According to Katrin Pargmae, spokesperson for the Estonian Informatics Center, computers from 178 countries, most of them remotely controlled by Russian hackers, attacked the Estonian cyber infrastructure.[47] The largest attacks measured 100 megabytes (MB) per second of traffic.[48]

---

[44] Fleury, Khurana, and Welch, "Towards A Taxonomy of Attacks Against Energy Control Systems," 8-9. Action describes the "activity the attack is performing on the target."
[45] Richards, "Denial-of-Service: The Estonian Cyberwar and Its Implications for U.S. National Security."
[46] Viira, "Cyber Attacks Against Estonia - Overview and Conclusions," 71. Viira describes the first wave as beginning on April 27, the date the attack was discovered. The researcher uses April 26, the date of the initiation of the attacks, as the beginning of the first wave.
[47] "2007 Cyber Attack on Estonia Launched by Kremlin-backed Youth Group."
[48] Ibid. Jose Nazario of Arbor Networks noted that the largest recorded attacks were 40 gigabytes (GB) per second. He observed that the type of attack directed at Estonia was simple; it was "just a lot of people getting together and running the same tools on their home computers." See "Megabytes, Gigabytes, Terabytes ... What Are They?," *What's A Byte?*, n.d., at http://www.whatsabyte.com for a description of the terminology used to describe computer storage space and system memory. A bit is the smallest unit of data a computer uses; it represents

The First Phase

During the first phase, hacktivists used elementary psychological warfare to pursue their political objectives. In one example, attackers created a fake letter of apology from Andurs Ansip, Estonia's Prime Minister, for relocating the statue.[49] Another common technique was for hackers to deface the sites of prominent users. Using this method, hackers defaced a picture of Ansip on the website of his political party by giving him a Hitler-type moustache.[50] In other cases, government website traffic "included phrases like "*ANSIP_PIDOR=FASCIST.*"[51]

In these types of circumstances, the damage was "temporary and manageable."[52] The pattern repeated in many of these attacks left two impressions: that those responsible harbored political ill will and that they were native Russian speakers. Reports demonstrated that hackers employed dozens of variations on this theme and many contained profuse profanity.[53]

Aside from defacements and similar nuisance attacks, government websites that "normally receive 1,000 visits a day were receiving 2,000 visits every second." Some sites shut down for a few minutes, while others remained

---

two states of information: 0 or 1, yes or no, true or false. A kilobyte (KB) is 1,000 bytes and is equivalent to a typical paragraph. A MB is 1,000 kilobytes and equates to a small book or 500 pages of text. A GB is 1,000 megabytes and equates to 30 feet of books on a library shelf. A terabyte (TB) is 1,000 gigabytes, which equates to 1,000 copies of the *Encyclopedia Britannica.* It would take 10 terabytes to hold the printed collection of the Library of Congress.

[49] Ruus, "Cyber War I: Estonia Attacked from Russia."

[50] Peter Finn, "Cyber Assaults on Estonia Typify a New Battle Tactic," *The Washington Post*, May 19, 2007, http://www.washingtonpost.com/wp-dyn/content/article/2007/05/18/AR2007051802122_pf.html.

[51] Ottis, "Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective." Mr. Ansip was the Estonian Prime Minister at the time.

[52] Ruus, "Cyber War I: Estonia Attacked from Russia."

[53] Ottis, "Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective."

offline for hours.[54] One reason for the more serious attacks appeared on April 27 when directions for ICMP flood attacks, a form of DoS attacks, surfaced on a wide range of Russian Internet chat rooms and blogs.[55]

To further enhance effectiveness, attackers used LiveJournal, a social media outlet, to target government agencies. Here users uploaded the email addresses of Estonia's parliament deputies; see Figure 4.3. Followers of LiveJournal were encouraged to distribute this email list and to "cause multiple letters to be sent to Estonia's deputies with 'congratulations on the Victory Day.'"[56] This action prompted attackers to send millions of emails to those on this list, which caused servers to drop offline for two days.[57]

An examination of the transition from the Phase I to Phase II portion of the attack revealed that cyber attackers found success using this approach. Figure 4.4 presents a graphical depiction of the effect of a DDoS attack. These data captured a cyber attack on the official website of the Estonian government (www.valitsus.ee) on April 29–30.

The red bars indicate a failure of the website to remain accessible. The green bars express the time in seconds in which users experienced a delay but remained able to access the site. This scenario repeated itself across Estonian

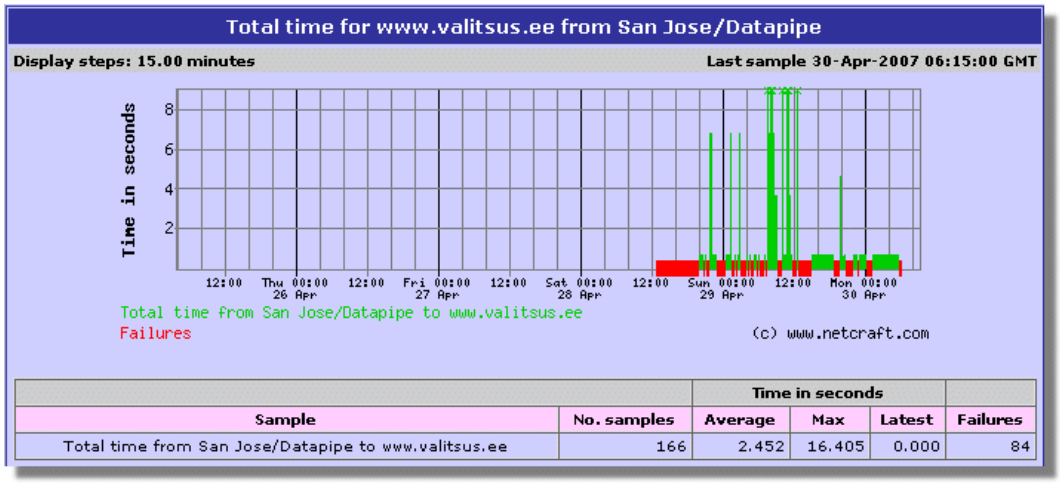
---

[54] Rhoads, "Cyber Attack Vexes Estonia, Poses Debate."
[55] Thilek, "Estonia Cyber Attacks 2007." These directions included commands that allowed others to gain access to and then convert a batch file that had been uploaded to this web address: http://fipip.ru/raznoe/pingi.bat. Goloskokov is the likely suspect as the originator of this attack. ICMP is "an extension to the Internet Protocol (IP)." "ICMP supports packets containing error, control, and informational messages. The ping command uses ICMP to test an Internet connection." See "ICMP," *Wedpodeia*, n.d., http://www.webopedia.com/TERM/I/ICMP.html. ICMP flooding is one of several types of DoS attacks.
[56] Ibid.
[57] Ibid.

governmental agencies, media, and banking throughout the first phase – the challenge magnified significantly in the second wave of attacks.

Figure 4.3: Email Addresses of Estonia's Parliament Deputies[58]

Figure 4.4: Graphical Depiction of Attack on the Estonian Government's Website[59]



		Time in seconds			
Sample	No. samples	Average	Max	Latest	Failures
Total time from San Jose/Datapipe to www.valitsus.ee	166	2.452	16.405	0.000	84

[58] Ibid.
[59] "IT Security Threat Summary for H1 2007: Social Engineering, Bank Scams, Cyber War and Mobile Spyware," n.d., http://www.f-secure.com/export/sites/fs_global_site/2007/1/WrapUp_H1_2007.pdf.

The Main Attack

The main attack took place in Phase II as seasoned hackers joined the attacks in progress, thus escalating the crisis. Estonians now faced a "full-scale (and apparently well-financed) campaign." Russian attackers used botnets to remotely command a million computers from countries around the world to target Estonia's cyber infrastructure with millions of malicious requests and emails. At the height of Phase II, Estonia received one thousand times its usual inbound email traffic flow.[60]

In the second phase, Russian websites continued to provide an outlet for instructions, motivation, and target lists. Figure 4.5 "illustrates how simple the most primitive attacks are to organize" because "with thousands attacking, even a primitive ping flood can cause trouble."[61] Seasoned hackers sought foot soldiers, or "script kiddies," to copy malicious programs from hacker websites. Hackers counted on these "relatively unsophisticated troublemakers" to copy "programs line for line off hacker websites," which was ideal in executing ping attacks.[62]

---

[60] Ruus, "Cyber War I: Estonia Attacked from Russia." Botnets are a "large number of remote controlled computers distributed all over the Internet and centrally controlled." See Christian Czosseck and Karlis Podins, *An Usage-Centric Botnet Taxonomy* (Talllinn, Estonia, n.d.), http://www.ccdcoe.org/articles/2011/Czosseck_Podins_An_Usage-Centric_Botnet_Taxonomy.PDF. For a portion of their financing, cyber attackers used PayPal to generate money to hire botnets. PayPal is an online service that allows users to transfer money securely.

[61] Ottis, "Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective."

[62] Joshua Davis, "Hackers Take Down the Most Wired Country in Europe," *Wired Magazine*, August 21, 2007, http://www.wired.com/politics/security/magazine/15-09/ff_estonia?currentPage=all. A ping attack is a "simple request for a response from a web server, repeated hundreds of times per second."

Figure 4.5: Screen Capture of Attack Instructions[63]

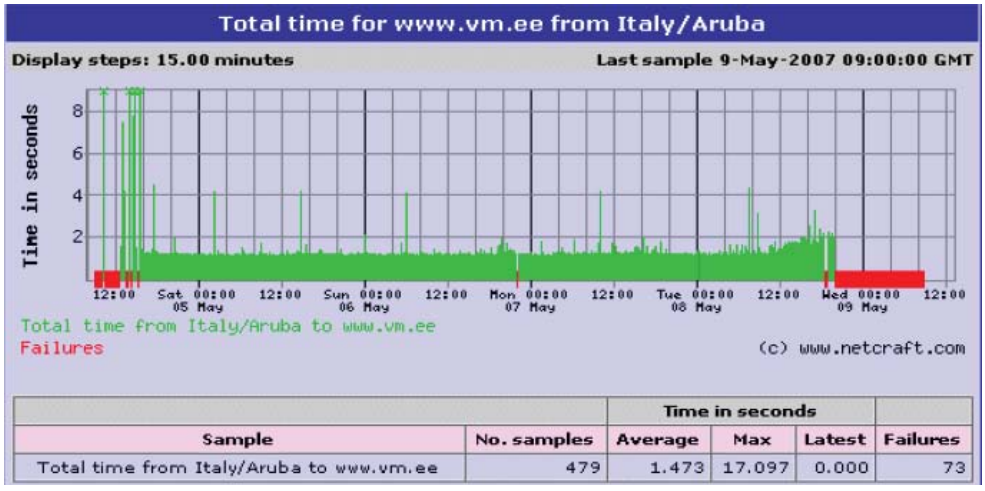
Attacks from script kiddies, botnets, and experienced hackers occurred intermittently until May 9.[64] At midnight, Moscow time, the heaviest attack of the war occurred – attackers sent up to four million packets of information per second for twenty-four hours."[65] Estonia's banking system felt the brunt of this attack. The next day, May 10, Estonia's largest bank, Hansabank, ceased operations. This was problematic because 97 percent of Estonia's banking took place online, and therefore, customers throughout Estonia could not use

[63] Ottis, "Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective."
[64] Estonians and Russians recognize May 9 as the anniversary of the end of WWII in Europe.
[65] Richards, "Denial-of-Service: The Estonian Cyberwar and Its Implications for U.S. National Security."

Hansabank's ATMs. Additionally, the attacks severed Hansabank from its international customers.[66]

Attackers escalated their level of effort on the government sector as well. See Figure 4.6 for a graphical depiction of the attacks leading up to and including May 9 against the Estonian Ministry of Foreign Affairs (www.vm.ee). This graph demonstrates a time delay (see green bar) due to continuous attacks from May 5 to May 8; however, on May 9, the ministry's site failed (see red bar) due to a greater level of effort from the attackers.

Figure 4.6: May 5–9 Attacks Against Estonia's Ministry of Foreign Affairs[67]



		Time in seconds			
Sample	No. samples	Average	Max	Latest	Failures
Total time from Italy/Aruba to www.vm.ee	479	1.473	17.097	0.000	73

Estonian officials traced some of the one million zombies (computers infected with bots) worldwide forcing Estonia's critical cyber infrastructure offline to countries as "dissimilar as the U.S., China, Vietnam, Egypt, and Peru."[68] The purposeful gathering of these zombies into botnets provided

[66] Ibid.
[67] Thilek, "Estonia Cyber Attacks 2007."
[68] Finn, "Cyber Assaults on Estonia Typify a New Battle Tactic."

botmasters a "large number of remote controlled computers" that were centrally controllable but widely dispersed.[69]

Nazario provided the best publicly available open-source data to examine the majority of the Phase II attacks. He used Arbor Network's Active Threat Level Analysis System (ATLAS) to collect data on the attacks from May 3 to 17. ATLAS is a "globally distributed network that Arbor claims can see 80 percent of the world's Internet traffic."[70]

During the two-week period leading to May 17, Nazario determined that Estonia received "128 unique DDoS attacks." In analyzing these attacks, he found that "115 were ICMP floods, four were TCP SYN floods, and nine were generic traffic floods."[71] Nazario also discovered that Estonia faced a distributed botnet. This meant that Estonia had a more difficult challenge in shutting down control of the botnet because it moved. To complicate the challenge, Nazario uncovered evidence that there were "different attacking groups … not just one botnet," and this made it harder to defeat the attackers.[72]

The ten largest attacks in Phase II pressured Estonia's systems with "ninety megabits of data a second … lasting up to ten hours each."[73] Landler and Markoff noted that this represented the equivalent of "downloading the entire

---

[69] Czosseck and Podins, *An Usage-Centric Botnet Taxonomy*. Criminal and other elements enjoy a lucrative market in providing botnets for hire to any customer with the money regardless of the motive.
[70] Sean Michael Kerner, "Estonia Under Russian Cyber Attack?" *InternetNews*, May 18, 2007, http://www.internetnews.com/security/article.php/3678606/Estonia+Under+Russian+Cyber+Attack.htm.
[71] Nazario, *Estonian DDoS Attacks – A Summary to Date*.
[72] Kerner, "Estonia Under Russian Cyber Attack?".
[73] Landler and Markoff, "Digital Fears Emerge After Data Siege in Estonia."

Windows XP operating system every six seconds for ten hours."[74] Nazario concluded that a "decent-sized botnet was behind the attack" as his analysis yielded that the "aggregate bandwidth … [maxed] out at nearly 100 [megabits per second]."[75]

Of the 128 attacks Nazario examined, ninety-five lasted less than one hour (see Table 4.2). However, over a short time span of several weeks, these attacks "translated to a very long-lived attack" with the longest attack delivering a "truly crushing blow."[76] Nazario observed that attackers varied the distribution of attacks, with more attacks occurring on some days than others (see Table 4.3).[77] The heaviest attacks took place on May 8–9, with the last major wave occurring on May 18.[78] After May 18, there were spurious attacks until May 23, when the cyber attacks ended.[79]

Table 4.2: Phase II – DDoS Attack Duration[80]

Attacks	Duration
17	Less than 1 minute
78	1 minute–1 hour
16	1 hours–5 hours
8	5 hours–9 hours
7	10 hours+

Table 4.3: Phase II – DDoS Attack Distribution[81]

Attacks	Date
21	May 3
17	May 4

[74] Ibid.
[75] Nazario, *Estonian DDoS Attacks – A Summary to Date.*
[76] Ibid.
[77] Ibid.
[78] Landler and Markoff, "Digital Fears Emerge After Data Siege in Estonia."
[79] Kaeo, "Cyber Attacks on Estonia Short Synopsis."
[80] Nazario, *Estonian DDoS Attacks – A Summary to Date.*
[81] Ibid.

31	May 8
58	May 9
1	May 11

Unexploited Vulnerabilities – A Large and Dangerous Pool

Recognizing and then closing unexploited vulnerabilities is a requirement for deterrence by denial. Common Vulnerabilities and Exposures (CVE) have identified 50,551 software vulnerabilities.[82] Therefore, Estonian cyber vulnerabilities exploited by Russian attackers were an extremely small portion of those available for malicious purposes. Yet, this vast pool of unexploited vulnerabilities permits an additional observation: Had Estonia developed the capability unilaterally or in concert with a broader coalition, perhaps it could have mined this set of vulnerabilities to either deter Russia with a threat of punishment or stood prepared to attack Russia should deterrence fail. In addition, had Estonia taken greater preventive efforts to close the threats to its IT systems from these vulnerabilities, Russia may have been deterred, as the success of its attacks would have been less certain.

In the first six months of 2007, Microsoft's Security Intelligence Report identified 3,400 new software vulnerabilities to add to the thousands in existence. The majority of these were classified as "high-severity" vulnerabilities and provided a "wide set of relatively easy-to-exploit targets for malicious attackers.[83]

[82] "Common Vulnerabilities and Exposures (CVE)," n.d., http://cve.mitre.org/. 50,551 vulnerabilities were identified as of May 9, 2012; see http://web.nvd.nist.gov/view/vuln/search.
[83] *Microsoft Security Intelligence Report: January Through June 2007* (Microsoft Corporation, 2007), 4. The National Vulnerability Database (NVD) provides severity rankings of "Low," "Medium," and "High" in addition to the numeric Common Vulnerability Scoring System (CVSS).

To exploit a computer system or single computer with the thousands of existing cyber vulnerabilities, one of the four following conditions must exist:

- Those that allow an attacker to execute commands as another user
- Those permitting an attacker to access data that is contrary to the specified access restrictions for that data
- Those that permit an attacker to pose as another entity
- Those that allow an attacker to conduct a DoS[84]

To exacerbate these four conditions, the SANS Institute (SysAdmin, Audit, Network, Security) has noted that two risks exist that "dwarf all others" and repeatedly "organizations fail to mitigate them."[85] The first of these risks occurred in the Estonia case as attackers exploited the vulnerability of Internet-facing websites. The second risk resided in vulnerabilities that potential attackers could have found in "client-side software that remained unpatched."[86]

Regarding the first risk, Internet website applications globally receive more than 60 percent of attempted attacks. In this type of attack, hackers seek to reconfigure websites with malicious code that invariably permits client-side exploitation. Client-side exploitations are the principal reason such vulnerabilities exist. SANS reported that 80 percent of the vulnerabilities associated with Internet websites were either SQL injection or Cross-Site Scripting (XSS) flaws.[87]

SQL injection is "an exploit that takes advantage of database query software that does not thoroughly test the query statement for correctness. Along with cross-site scripting, SQL injection is used by worms to break into websites

[84] "Common Vulnerabilities and Exposures (CVE)."
[85] "The Top Cyber Security Risks," *Sans*, September 2009, http://www.sans.org/top-cyber-security-risks/.
[86] Ibid. An Internet-facing website is one that is visible to external users. *Client-side* means that these actions are taking place on the user, or client, side of a client-server system and that the user's browser executes computer scripts. See "What Is Client-side?," *Webopedia Computer Dictionary*, n.d., http://www.webopedia.com/TERM/C/client_side.html.
[87] "The Top Cyber Security Risks."

and extract data or embed malicious code."[88] XSS "causes a user's Web browser to execute a malicious script." Russian attackers exploited these vulnerabilities in Estonia as described in the previous section; however, there were many additional nuances available to attackers to take advantage of these same vulnerabilities by using other tactics. For example, an attacker could place a hidden code in a "'click here' hyperlink attached to a URL (Uniform Resource Locator) that pointed to a nonexistent webpage. When the page is not found, the script is returned with the bogus URL, and the user's browser executes it," which exposes the user to potential exploitation.[89] SANS noted that many website proprietors remained susceptible to exploitation because they did not take proper precautions by scanning for known vulnerabilities.

The second risk pertains to the failure to patch or repair a program bug, which provides an open invitation for attackers to exploit known vulnerabilities. SANS reported that malicious actors often embed client-side vulnerabilities in popular computer software programs, such as Adobe PDF Reader, QuickTime, Adobe Flash, and Microsoft Office. Attackers could have exploited these trusted sites to trick users into exposing their computers to malicious code. Once a computer is infected, it can easily infect others in the network and network servers.[90]

Software developers continuously develop patches to counter emerging

---

[88] "SQL Injection Definition from PC Magazine Encyclopedia", n.d., http://www.pcmag.com/encyclopedia_term/0%2C2542%2Ct%3DSQL+injection&i%3D61172%2C00.asp#fbid=w_NKHxQxur_.

[89] "XSS Definition from PC Magazine Encyclopedia", n.d., http://www.pcmag.com/encyclopedia_term/0,2542,t=XSS&i=57401,00.asp#fbid=w_NKHxQxur_.

[90] "Spear Phishers," *The Federal Bureau of Investigation*, April 1, 2009, http://www.fbi.gov/news/stories/2009/april/spearphishing_040109.

vulnerabilities; however, in circumstances where users have relied upon pirated software, these automatic updates are not available. The Business Software Alliance (BSA) determined that 73 percent of software used by Russians in 2007 was pirated. The piracy rate for Estonia in 2007 was 51 percent.[91] High piracy rates indicate that users do not have access to the most up-to-date software security patches, which increases the opportunity for cyber exploitation, particularly in business and media sectors.

These factors suggest that two simple avenues of attack were available with which an attacker could have sought greater advantage by drawing from a large pool of unexploited vulnerabilities – social engineering and email malware. In executing a social engineering cyber attack, an "attacker uses human interaction (social skills) to obtain or compromise information about an organization or its computer systems."[92] Social engineering has provided an increasingly effective path for malicious actors to distribute malware. This method is widely in use because it is often easy to "trick the user into taking action that bypasses or lessens the effectiveness of the user's existing protection." In the months leading up to and including the Estonia cyber war, this worldwide practice resulted in escalating "infection rates for backdoor Trojans, bots, viruses, password stealers, and data-theft Trojans."[93]

Email is central to modern communication; therefore, email malware

---

[91] *2007 Global Software Piracy Study* (Business Software Alliance, May 2008), http://global.bsa.org/idcglobalstudy2007/studies/summaryfindings_globalstudy07.pdf.
[92] "Avoiding Social Engineering and Phishing Attacks," *United States Computer Emergency Readiness Team*, October 22, 2009, http://www.us-cert.gov/cas/tips/ST04-014.html.
[93] *Microsoft Security Intelligence Report: January Through June 2007*, 5. Although these data reflect Microsoft's assessment of worldwide vulnerabilities, the piracy rates in both Russia and Estonia suggest that high-use sectors of pirated software such as media and business may be disproportionately vulnerable.

could have been more thoroughly propagated to take advantage of additional unexploited vulnerabilities. In the first half of 2007, "classic email worms comprised the single largest email-borne malware threat, representing 49.0 percent of the total malware detected in email." Phishing and email attacks accounted for 37 percent of email malware detections in this period.[94]

Phishing or spear phishing is an effective and insidious tool for attackers to achieve access to an unsuspecting user's computer. Spear phishing is "a virtual trap ... that uses official-looking e-mails to lure" a targeted actor to a fake website to deceive the target into revealing passwords and other personal information.[95] An added objective of many attackers is to establish "backdoors."[96] This permits a hacker to exploit a target's computer or network repeatedly. An expansion of this technique, particularly in the preparatory phase of a cyber war, could have proven to be quite effective.

At the time of the Estonia cyber war, Microsoft's vulnerability detection and removal tool recognized eighty-nine families of malware. This represented thousands of vulnerabilities that included bots and backdoors, Trojans, password stealers, and a broad range of traditional virus threats.[97] The problem defenders face is that the authors of this malware have continuously introduced new

---

[94] Ibid., 32. These statistics are based on worldwide data and are suggestive of the high threat such activity posed to information-centric states during the period of the Estonia cyber war.
[95] "Spear Phishers."
[96] "What Is Backdoor?," *Webopedia Computer Dictionary*, n.d., http://www.webopedia.com/TERM/B/backdoor.html. A *backdoor*, also known as a *trapdoor*, is "an undocumented way of gaining access to a program, online service or an entire computer system." The programmer who designed and installed the computer code generally only knows about the access to a backdoor.
[97] *Microsoft Security Intelligence Report: January Through June 2007*, 42–44.

techniques to "evade detection and to thwart removal attempts."[98] This provides the attacker with an offensive advantage as defenders have struggled to keep "abreast of security updates, and applying critical security patches for all software used on [one's] system, as soon as those patches become available."[99] Also, this serves as an example of the dynamic nature required for effective cyber deterrence. Cyber deterrence is similar to other forms of deterrence in that countermeasures must be constantly updated to reflect changing technologies.

While this large and ever-growing pool of unexploited vulnerabilities existed, the challenge from DoS attacks must also factor into offensive and defensive calculations. As noted previously, DoS attacks are a matter of mathematics; therefore, attackers may be able to field larger botnets more easily than some defenders can adapt.

Deterrence by Denial – What Estonia Could Have Done

Nashe exploited a vulnerability related to the configuration of a system component – the back end of the system's databases.[100] Defending against this exploit did not require knowledge of the attacker. It required the technical expertise to locate and resolve the back-end exploit and access to international coordination to "pick off" zombie IP addresses to repel the DDoS attack.

Additional defensive enhancements might have caused attackers to rethink their decision calculus. For example, fielding excessive bandwidth to absorb

[98] Ibid., 53.
[99] Ibid., 41.
[100] Removal of this vulnerability does not suggest that attackers did not have others that could have been used instead. The technical process of identifying and closing vulnerabilities is the requirement needed for denial by defensive means, not the specifics related to eliminating this single vulnerability.

DDoS bandwidth peaks and enhancing the ability to monitor application and network traffic might have proven beneficial.[101] Several other defensive measures could also have helped deter the attacks. The approaches below relate to cyber surveillance. These early warning and detection efforts might have increased the risk for Russian attackers.

First, regarding DDoS attacks, Estonia might have enhanced its ability to detect and stop malicious users. This would have required greater attention to in-country capability to recognize known attack sources, identify bots, and determine more quickly whether an attacker was a bot or person. Known attack sources are responsible for a high percentage of DDoS attacks, and Estonia could have monitored these sources with a continuously updated list of malicious IP addresses prior to the attack. Many attackers use automated resources (bots) to conduct DDoS attacks. These "bot agents have unique characteristics" that can be recognized with existing tools, and validation tests exist to determine "whether a web visitor is a human or a bot." If a browser "accepts cookies, performs JavaScript calculations, or understands HTTP redirects," then it is probably not a bot.[102]

While precise data are unavailable on the number of Russian cyber attackers in the Estonian case, it is conceivable that the core hackers numbered in the dozens and that botnet herders represented an even smaller number. Although indeterminable from available information, Estonia, with advanced preparation,

---

[101] "4 Steps to Defeat a DDoS Attack on Your Organisation," *The Data Chain*, n.d., http://www.thedatachain.com/articles/2011/8/4_steps_to_defeat_a_ddos_attack_on_your_organisation. The challenge with increasing bandwidth is that it is expensive, and determined attackers can simply rent more bots to overwhelm one's network.
[102] Ibid.

may have been able to mount its own cyber force. Additionally, it is reasonable to assume that Estonia could have purchased, albeit from criminal sources, botnet capability to hold Russian IT systems at risk.

Second, Estonia needed better means to detect and stop malicious requests. This required greater capacity to identify an excessive number of requests and the means to prevent known network and application DDoS attacks. Because "automated attack sources almost always request webpages more rapidly than standard users," this is an indicator Estonia could have used to indicate the presence of a malicious request. Additionally, the types of DDoS attacks used against Estonia could have been "detected through unusual user activity and known application attack signatures" had a more aggressive defense posture existed pre-attack. Because normal web traffic is mimicked in an application DDoS attack, detection can be difficult. Estonia could have used a "combination of application-level and anomaly detection" to "identify and stop malicious traffic."[103]

Regarding SQL injections, three defensive actions might have deterred the attackers. The first, input validation, requires that "all data that the end-user can possibly influence be validated before being accepted or stored." Second, Estonia could have limited database privileges to the "fewest necessary to perform its function." Third, the back-end database should have been hardened and access

[103] Ibid.

restricted to "powerful stored procedures" to limit damage in the event of a compromise.[104]

These defensive measures, which may have formed a robust denial approach, did not appear to be in place. Instead, the world witnessed for the first time cyber attackers forcing a government "to defend its population and commerce in cyber war." The major defensive tool used by Estonian IT managers was to block international access to Estonian servers. Both the attack and response resulted in what was "akin to a modern blockade of a country without the concomitant deployment of any conventional weapons."[105]

Punishment – A Basis for Cyber Deterrence

An opportunity for Estonia to deter Russia and Nashe may have resided with deterrence by punishment. This section first examines perpetrators that have been identified, alleged perpetrators, and the links between the two. By studying the perpetrators, we learn whether attribution is possible. Next, the kinetic and cyber non-kinetic means available to Estonia to retaliate are considered. If the means to retaliate against a known attacker are present, then punishment may serve as a basis for cyber deterrence.

Aggressors operating from within Russia remotely orchestrated the cyber attacks against Estonia.[106] There is no evidence to suggest that the origin of these

---

[104] *Common Application Security Vulnerabilities* (DAS EISPD - Enterprise Security Office, April 8, 2008), http://www.oregon.gov/DAS/EISPD/ESO/docs/ESO_App_Sec_Vulns.pdf?ga=t.
[105] Laasme, "Estonia: Cyber Window into the Future of NATO," 59. Estonia's actions were tantamount to a cyber self-blockade.
[106] Fleury, Khurana, and Welch, "Towards A Taxonomy of Attacks Against Energy Control Systems," 7. The origin is the "location of the attacker with respect to the target." The Estonian cyber attacks had remote origins as they originated outside of the target sites. Fleury et al noted that these kinds of attacks "usually occur due to an unsecured connection such as an open wireless

attacks was local. What remained unclear was a full accounting of Russian government participation in the attacks. However, as evidence in this section will demonstrate, it is beyond dispute that actors within the Russian government used an internal proxy non-state actor (Nashe) to attack Estonia. In this case, the capacity to attribute the attack to Russia is sufficient; however, it is noteworthy that the time required to attribute the attack far surpassed the duration of the war.[107]

Attribution and a threat-based calculus are essential in cyber deterrence by punishment. As demonstrated in the bipolar Cold War era, attribution is most possible with two state actors and becomes more challenging as the number of actors increases. Attribution, and thus deterrence by punishment, becomes less possible, but not impossible, as non-state actors enter the equation.

The Identified Perpetrators

As the protests calmed due to the desecration of the Unknown Soldier, Russian web forums excoriated Estonia, which sparked the cyber war. Website managers whipped homegrown cyber patriots into a frenzy to protect Russia from the "F---ing Estonian Fascists." These same sites proliferated a strategic approach to destroy the cyber networks that had become critical to Estonia's government and private sector by offering simple directions to "organize and launch" a DDoS attack.[108]

---

network or a trusted third-party physical connection." An attack of local origin requires that an attacker have physical access to the computers or associated equipment.

[107] The delay in attribution meant that punishing identified perpetrators was not possible during the war. This does not mean that an actor cannot threaten an anticipated perpetrator or actually punish an identified perpetrator well after the occurrence of the malicious act. This has served as a basis for deterrence by punishment in both criminal justice and nuclear deterrence theory.

[108] Ruus, "Cyber War I: Estonia Attacked from Russia."

Malicious actors faced a two-fold problem with using zombies to stage a DDoS attack. First, the attacker must inject a virus into the zombie, which leaves an IP signal. Second, after the zombie downloads the virus, the computer needs instructions. This means that that the attacker who implanted the virus has to send a command for the zombie to attack the intended target. This command contains the attacker's IP address, which the attacker has spoofed. It is possible to trace back an attacker's actual IP address; however, this requires capabilities that few states possess, and even then, the process still may require years of effort with no guarantee of success.[109]

Research indicated that many of the actors who executed the attacks were motivated to strike at Estonia as an act of protest and that while official Russian sources may have provided inspiration, it appears they acted on their own accord.[110] The evidence indicated that these hacktivists included experienced hackers with the ability to write malicious code and locate botnets as well as script kiddies that only needed to follow simple directions on a webpage to participate in an attack.[111]

---

[109] Thilek, "Estonia Cyber Attacks 2007," December 28, 2009, http://meeting.afrinic.net/afrinic-11/slides/aaf/Estonia_cyber_attacks_2007_latest.pdf. There are a number of ways for a hacker to spoof an IP address. There are two simple methods. First, one may use a CGI (Common Gateway Interface) proxy to connect to another Internet service to request information instead of one's own. This is commonly referred to as "bouncing your IP address." Second, one could use a separate program for the task, such as TOR. With this or a similar program, once installed, the user only needs to press the appropriate button in an Internet browser to become anonymous. Note: world-class hackers would use more complex methods than these simple methods. See Necrostatic, "The Untraceable Man: How to Spoof Your IP Address and How It Works," *The Untraceable Man*, January 15, 2009, http://untraceableman.blogspot.com/2009/01/how-to-spoof-your-ip-address-and-how-it.html.

[110] This does not constitute a concession that Russia agents did not assist by inciting patriotic hackers or providing resources to hire botnets.

[111] Richards, "Denial-of-Service: The Estonian Cyberwar and Its Implications for U.S. National Security." "Hacktivist" is short for "hacker activist"; see Ottis, "A Systematic Approach to Offensive Volunteer Cyber Militia," 7.

In January 2008, Estonian authorities arrested 20-year-old Dmitri Galushkevich, an ethnic Russian student living in Estonia, and charged him with participating in the 2007 cyber attacks. Using his personal laptop computer, Galushkevich took Estonia's Reform Party website offline for ten days with a DoS attack.[112] Because the acts he committed originated in Estonia, authorities had access to sufficient evidence for his conviction.[113] Galushkevich pled guilty, and the Estonian court fined him 17,500 kroons ($1,650 U.S. dollars) and then subsequently released him. Throughout this process, he maintained that he was acting in response to the statue's relocation and that he was not an agent for Russia's spy services or a member of Russia's military.[114] To date, the Estonian government has made no subsequent arrests.[115] The Russian government has made the Estonian efforts to bring responsible parties to justice more difficult by refusing to cooperate on any aspect of the investigation.[116] However, this demonstrates that attribution is possible – cyber perpetrators can be identified and tried.

Attribution at a higher level occurred with a breakthrough that emerged on March 3, 2009. During a panel discussion on twenty-first-century information warfare, Sergei Markov, State Duma Deputy from the pro-Kremlin Unified Russia party, said, "About the cyber attack on Estonia ... don't worry, that attack

---

[112] Ibid.
[113] Ottis, "Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective."
[114] Kevin Poulsen, "'We Traced the Cyberwar — It's Coming From Inside the Country!'" *Wired*, January 24, 2008, http://www.wired.com/threatlevel/2008/01/we-traced-the-c/#previouspost.
[115] Richards, "Denial-of-Service: The Estonian Cyberwar and Its Implications for U.S. National Security."
[116] Ruus, "Cyber War I: Estonia Attacked from Russia."

was carried out by my assistant." [117] Markov refused to divulge his assistant's name; however, he said that his assistant determined on his own that "something had to be done to these fascists" and "launched a cyberwar."[118] That same month, Konstantin Goloskokov revealed that he was Markov's assistant.[119]

Konstantin Goloskokov, a commissar in the Nashe youth group, stated that he "and some friends had launched the attack." Goloskokov said the action was an act of cyber defense, not a cyber attack, and that they "taught the Estonian regime the lesson that if they act illegally, [they] will respond in an adequate way."[120] Goloskokov denied that he was acting on the orders of Russian government officials. When asked about his role in the attacks, he said that he and his friends did not break any laws; "we just visited the various Internet sites, over and over, and they stopped working."[121]

It is unlikely that Goloskokov could have accomplished a cyber attack of this magnitude "without at least tacit support from the Kremlin." Further, Russian experts note that Goloskokov's brazen admission of his role and that of Nashe in the attacks indicated that he did not fear retribution. This helps to legitimize the argument of those who believe the "attack was backed by higher forces."[122]

---

[117] "Behind The Estonia Cyberattacks," *RadioFreeEurope/RadioLiberty*, March 6, 2009, http://www.rferl.org/content/Behind_The_Estonia_Cyberattacks/1505613.html.
[118] Ibid.
[119] "2007 Cyber Attack on Estonia Launched by Kremlin-backed Youth Group."
[120] Ibid.
[121] "2007 Cyber Attack on Estonia Launched by Kremlin-backed Youth Group."
[122] Chloe Arnold, "Russian Group's Claims Reopen Debate on Estonian Cyberattacks," *RadioFreeEurope/RadioLiberty*, March 30, 2009, sec. Features, http://www.rferl.org/content/Russian_Groups_Claims_Reopen_Debate_On_Estonian_Cyberattacks_/1564694.html. Shackelford agrees – he cites a Russian hacker, SpORaw, who believes that the "most efficient online attacks on Estonia could not have been carried out without the blessing of the Russian authorities." See Scott J. Shackelford, "From Nuclear War to Net War: Analogizing Cyber Attacks in International Law," *Berkeley Journal of International Law* 27, no. 1 (2009): 208,

The Alleged Perpetrators

Russian non-state actors were responsible for the majority of the Estonian attacks, which came in the form of DDoS attacks.[123] It is difficult to trace the precise origins of these types of attacks because they involve large numbers of home computers that hackers remotely control. In the Estonian case, an investigator looking only at logs would see attacks coming from the "IP addresses of home user computers from all over the world."[124] Tracing the IP addresses of home users is simple; determining the origin of the bot herder is difficult, but not impossible.

Officially linking the Russian government to the attacks was difficult. During the crisis, Ansip directly accused the Russian government of being responsible.[125] However, this early attribution of the attacks to Russia did not hold up under the initial scrutiny. Some concluded that the Russians were culpable because attacks had emanated from a single Russian government computer. Later, it was determined that this computer was a zombie, unknown to the Russian government.[126]

---

http://heinonline.org.ezproxy.library.tufts.edu/HOL/Page?handle=hein.journals/berkjintlw27&id=194&div=&collection=journals.

[123] "Search Security," *TechTarget*, n.d., http://searchsecurity.techtarget.com/definition/distributed-denial-of-service-attack. A DDoS attack is "one in which a multitude of compromised systems attack a single target, thereby causing a denial of service for users of the targeted system." The targeted system's capacity to process requests is overwhelmed by a "flood of incoming messages," which forces the targeted system to shut down or drop off line.

[124] Viira, "Cyber Attacks Against Estonia - Overview and Conclusions," 72. An IP address is an "exclusive number all information technology devices use which identifies and allows them the ability to communicate with each other on a computer network." See "What Is An IP Address," *What Is My IP .com*, n.d., http://www.whatismyip.com/faq/what-is-an-ip-address.asp.

[125] "Estonia Hit by 'Moscow Cyber War,'" *BBC*, May 17, 2007, sec. Europe, http://news.bbc.co.uk/2/hi/europe/6665145.stm.

[126] James A. Lewis, *Cyber Attacks Explained* (Washington, D.C.: Center for Strategic and International Studies, June 15, 2007), http://csis.org/files/media/csis/pubs/070615_cyber_attacks.pdf.

Several weeks after the attacks concluded, Estonian ministers conceded that the "Russian government may not have been responsible, after all."[127] This did not diminish charges against Russia that its agents "could have used chat rooms and email to incite patriotic Russian hackers and cyber criminals" to attack Estonia.[128] The circumstantial evidence supporting a theory of Russian government involvement becomes somewhat more credible as the links that connect identified and alleged perpetrators are considered.

Links that Connect Identified and Alleged Perpetrators

Jeffrey Carr argues that given the anonymous nature of the Internet, those who attempt to find evidence that conclusively links the Russian government to the Estonian cyber attacks have adopted a "naive" goal that does not "accurately represent the relationships that have been built over the years between Russian politicians and organized youth associations."[129] Carr's research established that there was a three-tiered structure that "established command and control by the Kremlin through [Nashe] and other groups."[130] The membership of these groups included hackers, who were organized and receptive to recruiting other hackers to participate in malicious activity.

The cyber attacks from Nashe and other groups had the logistical support of Russian organized crime. As Nashe and Russian organized crime groups paired up to conduct cyber attacks, the arrangement provided the Russian

---

[127] Noah Shachtman, "'Cyberwar' Panic Over; Estonia Asks for Russian Help to Find Hackers," *Wired*, June 7, 2007, http://www.wired.com/dangerroom/2007/06/cyberwar_panic_/#previouspost. NATO and European Commission experts were unable to prove the Russian government participated in the Estonian cyber attacks; see Beidleman, *Defining and Deterring Cyber War*, 21.
[128] Lewis, *Cyber Attacks Explained*.
[129] Carr, *Inside Cyber Warfare*, 119.
[130] Ibid.

government a "cover of plausible deniability."[131] This dynamic between the Russian government, Nashe and other similar groups, and organized crime plausibly captured what took place in Estonia in 2007.[132]

Additionally, the Asymmetric Threats Contingency Alliance (ATCA) "uncovered evidence of alleged collusion between Russia and the botnet owners."[133] ATCA claimed that attackers hired botnets to "amplify the impact of their assault." As evidence, they note that the precise period of the attack, which started abruptly during the main phase on May 9 and ended just as sharply on May 10, suggested a timeline that when combined with the attack's effects indicated a botnet-for-hire approach.[134]

Given this analysis, Estonia and the international community could have held the Russian government accountable and thus subject to retribution, but an obvious problem exists. Consider that the director of the Russian Military Forecasting Centre stated, "The attacks against Estonia had not violated any international agreements because no such agreements exist."[135] This meant that if

---

[131] Ibid. Shachtman sustained Carr's theory in observing that "part of the ingenuity of using [Nashe] as cyberwarfare arm is the group's nominally independent status: While the group does the Kremlin's bidding, its funding comes from pro-business owners looking to ingratiate themselves with the regime. Even if they claim credit for the attacks, they are still one level removed from the Russian government." See Shachtman, "'Cyberwar' Panic Over; Estonia Asks for Russian Help to Find Hackers."

[132] Miriam Elder, "Polishing Putin: Hacked Emails Suggest Dirty Tricks by Russian Youth Group," *The Guardian*, February 7, 2012, http://www.guardian.co.uk/world/2012/feb/07/putin-hacked-emails-russian-nashi. The group Anonymous hacked and then published hundreds of emails from/to Nashe's first leader, Vasily Yakemenko, and other members sent between November 2010 and December 2011. Although unrelated to the Estonia war, these "emails appear to confirm critics' longstanding suspicions that the group uses sinister methods, funded by the Kremlin, to attack perceived enemies and pay for favourable reports while claiming that Putin's popularity is unassailable."

[133] Iain Thomson, "Russia 'Hired Botnets' for Estonia Cyber-war," *V3*, May 31, 2007, http://www.v3.co.uk/v3-uk/news/1974750/russia-hired-botnets-estonia-cyber-war.

[134] Ibid.

[135] Beidleman, *Defining and Deterring Cyber War*, 20–21.

Estonia and the community of nations wanted to hold the Russian government responsible for the attacks, they would not have legal justification. The "lack of international norms, laws, and definitions to govern state actions in cyberspace has led to a gray area that can be exploited by aggressive states as long as their actions skirt the imprecise thresholds" in agreed-upon international accords.[136]

Despite a lack of agreed-upon international laws and norms, it should be troubling to developed states that a Russian non-state actor has accepted responsibility for the Estonian cyber attacks. This implies that in Russia, there is a "private militia or stateless power" that can successfully attack the "commerce and government of any country in the world" and get away with it.[137] This case demonstrates two factors relating to the origin or attribution of cyber attacks and state security. First, a non-state actor with cyber capabilities can pose a threat to a state's national security.[138] Second, cyber attacks "can be a matter of national security, even if the attacks are difficult to attribute to a state actor."[139]

Some critics argue that deterrence by punishment is impossible without precise attribution to a guilty state actor. This suggests that a state cannot be held accountable for the actions of non-state actors within its borders. Some scholars suggest the international community should move toward a norm that holds states responsible for the activities of groups under their control.[140] Broad acceptance of such a norm may aid a deterrence-by-punishment approach.

---

[136] Ibid.
[137] Häly Laasme, "Estonia: Cyber Window into the Future of NATO," *Joint Force Quarterly*, no. 63 (2011): 59, http://www.ndu.edu/press/lib/images/jfq-63/JFQ-63.pdf.
[138] Ottis, "A Systematic Approach to Offensive Volunteer Cyber Militia," 25.
[139] Ibid., 10.
[140] The Fletcher/MIT Lincoln Laboratories Cyber Working Group charged with developing an International Cyber Code of Conduct proposed in working drafts (October 2011–March 2012) that

Estonia's Retaliatory Means

The previous section demonstrated that attribution was possible. An additional requirement to establish a basis for deterrence by punishment lies with the means available to Estonia to retaliate. In principle, retaliation could come in the form of a kinetic response or cyber non-kinetic retaliatory strike.[141] At issue in this case is the means available for Estonia to retaliate.

Kinetically, Estonia is not a nuclear-capable state. Conventionally, the size of their force and military hardware capabilities were grossly inadequate to embark on a course of conventional retaliatory strikes in response to Russian cyber attacks. Estonia ranks 126th globally in the size of their professional armed forces with 5,000 service members, while Russia ranks second with 1,520,000 military members.[142] In comparing military hardware capabilities, Estonia's Navy has four vessels – one fast attack missile craft, three mine hunters, and one minelayer. Its Army has forty-eight towed artillery pieces and no tanks. The Estonian Air Force has three airplanes – two transport aircraft and one training

---

states be held accountable for the actions of groups under government control. Under this construct, a state would not be held accountable for zombie attacks emanating from its territory that are controlled by attackers in another state.

[141] The reader may recall an earlier chapter, which presented the U.S. policy declaration in July 2011 that stated it reserves the right to respond to cyber attacks with kinetic forces. Mindful of this declaration, Estonia (theoretically) could have embarked on a similar course. However, from a practical perspective this was not an option given Estonia's military force structure.

[142] "Military Statistics - Armed Forces Personnel by Country," *NationMaster*, 2002 2001, http://www.nationmaster.com/graph/mil_arm_for_per-military-armed-forces-personnel. Estonia's professional military force is augmented with conscripts, which lasts "11 months for junior NCOs and reserve platoon leaders." Approximately 2,000 of Estonia's 5,000 military personnel are conscripts. Estonia has 360,440 men available to serve between the ages of 15 to 49 (145th globally). In comparison, Russia has 36,219,908 men available to serve between ages 15 and 49 (eighth globally). Estonia's wartime mobilization plan calls for 16,000 personnel, which is slightly more than 1 percent of Russia's peacetime military force; see "European Defence Information - Estonia."

aircraft – and three helicopters.[143] Russian military hardware includes 22,950 tanks, 12,765 towed artillery pieces (not including self-propelled guns or rocket artillery), 2,749 aircraft, and 233 Navy ships.[144] The facts of the case are clear – a basis for Estonia to deter Russia by punishment through kinetic means did not exist.

Non-kinetically, there is no evidence that Estonia possessed the retaliatory means to respond with offensive cyber capabilities. With attribution a surmountable challenge, Estonia would have needed such an offensive cyber capability and the will to exercise that capability to deter by punishment. The fact that Estonia did not use offensive cyber counterattacks does not mean that they did not possess these capabilities, but given the circumstances, it is a strong indicator that this option was not available.

Because of Estonia's advanced IT architecture, there is ample reason to suggest that Estonia had the technical proficiency to pursue an offensive capability. Had it chosen to do so, Estonia (or any other determined actor) could have located and held some Russian cyber vulnerabilities at risk. Estonia, with advanced preparation, may have been able to develop a formidable cyber force, but it did not. Further, Estonia or actors acting on Estonia's behalf may have been able to purchase botnet capability to hold Russian IT systems at risk – but once again, this did not occur. Despite the possibility of assigning attribution, the actual retaliatory means at Estonia's disposal suggests the limitations of a

[143] "European Defence Information - Estonia," *armedforces*, 2012, http://www.armedforces.co.uk/Europeandefence/edcountries/countryestonia.htm.
[144] "Russia Military Strength," *Global Firepower*, July 1, 2011, http://www.globalfirepower.com/country-military-strength-detail.asp?country_id=Russia.

deterrence concept based on punishment and further highlights the need for denial-based deterrence. This determination is based on the assumption that punishment options were restricted to Estonia's capabilities.[145]

Cooperation – From Ad Hoc Response to a Basis for Cyber Deterrence

An opportunity for Estonia to deter Russia and Nashe may have rested upon deterrence through cooperative measures. This section examines the cooperation between Estonia and non-adversarial members of society during the war, the degree of cooperation that can exist between the adversaries, and the law of war and additional legal frameworks applicable to this case. By studying these circumstances, it is possible to determine what may be needed to strengthen cooperation, which may provide a basis for cyber deterrence.

Estonia relied upon ad hoc cooperation during the 2007 cyber war. Their experience, gleaned from the facts of the case, suggests that cooperation in sharing information during and between attacks should not be an afterthought but rather a critical component of cyber deterrence theory – a component that could be developed and nurtured just as carefully as the ability to punish or deny because these types of cooperative relationships are essential in cyber deterrence. Additionally, the circumstances of the case suggest that the parties may have benefited from pledges, agreements, or treaties based upon evolving norms and customary international law. This is not a new concept as deterrence literature

[145] As discussed above, Estonia's kinetic capabilities were anemic and the status of its non-kinetic capabilities indeterminable. As a member of NATO, Estonia could have benefited from the collective capabilities of the alliance had Article 5 been in play. Absent Article 5, the researcher stands by the determination as stated that the need for denial-based deterrence is elevated.

described the long-standing utility of intra- and inter-alliance cooperation as well as the basis for cooperation that can exist in adversarial relationships.

Cooperation Between Estonia and Non-adversarial Members of Society During the War

Estonia's post hoc approach of denying access to the perpetrators of these cyber attacks worked because it was able to gain international help four days into the war. This cooperation centered in two areas: "research and investigations" and "collaboration to filter traffic."[146] Hillar Aarelaid, director of CERT Estonia (CERT-EE), led the country's response.

Aarelaid, formerly a police officer, brought ten years of cyber crime experience to his position. Aarelaid had one additional critical asset that proved to be a game changer. Over many years, he and other IT colleagues from government and the private sector developed a "tight social network." During the crisis, this "team of friends," which comprised cyber security experts from "ISPs, media, banks, and government agencies," gave Estonia an immediately available "informal rapid reaction force to counter the attacks."[147]

This team was still insufficient; in the first few days of the attack, they were limited to doing little beyond increasing server capacity and blocking incoming message traffic. CERT-EE immediately reached out to Finland, Germany, Slovenia, and others and obtained some assistance.[148] Aarelaid

[146] Nazario, "Political DDoS: Estonia and Beyond," 49.
[147] Ruus, "Cyber War I: Estonia Attacked from Russia."
[148] Ibid. NATO sent one observer.

received a break four days after the attacks began, when by chance he was having dinner with "three world-renowned IT experts [who] were visiting Estonia."[149]

These experts were Kurtis Lindqvist, Patrik Fältström, and Bill Woodcock. Lindqvist, CEO of Netnod Internet Exchange, managed "one of the thirteen Domain Name System's root servers in the world." Fältström was an engineer with Cisco and a "cyber security advisor to the Swedish government," while Woodcock served as a "research director of Packet Clearing House and member of the board of directors of the American Registry of Internet Numbers."[150]

Lindqvist was "vetted" – this meant that he was one of the few people in the world that are "trusted by the world's largest ISPs and can ask them to kick rogue computers off the network." This was crucial for Aarelaid because to defeat the DDoS attacks, he needed to force the attacking computers offline. Once the origins of the attacking zombies were determined, then he "needed to persuade ISPs around the world to blacklist the individual attacking computers that would otherwise overwhelm Estonia's bandwidth." Because these ISPs did not know Aarelaid, he needed one of the vetted to intercede.[151]

At the end of dinner, Aarelaid had increased his "social network" by adding key international experts. Lindqvist, along with Fältström and Woodcock, also vetted, agreed to go to CERT-EE headquarters.[152] Working all night, the

[149] Laasme, "Estonia: Cyber Window into the Future of NATO," 59.
[150] Ibid. A blacklist is a list of unwanted email or IP addresses that can be filtered/blocked because they participate in malicious behavior or contain vulnerabilities that permit exploitation by others.
[151] Davis, "Hackers Take Down the Most Wired Country in Europe."
[152] Ibid.

team monitored "incoming traffic in order to pinpoint the attacking rogue computers." Each time they identified a zombie's address, the vetted "asked network operators throughout the world to block its IP – the data link to the Internet – at the source." By sunrise, CERT-EE stopped the attacks of "hundreds of thousands of zombie computers," and in doing so, Estonian computer traffic was close to normal – the "tide of Cyber War I had changed."[153] However, attackers adjusted to the CERT-EE counterattack.[154]

With help, CERT-EE took measures to defend against a deluge of DDoS attacks. The first step, filtering "all communication from outside of Estonia," severed Estonia from the Internet. To counter this defensive move, attackers "recruited bots inside Estonia and continued the DDoS against critical servers."[155]

Next, security administrators discovered their back-end database vulnerability (a key exploitation discussed previously). To counter this flaw, "they threw together a large number of cache servers to store static copies of webpages" from the back-end databases. Security administrators used SQUID as a primary tool. SQUID is "an open-source server product designed to store up and serve up content that is requested repeatedly." Within seventy-two hours of fielding "SQUID farms," Estonia was online.[156]

Cooperation Between Adversaries

During the Cold War, the U.S. and USSR were adversaries, but they cooperated to avoid mutual suicide. The basis for U.S.-Soviet cooperation was

[153] Ruus, "Cyber War I: Estonia Attacked from Russia."
[154] Richard A. Clarke and Robert K. Knake, *Cyber War: The Next Threat to National Security and What to Do About It*, 1st ed. (New York: Ecco, 2010), 13-15.
[155] Stiennon, *Surviving Cyberwar*, 89.
[156] Ibid., 89–90.

that each party wanted to survive. In a nuclear attack, given the immediate level of readiness, retaliation would have occurred.

The criminal justice system was/is possible because of cooperation and agreed-upon norms between and among governments and their law-abiding populations. Criminal acts represent a failure of criminal justice deterrence; however, criminals sometimes cooperate with their adversaries (law enforcement).[157] Without cooperation and accepted norms, Cold War and criminal justice deterrence would have proven far more difficult.[158] The same may be true of cyber deterrence but we do not know yet.

Estonia – The Law of War and Additional Legal Frameworks

In the context of this case, this section examines the law of war and cyber war, applicable customary international law, and international legal regimes that directly and indirectly govern cyber attacks. Given this analysis, the study will discuss what we have learned to support the contention that a basis exists for deterrence through cooperation. Allies and adversaries have found cause to cooperate throughout the recent century, and the law of war offers a prime example.

Law of War and Cyber War

The law of war, established in customary international law, encompasses the global community of nations' recognition of *jus ad bellum* and *jus in bello*. For Estonia to invoke self-defense under *jus ad bellum*, it was necessary to

[157] For example, criminals that serve as informants are in a cooperative relationship with their adversaries.
[158] Abram Chayes and Antonia Handler Chayes, *The New Sovereignty: Compliance with International Regulatory Agreements* (Cambridge, Mass.: Harvard University Press, 1995), 115. Norms are critical to "achieving cooperative action."

"decide if a cyber exploit constituted an armed attack."[159] Thomas Wingfield concluded that the Russian cyber attacks on Estonia were "quantitatively damaging enough, or qualitatively 'military' enough, to be properly characterized under international law as uses of force."[160] However, this determination is subjective as it relied upon Michael Schmidt's seven-factor qualitative scale;[161] therefore, such a determination is ambiguous until the international community can agree upon "when and what circumstances, a disruptive exploit in cyberspace could be considered an armed attack."[162] While we cannot be certain, such ambiguity could mean that both Estonia and Russia might have felt justified that their actions were consistent (or at least not inconsistent) with the laws of war.

This ambiguity is also fueled by a "general consensus" that the United Nations (UN) Charter's Article 2(4) "prohibits only physical armed force" in the historic kinetic sense, while cyber attacks "may violate the customary international law norm of nonintervention."[163] Because Russia attempted to hide its cyber attacks on Estonia by using Nashe as a proxy actor, this may constitute an unlawful use of force. Stemming from Russia's use of force, Estonia acknowledged it was a victim, and its allies denounced the attacks.[164]

---

[159] Lewis, *A Note of the Laws of War in Cyberspace*, 2.
[160] Thomas C. Wingfield, "International Law and Information Operations," in *Cyberpower and National Security*, 1st ed. (Washington, D.C: National Defense University Press, 2009), 532.
[161] Ibid., 527–532. The seven factors in Michael Schmitt's qualitative scale are severity, immediacy, directness, invasiveness, measurability, presumptive legitimacy, and responsibility. Wingfield concluded that there was "one factor in the high range (immediacy), three factors in the moderate range (severity, directness, and invasiveness), and three factors in the low range (measurability, presumptive legitimacy, and responsibility)."
[162] Lewis, *A Note of the Laws of War in Cyberspace*, 2.
[163] Hathaway et al., "The Law of Cyber-Attack," 28–29. The customary international law norm of nonintervention "prohibits states from interfering in the internal affairs of other states"; see page 27. It must be pointed out that the authors of the UN Charter did not contemplate the challenges posed by cyber war.
[164] Ibid., 29.

Ambiguity extending from these factors existed during the war and continues as of this writing because the North Atlantic Treaty Organization (NATO) has "indicated that cyber-attacks trigger states parties' obligations under Article 4 of the NATO treaty."[165] This suggests that NATO member states "believe that cyber-attacks violate the customary norm of nonintervention or a related international law norm." However, the "fact that a cyber-attack is unlawful does not necessarily mean that armed force can be used in response."[166] The UN Charter offers two exceptions to Article 2(4) that are applicable to the case. Use of force exceptions are provided for in Article 39 when actions are taken as "part of collective security operations" and in Article 51 where actions are taken in self-defense.[167] Under the UN Charter, Estonia could lawfully defend itself, and although it chose not to act, NATO was within the bounds of the law to collectively respond.

NATO's Article 5 in the North Atlantic Treaty states:[168]

> The Parties agree that an armed attack against one or more of them in Europe or North America shall be considered an attack against them all and consequently they agree that, if such an armed attack occurs, each of them, in exercise of the right of individual or collective self-defence recognised by Article 51 of the Charter of the United Nations, will assist the Party or Parties so attacked by taking forthwith, individually and in concert with the other Parties, such action as it deems necessary, including the use of armed force, to restore and maintain the security of the North Atlantic area.
>
> Any such armed attack and all measures taken as a result thereof shall immediately be reported to the Security Council. Such

[165] Ibid. NATO's Article 4 "applies only when the territorial integrity, political independence or security of any of the parties is threatened."
[166] Ibid.
[167] Ibid., 30.
[168] "NATO - The North Atlantic Treaty," *NATO*, April 4, 1949, http://www.nato.int/cps/en/natolive/official_texts_17120.htm.

> measures shall be terminated when the Security Council has taken the measures necessary to restore and maintain international peace and security.

Because NATO did not define the cyber attacks against Estonia as an "armed attack" or "clear military action," this meant that the collective self-defense clause in Article 5 was not exercised.[169] In response to the Estonian war and since then, NATO has remained cautious and emphasized national sovereignty in responding to cyber attacks instead of invoking Article 5.[170]

Jus in bello derives from customary international law and international conventions (the Hague and Geneva) and treaties.[171] This establishes the rules that states agreed to use in war, which feature three main principles: distinction, proportionality, and neutrality. Applying these principles to the Estonian cyber war is challenging because it is difficult to distinguish between military and civilian targets. Determining proportionality is also challenging because the effects were in almost every case temporary.[172] The enforcement of neutrality was complicated by Russia's efforts to conceal the origin of the cyber attacks.[173]

The laws of war, as they currently exist, do "not regulate the vast majority of cyber-attacks."[174] As Estonia experienced massive cyber attacks, international legal regimes pertaining to cyber war had not "caught up" with the technological

---

[169] Ian Traynor, "Russia Accused of Unleashing Cyberwar to Disable Estonia," *Guardian* (Brussels, Belgium, May 16, 2007), http://www.guardian.co.uk/world/2007/may/17/topstories3.russia.
[170] Joshua McGhee, "NATO and Cyber Defense: A Brief Overview and Recent Events," *Center for Strategic & International Studies*, July 8, 2011, http://csis.org/blog/nato-and-cyber-defense-brief-overview-and-recent-events.
[171] Lewis, *A Note of the Laws of War in Cyberspace*, 2.
[172] Deterrence, in part, is based on disproportionality of response; therefore, an overwhelming response is a basis for deterrence. This suggests that states that seek to deter their adversaries may create the conditions to violate *jus in bello.*
[173] Hathaway et al., "The Law of Cyber-Attack," 35.
[174] Ibid., 44.

challenges Estonia experienced. There have been no modifications to the Law of Armed Conflict, the Geneva Accords, or an accepted rethinking of Just War theory as the era of cyber war emerged. Ambiguity and limits on the law of war "do not necessarily mean that these cyber-attacks are unregulated."[175] Additional customary international law and legal regimes offer some evidence of movement to adapt to the challenges of cyber attacks and cyber war.

Customary International Law of Countermeasures

Sources of customary international law are "international conventions, international custom, and the general principles of law common to civilized nations"[176] Beyond the law of war, these sources inform the customary international law of countermeasures. This law "governs how states may respond to international law violations that do not rise to the level of an armed attack justifying self-defense—including, implicitly, cyber-attacks." An injured state may respond to a violation of international law with "countermeasures to bring the responsible state into compliance with the law." Cyber attacks that "do not rise to the level of an armed attack [may] violate the customary international law norm of nonintervention."[177]

In this case, Russia, through its cyber attacks on Estonia, violated its obligation not to intervene in another sovereign state. Therefore, it was lawful for Estonia to employ countermeasures. Unfortunately, Estonia did not use a

---

[175] Ibid.
[176] Carr, *Inside Cyber Warfare*, 62–63.
[177] Hathaway et al., "The Law of Cyber-Attack," 45. Countermeasures are "unilateral measures taken by states as a response to hostile or unfriendly acts of another state regardless of whether the unilateral measures taken are legal per se or require a special justification." See Hjortur Bragi Sverrisson, *Countermeasure, the International Legal System, and Environmental Violations* (Cambia Press, 2008), 2. http://www.elibraryplus.com/elpreader.cfm?bookid=9781604975406&page=2.

potentially important countermeasure: active defenses. Active defenses attempt to disable the source of an attack, whereas passive defenses such as firewalls that were used by Estonia "merely attempt to repel cyber-attacks."[178]

International Legal Regimes Directly Applicable to Cyber War

The next two sections examine legal regimes that are directly and indirectly applicable to cyber attacks and cyber war. There are no encompassing international legal frameworks that directly or indirectly apply to cyber attacks.[179] With the exception of Council of Europe's Convention on Cybercrime, "most international agreements have not proceeded beyond the stage of discussing future strategies."[180] The UN and NATO have made some efforts, albeit non-encompassing, to directly regulate cyber attacks.

Council of Europe

The Council of Europe's Convention on Cybercrime is an international treaty that addresses cybercrime and currently has forty-six signatories and thirty ratifiers.[181] The treaty does not address cyber attacks or cyber war in any manner and was therefore of limited value in the Estonia case. However, as of the timeframe of the Estonian war (and since), the 2001 Convention on Cybercrime remains the most significant international cooperative efforts in the cyber domain. A significant feature of the treaty requires parties to "adopt legislative and other measures ... to establish criminal offenses under its domestic law."[182]

---

[178] Ibid., 46.
[179] Ibid., 48.
[180] Ibid., 54.
[181] Joseph S. Nye, Jr., "Power and National Security in Cyberspace," 19. The U.S. has ratified the treaty, while Russia and China remain non-signatories.
[182] Council of Europe, "Convention on Cybercrime."

The treaty identified criminal offenses that address several categories of cyber crime, which include offenses against the confidentiality, integrity, and availability of computer data and systems (illegal access, interception, data interruption, system interference); computer-related offenses (forgery and fraud); content-related offenses (child pornography); and copyright infringements.[183] Additionally, the treaty provided for jurisdiction, extradition, and mutual assistance. It mandated that parties "establish jurisdiction," defining this as a state's territory, properly configured ships, and airplanes, and stipulated that nationals were subject to criminal sanctions for illicit cyber acts committed outside of the home territory.[184]

Cooperation featured prominently in the treaty given mutual assistance and extradition clauses. The treaty required that parties "afford one another mutual assistance to the widest extent possible for the purpose of investigations or proceedings." Because of the mutual assistance that had developed between member nations, Estonia was in an improved position to seek help during the war. Extradition provisions extend to circumstances where acts are "punishable under the laws of both Parties concerned by deprivation of liberty for a maximum period of at least one year, or by a more severe penalty."[185]

The treaty was limited in that it "addressed only a portion of the overall challenge." Yet, it has failed because its membership is regional in nature and because it has done nothing to "regulate most attacks by state parties."[186]

---

[183] Ibid.
[184] Ibid.
[185] Ibid.
[186] Hathaway et al., "The Law of Cyber-Attack," 52.

Additionally, among these largely regional members, consensus was achieved on cyber crime "only by adopting vague definitions that are subject to different interpretations by different states."[187] Because of differences over definitions of cyber crime, many nations outside of the Council of Europe chose not to support the treaty.[188]

United Nations

The role of the UN has been "largely limited to discussions and informational sharing," and therefore the organization did not assist Estonia during the war. The UN's limited cyber security actions have included several vague resolutions, which "have not required any specific action by UN members." After the Estonian war, in July 2010, cyber experts from fifteen nations (including the U.S., Russia, and China) proposed a set of cyber security recommendations to the UN Secretary-General. Although these recommendations were vague, they may eventually prove useful in brokering differences between Russia and the U.S.[189]

North Atlantic Treaty Organization

NATO did little in response to the 2007 cyber-attack on Estonia, laying bare that it "lacked both coherent cyber doctrine and comprehensive cyber strategy."[190] In the aftermath of the Russia-Estonia cyber war, NATO continued to investigate the proper way to respond to cyber attacks and their obligations to

---

[187] Jack Goldsmith, "Cybersecurity Treaties: A Skeptical View," *Hoover Institution*, 2011, 3, http://www.scribd.com/doc/57295186/Cybersecurity-Treaties-A-Skeptical-View-by-Jack-Goldsmith. Beyond the use of vague definitions, "many nations conditioned their consent on declarations and reservations (the United States had more than a half dozen) that further diluted the scope of covered crimes."
[188] Ibid., 4.
[189] Hathaway et al., "The Law of Cyber-Attack," 48–50.
[190] Ibid., 50.

member states. With the 2007 Estonia and 2008 Georgia cyber war experiences as catalysts, NATO moved towards articulating strategies and taking actions to counter cyber attacks on member states.

Prior to the 2007 cyber war, NATO "concentrated on securing its own operational systems without realizing that it also should have been assisting its members in protecting theirs."[191] This effort primarily consisted of the Alliance establishing the NATO Computer Incident Response Capability (NCIRC) in 2002. In response to the 2007 war, NATO altered its approach to the cyber security threat by "extending the development of cyber defense capabilities" to individual member states and embarking on a series of initiatives.[192]

In 2008, NATO member states ratified the NATO Cyber Defense Policy, created the Cyber Defense Management Authority, and established the Cooperative Cyber Defense Center of Excellence (CCD COE).[193] Of these efforts, the CCD COE, or "the center," which became operational in Tallinn, Estonia in October 2008, has significantly enhanced member cooperation around its goal of increasing cyber security.[194]

The charter of the CCD COE is to "conduct cyberterrorism response research and establish a standard protocol for responding to a cyber attack."[195] Aside from Estonia, the CCD COE had nine sponsoring nations: Latvia, Lithuania, Germany, Hungary, Italy, Poland, Slovakia, Spain, and the U.S.[196] The

[191] Laasme, "Estonia: Cyber Window into the Future of NATO," 58.
[192] Ibid.
[193] Ibid., 61.
[194] "Cyber Defense," CCD COE, n.d., http://www.ccdcoe.org/.
[195] Richards, "Denial-of-Service: The Estonian Cyberwar and Its Implications for U.S. National Security."
[196] "Cyber Defense."

organization is not operational, unlike national CERTs. The long-term objective of CCD COE is to serve as a catalyst for helping NATO's cyber defense transformation.[197]

The CCD COE has used a series of conferences and various publications to educate members. The center held its first international Conference on Cyber Warfare in June 2009, with thirteen countries participating. In 2010, the center held two major workshops, a Cyber Defense Workshop in May and another workshop on the Cyber Commons in October.[198] The CCD COE held three additional international conferences, in June 2010, June 2011, and March 2012. The presentations at these conferences focused on strategic policy viewpoints and technical cyber challenges and solutions to inform attendees on the most up-to-date ideas for the topics covered. These international conferences and their proceedings have advanced the level of knowledge of all major cyber security themes to include cyber deterrence.

Aside from the CCD COE, NATO has made significant strides in its cyber defense posture, but much work remains. The alliance reached a milestone on January 22, 2010 when it formally defined *computer network attack*.[199] However, NATO stopped short of moving beyond this definition to define cyber war or describe circumstances in which it would respond to cyber attacks.

---

[197] Ottis, "A Systematic Approach to Offensive Volunteer Cyber Militia," 185.
[198] Laasme, "Estonia: Cyber Window into the Future of NATO," 62.
[199] Ibid., 61. A computer network attack is an "action taken to disrupt, deny or degrade information resident in a computer and/or computer network, or the computer and/or computer network itself."

NATO's 2010 Strategic Concept outlined the need to "develop further our ability to prevent, detect, defend against, and recover from cyber-attacks."[200] Unfortunately, the Strategic Concept did not "contribute much toward clarifying ambiguities" associated with terminology and commitments to defend member states against cyber attacks.[201] However, building upon the 2010 Strategic Concept, a task emerged from NATO's 2010 Lisbon Summit to develop an "in-depth cyber defence policy by June 2011."[202]

The North Atlantic Council met this deadline as NATO Defense Ministers approved the *NATO Policy on Cyber Defence* on June 8, 2011. The focus of this policy was to protect its "own communication and information systems." To satisfy the challenge inherent in its focus, the policy relied on an objective of constructing a "coordinated approach to cyber defense" by incorporating "planning and capability development, and response mechanisms for cyber attack." Two key principles provided the foundation to satisfy this objective: prevention and resilience.[203]

Despite this progress, it appears that NATO did not fully appreciate the harsh lessons learned by Estonia and Georgia during their cyber wars. The utility

---

[200] "Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organisation" (NATO, 2010), http://www.nato.int/lisbon2010/strategic-concept-2010-eng.pdf.
[201] Laasme, "Estonia: Cyber Window into the Future of NATO," 61.
[202] "Lisbon Summit Declaration: Issued by the Heads of State and Government Participating in the Meeting of the North Atlantic Council in Lisbon," NATO, November 20, 2010, http://www.nato.int/cps/en/natolive/official_texts_68828.htm.
[203] "Defending the Networks: The NATO Policy on Cyber Defence" (NATO Public Diplomacy Division, 2011), http://www.nato.int/nato_static/assets/pdf/pdf_2011_09/20111004_110914-policy-cyberdefence.pdf. Drafters of the policy concluded that "certain threats will persist despite all efforts to protect and defend against them," which drove their prevention and resilience approach. Prevention means increasing the "level of preparedness and mitigating risk by limiting disruptions and their consequences." Resilience means the capacity to "facilitate rapid recovery in the aftermath of an attack."

of the *NATO Policy on Cyber Defence* comes into question when one examines NATO's "collective response" approach to the cyber challenge. The policy stated that all responses are "subject to decisions of [the] North Atlantic Council" and that in considering taking action in response to a cyber incident, NATO will "maintain strategic ambiguity as well as flexibility." Immediately afterward, the document reads, "NATO will provide coordinated assistance if an Ally or Allies are victims of a cyber attack."[204] This choice of words provides NATO with a "hedge" to avoid action while at the same time offering undefined "coordinated assistance" to those under cyber attack.

Five years after the Estonia cyber war, NATO has "no guidelines for response to a cyber attack ... or the networks (such as public or private) that would be involved."[205] With the exception of the limited role of the CCD COE, this suggests that NATO is basically useless to help countries deter or respond to cyber attacks as in these circumstances it will "only activate Article 4 of the NATO treaty, which calls upon members to 'consult together' in cases of cyber-attacks." Under Article 4, members are not bound to "assist each other, as would be required under Article 5."[206] In a November 2011 discussion, former Chief of Staff of NATO's SHAPE Karl-Heinz Lather confessed that there is "currently is no 'recipe' which NATO can use to clearly respond to cyber attacks." He said

[204] Ibid.
[205] Amber Corrin, "NATO Cyber Defense Lags," *Federal Computer Week*, February 2, 2012, http://fcw.com/articles/2012/02/02/nato-cyber-defense-lagging.aspx.
[206] Hathaway et al., "The Law of Cyber-Attack," 51.

Article 5 was "off the table for the alliance" because "Article 5 responses require very concrete targets, which you don't have with cyber attacks."[207]

International Legal Regimes Indirectly Applicable to Cyber Attacks

International legal regimes that indirectly regulate cyber attacks include International Telecommunications Law, Aviation Law, Law of Space, and Law of the Sea. These regimes regulate portions of the cyber domain that may be used in cyber attacks. They pre-date the emergence of cyber attacks and therefore do not "expressly regulate or prohibit cyber-attacks."[208] However, it is likely that some cyber attacks on Estonia transited international wire communications and satellites and therefore may have been subject to some minimal measure of legal protection from International Telecommunications Law and the Law of Space.

The problem Estonia faced is that with telecommunications law, there are no limits on military use or a mandatory reporting requirement; therefore, there are currently no "teeth" to this law regarding cyber transgressions.[209] Regarding space law, follow-on agreements from the 1967 Space Treaty such as the Agreement Relating to the 1971 International Telecommunications Satellite Organization (Telecommunications Satellite Organization) and the Convention of the 1979 International Maritime Satellite Organization (Maritime Satellite Organization) "have little impact on cyber attacks." The controlling organizations

[207] Robin Tim Weis, "Can NATO Adapt to Cyber Warfare?," *FrumForum*, November 29, 2011, http://www.frumforum.com/can-nato-adapt-to-cyber-warfare.
[208] Hathaway et al., "The Law of Cyber-Attack," 54.
[209] Ibid., 55–57.

for these agreements are not positioned to "promulgate public regulations related to cyber attacks."[210]

Strengthening Cooperation to Deter Cyber War

We have learned from the case that is difficult to support a contention that a basis exists for cyber deterrence through cooperation as a stand-alone component of the triadic concept. On the eve of the Estonia cyber war, the international community had made progress with mutual assistance and extradition in combating cybercrime through the Convention on Cybercrime. Yet, aside from perhaps a head start on the tactical cooperation used in the war, this did little to help Estonia.

Analysis of the decade-long Cybercrime Convention indicated, "nations significantly disagree about what digital practices should be outlawed and are deeply skeptical about even the weakest forms of international cooperation in this area."[211] This prevailing attitude has spilled over into efforts to strengthen cooperation to deter cyber war. Much work remains to adapt existing and create new institutions and regimes to address cyber vulnerabilities pertaining to cyber attacks. This is complicated in an international environment in which, according to Joseph Nye, there is skepticism that support exists for a multilateral cyber treaty, agreement, or pledge.[212] Attention in two areas may help resolve this impasse: an alignment of interests and a more certain verification posture.

---

[210] Ibid., 60–61.
[211] Goldsmith, "Cybersecurity Treaties: A Skeptical View," 4.
[212] Joseph S. Nye, Jr., "Power and National Security in Cyberspace," 20. A pledge is a nonlegal agreement used by international lawyers in lieu of a formal contract or agreement, which permits "states to accept more risks in the face of uncertainty." Examples of pledges include the 1975 Helsinki Final Act, and the Proliferation Security Initiative initiated in 2003. See Kal Raustiala,

First, a prerequisite to a treaty, agreement, or pledge is an alignment of interests. Without the prospect of mutual gain, "there is no incentive to enter into a contract or to comply with it." What we learn from the Estonia case is that it is unclear if a "mutually beneficial deal is possible in theory."[213] It does not seem reasonable that Russia or other cyber powers such as the U.S. or China would concede cyber advantages to states with less cyber capabilities without receiving something in return. Further, as Goldsmith observed, "when nations disagree sharply over the matter to be regulated, they tend to agree (if at all) in vague generalities that are not terribly useful for fostering true cooperation."[214] This portends poorly for strengthening cooperation to enhance cyber deterrence.

Next, assuming that states are able to align interests to form a consensus on an agreement, significant verification problems with any cybersecurity agreement remain. These challenges are linked to attribution; however, the Estonia case has demonstrated that attribution is possible. The prime concerns focus less on the actor and more on the confidence that "transparency measures are in fact transparent, or that revealed doctrine is actual doctrine."[215]

Assuming shared interests and verification are achievable, international cooperation can help deter cyber war "given the transnational nature of the challenge." While developing norms is essential, more is needed to forge an international agreement or even a pledge. Such an effort must contain an agreed-

---

"Form and Substance in International Agreements," *The American Journal of International Law* 99, no. 3 (July 2005): 582-584.

[213] Goldsmith, "Cybersecurity Treaties: A Skeptical View," 4.

[214] Ibid., 7.

[215] Ibid., 12. It must be pointed out that norms cannot "get much purchase in a world without serious attribution and verification; anonymity is a norm destroyer."

upon definition of cyber attack and cyber war. Second, main features of the Convention on Cybercrime should be incorporated into a framework focused on cyber attack and cyber war. For example, "more robust international cooperation in evidence collection and criminal prosecution of those participating in cross-national cyber-attacks" may help deter cyber warfare. [216]

Cooperation can help deter, but left to its own design, one remains skeptical of the concept as a basis for deterrence. However, when combined with denial measures, a critical and highly relevant feature of cyber deterrence theory emerges because it is "almost impossible to defend any country's electronic infrastructure solely with its own resources, as the cyber attacks on Estonia demonstrated."[217]

What is required is a combination of international cooperation and denial-inspired compellence.[218] In short, cyber deterrence is made possible by the joining of forces with other nations to pursue cyber attackers and share information on threats while simultaneously locking down cyber networks by hardening and otherwise eliminating or reducing vulnerabilities.

The facts of the case demonstrated that Estonia had a keen incentive to cooperate. Given the global cyber challenge, the Estonian experience served as convincing evidence that nations reliant upon cyber infrastructures would benefit

[216] Hathaway et al., "The Law of Cyber-Attack," 70–71.
[217] Laasme, "Estonia: Cyber Window into the Future of NATO," 63.
[218] States will also need to pursue parallel internal actions to develop their criminal justice systems to a set international standard. For example, this process is underway in states that are parties to the Council of Europe Convention on Cybercrime; however, in this Convention the parallel international and domestic actions are limited to cybercrime.

from cooperative alliances and agreed-upon defensive commitments in combination with bolstering denial capabilities as a means to deter cyber war.

Summary

The purpose of this case was to foster greater understanding for the requirements to deter cyber war by applying the triadic components of cyber deterrence theory: punishment, denial, and cooperation. The first triadic component explored is denial in which four elements were examined: exploited and unexploited vulnerabilities, targets, and defensive actions.

By understanding the vulnerabilities that were attacked and those that could have been attacked, we begin to see requirements, which serve as a basis for cyber deterrence by denial. Exploited vulnerabilities were studied across four areas: Internet dependence, system weaknesses, hardware exploitations, and software exploitations. Here we discovered the actual vulnerabilities that formed the basis for the cyber attacks against Estonia as well as other vulnerabilities that could have been exploited. We learned that Estonia is heavily dependent upon the Internet, with nearly 60 percent of its population having Internet access. This would suggest that Estonia's higher usage rate implied a greater vulnerability to attacks on the Internet. Because of this high level of dependence, two requirements appear useful: possessing a secure line of communication and employing cyber defenses as a whole-of-society endeavor.

System weaknesses in Estonia permitted attacks on network configurations. As explained in detail with examples in the case, this meant that hackers were able to "gain improper access" when a resource is not configured

appropriately. This suggests that recruiting and training IT professionals to adapt to the rapid pace of technological innovation and increasing self-inspection processes are important requirements.

As the reader may recall, the explanations of hardware and software exploitations were in-depth, highly technical, and complex. In setting the requirements for deterrence theory, what mattered in the Estonia case is that their circumstance improved when they, with outside cooperation, had the capability to recognize that an exploit was under way and then take action to deny the attacker the benefit of that exploit. This suggests that in addition to well-trained personnel, passive defense must be a requirement to deter hardware and software exploitations. Further, the case illustrates that resilience, or the capacity to recover quickly, should serve as perhaps the most important requirement in deterring hardware and software exploitations because of the futility it injects into the attacker's decision calculus.

The targets selected for exploitation by Russian attackers in Estonia were largely networks and individual users.[219] A continuous process of evaluating vulnerabilities and potential vulnerabilities and repairing them without delay is an imperative. Satisfying this requirement is necessary to protect the categories of targets that were attacked (networks and users) while also ensuring that attacks against additional target categories not attacked (systems, processes, and data) are

[219] Fleury, Khurana, and Welch, "Towards A Taxonomy of Attacks Against Energy Control Systems," 9. Networks are made up of the "computers, switches, hubs, etc. connected either via wires or wirelessly." In attacking a network, the malicious actor seeks to "make communications among the computers and switches difficult or impossible." A user is a person with "authorized access to a system." In attacking a user, the perpetrator generally seeks to "illicitly gain information from the user for later use," for example, gaining access to the user's password.

equally deterred.[220] In addition to the passive defense measures mentioned above, an added requirement for this aspect of denial is the use of cyber red teams to test continuously one's vulnerability to attack.

Defensive actions were post hoc and reactive and required cooperation to stave off the attacks. In Estonia, collaboration several days into the war resulted in access to invaluable research and investigative capabilities, which helped filter traffic and complicate attackers' techniques until the attacks subsided. One could argue that the defenders prevailed, as the attacks ceased in a matter of days. However, this would ignore the circumstantial evidence that the attackers quit on their terms. In the Estonia case, it appeared that the Russian attackers adjusted to every defensive move until their political objectives were satisfied.[221]

Unexploited vulnerabilities provide us insight into avenues for attack that could have been used but were not. It is impossible to determine precise reasons why these avenues were not pursued by Russian attackers. In the six months leading up to this case, 3,400 new software vulnerabilities were discovered. With only a handful of known vulnerabilities used in the attacks, the potential for the use of other attack options was likely present. However, given the attackers' success, it appears they selected their avenues of attack well. In Estonia, attackers

---

[220] Ibid. Data are defined as "information suitable for processing by humans or machines," while systems are made up of "one or more connected components that can perform substantial computations." In short, a system is a computer. In both cases, data and individual computers were not targeted. I interpreted efforts to steal passwords that involved a user's computer as an attack on that user and not on the computer. I suspect that access to additional (classified) information on these attacks would likely yield some examples of malicious activity in all five target categories that have been used in this study: network, process, system, data, and user. Any minor oversights in this area will have no bearing on the requirements for deterrence that emerged from the study.

[221] This assumes that the Russian objective at this point was to teach the Estonians a lesson. If the Russians intended on returning the statue to its original site, then they failed – there is no evidence that this was the circumstance.

exploited vulnerabilities predominantly through Internet-facing sites and client-side software. From these circumstances, two requirements arise: the need for enhanced detection and monitoring in conjunction with active defense and the need for states to either find on their own or purchase zero-day vulnerabilities.

The second triadic component explored was punishment in which two elements were examined: attribution and offensive/retaliatory means. This case demonstrated that attribution is possible, although it occurred after the cessation of open hostilities. This fact should have no bearing on the utility of attribution and hence punishment as a core component of the triadic concept.

The actors in this case had differing capabilities, kinetically and non-kinetically. This suggests the importance of a requirement to tailor cyber deterrence for differing classes of actors.[222] It mattered that Russia was a nuclear power with overwhelming conventional superiority over Estonia.

Retaliatory means are a critical component of punishment. Because of the drastic mismatch in kinetic capabilities between the attacker and defender, it is quite telling to ask that given certain attribution: What capabilities would Estonia have had to possess to exploit available vulnerabilities to punish their Russian attackers? Kinetically, we know that Estonia ranks 126th globally. Unfortunately, the researcher was unable to assess its cyber capabilities. However, given the advanced IT structure of Estonia, one would think the potential to develop retaliatory capability could be present.

[222] This idea builds upon the work of Keith Payne, Elaine Bunn, and Geoffrey French on tailoring, which is discussed in previous chapters.

What is known is that Estonia, despite being the most wired nation in Europe, mounted no cyber counteroffensive. This means that even though attribution proved possible, albeit belatedly, Estonia did not possess the capability to deter Russia by punishment. From this case, a striking requirement springs forward: Cyber deterrence should be tailored to account for differences in kinetic and non-kinetic capability.

The combination of denial and cooperation offers the strongest basis for cyber deterrence because of Estonia's diminutive retaliatory capabilities. However, it must be noted that had NATO invoked Article 5, Estonia's retaliatory capacity would have been bolstered by the alliance's collective self-defense pact. The circumstances of the case revealed the value of cooperation in the triadic construct by considering the relationships between non-adversaries and adversaries.

Estonia relied upon its domestic IT social network and a small number of international experts that, by chance, happened to be in Estonia around the time when the war began. Although a member of NATO, the alliance beyond sending one observer (belatedly) was useless during the war. It is an important factor that NATO did not perceive the cyber war against one of its members as an armed attack, which would have invoked an Article 5 response. The circumstances indicated that a useful requirement for deterrence by cooperation is to establish a priori relationships between non-adversaries. From a broader perspective, cooperation to develop norms[223] as a path to future cyber agreements is crucial.[224]

[223] In addition to norms, a cyber deterrence concept could contain enforcement mechanisms as well.

The facts of the case when applied to this theory reveal five observations:

1. Attribution matters but is not an insurmountable challenge.
2. Smaller states can potentially deter larger states from initiating a cyber war.
3. Cyber vulnerability can be mitigated – this provides a basis for deterrence by denial.
4. Deterrence by denial can prevent an attacker from succeeding.
5. Cooperative relationships are necessary in cyber deterrence but must be realized in conjunction with the application of denial capabilities.

Cyber deterrence theory did not fail in this case because it was not present before the attack. However, while it is indeterminable if the Estonians could have deterred the cyber war by using the triadic concept, the facts shed light on the requirements that may form the basis for such a theory.

[224] *A Preliminary Report on the Cyber Norms Workshop* (Cambridge, Mass.: Massachusetts Institute of Technology, October 2011), http://ecir.mit.edu/events/conferences/184-cyber-norms-conference. The report targeted the following areas in which norm developments were needed: 1. States need to recognize the international implications of their technical decisions, and act with respect for one another's networks and the broader Internet. 2. States should act within their authorities to help ensure the end-to-end interoperability of an Internet accessible to all. 3. States should respect the free flow of information in national network configurations, ensuring they do not arbitrarily interfere with internationally interconnected infrastructure. 4. States should recognize and act on their responsibility to protect information infrastructures and secure national systems from damage or misuse.

Chapter 5: Russia vs. Georgia

"Cyber attacks are a part of the information war; making your enemy shut up is a potent weapon of modern warfare."

– Alexander Denezhkin[1]

Introduction

The world's second cyber war, ignited by a dispute over South Ossetia, took place between Russia and Georgia. This short war was the "first example of a cyber-based attack that coincided directly with a land, sea, and air invasion by one state against another."[2]

The war consisted of two phases. A rehearsal phase for the main thrust of cyber attacks that would follow, Phase I, occurred on July 19, 2008. This attack was a component of a strategic campaign consisting of weeks of "cyberspace reconnaissance," which included probing and scanning that paved the way for the attacks to begin suddenly on August 7, 2008.[3, 4]

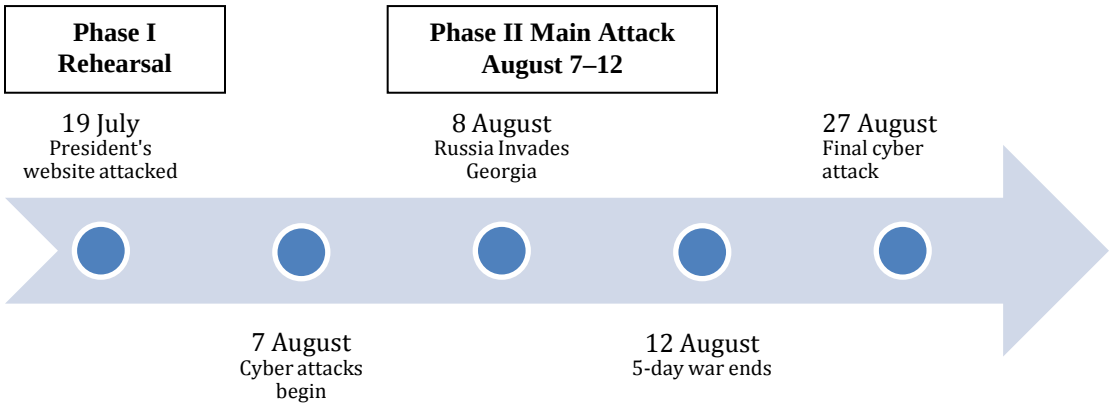
The main attack, Phase II, occurred between August 7 and August 12, 2008. In this phase, Georgia experienced crippling cyber attacks against its government, media, and banking sector before, during, and after Russia's ground, air, and naval invasion. Russia's goal was to overload, with the intent of temporarily impairing, Georgia's cyber network to limit the country's ability to

---

[1] Jart Armin, "RBN-Georgia Cyberwarfare-Continuation...," *Russian Business Network (RBN)*, August 2008, http://rbnexploit.blogspot.com/2008/08/rbn-georgia-cyberwarfare-continuation.html. Alexander Denezhkin is the editor of the Russian journal Cybersecurity.ru.
[2] Jeffrey Carr, *Inside Cyber Warfare*, 1st ed. (Sebastopol, Calif: O'Reilly Media, 2010), 3.
[3] David Hollis, "Cyberwar Case Study: Georgia 2008," *Small Wars Journal* (January 6, 2011): 4.
[4] Terry Fleury, Himanshu Khurana, and Von Welch, "Towards A Taxonomy of Attacks Against Energy Control Systems," in *Proceedings of the IFIP International Congerence on Critical Infrastructure Protection*, 2003, 7–8, http://www.ncsa.illinois.edu/People/hkhurana/IFIP_CIP_08.pdf. A potential attacker probes a system to learn its characteristics. An attacker scans a system to "access targets sequentially for the purpose of determining specific characteristics."

"distribute their point of view about the ongoing military conflict." A secondary Russian objective was to deprive Georgian citizens of real-time information.[5] To achieve this outcome, attackers primarily used variations of flood attacks, although efforts to modify some target's websites through defacement met with success.[6] See Appendix C for additional background information on events leading to the war.

Figure 5.1: 2008 Georgia Cyber Attacks Timeline[7]



As in the previous case, we cannot know whether deterrence based on an approach centered on a triadic relationship between denial, punishment, and

[5] Eneken Tikk et al., *Cyber Attacks Against Georgia: Legal Lessons Identified* (Tallinn, Estonia: CCDCOE, November 2008), 16, http://www.carlisle.army.mil/DIME/documents/Georgia%201%200.pdf.

[6] Fleury, Khurana, and Welch, "Towards a Taxonomy of Attacks Against Energy Control Systems," 7–9. A flood occurs when an attacker "repeatedly accesses or overloads the target's capacity, possibly disabling the target." *Modify* means to "change the contents of the target." This research examines the offensive cyber actions taken against the Georgians. It does not include the actions taken that established the preconditions for DDoS attacks via botnets. To locate vulnerable computers in which to insert a malicious bot, one would likely need to probe potential targets. To probe means to "determine characteristics of a system." Scanning, which is attempting to "access targets sequentially to determine specific characteristics," may also prove useful. Lastly, a hacker may spoof an intended victim; this requires assuming the "appearance of a different entity in the system to access the target."

[7] Tikk et al., *Cyber Attacks Against Georgia: Legal Lessons Identified*, 36–43. The researcher developed this timeline by drawing upon information provided in the accompanying citation.

cooperation would have prevented the cyber attack against Georgia. We can determine the extent of vulnerability, together with the actual vulnerabilities that formed the basis for the cyber attacks against Georgia. We can also assess the capabilities possessed by Georgia to exploit the vulnerabilities of the attackers. What would Georgia have had to protect in order to deny the attackers the targets attacked? What capabilities would Georgia have had to possess to punish the attackers, assuming of course that attribution could be established? It is unknown if this triadic arrangement would have elevated the costs to deter the cyber war in this circumstance. However, the case study assesses this deterrence concept by reference to what was attacked.

Georgia – The Second Cyber War

Kenneth Corbin argued that the 2008 Russia-Georgia war offered "conclusive proof that cyberwar has come into its own."[8] Richard Stiennon similarly referred to Georgia as the "first cyberwar."[9] Tikk et al disagreed, concluding that Russia's cyber attacks on Georgia did not satisfy the international definition of "war"[10] because the "objective facts of the case are too vague to meet the necessary criteria" for Law of Armed Conflict (LOAC) applicability.[11]

"European Union (EU) Forms CERT Group to Fight Cyber Attacks," *International ICT Policies and Strategies*, June 18, 2011, http://ictps.blogspot.com/2011/06/european-union-eu-forms-cert-group-to.html.

[8] Kenneth Corbin, *Lessons From the Russia-Georgia Cyberwar* (UK: The Institute of Communications Studies, University of Leeds, n.d.), http://ics-www.leeds.ac.uk/papers/vp01.cfm?outfit=gdr&folder=442&paper=750.

[9] Richard Stiennon, *Surviving Cyberwar* (Lanham, Md: Government Institutes, 2010), 95. Stiennon wrote that "we will not experience information warfare until two adjacent networked countries engage in network attacks concurrent with tanks rolling across their borders" and noted that this happened on August 8, 2008, with the start of the Russia-Georgia war. See page ix.

[10] Tikk et al., *Cyber Attacks Against Georgia: Legal Lessons Identified*, 18.

[11] Ibid., 23. Tikk et al relied upon the research of Schmitt and Solce to argue that it was "problematic to apply [the] LOAC to the Georgian cyber attacks" because the [cyber attacks] did not rise to the legal standard to "trigger" the LOAC.

In the case of the Russia-Georgia war, unlike the Estonia case, offensive cyber attacks were not the sole force applied. Russian actors used cyber attacks to help seize the initiative at the outset of a conventional war, and cyber attacks continued as a core component of Russia's attack strategy through the war's duration.[12] The fact that cyber attacks were a part and not the totality of Russia's application of force should not call into question reference to Russia's 2008 attack on Georgia as a cyber war.[13]

The Russia-Georgia war was the second time in history when cyber attackers targeted an entire country and therefore sustains Stiennon and Corbin's determination that this case meets the threshold of a cyber war. However, this study has relied upon time-tested Clausewitzian ideals to define cyber war more narrowly as the continuation of state policy by cyber means.[14] This narrower definition is also satisfied as Carr's Project Grey Goose provided plausible evidence of a dynamic between the Russian government, Russia's cyber militia,

---

[12] Billy K. Rios, "Sun Tzu Was a Hacker: An Examination of the Tactics and Operations from a Real World Cyber Attack," in *The Virtual Battlefield: Perspectives on Cyber Warfare* (Amsterdam: Ios Press, 2009), 150.

[13] To help resolve differences of opinion, this study again uses Thomas Rid's taxonomy of war. Rid argued that an act of war must have three components: "It has to be potentially violent, purposeful, and political"; see Thomas Rid, "Think Again: Cyberwar," *Foreign Policy*, April 2012." The cyber attacks in Georgia meet the threshold of Rid's definition of cyber war in each of these areas. They were violent because Georgia's attackers used a form of physical force to "damage"; see "Coulomb Force." The attacks were purposeful because the cyber militia had both the means and an end. In the Georgia case, Russia's cyber militia was the prime attacker. This militia had the capabilities – or access to them – and a desired goal to separate Georgia's government and media from the population. Lastly, the root cause of the Russia-Georgia war was political differences. The application of force by cyber and conventional military means settled these differences with a variety of instruments, techniques, and strategies in the service of a political battle. See Reet Oorn, "'Cyber War' and Estonia: Legal Aspects," in *Information Technology in Public Administration of Estonia - Yearbook 2007* (Tallinn, Estonia: Ministry of Economic Affairs and Communications, 2008), 74, http://www.riso.ee/en/files/IT_yearbook_2007_final.pdf.

[14] Carl von Clausewitz in *On War* famously wrote that war "is nothing but the continuation of policy with other means." This research purposely structures the definition of cyber war from a state-centric perspective. Non-state actors may conduct cyber attacks and engage in cyber espionage; however, they are, at this time and for the near future, incapable of waging cyber war.

and organized crime in the 2008 Georgian cyber attacks.[15] As in the Estonia case, Russia supported a non-state proxy actor in attacking Georgia's information infrastructure to achieve state policy goals in the second example of a cyber war.

Denial – Defensive Action as a Basis for Cyber Deterrence

An opportunity for Georgia to deter Russia and its cyber militia may have rested upon deterrence by denial through defensive measures. Evidence that links identified and alleged perpetrators will be presented later in the chapter when attribution is examined. The purpose of this section is to examine the weaknesses and vulnerabilities that Russia exploited to attack Georgian cyber targets as well as unexploited vulnerabilities that either party could have used but did not. By studying these vulnerabilities in combination with the targets and means of attack Russia used, it is possible to isolate requirements, which may provide a basis for cyber deterrence by denial.

Vulnerability – A Function of Internet Dependence, IT Sophistication, and Geography

Three factors served as bases for Georgia's vulnerability to cyber attack: the country's level of dependence on the Internet, the sophistication of its information architecture, and the geographical location of critical external components that supported online connectivity. Georgia's dependence upon the Internet in 2008 was less than that of Estonia in 2007. Because Georgia was a "much less advanced Internet society," the impact of Russian cyber attacks, although significant, was less severe than that of the attacks experienced by

[15] Jeffrey Carr, *Inside Cyber Warfare*, 1st ed. (Sebastopol, Calif: O'Reilly Media, 2010), 115–130.

Estonia.[16] The Georgian population in 2008 had "seven Internet users per 100 people," while Estonia had fifty-seven per 100 people in 2007.[17]

The level of sophistication of Georgia's information infrastructure contributed to a "lack of dominance in cyberspace operations" during the war. This causal factor hampered "Georgia's ability to conduct national-level strategic communications."[18] In contrast to Estonia where an overreliance on its information architecture served as a vulnerability, the reverse was true in Georgia's situation, yet this exposed a different vulnerability. Georgia's lack of a sophisticated infrastructure proved to be a vulnerability as this contributed to an inability to "recover cyberspace and informational capabilities during [a] critical period" of the war. Therefore, the Russians were able to synchronize their operations in such an efficient manner that they only required a temporary window into Georgia's cyberspace to help impose their will on the physical battlefield.[19]

This was not difficult for the Russians; in 2008, Georgia's information infrastructure consisted of "five companies operating in the Georgian Internet access and services market." One of these, Caucasus Network Tbilisi, controlled 90 percent of the commercial Internet service provider market.[20] These companies depended upon fiber optic cables extending from neighboring

[16] Scott W. Beidleman, *Defining and Deterring Cyber War* (Carlisle Barracks, PA: U.S. Army War College, June 1, 2009), 5, http://www.hsdl.org/?view&did=28659.
[17] Tikk et al., *Cyber Attacks Against Georgia: Legal Lessons Identified*, 5.
[18] Hollis, "Cyberwar Case Study: Georgia 2008," 8–9.
[19] Ibid.
[20] Tikk et al., *Cyber Attacks Against Georgia: Legal Lessons Identified*, 6–7.

countries for Internet connectivity.[21] Therefore, Georgia was vulnerable due to the small size of its cyber infrastructure and its dependence upon the infrastructure of neighboring countries.

Georgia had two primary IP transit options available, TTnet (a subsidiary of Turk Telecom), based in Turkey, and Azerbaijan's Delta Telecom, which Russia controlled.[22] Additional connectivity was available from Europe; however, nearly all of Georgia's Internet access came from Turkey and Russia. This meant that Russia had access to a "high bandwidth connection for Russian bots" to flood Georgia. To add to Georgia's challenge, "Turk Telecom, the main upstream for Georgia in Turkey, [was] also a major source of bots."[23]

Of these two main channels of connectivity, Georgia was more dependent upon Russia because "nearly half of Georgia's thirteen links to the worldwide network" passed through Russia. Although the majority of Georgia's 309 networks were routed through "Turkish or Azerbaijan service providers ... the latter [was] then routed on via Russia."[24] Georgia's location and dependence upon neighboring countries made it a "good target for coordinated cyber assault and isolation."[25] Russian attackers took advantage of these factors, Georgia's

---

[21] Earl Zmijewski, "Georgia Clings to the Net," *Renesys*, August 10, 2008, http://www.renesys.com/blog/2008/08/georgia_clings_to_the_net.shtml. These internet carrying fiber optic cables were built alongside the "Baku-Tbilisi-Ceyhan (BTC) pipeline, a major source of European oil that is not under Russian control and is projected to carry 1 million barrels a day by 2009."

[22] Jose Nazario and Andre M. DiMino, "An In-Depth Look at the Georgia-Russia Cyber Conflict of 2008", n.d., 8, http://www.shadowserver.org/wiki/uploads/Shadowserver/BTF8_RU_GE_DDOS.pdf.

[23] Jose Nazario, "Politically Motivated Denial of Service Attacks," in *The Virtual Battlefield: Perspectives on Cyber Warfare* (Amsterdam: Ios Press, 2009), 167. Nazario relied upon the analysis of Bill Woodcock at Packet Clearing House, who demonstrated that most all of Georgia's Internet connectivity routes transit Russia or Turkey.

[24] Tikk et al., *Cyber Attacks Against Georgia: Legal Lessons Identified*, 6.

[25] Ibid.

systems weaknesses, and inherent vulnerabilities in the cyber domain to expose the country to cyber attack.

Vulnerability – A Function of System Weaknesses

Attackers exploited the configuration and design/specification of Georgia's cyber network to conduct DDoS attacks and web defacements.[26] Specification vulnerabilities resulting from weak points in system design aided hackers in DDoS attacks.[27] Exploitation of these systems weaknesses against government and media targets made it possible for Russian attackers to achieve their purpose of making "it harder for the Georgians to determine what was happening."[28]

Georgia could have reduced the weaknesses of its networks and closed vulnerabilities in its systems by hardening and enhancing the resilience of its systems. This would have increased Russia's level of effort and helped minimize inducements for cyber attack by eliminating or reducing vulnerabilities. Engineering resilience into computer networks may inject a sense of futility into

[26] Fleury, Khurana, and Welch, "Towards a Taxonomy of Attacks Against Energy Control Systems," 9–10. Vulnerability "describes why an attack can be successful." It does not "specify the actual target that is vulnerable, but rather the weakness in the system that can be exploited." When a system is not properly configured, "a hacker can gain improper access." Examples include "poor account management where certain unused accounts and/or services have (possibly high-level) access to the system; components with known flaws that are not correctly patched; weak or non-existent authentication (including unchanged passwords); and misconfigured perimeter protection and/or access control policy." If design flaws are present in a process or component, "these flaws can be utilized in unintended ways to gain access to the system."

[27] Configuration vulnerabilities were present in some applications, which permitted SQL injections in back-end components, which will be explained in a following section.

[28] John Bumgarner and Scott Borg, *Overview by the US-CCU of the Cyber Campaign Against Georgia in August of 2008* (U.S. Cyber Consequences Unit, August 2009), 5, http://www.registan.net/wp-content/uploads/2009/08/US-CCU-Georgia-Cyber-Campaign-Overview.pdf.

the attackers' decision calculus that could elevate a state's deterrence posture.[29] Georgia could have increased the resiliency of its computer networks by pursuing the following four goals:[30]

1. **Anticipating:** maintaining a state of informed preparedness in order to forestall compromises of mission/business functions from adversary attacks
2. **Withstanding:** continuing essential mission/business functions despite successful execution of an attack by an adversary
3. **Recovering:** restoring mission/business functions to the maximum extent possible subsequent to successful execution of an attack by an adversary
4. **Evolving:** changing missions/business functions and/or the supporting cyber capabilities to minimize adverse impacts from actual or predicted adversary attacks

To fulfill these goals, Georgia would have had to purposefully engineer cyber resiliency as a component of its mission assurance posture. Such an approach would involve of a number of disciplines: information system security engineering, resilience engineering, survivability, dependability, fault tolerance, and business continuity and contingency planning.[31] Publicly available literature regarding Georgia's IT structure prior to the war did not reveal the extent to which Georgia may have had these mechanisms in place.

The relative ease that the cyber militia enjoyed in holding Georgia's IT infrastructure at risk suggests a lack of sophistication on the defender's part that

[29] Maintaining the effectiveness of defensive efforts can be difficult to sustain due to the rapidly changing nature of cyber technology.
[30] Deborah J. Bodeau and Richard Graubart, *Cyber Resiliency Engineering Framework* (MITRE, September 2011), iii, http://www.mitre.org/work/tech_papers/2012/11_4436/11_4436.pdf.
[31] Bodeau and Graubart, *Cyber Resiliency Engineering Framework*, iii. Examples of international efforts that focus on network resilience include the Multiannual Thematic Program from the European Network and Information Security Agency (ENISA), which has "the ultimate objective to collectively evaluate and improve the resilience of public communications in Europe," and ReSIST, "established under the European Commission's Sixth Framework Programme to bring together leading researchers active in the multidisciplinary domains of Dependability, Security, and Human Factors." See pages 54-55.

implies cyber resiliency was not a forethought. The ramifications of this are magnified further when considered with the rapid pace of technological advancements and the ingenuity of modern cyber attackers. In short, Georgia faced a difficult chore to stay abreast, much less ahead, of emerging vulnerabilities. Given Georgia's dependence upon Russia, Turkey, and other external agents for Internet connectivity, its cyber security was spectacularly vulnerable. In the Georgia case, the weaknesses that made the attackers' offensive actions possible were susceptible to denial by defensive measures.

Russian Exploitation of Georgia's Cyber Vulnerabilities

Cyber attacks against Georgian targets were possible because Russian attackers identified and exploited hardware and software vulnerabilities. The exploitation of these vulnerabilities posed a significant problem; however, had Georgia mitigated its cyber vulnerabilities, cyber war or the use of cyber attacks in conjunction with a conventional kinetic war may not have been possible. Recognizing and then closing vulnerabilities is a requirement for deterrence by denial.[32]

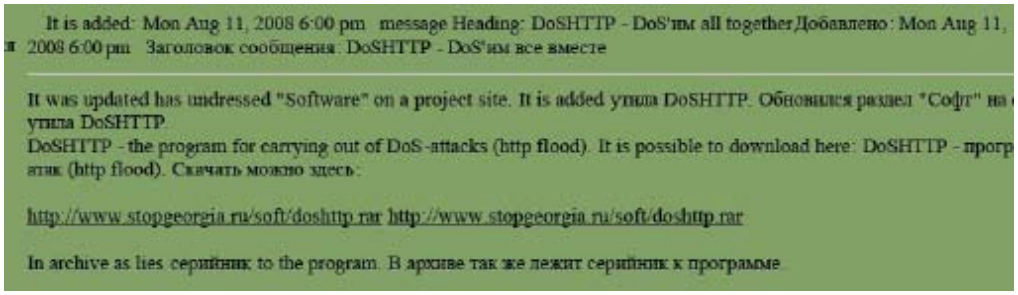
How Cyber Exploitations May Take Place

To understand vulnerabilities inherent in DoS attacks, it is necessary to understand more about these attacks. The previous chapter covers these explanations in depth.[33] There are many forms of DoS attacks: flood attacks, logic/software attacks, mail bombing, permanent denial-of-serve (PDoS) attacks,

[32] This claim extends only to cyber war and is not to be taken by the reader as a comment on Georgia's capacity to deter conventional war with Russia.
[33] See expanded text in Estonia case, under section "How Cyber Exploitations May Take Place."

accidental denial-of-service attacks, and DDoS attacks.[34] In addition, hackers also may use malware in cyber attacks to destroy computer hardware and software and to remotely take control of unsuspecting user's computers. These forms of attack were effective in the Russia-Georgia war because they overwhelmed cyber-related targets and quickly isolated the Georgian government and media from the population. Russian forums offered easy access to tools for novices to initiate these DDoS attacks (see Figure 5.2).

Figure 5.2: StopGeorgia.ru Forum Leaders Provide Access to DoS Tool[35]


It is added: Mon Aug 11, 2008 6:00 pm message Heading: DoSHTTP - DoS'им all together Добавлено: Mon Aug 11, 2008 6:00 pm Заголовок сообщения: DoSHTTP - DoS'им все вместе

It was updated has undressed "Software" on a project site. It is added утила DoSHTTP. Обновился раздел "Софт" на утила DoSHTTP.
DoSHTTP - the program for carrying out of DoS -attacks (http flood). It is possible to download here: DoSHTTP - програ атак (http flood). Скачать можно здесь:

http://www.stopgeorgia.ru/soft/doshttp.rar http://www.stopgeorgia.ru/soft/doshttp.rar

In archive as lies серийник to the program. В архиве так же лежит серийник к программе

How Cyber Exploitations May Be Conducted by Overloading Servers

Hackers used several variants of flood and ping attacks to overwhelm Georgian networks.[36] Four types of flood attacks were discovered: ICMP, TCP SYN, TCP RST, and HTTP flooding.[37] On the surface, this suggested that attackers exploited Georgia with a "brute force" approach.[38] However, a brute force DDoS attack, by definition, is one in which the attacker "sends as much

[34] Richards, "Denial-of-Service: The Estonian Cyberwar and Its Implications for U.S. National Security." Mail bombing is the purposeful transmission of massive amounts of unwanted email to a target's(s') account.
[35] Jeff Carr, *Russia/Georgia Cyber War - Findings and Analysis* (Project Grey Goose, October 17, 2008), 14, http://www.scribd.com/doc/6967393/Project-Grey-Goose-Phase-I-Report.
[36] Fleury, Khurana, and Welch, "Towards A Taxonomy of Attacks Against Energy Control Systems," 7–8. A flood occurs when an attacker "repeatedly accesses or overloads the target's capacity, possibly disabling the target."
[37] Tikk et al., *Cyber Attacks Against Georgia: Legal Lessons Identified*, 36.
[38] The researcher suspected but could not validate that Georgian web server configurations were also a contributing factor to the success of flood attacks (as in the Estonia case).

traffic as he can to consume network resources ... without any knowledge of the system design."[39]

The facts confirm that attackers relied upon "more sophisticated attacks ... by aiming at hurting a weak point in the victim's system design."[40] Sophisticated DDoS attacks include HTTP and TCP SYN floods, both used against Georgia. These attacks were sophisticated because each was tailored to Georgia's systems design with the objective of enhancing the effectiveness of the attack.

By using these sophisticated attack vectors, Russia's cyber militia reduced the cost of the attacks, the number of zombies they needed to rent, and the level of effort needed to coordinate attacks. Additionally, "designing a sophisticated attack tool requires only a one-time effort of understanding the system design in order to find its weak point." This aided Russia's strategy of using seasoned hackers to provide novice users "an 'off the shelf' attack tool" that could be executed by those without hacking knowledge.[41]

Using DDoS Attacks to Exploit Hardware Vulnerabilities

Hackers used two variants of flood attacks to overwhelm hardware components of Georgia's networks: ICMP and HTTP flooding. ICMP flooding ties up the "server so that legitimate user requests go unfulfilled." It works by "sending the victim's IP network address to broadcasting computers, which in turn 'broadcast' the IP address to other computers, beginning a chain reaction."

---

[39] U. Ben-Porat, A. Bremler-Barr, and H. Levy, "Evaluating the Vulnerability of Network Mechanisms to Sophisticated DDoS Attacks," in *INFOCOM 2008. The 27th Conference on Computer Communications. IEEE*, 2008, 1.
[40] Ibid.
[41] Ibid., 1–2.

These responses, in the form of information packets, overload the victim's IP address when returned.[42]

In an HTTP flood, attackers overload the targeted server with random requests to overwhelm the server, thus causing it to crash. Because it is difficult to discern legitimate packets from those that are malicious, this type of DDoS attack is hard to detect. Additionally, a DDoS attack that uses an HTTP flood vector targets the both the server's TCP/IP stack and the web server, which complicates defeating the attack.[43]

Using DDoS Attacks to Exploit Software Vulnerabilities

Hackers used two variants of flood attacks to overwhelm software components of Georgia's networks: TCP SYN and TCP RST flooding. TCP SYN floods "overload a victim's server by exploiting communication protocols." This occurs when an attack transmits "information requests with a false 'return address' to a server, which unsuccessfully attempts to return contact until it times out."[44] A TCP RST flood is possible because "an established TCP connection can be reset by sending a suitable TCP packet with the RST or SYN flag set. Since a source IP address and port can be forged, this may potentially be exploited by a

[42] Richards, "Denial-of-Service: The Estonian Cyberwar and Its Implications for U.S. National Security." ICMP flooding is also known as "smurfing."
[43] Atul Khachane, "How to Prevent HTTP Flood Attack from Your Dedicated Server?," *Web Hosting Issues*, August 24, 2010, http://webhostingissues.blogspot.com/2010/08/how-to-prevent-http-flood-attack-for.html.
[44] Richards, "Denial-of-Service: The Estonian Cyberwar and Its Implications for U.S. National Security." This process "clogs the system" in that it "renders the server unavailable to respond to other legitimate requests."

malicious person to reset a connection between other systems." When used maliciously, a TCP RST interferes with Internet connectivity.[45]

DoS, DDoS, and other attack vectors were successful because they took advantage of vulnerabilities in Georgia's cyber infrastructure. Aware of these vulnerabilities, Russian hackers customized many of the cyber attack tools used against Georgia. For example, hackers developed "three different software applications designed for stress tests," which were used to flood Georgia's servers with HTTP packets to judge the servers capacity to manage traffic. Russian hackers also reengineered a fourth tool by taking a software application originally designed to enhance website functions and adapting it to "request random, non-existent pages." This particular tool was efficient because once deployed, Georgian servers "rapidly exhausted their computing capacity searching for the pages that weren't there."[46]

Using Ping Attacks to Exploit Software Vulnerabilities

Ping attacks are different from flood attacks, which designers have engineered to overload targets.[47] Ping attacks are logic/software attacks that break communication protocols by forcing errors. When an attacker sends a "group of pings (packets of information) that exceed the maximum size allowed

[45] "Cisco IOS TCP Connection Reset Denial of Service Vulnerability," *Secunia Stay Secure*, n.d., http://secunia.com/advisories/11440/. TCP RST is a TCP reset attack.
[46] Bumgarner and Borg, *Overview by the US-CCU of the Cyber Campaign Against Georgia in August of 2008*, 4–5. The US-CCU tested these HTTP attack tools and discovered that they "proved far more effective than the ICMP-based attacks that the Russians had used on Estonia." This tool, as posted by attackers, "simultaneously targeted seventeen different Georgian websites."
[47] Tikk et al., *Cyber Attacks Against Georgia: Legal Lessons Identified*, 9–10.

by the system," the system crashes because it is unable to "reassemble the packets."[48]

Exploiting Software Vulnerabilities in Back-end Databases – The Main Culprit

In addition to customizing flood attacks, Russian hackers introduced "SQL injection attacks in conjunction with DoS attacks." This was an alarming development for several reasons:[49]

- SQL injection attacks could indicate that all data stored in the back-end databases could have been pilfered or altered.
- Attackers that had pilfered the back-end databases via SQL injection could have access to legitimate username and password combinations, allowing them to masquerade as legitimate users.

The ability of Georgian cyber defenders to detect a "targeted SQL injection attack designed to pilfer data or compromise the underlying system during a rigorous, traditional DDoS" proved challenging, especially when a "DoS attack included SQL injection attacks designed to cause a DoS condition."[50]

SQL injections were the most common method for defacement of Georgian websites. This technique "exploits a security vulnerability occurring in the database layer of an application."[51] The SQL injection uses data that have not been properly validated as part of a command (or query). These "specially

---

[48] Richards, "Denial-of-Service: The Estonian Cyberwar and Its Implications for U.S. National Security."
[49] Carr, *Russia/Georgia Cyber War - Findings and Analysis*, 9.
[50] Ibid., 4.
[51] Eneken Tikk, Kadri Kaska, and Liis Vihul, *International Cyber Incidents: Legal Considerations* (Tallinn, Estonia: Cooperative Cyber Defence Centre of Excellence (CCD COE, 2010), 114, http://www.ccdcoe.org/publications/books/legalconsiderations.pdf. The vulnerability is "present when user input is either incorrectly filtered for string literal escape characters embedded in SQL statements or user input is not strongly typed and thereby unexpectedly executed." SQL is a "database computer language designed for the retrieval and management of data in relational database management systems (RDBMS), database schema creation and modification, and database object access control management."

crafted" data "trick the application into executing unintended commands or changing data." This allows the attacker to "create, read, update, alter, or delete data stored in the back-end database."[52] Because this type of website defacement affects the back-end database rather than the front-end static web application files, efforts to track changes would not have detected the attack while in progress.[53]

Russian efforts to discover and act upon these vulnerabilities began weeks before the war but went undetected by Georgia. As evidence, see Figure 5.3 and note that the July 1 log dates are associated with SQL injection queries used in later cyber attacks. Therefore, over a month before the main cyber attacks began, "SQL injection attacks started with simple fingerprinting of the back-end database servers being used by the vulnerable applications." Analysis of these logs revealed that hackers were able to determine usernames and passwords from these attacks. Access to this information provided a foundation for Russia's cyber attacks on Georgia.[54]

Figure 5.3: Evidence of SQL Injection Attacks from Georgia Log Files[55]

```
[Tue Jul 01 05:32:43 2008] [error] [client 91.XXX.XXX.XXX] File does not exist:
/home/virtual/XXX/public_html/small4, referer: http://www.XXX.gov.ge/full_text.php?nid=-
6038%2union%20select%201,2,3,4,5/*
[Tue Jul 01 05:33:19 2008] [error] [client 91.XXX.XXX.XXX] File does not exist:
/home/virtual/XXX/public_html/small4, referer: http://www.XXX.gov.ge/full_text.php?nid=-
6038%2union%20select%20unhex(hex(version())),2,3,4,5/*
[Tue Jul 01 05:33:35 2008] [error] [client 91.XXX.XXX.XXX] File does not exist:
```

[52] "SQL Injection Tutorial: Learn About SQL Injection Vulnerabilities and Prevention." A database is a system for collecting information to "organize, sort, and retrieve large amounts of data efficiently." Databases have two sections, a front and back end. The front end contains the "application objects, such as the queries, forms, reports, macros and modules" and is "used on the user's desktop." The front end is linked to the back end, which "stores the tables with the data" on a server because it is a "location shared by many users." The computer language or programming that retrieves information from databases is SQL. See "What Is a Database."

[53] "SQL Injection 2.0."

[54] Billy K. Rios, "Sun Tzu Was a Hacker: An Examination of the Tactics and Operations from a Real World Cyber Attack," in *The Virtual Battlefield: Perspectives on Cyber Warfare* (Amsterdam: Ios Press, 2009), 148.

[55] Ibid.

Seasoned hackers posted SQL injection attack tools alongside DDoS tools on Russian forums. This, combined with the posting of predetermined targets, allowed computer novices to take advantage of sophisticated methods to hold Georgian cyber vulnerabilities at risk.[56] This approach fostered a dynamic whereby the "exploitation of a single application level vulnerability [potentially] leads to further compromise and exploitation, long after the initial vulnerability is fixed." In this case, a "chain of events began with the targeted exploitation of a single vulnerability in a single application and grew into multiple attacks launched simultaneously, along with the beginning of a conventional campaign."[57]

Cyber Targets: Georgia's Networks a Focus of Russian Hackers[58]

Georgia faced crippling cyber attacks against its networks, processes, and, to a lesser extent, individual users.[59] Within Georgia's critical network infrastructure, 309 networks were located in Georgia at the time of the war. In the three-day period from August 8 to 10, nearly 35 percent of these networks were

[56] Ibid., 149.
[57] Ibid.
[58] Fleury, Khurana, and Welch, "Towards A Taxonomy of Attacks Against Energy Control Systems," 8-9. The target is "the resource that is being attacked."
[59] Ibid., 9. A network "consists of computers, switches, hubs, etc. connected via wires or wirelessly." Fleury et al define process as an application or "program running a computational device, [which] may consist of the actual program as well as any data being accessed by the process." A user is "someone with authorized access to a system." The researcher did not locate evidence that indicated individual systems (computers and peripheral devices) were targeted in the attacks, although given the methods used, this was in the realm of possibility. However, such attacks would have been necessary to build the botnets that were used against Georgia. There was no evidence that attackers manipulated data for monetary or other gain, yet, once again, given the attacker's methods, this could have easily taken place. Data consist of "information suitable for processing by humans or machines" or can be a "single resource such as a file stored on a hard drive or the transmission of such data across a communications network."

unusable for prolonged periods and almost 60 percent exhibited signs of instability.[60]

Aside from networks, attackers focused on processes. This permitted attackers to overwhelm Georgia's information systems with a small number of malicious computers.[61] There were also attacks on individual users. The defacement of the Georgian president's website is a prime example of such an attack. As previously explained, defacement attacks resulted from SQL injections.[62]

StopGeorgia, a Russian forum, initially inspired attackers to target thirty-six prominent websites, including the "embassies of the U.S. and U.K. in Tbilisi; the Parliament, Supreme Court, and Ministry of Foreign Affairs of Georgia; several news and media resources; and numerous other sites."[63] See Table 5.1 for a partial list of targeted governmental websites and Table 5.2 for a list of targeted media websites by the StopGeorgia forum.[64] These sites, along with TBC, Georgia's largest bank, and others, to include Georgia's most prominent hacker site, experienced DoS and DDoS attacks.[65]

Aside from President Saakashvili's site, several other websites experienced defacement. Hackers defaced the National Bank of Georgia "with a

---

[60] Zmijewski, "Georgia Clings to the Net."
[61] Carr, *Russia/Georgia Cyber War - Findings and Analysis*, 3–4.
[62] Ibid., 9. This allows attackers to gain access to "legitimate username and password combinations, [which allow attackers] to masquerade as legitimate users."
[63] Tikk et al., *Cyber Attacks Against Georgia: Legal Lessons Identified*, 10. Attackers did not substantively increase the number of targets attacked after the initial wave of attacks in the main cyber thrust. For the duration of the war, botnet attacks did not exceed eleven targets. See Bumgarner and Borg, *Overview by the US-CCU of the Cyber Campaign Against Georgia in August of 2008*, 4.
[64] Stiennon, *Surviving Cyberwar*, 98.
[65] Tikk et al., *Cyber Attacks Against Georgia: Legal Lessons Identified*, 8-9.

gallery of twentieth century dictators," while the Ministry of Foreign Affairs experienced defacement with a "collage of photos of Mikheil Saakashvili and Adolf Hitler" (see Figure 5.4). Additionally, the Computer Emergency Response Team for Estonia (CERT-EE) reported defacements of three Azerbaijan media outlets.[66]

Table 5.1: Governmental Targets Attacked by StopGeorgia Forum[67]

Target Description	URL
Autonomous Republic of Abkhazia	www.abkhazia.gov.ge
Ministry of Education and Science of the Republic of Georgia	www.mes.gov.ge
Republic of Georgia website providing standardized educational tests for students	www.naec.gov.ge
Parliament of the Republic of Georgia	www.parliament.ge
President of the Republic of Georgia	www.president.gov.ge

Table 5.2: Media Targets Attacked by StopGeorgia Forum[68]

Target Description	URL
Largest online forum in Georgia	www.forum.ge
Largest Georgian news page in English	www.civil.ge
Association Press	www.presa.ge
News portal	www.apsny.ge
Private television company	www.rustavi2.com
News portal in English	www.news.ge
News portal	interpress.ge
News portal	www.tbilisiweb.info

Russia Attacks Georgia

One needs to understand how cyber attacks are carried out in order to develop requirements for cyber deterrence. Merging a precise understanding of the circumstances of the attacks with previous analysis on the vulnerabilities that

[66] Ibid., 7–8. Sources drawn upon for this information were unclear as to "whether all three websites [Georgian President, Ministry of Foreign Affairs, National Bank] were defaced in the same way or whether two different types of defacements were carried out" as the description indicates. The URLs for the three Azerbaijan media outlets were www.day.az, www.today.az, and www.ans.az.
[67] Stiennon, *Surviving Cyberwar*, 98.
[68] Ibid.

were exploited and those available for exploitation helps create a basis for deterrence by denial in this case. In examining the cyber attacks against Georgia, the case study again used various components of the Fleury et al taxonomy. Particularly useful were the model's attack components of origin and action to conduct this analysis (see Annex A).[69]

As in the 2007 Estonia cyber war, attackers used variations of DDoS attacks and website defacements; however, the intensity of the attacks was much higher in the Georgia case.[70] The cyber campaign in the Russia-Georgia war consisted of a one-day rehearsal phase and a main phase, which lasted five days. The main phase of the cyber attacks coincided with the five-day conventional war and subsided on August 12. A final cyber attack took place on August 27, well into the Russian occupation that followed open hostilities.

The First Attack – A Dress Rehearsal

The first cyber attack of the war occurred on July 19, 2008 and began with a DDoS attack on the website of Mikheil Saakashvili, President of Georgia. The Shadowserver Foundation observed the attack as it occurred. They assessed that a command and control (C&C) server attacked the site with several different techniques. The C&C server commanded the bots to attack "with TCP,[71] ICMP,[72]

---

[69] Fleury, Khurana, and Welch, "Towards A Taxonomy of Attacks Against Energy Control Systems," 8–9. Action describes the "activity the attack is performing on the target."
[70] Tikk et al., *Cyber Attacks Against Georgia: Legal Lessons Identified*, 44.
[71] "TCP (Transmission Control Protocol)," *Search Networking*, March 15, 2012, http://searchnetworking.techtarget.com/definition/TCP. TCP is a "set of rules (protocol) used along with the IP to send data in the form of message units between computers over the Internet." IP handles the "actual delivery of the data," and TCP keeps "track of the individual units of data (called packets) that a message is divided into for efficient routing through the Internet."
[72] "ICMP," *Wedpodeia*, n.d., http://www.webopedia.com/TERM/I/ICMP.html. ICMP is "an extension to the Internet Protocol (IP)." "ICMP supports packets containing error, control, and informational messages. The ping command uses ICMP to test an Internet connection."

and HTTP[73] floods."[74, 75] Jose Nazario of Arbor Networks was able to determine that the "attacks were issued by [a] Machbot controller that had over 15,000 bots."[76] A Machbot controller is a "tool frequently used by Russian bot herders"[77] and is "primarily known to be popular in Eastern Europe."[78] The attack forced the website offline for more than 24 hours and slowed its ability to send and receive traffic for several days.[79]

To achieve this effect, attackers used a "well known Russian malware variant from the Pinch family" with the Machbot controller. Danchev reported that the inclusion of the message "win+love+in+Rusia" in the DDoS flood packets indicated Russian involvement. Additionally, the attackers made a mistake that further confirmed that Russian "botnet masters" initiated the attack. First, the malware had to phone back to a C&C server with a known history of "sharing DNS servers[80] with a provider of DDoS attacks on demand."[81]

---

[73] Khachane, "How to Prevent HTTP Flood Attack from Your Dedicated Server?" In an HTTP flood, an attacker overloads the targeted server with random requests to overwhelm the server, causing it to crash. Because it is difficult to discern legitimate packets from those that are malicious, this form of DDoS attack is problematic. Additionally, an HTTP flood DDoS attack targets the servers TCP/IP stack and the web server, which complicates defeating the attack.
[74] Fleury, Khurana, and Welch, "Towards A Taxonomy of Attacks Against Energy Control Systems," 7–8. A flood occurs when an attacker "repeatedly accesses or overloads the target's capacity, possibly disabling the target."
[75] Tikk et al., *Cyber Attacks Against Georgia: Legal Lessons Identified*, 36.
[76] Nazario and DiMino, "An In-Depth Look at the Georgia-Russia Cyber Conflict of 2008," 10.
[77] Stephen Adair, "The Website for the President of Georgia Under Attack - Politically Motivated?," *Shadowserver*, July 20, 2008, http://www.shadowserver.org/wiki/pmwiki.php/Calendar/20080720.
[78] Dancho Danchev, "Georgia President's Website Under DDoS Attack from Russian Hackers," *ZDNet*, July 22, 2008, http://www.zdnet.com/blog/security/georgia-presidents-web-site-under-ddos-attack-from-russian-hackers/1533.
[79] Nazario and DiMino, "An In-Depth Look at the Georgia-Russia Cyber Conflict of 2008," 10.
[80] Bradley Mitchell, "What Is a DNS Server?," *About.com Wireless / Networking*, n.d., http://compnetworking.about.com/od/dns_domainnamesystem/f/dns_servers.htm. The Domain Name System (DNS) manages the names of websites. It allows one to type a name instead of a number (IP address) into a web browser (such as Internet Explorer or FireFox), and the computer then finds that site. A DNS server is "any computer registered to join the DNS." These servers are arranged in a hierarchical order. At the top of this hierarchy are thirteen root servers that

The Phase I attack was a component of a strategic campaign consisting of weeks of "cyberspace reconnaissance," which included probing and scanning that paved the way for the attacks to begin suddenly on August 7.[82, 83] This view conflicts with the previously explained impression of some observers that no cyber reconnoitering was performed immediately preceding the war. Additionally, for several weeks prior to the five-day war, "Russian websites, chat rooms, and networks discussed the upcoming attacks."[84] During this process, Russian cyber militia leaders behind the StopGeorgia.ru forum vetted Lithuanian as well as Russian IP addresses with which to attack Georgia. They did this because of the lessons learned from Georgia's defensive move to block Russian IP addresses after the attack of President Saakashvili's website in July.[85]

The inclusion of cyber attacks in the Russian war plan was not ad hoc. As further evidence of the cyber attackers' sophistication, consider that attackers targeted both of Georgia's most accomplished hacker sites because of their capacity to organize cyber resistance and execute a cyber counteroffensive.[86]

"store the complete database of Internet domain names and their corresponding IP addresses." Japan, the UK, and Sweden each have one of these servers, and the remainder are in the U.S. Lower on this hierarchy are the DNS servers attacked in Georgia. These servers run a "special-purpose networking software, [which] features a public IP address and contains a database of network names and addresses for other Internet hosts."

[81] Danchev, "Georgia President's Website Under DDoS Attack from Russian Hackers."

[82] Hollis, "Cyberwar Case Study: Georgia 2008," 4.

[83] Fleury, Khurana, and Welch, "Towards A Taxonomy of Attacks Against Energy Control Systems," 7–8. A potential attacker probes a system to learn its characteristics. An attacker scans a system to "access targets sequentially for the purpose of determining specific characteristics."

[84] Hollis, "Cyberwar Case Study: Georgia 2008," 4.

[85] Carr, *Inside Cyber Warfare*, 15.

[86] Alex Michael, *Cyber Probing: The Politicisation of Virtual Attack* (Defence Academy of the United Kingdom, December 2010), 15, http://www.voltairenet.org/IMG/pdf/Cyber_Probing.pdf. These Georgian hacker sites were www.hacker.ge and www.warez.ge.

Cyber Attacks – The Main Thrust

The main thrust of the cyber attacks began late in the evening on August 7 and waned on August 12 with the conclusion of the five-day war. During the main phase, the barrage of DoS and DDoS attacks prevented Georgia's government from communicating externally or internally during the most crucial periods of the war. This had a "discouraging effect on Georgian nationals."[87] Those responsible for the cyber attacks were able to achieve this measure of effectiveness because they "had advance notice of Russian military intentions, and they were tipped off about the timing of the Russian military operations while these operations were being carried out."[88]

There were only a few hours between the start of the main cyber attack phase and the Russian conventional invasion. Therefore, there was insufficient time for Russian attackers to reconnoiter Georgian cyber systems immediately prior to the attack. This provided further evidence of premeditation and cooperation as the "speed of action" indicated that the cyber attackers had a "signal to go ahead" well before the first media reports.[89]

The height of the DDoS attacks and website defacements occurred on August 8, which coincided with the escalation of conventional warfare between Russia and Georgia.[90] On that day, the first full day of the war, there were

---

[87] Ibid, 15.
[88] Bumgarner and Borg, *Overview by the US-CCU of the Cyber Campaign Against Georgia in August of 2008*, 3.
[89] Ibid. The Russian cyber attackers "jumped directly to the sort of packets that were best suited to jamming websites under attack." This action, combined with others such as registering domain names and new websites, happened so rapidly that they had to have been prepared ahead of time.
[90] Tikk et al., *Cyber Attacks Against Georgia: Legal Lessons Identified*, 37.

eighteen TCP SYN floods and one TCP RST flood.[91] The attacks were unsophisticated in that they did not require a high degree of hacking skill, but nevertheless they were executed in a sophisticated manner.[92] This resulted in a greater intensity than that seen in the Estonian attacks, albeit with fewer computers participating.[93]

The tactics employed by Russia's cyber militia, as recounted previously, eliminated "centralized coordination of the attack." By using online forums, seasoned hackers were able to engage and empower citizens who had computer access to a target list and easy-to-use cyber attack tools.[94] These tactics allowed the militia to capitalize rapidly on "botnets and [C&C] systems that were ready before the Russian invasion." Throughout the duration of the five-day war, the militia was able to maintain a focused botnet attack on key targets.[95]

These tactics proved beneficial to Russia's cyber militia as after the initial thrust, postings on forums helped increase cyber attacks. A key to this increase was the forum leaders' ability to provide sufficient information so that novice computer users with "limited computer skills" could participate. This tactic resulted in shutting down with DDoS attacks or defacements with SQL injections

[91] Nazario and DiMino, "An In-Depth Look at the Georgia-Russia Cyber Conflict of 2008," 15.
[92] Bumgarner and Borg, *Overview by the US-CCU of the Cyber Campaign Against Georgia in August of 2008*, 4.
[93] Tikk et al., *Cyber Attacks Against Georgia: Legal Lessons Identified*, 44.
[94] Dancho Danchev, "The Russia Vs Georgia Cyber Attack," *Dancho Danchev's Blog - Mind Streams of Information Security Knowledge*, August 11, 2008, http://ddanchev.blogspot.com/2008/08/russia-vs-georgia-cyber-attack.html.
[95] Bumgarner and Borg, *Overview by the US-CCU of the Cyber Campaign Against Georgia in August of 2008*, 4.

an additional "forty-three targeted websites" beyond the "eleven targeted by botnets associated with organized crime."[96]

Project Grey Goose investigators discovered the method the Russia cyber militia used to execute a simpler and more effective attack strategy with fewer computers. With only one computer, a novice attacker using a provided script could disable "sites using a built-in feature of MySQL." MySQL is a "software suite widely used by websites to manage back-end databases." By exploiting an embedded feature with an SQL injection, a single attacker is able to "inject millions of junk queries into a targeted database, such that the Web servers behind the site become so tied up with bogus instructions that they effectively cease to function."[97]

SQL injections were also a popular method to deface websites.[98] Attackers used this method to deface President Saakashvili's website with a series of pictures in which Saakashvili and Hitler were making similar gestures or facial expressions (see Figure 5.4).[99] Attackers claiming to be a group from South Ossetia defaced the Georgian Parliament's website with the same image.[100]

---

[96] Ibid.
[97] Brian Krebs, "Report: Russian Hacker Forums Fueled Georgia Cyber Attacks," *Washington Post*, October 16, 2008, http://voices.washingtonpost.com/securityfix/2008/10/report_russian_hacker_forums_f.html.
[98] "SQL Injection 2.0."
[99] Dancho Danchev, "Coordinated Russia Vs Georgia Cyber Attack in Progress," *ZDNet*, August 11, 2008, http://www.zdnet.com/blog/security/coordinated-russia-vs-georgia-cyber-attack-in-progress/1670.
[100] Stephen Adair, "Georgian Websites Under Attack - DDoS and Defacement," *Shadowserver*, August 11, 2008, http://www.shadowserver.org/wiki/pmwiki.php/Calendar/20080906.

Figure 5.4: Saakashvili Website Defacement[101]

Statistics reveal that the combination of DDoS and defacement attacks such as these severely crippled Georgia's cyber capabilities at the time and place of the attacker's choice. These factors helped form a broad consensus that Russia's cyber attacks were coordinated from the start. Russian cyber attackers may have a learned a lesson regarding the utility of coordinated cyber strikes, as it was not until the second phase of the Estonian cyber war that evidence of coordinated attacks emerged.[102]

Data captured by Arbor Networks for August 8 revealed intense attacks on four targets. The longest attack lasted for slightly more than six hours, reaching an intensity of 814 Mbps (see Table 5.4).[103] In contrast, the greatest intensity of an attack in the Estonia cyber war measured 100 Mbps of traffic.[104] The

[101] Danchev, "Coordinated Russia Vs Georgia Cyber Attack in Progress." Danchev argued that a script kiddie would not go to the trouble or understand the psychological effect of coming up with pictures of Hitler and Saakashvili exhibiting similar gestures. He maintained that in all likelihood a "three-letter intelligence agency's propaganda arm" was the creative force for this defacement.
[102] Tikk et al., *Cyber Attacks Against Georgia: Legal Lessons Identified*, 9.
[103] Nazario and DiMino, "An In-Depth Look at the Georgia-Russia Cyber Conflict of 2008," 15.
[104] Ibid. Jose Nazario of Arbor Networks noted that the largest recorded attacks were 40 GB per second. He observed that the type of attack directed at Estonia was simple; it was "just a lot of people getting together and running the same tools on their home computers." See "Megabytes, Gigabytes, Terabytes ... What Are They?," *What's A Byte?*, n.d., at http://www.whatsabyte.com,

attacker's use of larger botnets with greater bandwidth may explain this increase in intensity.[105]

Nazario reported observations for August 8, which captured the early major attacks (see Table 5.5). He acknowledged that other attacks occurred but that they did not reach a point that triggered the alarm mechanism on Arbor's Internet collection process. As previously noted, there were SYN and RST floods; however, unlike in the Estonia attacks, Arbor Networks analysts did not observe any ICMP or UDP floods. Nazario concluded that the observed attacks "suggest a botnet (or multiple botnets)" because "these attacks were all globally sourced." Based on the level of intensity, these "attacks would cause injury to almost any common website."[106]

---

for a description of the terminology used to describe computer storage space and system memory. A bit is the smallest unit of data a computer uses; it represents two states of information: 0 or 1, yes or no, true or false. A kilobyte (KB) is 1,000 bytes and is equivalent to a typical paragraph. A megabyte (MB) is 1,000 kilobytes and equates to a small book or 500 pages of text. A gigabyte (GB) is 1,000 megabytes and equates to 30 feet of books on a library shelf. A terabyte (TB) is 1,000 gigabytes, which equates to 1,000 copies of the *Encyclopedia Britannica.* It would take 10 terabytes to hold the printed collection of the Library of Congress.

[105] Jose Nazario, "Georgia DDoS Attacks - A Quick Summary of Observations," DDoS and Security Reports: The Arbor Networks Security Blog, *Arborsert*, August 12, 2008, http://ddos.arbornetworks.com/2008/08/georgia-ddos-attacks-a-quick-summary-of-observations/.

[106] Nazario, "Georgia DDoS Attacks - A Quick Summary of Observations." ICMP is "an extension to the Internet Protocol (IP)." "ICMP supports packets containing error, control, and informational messages. The ping command uses ICMP to test an Internet connection." See "ICMP," *Wedpodeia*, n.d., http://www.webopedia.com/TERM/I/ICMP.html. ICMP flooding is one of several types of DoS attacks. *Ping* is a "standard software utility (tool) used to test network connections"; see Bradley Mitchell, "Ping," *Wireless/Networking*, n.d., ttp://compnetworking.about.com/od/network_ping/g/what-is-a-ping.htm. A UDP flood attack is "possible when an attacker sends a UDP packet to a random port on the victim system." Upon receiving the packet, the victim's system "will determine what application is waiting on the destination port. Because there is no application waiting in that port, it will generate an ICMP packet of destination unreachable to the forged source address." The victim's system will drop offline "if enough UDP packets are delivered to ports" on the system." See Paloma, "What Is a UDP Flood Attack?" UDP is the "main alternative to TCP and one of the oldest network protocols in existence. It was introduced in 1980." See Bradley Mitchell, "UDP," *Wireless/Networking*, n.d., ttp://compnetworking.about.com/od/networkprotocolsip/g/udp-user-datagram-protocol.htm.

Table 5.4: Georgia Cyber Attack Data for August 8, 2008[107]

Maximum duration	6 hours 6 minutes
Average duration	2 hours 17 minutes
Maximum packets per second (PPS)	2.1 million packets per second (Mpps)
Average PPS	540 thousand packets per second (Kpps)
Maximum bits per second (BPS)	814 megabits per second (Mbps)
Average BPS	211 Mbps
SYN floods	18
RST floods	1
Observed targets	4 distinct
Reporting ISP	3

Table 5.5: Arbor Networks Major Attack Observations for August 8, 2008[108]

Attacks	Target	Description	IP Address or URL
5	Silknet	Telecommunications and entertainment	213.131.44.138
3	Rustavi2	Private TV	213.157.196.25
10	Internews	Online nonprofit news organization	213.157.198.33
1	NetGazeti	Online newspaper	www.gazeti.ge

On August 12, at the conclusion of the five-day war, Russia's cyber attacks resulted in a "devastating impact on their targets."[109] STRATFOR assessed that:

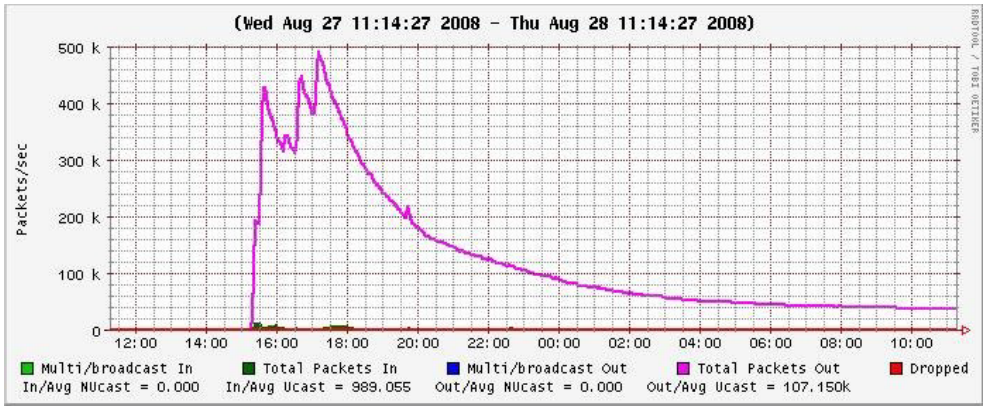
> Whatever history may ultimately decide about the events of Aug. 7–12, the decisive moment for Tbilisi to seek help and make that case abroad was during the hours and days after the Russian invasion began. Russia's cyber moves undermined its ability to do so. While this was not decisive here, it could have been in some other conflict.[110]

[107] Nazario and DiMino, "An In-Depth Look at the Georgia-Russia Cyber Conflict of 2008," 15. A packet is a single unit of "binary data capable of being routed through a computer network." Its purpose is to "improve communication performance and reliability"; to accomplish this, "each message sent between two network devices is often subdivided into packets by the underlying hardware and software." See Packet," *Wireless/Networking*, n.d., http://compnetworking.about.com/od/networkprotocols/l/bldef_packet.htm.
[108] Ibid.
[109] Stephen Adair, "Georgian Attacks: Remember Estonia?," *Shadowserver*, August 13, 2008, http://www.shadowserver.org/wiki/pmwiki.php/Calendar/20080906.
[110] STRATFOR, "Georgia, Russia: The Cyberwarfare Angle," *STRATFOR Global Intelligence*, August 12, 2008, http://www.stratfor.com/analysis/georgia_russia_cyberwarfare_angle.

The Russian cyber militia was not content with its success, and while botnet attacks stopped on the August 12, sporadic DDoS attacks continued against some prominent targets.[111]

One of these targets was GHN, the Georgian news agency, which was attacked again on September 8. In total, the GHN was paralyzed for two weeks. Another target of cyber attacks after the main attack was the Georgia Online news agency. The government of Georgia in its formal account of the war recorded that "it is interesting to note that Russian efforts to prevent Georgian Internet media resources from disseminating information continued even after the war."[112]

Figure 5.5: DDoS Attack Graph – August 27, 2008[113]



Beyond the end of the main attack phase, there was a final, massive DDoS cyber attack against Georgia's Ministry of Defense on August 27, 2008. The intensity of the attacks "peaked at approximately 0.5 million network packets per second, and up to 200–250 Mbits per second in bandwidth" (see Figure 5.5

[111] Nazario and DiMino, "An In-Depth Look at the Georgia-Russia Cyber Conflict of 2008," 23.
[112] Government of Georgia, *Russian Cyberwar on Georgia*, Russian Invasion of Georgia (Government of Georgia, November 10, 2008), 4–5, http://georgiaupdate.gov.ge/en/doc/10006881/Microsoft%20Word%20-%20CYBERWAR%20short%20version_111008.pdf.
[113] Danchev, "DDoS Attack Graphs from Russia Vs Georgia's Cyberattacks." The magenta line on the chart represents a "five-minute average; actual peaks were higher."

above). Once these attacks were blocked, the attackers began to cease their efforts.[114] Because this attack suddenly emerged and disappeared, Stiennon determined this indicated the attack was a "botnet under the control of a single agent." The purpose of the attack was unclear; however, the attack "demonstrated that whatever defensive measures Georgia had been able to put in place since the war were still ineffective."[115]

Unexploited Vulnerabilities – A Large and Dangerous Pool

Recognizing and then closing unexploited vulnerabilities is a requirement for deterrence by denial. Common Vulnerabilities and Exposures (CVE) have identified 50,551 software vulnerabilities.[116] Therefore, Georgian cyber vulnerabilities exploited by Russian attackers were an extremely small portion of those available for malicious purposes. Yet, this vast pool of unexploited vulnerabilities permits an additional observation: Theoretically, had Georgia developed the capability unilaterally or in concert with a broader coalition, perhaps it could have mined this set of vulnerabilities to either deter Russia with a threat of punishment or stand prepared to attack Russia if deterrence failed. In addition, had Georgia taken greater preventive efforts to close the threats to its IT systems from these vulnerabilities, Russia may have been deterred, as the success of its attacks would have been less certain.

---

[114] Dancho Danchev, "DDoS Attack Graphs from Russia Vs Georgia's Cyberattacks," *Dancho Danchev's Blog - Mind Streams of Information Security Knowledge*, October 15, 2008, http://ddanchev.blogspot.com/2008/10/ddos-attack-graphs-from-russia-vs.html. The attacks were HTTP queries, "requests for the main page script with randomly generated parameters" that are designed to "overload the web server in a way where every single request would need significant [Central Processing Unit] CPU time."

[115] Stiennon, *Surviving Cyberwar*, 100.

[116] "Common Vulnerabilities and Exposures (CVE)," n.d., http://cve.mitre.org/. 50,551 vulnerabilities were identified as of May 9, 2012; see http://web.nvd.nist.gov/view/vuln/search.

In the first six months of 2008, Microsoft's Security Intelligence Report identified more than 2,500 new software vulnerabilities to add to the thousands in existence. Nearly half of these were classified as "high-severity" vulnerabilities, and "more than 90 percent of the vulnerabilities disclosed in [this timeframe] affected applications, rather than operating systems."[117] The circumstances that applied in the Estonia case are also applicable in the Georgia case – to exploit an application or a computer system with the thousands of existing cyber vulnerabilities, one of the four following conditions must exist:[118]

- Those that allow an attacker to execute commands as another user
- Those permitting an attacker to access data that are contrary to the specified access restrictions for that data
- Those that permit an attacker to pose as another entity
- Those that allow an attacker to conduct a DoS

Because this treatment of unexploited vulnerabilities is strikingly similar to the Estonia case, the reader is asked to refer to the previous case to eliminate a broad swath of repetitive text. The remainder of this section will include some of the major points and information solely pertinent to this case. First, to address the above four conditions, the SANS Institute has noted that two risks arose.[119] In the Georgia case, attackers exploited the vulnerability of Internet-facing websites. The second risk resided in vulnerabilities that potential attackers could have found

[117] *Microsoft Security Intelligence Report: January Through June 2008* (Microsoft Corporation, 2008), 4. The report noted that a 19 percent reduction in vulnerability disclosures is positive; however, because 15 new vulnerabilities were created every day, this "can't really be considered good news"; see page 25. The National Vulnerability Database (NVD) provides severity rankings of low, medium, and high in addition to the numeric Common Vulnerability Scoring System (CVSS).
[118] "Common Vulnerabilities and Exposures (CVE)."
[119] "The Top Cyber Security Risks."

in "client-side software that remained unpatched."[120]

Russian attackers exploited these vulnerabilities in Georgia as they did in Estonia the year prior; however, there were many additional nuances available to attackers to take advantage of these same vulnerabilities through other tactics. For example, an attacker could use a hidden code in a "click here" hyperlink. Attackers often embed these client-side vulnerabilities in popular computer software programs to trick users into exposing their computers to malicious code. As we have now seen in both cyber war cases, once a computer is infected, it can easily infect the network and network servers.[121]

Software developers continuously develop patches to counter emerging vulnerabilities; however, automatic updates are not available for pirated software. The Business Software Alliance (BSA) determined that 68 percent of software used by Russians in 2008 was pirated. The piracy rate for Georgia in 2008 was 95 percent.[122] Such high piracy rates indicate that both Georgia and Russia do not have access to the most up-to-date software security patches, which increases the opportunity for cyber exploitation.

Two avenues of attack, social engineering and email malware, were available in Georgia from which to draw upon a large pool of unexploited vulnerabilities. Part of the reason these avenues are appealing is due to a

---

[120] Ibid. An Internet-facing website is one that is visible to external users. *Client-side* means that these actions are taking place on the user, or client-side, of a client-server system and that the user's browser executes computer scripts; see "What Is Client-side?" This second risk likely occurred in the Georgia case; however, the researcher was unable to locate proof in publicly available literature.

[121] "Spear Phishers."

[122] *08 Piracy Study* (Business Software Alliance, May 2008), 12, http://global.bsa.org/globalpiracy2008/studies/globalpiracy2008.pdf. Georgia's 95 percent piracy rate was the highest measured in the world.

decreasing trend between the Estonia and Georgia cyber wars in which the number of available "old" vulnerabilities that attackers exploited declined. This occurred because of the newfound attention to cyber vulnerabilities stemming from the 2007 war.

Many of the older, previously exploited vulnerabilities were fixed, which pushed attackers to "rely more on social engineering as a method for spreading malware than in the past."[123] This method is widely used because it is often easy to "trick the user into taking action that bypasses or lessens the effectiveness of the user's existing protection."[124] After the Estonia war and in the months leading up to the Georgia cyber war, backdoor and password-stealing tools increased significantly worldwide, which suggests "attackers were looking more aggressively to capture sensitive information from victims' computers or to control them."[125]

Email is central to modern communication; therefore, Russia and Georgia could have more thoroughly propagated email malware to take advantage of additional unexploited vulnerabilities. In the first half of 2008, "more than 90 percent of e-mail messages sent over the Internet were spam."[126] Spam is the "most common method bot-herders" and other attackers use to deliver lures.[127] Of note, "phishing attacks accounted for 2.5 percent of the total number of e-mail

---

[123] *Microsoft Security Intelligence Report: January Through June 2008*, 136.
[124] *Microsoft Security Intelligence Report: January Through June 2007*, 5. Data from 2007–2008 reflect Microsoft's assessment of worldwide vulnerabilities, while the piracy rates in both Russia and Georgia suggest that high-use sectors of pirated software such as media and business may be disproportionately vulnerable.
[125] *Microsoft Security Intelligence Report: January Through June 2008*, 136.
[126] Ibid., 67.
[127] Ibid., 16. The average spam lure "consists of an e-mail message with an enticing subject line."

messages blocked."[128] This may seem like a small number; however, when considering the totality of email traffic, this indicates a vast potential for exploitation.

At the time of the Georgia cyber war, Microsoft's vulnerability detection and removal tool identified its top twenty-five families of malware and unwanted software. This represented thousands of vulnerabilities that included Trojans, backdoors, password stealers and monitoring tools, exploits, and a broad range of traditional virus threats.[129] The problem defenders face is that the authors of this malware "attempt to evade detection by continually releasing new variants."[130] Therefore, a large and ever-growing pool of unexploited vulnerabilities and the continuing challenge this poses remain an integral factor in offensive and defensive calculations.

Deterrence by Denial – What Georgia Did

Georgia's technical responses, cyber counteroffensive measures, and use of a self-imposed cyber blockade proved ineffective.[131] The self-blockade was a defensive effort by the National Bank of Georgia to "sever its Internet connection for ten days, stopping most of the financial transactions dependent on that institution."[132] To counter this action, Russian cyber attackers "had their botnets send a barrage of traffic to the international banking community, pretending to be

---

[128] Ibid., 6.
[129] *Microsoft Security Intelligence Report: January Through June 2008*, 135.
[130] Ibid.
[131] Dr. Alison Russell, while a Ph.D. candidate at the Fletcher School, developed and refined the concepts of cyber blockades and self-imposed cyber blockades in the summer and fall of 2011. Dr. Russell shared her observations with the researcher in numerous discussions from June 2011 through May 2012.
[132] Bumgarner and Borg, *Overview by the US-CCU of the Cyber Campaign Against Georgia in August of 2008*, 6.

cyber attacks from Georgia." This resulted in an automatic reaction from many foreign banks to "shut down connections to the Georgian banking sector," which paralyzed Georgian banks, caused credit card systems to fail, and eventually led to the collapse of Georgia's cell phone infrastructure.[133]

Georgia relocated websites as its main defensive countermeasure to protect its information infrastructure. Georgian responses included temporary and permanent website relocations. Shadowserver reported that several "websites temporarily changed their IP addresses to loop back to the originating network in an attempt to thwart the attacks."[134] Other Georgian websites changed hosts. For example, the InterpressNews portal changed to Servage, "a worldwide hosting platform provider." Similarly, the daily online news site Civil.ge "temporarily switched to publishing their news coverage at a Blogger account."[135]

Permanent relocations proved more effective as they permitted Georgia to evade "DDoS attacks by rehosting its websites on U.S. servers with capacious fiber optic connections and adroit system managers."[136] With this maneuver, Georgia improved its cyber defense posture by limiting exposure of its vulnerabilities to attackers. This increased the challenge hackers faced because now they had to "simultaneously attack Georgia, the U.S. (Google and Tulip Systems), Poland, and Estonia."[137]

---

[133] Clarke, *Cyber War*, 19–20.
[134] Tikk et al., *Cyber Attacks Against Georgia: Legal Lessons Identified*, 14.
[135] Ibid., 14–15.
[136] Libicki and Project Air Force, *Cyberdeterrence and Cyberwar*, 105.
[137] Stephen W. Korns, "Botnets Outmaneuvered: Georgia's Cyberstrategy Disproves Cyberspace Carpet-bombing Theory," *Armed Forces Journal* (n.d.), http://www.armedforcesjournal.com/2009/01/3801084/.

Georgia moved the Ministry of Foreign Affairs (MFA) and official government news websites to Google's BlogSpot on August 8[138] to "keep the information flowing about what [was] going on in their country."[139] The MFA also mirrored its website in Estonia and Poland.[140] Additionally, Tulip Systems, based in Atlanta, Georgia (U.S.), accommodated relocation of the Georgian President's website and that of Rustavi2, Georgia's major TV station.[141]

Permanent website host changes were effective because these hosts had access to greater bandwidth to counter DDoS attacks and greater capacity to filter Internet traffic. However, the foreign hosts "had great difficulty in keeping the Georgian websites accessible, because of the larger volume of traffic that the attackers were generating."[142] Given this factor and the short duration of the war, the success of Georgia's response is questionable for three reasons:[143]

1. Russia's cyber militia was able to deny and degrade the Georgian government's ability to communicate, both internally and externally.
2. The Georgian government was unable to defend its sovereign territory in the cyberspace domain.
3. Russia's cyber militia was able to take down, at the time and place of its choosing, Georgian news and government websites in the areas that the Russian military planned to attack.

---

[138] Joshua E. Kastenberg, "Non-intervention and Neutrality in Cyberspace: An Emerging Principle in the National Practice of International Law", 2009, http://findarticles.com/p/articles/mi_m6007/is_64/ai_n42124170/pg_1/.
[139] Noah Shachtman, "Estonia, Google Help 'Cyberlocked' Georgia (Updated)," *Wired*, August 11, 2008, http://www.wired.com/dangerroom/2008/08/civilge-the-geo/#previouspost.
[140] Kastenberg, "Non-intervention and Neutrality in Cyberspace," 6.
[141] Danchev, "Coordinated Russia Vs Georgia Cyber Attack in Progress."
[142] Bumgarner and Borg, *Overview by the US-CCU of the Cyber Campaign Against Georgia in August of 2008*, 7. Georgia managed a single cyber counterattack against Russia with little damage. The counterattack targeted Russian sympathizers with a script on Russian websites that that tricked users into unwittingly attacking nineteen Russian websites.
[143] Hollis, "Cyberwar Case Study: Georgia 2008," 5–6.

Deterrence by Denial – What Georgia Could Have Done

Once again, defending against or preventing an exploit from these vulnerabilities did not require knowledge of the attacker. It required the technical expertise to locate and resolve the back-end exploit and access to international coordination to relocate critical Georgian websites to other countries to counter DDoS attacks. Additional defensive enhancements might have caused Russian attackers to rethink their decision calculus. Specific examples of defensive actions include fielding excessive bandwidth to absorb DDoS bandwidth peaks and enhancing the ability to monitor application and network traffic.[144] Other approaches that could have increased attackers' risk include early warning and detection efforts.

Regarding the DDoS attacks, Georgia could have improved its ability to detect and stop malicious users by developing the capability to recognize known attack sources, identify bots, and determine more quickly whether an attacker was a bot or person. Because many attackers use automated resources (bots) that can be recognized with existing tools, it is possible to determine "whether a web visitor is a human or a bot."[145] To stop malicious requests, Georgia needed greater capacity to identify an excessive number of requests and the means to prevent known network and application DDoS attacks. Georgia could have used

[144] "4 Steps to Defeat a DDoS Attack on Your Organisation." The challenge with increasing bandwidth is that it is expensive, and determined attackers can simply rent more bots to overwhelm one's network.
[145] Ibid.

a "combination of application-level and anomaly detection" to "identify and stop malicious traffic."[146]

Regarding SQL injections, three defensive actions might have deterred the attackers. The first, input validation, requires that "all data that the end-user can possibly influence be validated before being accepted or stored." Second, Georgia could have limited database privileges to the "fewest necessary to perform its function." Third, Georgia's back-end database should have been hardened and access restricted to "powerful stored procedures" to limit damage in the event of a compromise.[147]

These and other defensive measures that could have formed a robust denial approach did not appear to be in place. An examination of Georgia's technical, cyber counterattack, and self-imposed embargo countermeasures revealed that efforts to protect hardware were secondary to Georgian efforts to protect information by relocating websites. Georgia's early technical response consisted of installing filters to block Russian IP addresses and protocol exploited by hackers. Attackers quickly circumvented these countermeasures by "using foreign servers to mask their actual IP addresses, by employing attack software that spoofs IP addresses, and by changing protocols."[148]

Punishment – A Basis for Cyber Deterrence

Attribution and a threat-based calculus are essential in cyber deterrence by punishment. This section first examines identified perpetrators, alleged perpetrators, and the links between the two. By studying the perpetrators, we

[146] Ibid.
[147] *Common Application Security Vulnerabilities*.
[148] Ibid.

learn whether attribution is possible in this case. Next, the kinetic and cyber non-kinetic means available to Georgia to retaliate are considered. If the means to retaliate against a known attacker are present, then punishment may serve as a basis for cyber deterrence.

Aggressors operating principally from within Russia orchestrated the cyber attacks against Georgia.[149] There is no evidence to suggest that the origin of these attacks was local (to Georgia). As in the Estonia case, what remained unclear was a full accounting of Russian government participation in the attacks. However, as the evidence shows, it is beyond dispute that actors within the Russian government used an internal proxy non-state actor (Russian cyber militia) to attack Georgia. In this case, the capacity to attribute the attack to Russia is sufficient; however, once again it is noteworthy that the time required to attribute the attack surpassed the duration of the war.

The Identified Perpetrators

Dancho Danchev leveled blame for the Georgian cyber attacks on the citizens that helped form "Russia's self-mobilizing cyber militia." He suggested that this militia was the "product of a collectivist society" with the "capacity to wage cyber wars." He lamented that this cyber militia was a stand-alone agent

[149] Fleury, Khurana, and Welch, "Towards A Taxonomy of Attacks Against Energy Control Systems," 7. The origin is the "location of the attacker with respect to the target." The Georgian cyber attacks had remote origins as they originated outside of the target sites. Fleury et al noted that these kinds of attacks "usually occur due to an unsecured connection such as an open wireless network or a trusted third-party physical connection." An attack of local origin requires that an attacker have physical access to the computers or associated equipment.

and that the concern of the Russian government was not why such a group existed but rather why they didn't start the attacks earlier."[150]

Bumgarner's analysis supported a similar theory, which proposed the "cyber attacks against Georgian targets were carried out by civilians with little or no direct involvement on the part of the Russian government or military."[151] Further, he concluded that the Georgian cyber attacks required fewer civilian attackers than the Estonia attacks because Georgia's information infrastructure was smaller. Thus, the cyber militia required fewer computers to attack a system designed to handle less Internet traffic on a daily basis.[152]

Russian nationals conducted most of the attacks, although sympathizers from other countries, particularly from the Ukraine and Latvia, participated as well.[153] The attacks were effective despite the attackers' display of "a convincing amount of disorder without being at all random." Because of the cyber militia's ability to deliver a sufficient level of effectiveness, the use of Russian cyber military forces was not necessary.[154]

Without Russian military cyber forces, Russia's cyber militia was incapable of attacks of this magnitude. The cyber militia heavily depended upon additional support, which Russian organized crime provided. Web servers used to control and coordinate attacks had historic links to criminal enterprises. In addition, botnets used by the cyber militia were "associated with Russian

---

[150] Dancho Danchev, "Who's Behind the Georgia Cyber Attacks?," *Dancho Danchev's Blog - Mind Streams of Information Security Knowledge*, August 14, 2008, http://ddanchev.blogspot.com/2008/08/whos-behind-georgia-cyber-attacks.html.
[151] Bumgarner and Borg, *Overview by the US-CCU of the Cyber Campaign Against Georgia in August of 2008*, 2–3.
[152] Ibid., 4.
[153] Ibid., 2–3.
[154] Ibid.

organized crime." Bumgarner observed that Russian organized crime not only supported the cyber militia, it also undertook no deceptive efforts to hide the use of these tools; it was as if "they (Russian organized crime) wanted to claim credit for it."[155]

Seasoned hackers provided leadership and technical guidance and incited willing citizens to participate in Russia's cyber militia. Ottis noted that this cyber militia had an ad hoc nature, which meant that these hackers needed a uniting mechanism to connect with malleable citizens who were "willing and able to use cyber attacks in order to achieve a political goal."[156] Internet forums provided hackers a means of access to an eager citizenry.

Internet forums are "online meeting places for people who are interested in a particular subject."[157] On forums of this nature, most participants do not know each other in real life. Participation is usually anonymous, and members in cyber-related forums generally have diverse skills. This means that a few seasoned hackers can have a disproportional impact on the group and easily assume leadership roles.[158]

Project Grey Goose discovered that the participants in two forums, StopGeorgia.ru and Xakep.ru, "spent a significant amount of time discussing the merits and drawbacks of different kinds of malware, including DDoS tactics and tools," before and during the attacks.[159] The seasoned hackers, or leaders, in

---

[155] Ibid., 3.
[156] Ottis, "A Systematic Approach to Offensive Volunteer Cyber Militia," 307.
[157] Ibid., 308.
[158] Ibid.
[159] Jeff Carr, *Russia/Georgia Cyber War - Findings and Analysis* (Project Grey Goose, October 17, 2008), 3, http://www.scribd.com/doc/6967393/Project-Grey-Goose-Phase-I-Report. Project Grey Goose was an open source effort that began on August 22, 2008 to "examine how the

these forums had a definitive role in which they provided the "necessary tools, pinpointed application vulnerabilities, and provided general target lists for others to act upon."[160] The majority of the members, the "malleable citizenry," waited patiently for guidance from this "informal leadership chain (such as the forum administrator)."[161]

The relationship between leaders and followers in these forums was similar to that between a journeyman and his apprentice. A "distinct hierarchy" existed, which permitted a nearly ideal training situation for "nationalistic Russian hackers."[162] The capacity for members of these or similar forums to cause cyber harm became clearer in light of Project Grey Goose's analysis.[163]

An examination of more than 200 StopGeorgia.ru and Xakep.ru forum posts along with data from Georgian network servers revealed a five-step "cyber kill chain:"

1. Encourage novices through patriotic imagery and rhetoric to get involved in the cyber war against Georgia.
2. Publish a target list of Georgian government websites, which have been tested for access from Russian and Lithuanian IP addresses.
3. Discuss and select one of several different types of malware to use against the target website.
4. Launch the attack.
5. Evaluate the results (optional step).[164]

Russian cyber war was conducted against Georgian Websites and if the Russian government was involved or if it was entirely a grassroots movement by patriotic Russian hackers"; see page 2.

[160] Ibid., 14.

[161] Ibid.

[162] Ibid., 4.

[163] Carr, *Inside Cyber Warfare*, 15. Project Grey Goose analysis found that the StopGeorgia.ru forum had thirty members on August 9, 2008, and by mid-September membership topped 200.

[164] Carr, *Russia/Georgia Cyber War - Findings and Analysis*, 4–5. Within a week of beginning their research of the Xakep.ru forum, Project Grey Goose members, which were using U.S. IP addresses, were blocked from the forum. The blockade was lifted after ten days – which led Grey Goose members to speculate, "Nationalistic Russian hackers are not only based in Russia." Carr's team conducted a WHOIS search for the StopGeorgia.ru IP address, which is 75.126.142.110. This search linked the address to a Russian company, SteadyHose (*http://www.Steadyhost.ru*). The individual's name associated with this domain name was Sergey A. Deduhin, presumably an

Tikk et al also concluded there was "widespread consensus that the attacks appeared coordinated and instructed," which helped confirm Project Grey Goose's cyber kill chain theory.[165] In fact, there were similarities between the Georgia and Estonia cyber attacks because in both circumstances forum leaders placed downloadable attack scripts on Russian language message boards.[166]

Malware made available to forum rank-and-file members included instructions on how to execute a ping flood against the Georgian government and provided a list of targets susceptible to defacement via SQL injections.[167] Evgeny Morozov reported on the ease with which forum members could follow these instructions and thus join the "Russian digital army" within minutes.[168] Morozov used his success to argue that the cyber militia was not a tool managed in a "centralized fashion" by the Kremlin, which meant that the origin of the Georgian cyber attacks resided solely with the participants of the cyber militia.[169]

Using only his laptop and an Internet connection, Morozov located two avenues for the average citizen to participate in the cyber war, one creative and the other emotional. The creative option involved writing one's "own simple program," which he did with "readily available online instructions for those with

---

alias. The street address linked to the domain name was 88 Khoroshevskoe Shosse, Moskva (Moscow). The address was at an apartment building one block from GRU headquarters, which is at 76 Khoroshevskoe Shosse and immediately adjacent to Russia's Center for Research of Military Strength of Foreign Countries. Carr's team noted this was likely more than a coincidence." See page 109.

[165] Tikk et al., *Cyber Attacks Against Georgia: Legal Lessons Identified*, 12.

[166] Ibid., 9–10. Russian is a minority language in Georgia and Estonia; Tikk et al considered this a relevant factor in attributing the attacks to Russian nationals.

[167] Ibid.

[168] Evgeny Morozov, "An Army of Ones and Zeroes," *Slate*, August 14, 2008, http://www.slate.com/articles/technology/technology/2008/08/an_army_of_ones_and_zeroes.html.

[169] Ibid.

no software experience to develop a ping attack in less than thirty minutes."[170] Forums like StopGeorgia.ru provided an emotional option as they offered participants an opportunity to fight back by demonstrating that "aggression against Russia in cyberspace" had consequences. The StopGeorgia.ru forum provided a target list that "included plus and minus signs to indicate whether the sites were still accessible from Russia and Lithuania.[171]

Morozov's experience offered convincing evidence that further sustains Project Grey Goose's analysis that the origins of the Georgian cyber attacks are traceable to the Russian cyber militia, which effectively used forums such as those described. However, this does not mean that the cyber militia did not enjoy assistance from organized crime or the Russian government. Arbor Networks analysis revealed that the "major DDoS attacks observed were all globally sourced, suggesting a botnet (or multiple botnets) behind them."[172] As previously mentioned, this implicated Russian organized crime.

The Alleged Perpetrators

Russian non-state actors, organized as a cyber militia, were responsible for the majority of the Georgian cyber attacks, and they needed help.[173] It is

---

[170] Ibid. Morozov described that all he "had to do was create a blank text file, copy and paste the URLs of any websites that (he) wanted to attack, specify how many times these sites should be pinged, and copy and paste a few lines of code from the original instructions." Then he only had to "rename "it with a .BAT extension," which instantly converted it "into a file that Windows recognizes as an executable program."

[171] Ibid. StopGeorgia administrators provided DoSHTTP software, which contained advanced and beginner options. Morozov noted the following in choosing the "for beginners" option: "After entering a URL, I could initiate an attack by clicking something that said Start Flood. A flood did follow – war at the touch of a button." The plus signs indicated primary targets, while the minus signs indicated that a primary site was offline and therefore should not be attacked.

[172] Tikk et al., *Cyber Attacks Against Georgia: Legal Lessons Identified*, 12.

[173] "Search Security." A DDoS attack is "one in which a multitude of compromised systems attack a single target, thereby causing a denial of service for users of the targeted system." The

extremely difficult to trace the precise origins of their DDoS attacks because this involves large numbers of home computers that hackers have turned into "zombies."[174] In the Georgian as in the Estonian case, an investigator looking only at computer server logs would see attacks coming from the "IP addresses of home user computers from all over the world."[175] Tracing the IP addresses of home users is simple; determining the origin of the bot herder is difficult, but not impossible.[176]

Officially linking the Russian Business Network (RBN) to the attacks proves somewhat difficult. VeriSign, a leading Internet security company, has

---

targeted system's capacity to process requests is overwhelmed by a "flood of incoming messages," which forces the targeted system to shut down or drop offline.

[174] John Rob, "When Bots Attack," *Wired Magazine*, September 2007, http://www.wired.com/images/press/pdf/webwarone.pdf. A bot is a "remotely controlled piece of malicious software" that gives a hacker/bot herder control over an infected computer (zombie). Bot herders rent their networks of zombie computers (botnets) for DoS and other attacks. Hackers, in this case "bot herders," infected individual computers (zombies) with a "bot," which then placed these bot-infected zombies under their control. A proficient bot herder can develop a large collection of zombies, which form a botnet; this may involve tens of thousands, or more, computers forming a worldwide network

[175] Viira, "Cyber Attacks Against Estonia - Overview and Conclusions," 72. An IP address is an "exclusive number all information technology devices use which identifies and allows them the ability to communicate with each other on a computer network." See "What Is An IP Address."

[176] This is because malicious actors face a two-fold problem with using zombies to stage a DDoS attack. First, the attacker must inject a virus into the zombie; this leaves an IP signal. Second, after the zombie downloads the virus, the computer needs instructions. This means that that the attacker who implanted the virus has to send a command for the zombie to attack the intended target. This command contains the attacker's IP address, which the attacker has spoofed. It is possible to trace back an attacker's actual IP address; however, this requires capabilities that few states possess, and even then, the process still may require years of effort with no guarantee of success; see Thilek, "Estonia Cyber Attacks 2007," December 28, 2009, http://meeting.afrinic.net/afrinic-11/slides/aaf/Estonia_cyber_attacks_2007_latest.pdf. There are a number of ways for a hacker to spoof an IP address. There are two simple methods. First, use a CGI (Common Gateway Interface) proxy to connect to another Internet service to request information instead of one's own. This is commonly referred to as "bouncing your IP address." Second, use a separate program for the task, such as TOR. With this or a similar program, once installed, the user only needs to press the appropriate button in an Internet browser and the user is anonymous. Note: World-class hackers would use more complex methods than these simple methods. See Necrostatic, "The Untraceable Man: How to Spoof Your IP Address and How It Works," *The Untraceable Man*, January 15, 2009, http://untraceableman.blogspot.com/2009/01/how-to-spoof-your-ip-address-and-how-it.html.

identified the RBN as the "biggest cyber-organized crime gang in the world."[177] The RBN has been responsible for a variety of global online attacks and criminal undertakings during its tenure as a "safe house" for cyber-related attacks and crimes emanating from Saint Petersburg, Russia.[178] In the Georgia case, while there is no disagreement that the RBN played a role, the extent of the organization's involvement is subject to debate.[179]

Analysis from www.georgiaupdate.gov.ge attributed the cyber attacks to the RBN.[180] On the other hand, Shadowserver's experts concluded that the RBN's participation "did not amount to more than providing hosting services to the botnet [command and control servers] and it did not commit the DDoS attacks itself."[181] In contrast to Shadowserver, several sources offer evidence that people with a RBN affiliation as well as RBN assets may have played a role.

To help settle the debate, Armin determined that the Georgian cyber attacks relied upon TTnet Turkish Telekom and used IP addresses linked to previous RBN activity. He argued that the implications of attributing the attacks to the RBN were compelling given that "server actions, botnet methodology, and tools used" were familiar to the RBN.[182] Research indicated that attackers relied

---

[177] Gianmaria Vernetti, *The Power of Networking: An Insight On the Russian Business Network* (The International Network of Civil Society Organizations For the Social Struggle Against Transational Organized Crime, July 1, 2010), http://flarenetwork.org/report/enquiries/article/the_power_of_networking_an_insight_on_the_russian_business_network.htm. VeriSign further clarified the RBN as the "baddest of the bad."
[178] Marcus Sachs, "MPack Analysis," *ISC Diary*, June 20, 2007, http://isc.sans.edu/diary.html?storyid=3015.
[179] Tikk et al., *Cyber Attacks Against Georgia: Legal Lessons Identified*, 12.
[180] Stiennon, *Surviving Cyberwar*, 97–98.
[181] Tikk et al., *Cyber Attacks Against Georgia: Legal Lessons Identified*, 12.
[182] Armin, "RBN-Georgia Cyberwarfare-Continuation..."

upon six C&C servers. Some of the botnets operated by these servers existed for either "DDoS for hire" or "DDoS for extortion" purposes prior to the war.[183]

McQuaid was able go further than linking the use of RBN tools to the war; he connected individuals associated with the RBN to the cyber attacks. He determined that an RBN associate, Alexandr A. Boykov of Saint Petersburg, Russia, had direct responsibility for "carrying out the cyber 'first strike' on Georgia." Further, Andrew Smirnov, a computer programmer, also from Saint Petersburg, assisted Boykov in the attacks. McQuaid concluded that these men were not part of the Russian cyber militia as citizen "script kiddies" or "hacktivists" (seasoned activist hackers) but rather "leaders of RBN sections."[184]

Johnson concurred that servers used in the attacks were associated with RBN activities prior to the war. These servers took part in activities such as adult video websites, prostitution websites, and online gaming websites.[185] Johnson observed that based on these activities, logic suggests that a government would not have used these servers before or during the war. Additionally, he questioned the involvement of RBN as an institution in the war due to a lack of evidence. Johnson argued that the most likely suspects were the cyber militia or, as he called them, a "bunch of patriotic operators inside Russia."[186]

---

[183] Tikk et al., *Cyber Attacks Against Georgia: Legal Lessons Identified*, 12. In this case, "the HTTP-based botnet [command and control] server was reported to be a MachBot controller." This was a tool "frequently used by Russian bot herders, and the domain involved with this [command and control] server had, according to Steven Adair of the Shadowserver Foundation, seemingly bogus registration information" that ties these tools to Russia.

[184] "RBN - Georgia Cyberwarfare - Attribution & Spam Botnets," *Russian Business Network (RBN)*, August 2008, http://rbnexploit.blogspot.com/2008/08/rbn-georgia-cyberwarfare-attribution.html.

[185] Mike Johnson, "Georgian Websites Under Attack - Don't Believe the Hype," *Shadowserver*, n.d., http://www.shadowserver.org/wiki/pmwiki.php/Calendar/20080906.

[186] Ibid.

Johnson's account does not explain the cyber militia's use of RBN-associated botnets without RBN assistance. Further, his evidence does not counter McQuaid's contention that RBN affiliates personally aided in the attacks. Lastly, ignored in Johnson's perspective is insight into the source of funding for the botnet attacks. The cyber militia used servers with RBN ties, which implies that either the RBN or affiliated members supported the cyber attacks without compensation due to a sense of patriotism or elements of the Russian government or some other party provided financial support to hire botnets.

There is also insufficient evidence to determine with certainty a full accounting of the Russian government's role in the cyber attacks against Georgia. However, Jeffrey Carr and others offer convincing circumstantial evidence showing that elements of the Russian government were involved in the cyber attacks. As discussed in the Estonia case, there seems to be a wide public understanding that the attacks were at least tolerated by the Russian authorities, if not coordinated or supported by them.[187]

Tikk et al offered circumstantial evidence of Russia government involvement: There was a "large-scale collision of interests between [Georgia] and Russian authorities," and the "coordination of and support to attacks took place mainly in the Russian language and was conducted on Russian or Russia-friendly forums."[188] Project Grey Goose explained that it had become standard operating procedure for the Russian government to distance "itself from the Russian nationalistic hacker community," which permitted officials to gain

[187] Tikk et al., *Cyber Attacks Against Georgia: Legal Lessons Identified*, 13.
[188] Ibid.

plausible deniability for cyber attacks "while passively supporting and enjoying the strategic benefits of their actions."[189] Therefore, an intentional policy that created such distance could only yield circumstantial evidence.

Despite its strategy of maintaining plausible deniability, there is evidence that current and former Russian officials "endorse cyber warfare and/or cyber attacks initiated by their country's hacker population."[190] For example, Nikolai Kuryanovich, a member of the Russian Duma, said in March 2006, "In the very near future many conflicts will not take place on the open field of battle, but rather in spaces on the Internet, fought with the aid of information soldiers, that is, hackers. This means that a small force of hackers is stronger than the multi-thousand force of the current armed forces."[191]

Anatoly Tsyganok, a retired military officer and director of the Moscow Institute of Political and Military Analysis' Center of Military Forecasting, wrote of the 2008 Georgian cyber attacks in a manner that implicated the Russian government. In characterizing Russian actions following Georgia's cyber attack on Russian media outlets, he observed, "The response followed shortly as the sites of the Georgian President, parliament, government, and foreign ministry suffered malicious hacks."[192] His use of the phrase "the response followed shortly"

---

[189] Carr, *Russia/Georgia Cyber War - Findings and Analysis*, 3. In this report, Project Grey Goose relied upon open source materials to examine the origins of the cyber war. The report used data "collected from two Russian hacker forums, www.xakep.ru and www.stopgeorgia.ru, along with network log files detailing 29,000 status events indicating the Up/Down status of 149 Georgian websites"; see page 2.
[190] Ibid.
[191] Ibid., 7.
[192] Carr, *Inside Cyber Warfare*, 17.

implied that the cyber attack was a "state action rather than a civilian one," not a "spontaneous grassroots action of so-called hacktivists."[193]

Links that Connect Identified and Alleged Perpetrators

Jeffrey Carr argues that given the anonymous nature of the Internet, those who attempt to find evidence that conclusively links the Russian government to the Georgian cyber attacks have adopted a "naive" goal that does not "accurately represent the relationships that have been built over the years between Russian politicians and organized youth associations" or Russia's cyber strategy.[194] Yet, Carr's research established a link between identified and alleged perpetrators with his three-tiered structure that "established command and control by the Kremlin through [Nashe] and other groups."[195]

Considering the composition of Russia's cyber militia and its need for external support, Carr's model noted that the membership of these groups included hackers, who were organized and receptive to recruiting other hackers to participate in malicious activity. The cyber attacks from Nashe and other groups had the logistical support of Russian organized crime. As Nashe and Russian organized crime groups paired up to conduct cyber attacks, the arrangement provided the Russian government a "cover of plausible deniability."[196] This dynamic between the Russian government, Nashe and other similar groups, and

---

[193] Ibid.
[194] Ibid., 119.
[195] Ibid.
[196] Ibid. Shachtman sustained Carr's theory in observing that "part of the ingenuity of using Nashi as cyberwarfare arm is the group's nominally independent status: While the group does the Kremlin's bidding, its funding comes from pro-business owners looking to ingratiate themselves with the regime. Even if they claim credit for the attacks, they are still one level removed from the Russian government." See Shachtman, "'Cyberwar' Panic Over; Estonia Asks for Russian Help to Find Hackers."

organized crime plausibly captured what took place in Estonia in 2007 and again in Georgia in 2008.

Evidence of elements of the Russian government's role in the attacks, beyond the conjecture of scholars and statements of officials, became clearer in February 2009. Russian media reported that the "Russian government sponsor[ed] and [paid] leaders of Russian youth organizations to engage in information operations, up to and including hacking, to silence or suppress opposition groups."[197] This report gains credibility when weighed in conjunction with Socor's article appearing in the *Eurasia Daily* on April 16, 2009.

Socor reported that Georgian authorities detained Aleksandr Kuznetsov, a commissar in the Russian youth group Nashe, and twenty other Nashe members. Kuznetsov and the others were en route to South Ossetia from Moscow, without visas, to organize a protest. Kuznetsov had in his possession a letter of endorsement from the Duma's Committee on Youth Affairs, "requesting Russian officials along the way from Moscow to Tskhinvali to assist the 'Moscow-Tskhinvali-Tbilisi Motorcade' in its mission."[198]

During his interrogation, Kuznetsov corroborated the February report that Nashe was "financed through the office of Vladislav Surkov, first deputy head of the Russian presidential administration."[199] Surkov is both a strong Nashe supporter and close friend of Vladimir Putin. Carr concluded that Surkov's intentions with Nashe were to position it and other Russian youth organizations to

---

[197] Ibid., 115.
[198] Vladimir Socor, "'Nashi' Foray into Georgia Stopped in Time," *Eurasia Daily Monitor* 6, no. 74 (April 17, 2009), http://www.jamestown.org/single/?no_cache=1&tx_ttnews%5Btt_news%5D=34871.
[199] Ibid.

"enforce the Kremlin's will" to "ensure the domination of pro-Kremlin views on the Internet."[200]

Surkov's intentions regarding information operations (IO) objectives via the Internet surfaced in a March 2009 conference. Surkov said, "To every challenge there should be a response, or better still, two responses simultaneously." He clarified what he meant by this statement in suggesting that if a "user turns up on LiveJournal talking about protests in Vladivostok, ten Kremlin spin doctors should access his blog and try to persuade the audience that everything that was written is lies." Surkov's rationale demonstrates the Russian IO model appears to have been used against Georgia in 2008.[201]

Georgia's Retaliatory Means

The previous section demonstrated that attribution is possible. An added requirement to establish a basis for deterrence by punishment lies with Georgia's means to retaliate. The availability of retaliatory means is a crucial component in assessing case-driven requirements for cyber deterrence.

Kinetically, Georgia is not a nuclear-capable state. Conventionally, the size of their force and military hardware capabilities were inadequate to embark on a credible course of conventional retaliatory strikes in response to Russian cyber attacks. Georgia ranks 88th globally in the size of its professional armed forces with 37,000 service members,[202] while Russia ranks second with 1,520,000

[200] Carr, *Inside Cyber Warfare*, 116.
[201] Ibid. See pages 161-171 for an explanation of Russia's IO doctrine.
[202] "Georgia Military Strength," *Global Firepower*, n.d., http://www.globalfirepower.com/country-military-strength-detail.asp?country_id=Georgia.

military members.[203] In comparing military hardware capabilities, Georgia's Navy has nine vessels that are patrol craft. Its Army has 400 towed artillery pieces and 200 tanks. The Georgian Air Force has 654 aircraft and 476 helicopters.[204] Russian military hardware includes 22,950 tanks, 12,765 towed artillery pieces (not including self-propelled guns or rocket artillery), 2,749 aircraft, and 233 Navy ships.[205] The facts of the case are clear – a basis for Georgia to deter Russia by punishment through kinetic means did not seem feasible.

Non-kinetically, there is no evidence to suggest that Georgia possessed the retaliatory means to respond with offensive cyber capabilities. With attribution a surmountable challenge, Georgia would have needed a more credible offensive cyber capability and the will to exercise that capability to deter by punishment. The fact that Georgia used only limited offensive cyber counterattacks does not mean that they did not possess additional capabilities – but given the circumstances, it is a strong indicator that this option was not fully developed.

Although Georgia did not possess an IT architecture as advanced as Estonia's, there is reason to suggest that Georgia had the technical capacity to have pursued a more advanced offensive capability. Had it chosen to do so, Georgia could have likely located and held some Russian cyber vulnerabilities at greater risk. While precise data are unavailable on the number of Russian cyber attackers in the Georgian case, it is conceivable that the core hackers numbered in

---

[203] "Military Statistics - Armed Forces Personnel by Country." Georgia has 1,302,829 men available to serve between the ages of 15 to 49 (109th globally). In comparison, Russia has 36,219,908 men available to serve between ages 15 and 49 (eighth globally).
[204] "Georgia Military Strength."
[205] "Russia Military Strength."

the dozens and botnet herders represented an even smaller number. As evidence, consider that "despite the growing prevalence of malware, the number of skilled malware creators may actually be quite small."[206] Therefore, in the cyber domain many state and non-state actors have the potential to develop or hire a small cadre of talented hackers from which to construct a potent offensive cyber force.

Georgia briefly mounted a cyber counterattack against select Russian media outlets, but it was not very successful. Two days into the war, on Sunday August 10, Russian news agency RIA Novosti was "disabled for several hours" by Georgian hackers.[207] In another instance, Georgian hackers were able to replace a Russian news website's "content with a news feed from a pro-Georgian source."[208] Georgia, with advanced preparation, may have been able to mount a more formidable offensive cyber force, but it did not. Additionally, Georgia or agents acting in its behalf may have been able to purchase botnet capability to hold Russian IT systems at risk, which also did not occur. Despite the possibility of assigning attribution, the actual retaliatory means at Georgia's disposal suggests the limitations of a deterrence concept based on punishment and further highlights the need for denial-based deterrence. This determination is based on

---

[206] *Microsoft Security Intelligence Report: January Through June 2008*, 13. Microsoft "analyzes millions of unique malware samples every year; almost all of these are variations belonging to existing malware families, many of which are themselves simply modifications of other families." In the case of Sven Jaschen, "the 17-year-old creator of the Win32/Sasser and Win32/Netsky worms, was arrested by German authorities in 2004, as much as 80 percent of the malware code in active circulation at the time was believed to have ultimately originated from him."

[207] "RIA Novosti Hit by Cyber-attacks as Conflict with Georgia Rages," *RIA Novosti*, August 10, 2008, http://en.rian.ru/russia/20080810/115936419.html.

[208] "Georgia Hackers Strike Apart from Russian Military," *The Washingtion Times*, August 19, 2008, http://www.washingtontimes.com/news/2008/aug/19/georgia-hackers-strike-apart-from-russian-military/.

the assumption that punishment options were restricted to Georgia's capabilities.[209]

Cooperation – From Ad Hoc Response to a Basis for Cyber Deterrence

An opportunity for Georgia to deter Russia and its cyber militia may have rested upon deterrence through cooperative measures. This section examines the cooperation between Georgia and non-adversarial members of society during the war, the degree of cooperation that can exist between the adversaries, and the law of war and additional legal frameworks applicable to this case. By studying these circumstances, it is possible to determine what may be needed to strengthen cooperation, which may provide a basis for cyber deterrence. Because of the similarities between this and the previous case, only the salient issues pertaining to Georgia will be offered in the following cooperation-related sections.

Georgia relied upon ad hoc cooperation during the 2008 cyber war. Their experience, gleaned from the facts of the case, suggests that cooperation in sharing information should not be an afterthought but rather a critical component of cyber deterrence theory – a component that must be developed and nurtured just as carefully as the ability to punish or deny because these types of cooperative relationships are essential in cyber deterrence.

Cooperation Between Georgia and Non-adversarial Members of Society During the War

[209] Georgia's kinetic capabilities were better than Estonia's but still insufficient to challenge Russia. The status of its non-kinetic capabilities was indeterminable. However, Georgia unlike Estonia was not as a member of NATO and therefore would not have benefitted from the collective capabilities of the alliance had Article 5 been in play. Therefore, Georgia would require a greater reliance on denial-based deterrence than Estonia.

Cooperation featured early in Georgia's defensive response to the cyber attacks. Georgian officials quickly contacted their counterparts in Estonia, who provided connections to their "informal network of international cyber-security experts."[210] Rapidly, Georgian coordination efforts grew to link Georgia's university Computer Emergency Readiness Team (CERT) with CERT-Estonia (CERT-EE), CERT-Poland (CERT-PL), and CERT-France (CERT-FR).[211]

Georgia's university system CERT, which "normally provided computer and network security technical support to Georgia's higher education institutions," coordinated Georgia's response as it "assumed the role of national CERT during the cyber attacks." Their efforts resulted in an arrangement to help address the political and media coverage challenges and to assist in determining and employing appropriate technical countermeasures.[212] CERT-EE provided Georgia with two cyber security experts[213] who worked in Georgia from August 12 to 16. CERT-PL analyzed IP data and transmitted "abuse messages," while CERT-FR assisted in "collecting log files." Poland also offered additional assistance as officials granted Georgia access to the President of Poland's website to disseminate information.[214]

Georgia's response was impressive but ad hoc. For example, Chief Executive Officer of Tulip Systems Nino Doijashvili happened to be vacationing

[210] Bumgarner and Borg, *Overview by the US-CCU of the Cyber Campaign Against Georgia in August of 2008*, 7.
[211] Tikk et al., *Cyber Attacks Against Georgia: Legal Lessons Identified*, 45.
[212] Ibid.
[213] Stiennon, *Surviving Cyberwar*, 100.
[214] Tikk et al., *Cyber Attacks Against Georgia: Legal Lessons Identified*, 14–15.

in Georgia, his native homeland, when the war began on August 7.[215] Doijashvili's permission for Georgia for use of Tulip Systems' U.S.-based servers to relocate critical websites took place without the permission of the U.S. government.[216] Tom Burling, a Tulip Systems employee, reported that Tulip's servers were at times receiving up to 68,000 simultaneous connection requests.[217] This meant that Russian cyber attackers "followed and turned their DDoS attacks against the U.S. site," resulting in the U.S. "effectively [experiencing] cyber collateral damage."[218] This indicates the presence of an obvious danger, which suggests that inter-state cooperative efforts during cyber wars should be conducted with awareness by states of the actions of its citizens actively participating in these wars. There was no agreement in force to address these circumstances. Further, there was no potential for intervention by an international organization because one with an appropriate charter did not exist for Georgia to call upon for assistance.[219]

Cooperation Between Adversaries

Adversarial relationships can form the basis for cooperation. Such a basis has long existed among nuclear-capable adversaries and in the criminal justice

[215] Danchev, "Coordinated Russia Vs Georgia Cyber Attack in Progress." Manta described Tulip Systems Inc. in Atlanta, Georgia as a "private company which is listed under business services" with an "annual revenue of $790,000 and ... a staff of thirteen." See "Nino Doijashvili," *Manta*, n.d., http://www.manta.com/g/mm7g533/nino-doijashvili.
[216] Kastenberg, "Non-intervention and Neutrality in Cyberspace," 6.
[217] "Russia Conducts Cyber Attacks Against Georgia," *Agence France-Presse*, August 20, 2008, http://technaute.cyberpresse.ca/nouvelles/internet/200808/13/01-19650-la-russie-mene-des-cyber-attaques-contre-la-georgie.php.
[218] Kastenberg, "Non-intervention and Neutrality in Cyberspace," 6.
[219] Bumgarner and Borg, *Overview by the US-CCU of the Cyber Campaign Against Georgia in August of 2008*, 7.

system. Effective cyber deterrence, just as with its predecessors, requires cooperation and an acceptance of norms from which to forge agreements.

Because it is a lesser cyber and military power and neither a member of the EU or NATO, Georgia would likely face difficulty in deterring Russia from engaging it in cyber war.[220] However, were Georgia to have the protective assurances that come from a framework of supportive international agreements and the collaboration of an alliance committed to engaging on its behalf (in conjunction with robust denial capabilities), Georgia's cyber deterrence prospects could change because they may alter an attacker's risk calculus.

Georgia – The Law of War and Additional Legal Frameworks

As Georgia came under cyber attack, international legal regimes pertaining to cyber war had not "caught up" with the technological challenges Georgia experienced. For example, there had been no modifications to the Law of Armed Conflict, the Geneva Accords, or an accepted rethinking of Just War theory. These institutional and regime factors represented vulnerabilities facing state actors in the cyber domain. The facts of this case suggest that these vulnerabilities are reduced by strategic cooperation in the development of norms, legal regimes, and cyber institutions, while the tactical cooperation that is required to share vulnerability and threat data reduces exposure to technical exploits.

International Legal Regimes Directly Applicable to Cyber War

The next two sections examine legal regimes that are directly and

[220] This should not be interpreted by the reader to imply that deterring Russia from engaging in cyber war with Georgia is impossible. Actually, the researcher believes it possible for Georgia to deter Russia with a combination of denial and cooperative measures.

indirectly applicable to cyber attacks and cyber war. At the time of the Georgian cyber attacks, many governments were reviewing their vulnerability to DDoS and other forms of attack in response to Estonia's cyber war. Some nations were in the process of assessing the need to build cyber attack programs, and most every government contained groups that publicly worried about being victimized. In this environment, the UN, Council of Europe, EU, and NATO continued to investigate their proper "role in responding" to cyber attacks and their "responsibilities and obligations" as member states. With the Estonia and Georgia cyber war experiences as catalysts, these institutions moved at varying paces towards articulating strategies and taking measured actions to counter cyber attacks on member states. The role of the UN in regulating cyber attacks has been "largely limited to discussions and informational sharing," and therefore the organization was not positioned to assist Georgia during the war.[221]

Council of Europe[222]

As of the timeframe of the Georgian war (and since), the 2001 Council of Europe Convention on Cybercrime is the most significant international cooperative efforts in the cyber domain. This international treaty, which addressed cybercrime, has forty-six signatories and thirty ratifiers.[223] Cooperation featured prominently in the treaty given mutual assistance and

---

[221] Oona A. Hathaway et al., "The Law of Cyber-Attack," *California Law Review* (2012): 48-50.
[222] "The Council of Europe in Brief," *Council of Europe*, n.d., http://www.coe.int/aboutCoe/index.asp?page=nepasconfondre&l=en. The Council of Europe is an "international organization in Strasbourg which comprises 47 countries of Europe." Its purpose is to "promote democracy and protect human rights and the rule of law in Europe."
[223] Joseph S. Nye, Jr., "Power and National Security in Cyberspace," 19. The U.S. has ratified the treaty, while Russia and China remain non-signatories. Estonia signed the treaty on November 23, 2001, and Georgia signed on January 4, 2008; see "Convention on Cybercrime: Member States", May 23, 2012, http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=ENG.

extradition clauses.[224] Because of the mutual assistance that had developed between member nations and improved upon during and after Estonia's war, Georgia was in an improved position to seek help during the war.[225]

European Union[226]

Although the EU lacks a common cyber policy or a "vision of present-day cyber security," it has taken concrete actions to help protect member states in the aftermath of its inaction during the cyber wars.[227] In the May 2010 *Digital Agenda for Europe*, the EU presented an action plan covering a range of information and communication technologies.[228] While one may find references to "cyber attack" in this and other EU cyber-related documents, the EU has methodically categorized breaches in cyber security as criminal matters and therefore a jurisdiction for law enforcement.

The *Digital Agenda for Europe* called for establishing a CERT in Europe. The agenda described the need for "cooperation between CERTs and law enforcement agencies" to help "prevent cybercrime and respond to emergencies, such as cyber attacks."[229] Because of this recommendation, in June 2011, the EU formed CERT-EU to unite European cyber security experts. EU authorities gave

---

[224] Council of Europe, "Convention on Cybercrime."
[225] See the section titled "Cooperation Between Estonia and Non-adversarial Members of Society During the War" in the previous chapter.
[226] "The Council of Europe in Brief." The EU has "twenty-seven members that have delegated some of their sovereignty so that decisions on specific matters of joint interest can be made democratically at the European level. No country has ever joined the EU without first belonging to the Council of Europe."
[227] "European Union Needs Common Cyber Policy," *Estonian Ministry of Foreign Affairs*, March 22, 2012, http://www.vm.ee/?q=en/node/14012.
[228] "A Digital Agenda for Europe" (European commission, May 19, 2012), http://ec.europa.eu/information_society/digital-agenda/documents/digital-agenda-communication-en.pdf. The researcher was unable to locate in this (or any other) EU document an effort to define *cyber attack* or *cyber war.*
[229] Ibid., 17.

the team one year to "share its expertise" and to demonstrate that it has the ability to "effectively and efficiently respond to cyber threats and incidents on a 24x7 basis."[230]

The purpose of CERT-EU resides in bringing greater technical expertise to the cyber security challenge as its scope includes "prevention, detection, response, and recovery."[231] This organization is a complement to the European Network and Information Security Agency (ENISA), which the EU established in 2004. Also, as it is an organization with a counter-cybercrime approach, ENISA's prime purpose is to build member states' capacity to "prevent, address, and respond to network and information security problems."[232] While the EU remained fixed on its posture of considering cyber attacks as forms of cyber crime, NATO began to take measured steps to help alleviate state-centric national security cyber challenges.

North Atlantic Treaty Organization (NATO)

NATO, having done little in the way of supporting either Estonia or Georgia during their cyber wars, was prompted by these experiences to move toward articulating strategies and taking actions to counter cyber attacks on member states. In 2008, NATO member states ratified the NATO Cyber Defense Policy, created the Cyber Defense Management Authority, and established the

---

[230] "European Union (EU) Forms CERT Group to Fight Cyber Attacks," *International ICT Policies and Strategies*, June 18, 2011, http://ictps.blogspot.com/2011/06/european-union-eu-forms-cert-group-to.html. In mid-2012, at the end of the preparatory year, the EU will make a formal decision on the "conditions for establishing a full-scale" CERT-EU; see "Cert-eu", n.d., http://cert.europa.eu/cert/plainedition/en/cert_about.html.

[231] "RFC 2350" (CERT-EU, October 25, 2011), http://cert.europa.eu/static/RFC2350/RFC2350_CERT-EU_v1_0.pdf.

[232] "ENISA - Securing Europe's Information Society — ENISA", n.d., http://www.enisa.europa.eu/.

Cooperative Cyber Defense Center of Excellence (CCD COE, or "the center").[233] Of these efforts, the center has significantly enhanced member cooperation around its goal of increasing cyber security with a series of conferences and various publications to educate members.[234]

Building upon the 2010 Strategic Concept, the North Atlantic Council approved the *NATO Policy on Cyber Defence* on June 8, 2011. This policy relied on an objective of constructing a "coordinated approach to cyber defense" by incorporating "planning and capability development and response mechanisms for cyber attack."[235] Despite this progress, the utility of the *NATO Policy on Cyber Defence* comes into question when one examines NATO's collective response approach to the cyber challenge.

NATO's Policy on Cyber Defence stated that all responses are "subject to decisions of [the] North Atlantic Council" and that in considering taking action in response to a cyber incident, NATO will "maintain strategic ambiguity as well as flexibility."[236] This choice of words provides NATO with a hedge to avoid action while at the same time offering undefined coordinated assistance to those under cyber attack. Several years after the Georgia and Estonia cyber wars, NATO still has no established rules for responding to a cyber attack or a definition of cyber war.[237]

---

[233] Laasme, "Estonia: Cyber Window into the Future of NATO," 61.
[234] "Cyber Defense," CCD COE, n.d., http://www.ccdcoe.org/.
[235] "Defending the Networks: The NATO Policy on Cyber Defence."
[236] Ibid.
[237] Corrin, "NATO Cyber Defense Lags."

International Legal Regimes Indirectly Applicable to Cyber Attacks

International legal regimes that indirectly regulate cyber attacks include International Telecommunications Law, Aviation Law, Law of Space, and Law of the Sea. Each of these regimes regulates some portion of the cyber domain that may be used in cyber attacks. Despite this regulatory responsibility, Georgia was ill served by these regimes as they pre-date the emergence of cyber attacks and therefore do not "expressly regulate or prohibit cyber-attacks."[238]

Strengthening Cooperation to Deter Cyber War

We have learned from the case that is difficult to support a contention that a basis exists for cyber deterrence through cooperation as a stand-alone component of the triadic concept. On the eve of Georgia's cyber war, individual states' CERT programs came to aid Georgia; however, the international community as collective institutions had made virtually no progress beyond the mutual assistance and extradition efforts noted in the Convention on Cybercrime.

Progress in building international cooperation and norm development in pursuing international cyber crime has been noteworthy. However, a multilateral cyber treaty, agreement, or pledge is needed to strengthen cooperation[239] in addressing cyber attacks and cyber wars that threaten a nation's security.[240] As it

---

[238] Hathaway et al., "The Law of Cyber-Attack," 54.

[239] Joseph S. Nye, Jr., "Power and National Security in Cyberspace," 20. A pledge is a nonlegal agreement used by international lawyers used in lieu of a formal contract or agreement, which permits "states to accept more risks in the face of uncertainty." Examples of pledges include the 1975 Helsinki Final Act, and the Proliferation Security Initiative initiated in 2003. See Kal Raustiala, "Form and Substance in International Agreements," *The American Journal of International Law* 99, no. 3 (July 2005): 582-584.

[240] See "Cybercrime: a Threat to Democracy, Human Rights and the Rule of Law," *Council of Europe*, n.d., http://www.coe.int/web/coe-portal/what-we-do/rule-of-law/cybercrime. The Council of Europe Convention on Cybercrime, "which entered into force in July 2004, is the only binding international treaty on the subject to have been adopted to date. It lays down guidelines for all

currently stands, neither the UN, NATO, EU, nor any other international organization knew in 2008 or has since determined "accepted definitions on the subject of cyber defense and security."[241] Without the previously described level of cooperation among the cyber powers, deterrence becomes more challenging because many states, like Georgia and Estonia, require the support of alliances or outside intervention to build and sustain an effective deterrence equation.

The aftermath of Georgia's cyber war was different from that of the Estonian case, where the international community widely condemned the attacks. Following the Georgia war, there was not a similar outcry of international condemnation but rather subtle reconfirmation of the necessity to continue policy responses inspired by the Estonian experience. Yet, despite the second occurrence of cyber war in as many years, "no consensus [emerged] on how to respond."[242] As of this writing, there is "no legal foundation in international law to treat [attacks] as anything else but computer crimes," and there are no international agreements to address cyber attacks or cyber war.[243] Such an agreement and the pre-requisites as described in the previous chapter are necessary if cooperation is to be strengthened in any meaningful way.

The evidence in this case demonstrated that Georgia had an incentive to cooperate; therefore, it sought cooperation. Given the continuing global cyber challenge, the Georgian experience served as convincing evidence that nations

---

governments wishing to develop legislation against cybercrime." Cyber war or attacks between states do not have a similar agreement in force.

[241] Laasme, "Estonia: Cyber Window into the Future of NATO," 60.

[242] Shackelford, "From Nuclear War to Net War," 218.

[243] Oorn, "'Cyber War' and Estonia: Legal Aspects," 74. It was only in March 2008 that computer crimes, previously a criminal offense, were treated as offenses against the state.

reliant upon cyber infrastructures would benefit from cooperative alliances and agreed-upon defensive commitments in combination with bolstering denial capabilities as a means to deter cyber war. Strengthening cooperation in advance of future conflict is a powerful means to deter cyber war.

Summary

The purpose of this case was to increase our understanding of the requirements to deter cyber war by applying the triadic components of cyber deterrence theory: punishment, denial, and cooperation. The first triadic component explored is denial in which four elements were examined: exploited and unexploited vulnerabilities, targets, and defensive actions.

By understanding the vulnerabilities that were attacked and those that could have been attacked, we begin to see requirements that serve as a basis for cyber deterrence by denial. Exploited vulnerabilities were studied across four areas: Internet dependence, system weaknesses, hardware exploitations, and software exploitations. Here we discovered the actual vulnerabilities that formed the basis for the cyber attacks against Georgia as well as other vulnerabilities that could have been exploited.

We learned that Georgia was not highly dependent upon the Internet as only 7 percent of its population had Internet access. This would suggest that Georgia's lower usage rate resulted in reduced vulnerability to attacks on the Internet. However, Georgia was perhaps more vulnerable to cyber attack, and because of its small IT structure, it was less able to respond. Further, as the case explored in detail, Georgia was highly susceptible to Russian cyber attacks given

the Internet pathways into the country. This implies that geographic pathways matter in the cyber domain and that cyber choke points exist and can therefore be exploited. Because of these circumstances, two requirements appear useful: possessing a secure line of communication and the employment of cyber defenses as a whole-of-society endeavor.

System weaknesses in Georgia permitted attacks on network configurations as discussed in the previous case. However, in the Georgia war, there was a noticeable increase in attacks on specification and design vulnerabilities. Russian attackers apparently learned between the cyber wars the benefit to be gained from tailoring attacks to target process design flaws because system weakness was less evident in the 2007 war. Because technological overhauls are costly and infeasible, this suggests that recruiting and training IT professionals to adapt to the rapid pace of technological innovation and increasing self-inspection processes are necessary requirements.

Hardware and software exploitations examined in this case were in-depth, highly technical, and complex. In the Georgia war, Russia's tailoring of flood attacks meant that far fewer zombie computers were needed for the DDoS attacks. What mattered in the Georgia case is that its circumstance improved when, with outside cooperation, it had the capability to recognize that an exploit was underway and then take action to deny the attacker the benefit of that exploit by moving critical websites to other countries. This suggests that in addition to well-trained personnel, passive defenses must be a requirement to deter hardware and software exploitations. Further, the case illustrates that resilience should serve as

an important requirement because of the futility it may create in the attackers' calculus.

The targets selected for exploitation by Russian attackers in Georgia were largely networks, processes, and individual users.[244] A continuous process of evaluating vulnerabilities and potential vulnerabilities and repairing them immediately is an imperative. Satisfying this requirement is necessary to protect the categories of targets that were attacked (networks, processes, and users) while also ensuring that attacks against additional target categories not attacked (systems and data) are equally deterred.[245] In addition to the passive defense measures mentioned previously, an added requirement for this aspect of denial is the use of cyber red teams to continuously test one's vulnerability to attack.

Defensive actions were post hoc, reactive, and required cooperation to stave off the attacks. In Georgia, cooperation featured prominently, and while there were some technical responses, the core of Georgia's defensive strategy centered on website relocation to other countries that were not under attack and, in some cases, the use of a self-blockade. One could again argue that the defenders prevailed as the attacks ceased in a matter of days. However, this

[244] Fleury, Khurana, and Welch, "Towards A Taxonomy of Attacks Against Energy Control Systems," 9. Networks are made up of the "computers, switches, hubs, etc. connected either via wires or wirelessly." In attacking a network, the malicious actor seeks to "make communications among the computers and switches difficult or impossible." A user is a person with "authorized access to a system." In attacking a user, the perpetrator generally seeks to "illicitly gain information from the user for later use," for example, gaining access to the user's password.
[245] Ibid. Data are defined as "information suitable for processing by humans or machines," while systems are made up of "one or more connected components that can perform substantial computations." In short, a system is a computer. In both cases, data and individual computers were not targeted. I interpreted efforts to steal passwords that involved a user's computer as an attack on that user and not on the computer. I suspect that access to additional (classified) information on these attacks would likely yield some examples of malicious activity in all five target categories that have been used in this study: network, process, system, data, and user. Any minor oversights in this area will have no bearing on the requirements for deterrence that emerged from the study.

would ignore the circumstantial evidence that the attackers quit on their terms. In the Georgia case, it appeared that the Russian attackers adjusted to every defensive move until their political and military objectives were satisfied.

Unexploited vulnerabilities provide us insight into avenues for attack that could have been used but were not. Once again, it is impossible to determine precise reasons why these avenues were not pursued by Russian attackers. In the six months leading up to this case, 3,500 new software vulnerabilities were discovered. With only a handful of known vulnerabilities used in the attacks, the potential for the use of other attack options was likely present. This was particularly the case in Georgia as its piracy rate was 95 percent. Because pirated software is not routinely updated with security patches, Georgia was far more susceptible to vulnerabilities emerging from these security lapses.

Given the attackers' success, it appears they selected their avenues of attack well. In Georgia, attackers exploited vulnerabilities predominantly through Internet-facing sites and client-side software. There was a significant change as a result of the Estonia war in that Georgia's IT professionals before the start of hostilities resolved many older vulnerabilities. This forced Russian attackers to concentrate more on social engineering and email malware to exploit Georgian networks and users. From these circumstances, two requirements seem appropriate: the need for enhanced detection and monitoring in conjunction with active defense and a need for states to either find on their own or purchase zero-day vulnerabilities.

The second triadic component explored was punishment in which two elements were examined: attribution and offensive/retaliatory means. The Georgian case demonstrated that attribution is possible, although it occurred after the cessation of open hostilities. This fact should have no bearing on the utility of attribution and hence punishment as a core component of the triadic concept.

The actors in this case had differing capabilities, kinetically and non-kinetically. This suggests the importance of a requirement to tailor cyber deterrence for differing classes of actors.[246] It mattered that Russia was a nuclear power with overwhelming conventional superiority over Georgia.

Retaliatory means are a critical component of punishment. Because of the drastic mismatch in kinetic capabilities between the attacker and defender, it is quite telling to ask that given certain attribution: What capabilities would Georgia have had to possess to exploit available vulnerabilities to punish their Russian attackers? Kinetically, we know that Georgia ranks 88th globally. Unfortunately, the researcher was unable to assess its cyber capabilities.

What we do know is that Georgia mounted a feeble cyber counteroffensive with virtually no impact. This means that even though attribution proved possible, albeit belatedly, Georgia did not possess the capability to deter Russia by punishment. From these factors, we may surmise that cyber deterrence should be tailored to account for differences in kinetic and

[246] This idea builds upon the work of Keith Payne, Elaine Bunn, and Geoffrey French on tailoring, which is discussed in previous chapters.

non-kinetic capability. It is a matter of prudence to treat a peer kinetic power differently than a less capable actor.

The combination of denial and cooperation offers the strongest basis for cyber deterrence because of Georgia's inadequate retaliatory capabilities. This is more the case for Georgia because as a non-NATO member, it has no chance of Article 5 protection in the future, should NATO's view of cyber attacks and cyber war change. The circumstances of the case revealed the value of cooperation in the triadic construct by considering the relationships between non-adversaries and adversaries.

Georgia benefitted from the assistance of CERT teams from Estonia, Poland, and France; however, there was no international framework beyond the Convention on Cybercrime to help them. Georgia also took advantage of a relationship in which a U.S. citizen, born in Georgia, used his company to host critical Georgian websites. Poland offered official assistance; however, efforts taking place in the U.S. did not have the permission or support of the U.S. government. After the Georgian websites were relocated to the U.S., the cyber attacks continued. Thus, the cyber war widened, this time without incident; however, because of the nature of the domain and the dearth of international norms such behavior could have a less fortunate outcome in future cyber wars. The circumstances indicated that a useful requirement for deterrence by cooperation is to establish a priori relationships between non-adversaries. From a

broader perspective, cooperation to develop norms[247] as a path to future cyber agreements is crucial.[248]

The facts of the case when applied to this theory reveal five observations that are strikingly similar to the Estonia case:

1. Attribution matters but is not an insurmountable challenge.
2. Smaller states can potentially deter larger states from initiating a cyber war.
3. Cyber vulnerability can be mitigated but it is not easy.
4. Deterrence by denial can prevent an attacker from succeeding.
5. Cooperative relationships are necessary in cyber deterrence but must be realized in conjunction with the application of denial capabilities.

Cyber deterrence theory did not fail in this case because it was not present before the attack. However, while it is indeterminable if the Georgians could have deterred the cyber war by using the triadic concept, the facts shed light on the requirements that may form the basis for such a theory.

[247] In addition to norms, a cyber deterrence concept could contain enforcement mechanisms.
[248] *A Preliminary Report on the Cyber Norms Workshop* (Cambridge, Mass.: Massachusetts Institute of Technology, October 2011), http://ecir.mit.edu/events/conferences/184-cyber-norms-conference. The report targeted the following areas in which norm developments were needed: 1. States need to recognize the international implications of their technical decisions, and act with respect for one another's networks and the broader Internet. 2. States should act within their authorities to help ensure the end-to-end interoperability of an Internet accessible to all. 3. States should respect the free flow of information in national network configurations, ensuring they do not arbitrarily interfere with internationally interconnected infrastructure. 4. States should recognize and act on their responsibility to protect information infrastructures and secure national systems from damage or misuse.

Chapter 6: Analysis and Conclusion

"All I can tell you is that technologically the capability to paralyze this country is there now."

– Leon Panetta[1]

Introduction

The intent of this chapter is to recall the purpose, problem, puzzle, research questions, and hypotheses of this study as a precursor to presenting analysis that explains the similarities and differences between the cases based upon the independent variables and other factors useful in determining the requirements for cyber deterrence theory. Building upon these requirements, a theory of cyber deterrence is offered prior to concluding the study with applicable implications, recommended areas for future study, and final thoughts.

Purpose of This Research – A Quest Fulfilled

The purpose of this research is to understand the nature of cyber war and cyber attacks in order to develop requirements for a theory of cyber deterrence. Definitional consistency has plagued international and domestic efforts to address this growing security concern. This study defined cyber war as the continuation of state policy by cyber means and cyber attack as the use of cyber capabilities to cause harm.[2] This research satisfied the challenge of developing requirements for cyber deterrence; however, the task was difficult because of the nature of the

[1] Edwin Mora, "Panetta Warns of Cyber Pearl Harbor: 'The Capability to Paralyze This Country Is There Now'," *CNS News*, June 13, 2012, http://cnsnews.com/news/article/panetta-warns-cyber-pearl-harbor-capability-paralyze-country-there-now. Comments made in response to question from Lindsey Graham regarding a potential cyberattack on the U.S.

[2] Johnson, "Toward a Functional Model of Information Warfare." Characteristics that distinguish cyber attacks from cyber war were adapted from Johnson's work, which focused on traditional forms of information attack. Cyber attacks may be distinguished from cyber war by their limited goals and their supporting role for political, economic, or military activities.

cyber domain, which is shrouded in secrecy, highly technical, complex, and replete with rapid changes. An added challenge existed as only two cases of cyber war existed from which to conduct this study. Despite this small number of cases and therefore a reduced pool of actors, observations from the body of available evidence revealed the forthcoming requirements, which support the theory of cyber deterrence offered near the end of this chapter.

Regarding the cases of cyber war, we do not know if their number is small because most actors do not have the inclination to engage in this behavior or if other factors are causal. Perhaps individual values or those inherent in culture at large have served a great purpose in this regard. Regardless, the havoc unleashed in these two known cyber wars by a diminutive minority found principally in one country demanded a serious research inquiry because the potential for global harm is too great to ignore.

The Research Problem – What We Learned Helps Mitigate the Challenge

The problem guiding this research is that without imposed costs and/or denied benefits, state and non-state actors will further develop and refine capabilities that have the ability to take advantage of cyber vulnerabilities. The requirements for cyber deterrence that emerged in this process that were grounded in preceding deterrence theories and forged from the previously described vulnerability-based assessments shed light on the potential of the suggested theory to offer redress to the stated problem in the form of a triadic framework of denial, punishment, and cooperation tailored for actors as explained herein.

The Research Puzzle – No Longer As Perplexing

In initially approaching this research, I was puzzled that U.S. policy makers were recasting elements of deterrence theory from the Cold War and post-Cold War eras and applying it to cyber policy when its relevance was unclear. The current approach adopted by states, major multinational corporations, and others is not working. In the cases studied, which were from 2007 and 2008, there was not a failure of deterrence because deterrence did not exist in the first place. Several years after these cyber wars, there is still little or no deterrence in place to satisfy a current and ever-growing challenge suggested by the stated problem. In the course of the study, particularly the literature review chapters, the puzzle dissipated. I witnessed in scholarly works and public policy documents a classic approach to a new challenge in a large bureaucracy as explained by aspects of Graham Allison's Organizational Behavior (Model II) and Governmental Politics (Model III) approaches.[3]

From an organizational behavior perspective, I observed that the structure of organizational missions and fractionated power contributed to the failed U.S. approach to cyber deterrence – as evidence, consider that both the Clinton and Bush '43 administrations issued policy positions on cyber deterrence. However, in both administrations, these efforts went nowhere as within the U.S. government, the arbiter of the nation's approach to cyber security resided in the intelligence community. First, this arbiter was the National Security Agency (NSA), and eventually it took the form of a concert between the NSA and U.S.

[3] Graham T. Allison, *Essence of Decision: Explaining the Cuban Missile Crisis*, 2nd. ed. (New York: Longman, 1999). See Chapter 3, Model II: Organizational Behavior, pages 143-198, and Chapter 5, Model III: Governmental Politics, pages 255-324.

Cyber Command.[4] Due to the capabilities inherent in the U.S. intelligence community, it has successfully secured a de facto position of leadership on cyber security matters for the U.S. government.

The leading role intelligence has played in the evolution of cyber deterrence has proved problematic. The culture of this institution has vigorously sought to protect the U.S. government's approach to cyber security from what may be exploited for intelligence purposes. Allison precisely described such circumstances as he reflected on "group processes and their effects on choices and action."[5] In short, what this means is that the U.S. does not have a policy of cyber deterrence in place because those who control the levers of power see an advantage in an alternative that does not include cyber deterrence. Insider accounts of recent U.S. cyber activity indicate that the "[Obama] administration was resistant to developing a grand theory for a weapon whose possibilities they were still discovering."[6] Perhaps this research or research of this nature will help move these levers of power to see the advantage in a well-executed strategy of cyber deterrence based in theory.

Research Questions – Answered With Impact

To guarantee that the outcome of this research would not be subject to charges of presupposing the results, I designed and conducted an inquisitive study. The fundamental research question I asked was, what are the requirements

[4] This trend continues even though the U.S. Department of Homeland Security holds statutory authority over the mission. This may have occurred as the predominance of technical expertise resides in the NSA.
[5] Allison, *Essence of Decision*, 263.
[6] "Cyber Wars," *Chicagotribune.com*, June 24, 2012, http://www.chicagotribune.com/news/opinion/editorials/ct-edit-cyber-0624-jm-20120624,0,1667062.story.

for cyber deterrence theory to deter cyber war against states and non-state actors? To help answer this, I formulated two secondary research questions:

1. What can be learned about the requirements for cyber deterrence theory from criminal justice deterrence, nuclear deterrence, and existing cyber deterrence theories?
2. How do states and non-state actors in the cyber domain exploit vulnerabilities?

In response to the first supporting question, I found the journey through centuries of criminal justice deterrence, decades of nuclear deterrence, and years of recent research about cyber deterrence a richly rewarding experience. The reader is encouraged to review the culminating sections in chapters 2 and 3 in which the requirements for respective theories were mined and carefully presented. The literature revealed several trends that cyber scholars should take care to recall: Theories take time to develop and will evolve, which also takes time; successive deterrence theories have built upon their theoretical predecessors, and the core concepts have remained constant; and the role of theory is to explain, which means that it is normal for strategy and policy to predate theory. However, once developed and validated, theory should inform strategic and policy evolutions.

Punishment and denial featured prominently across all variations of deterrence theory. Cooperation was more important in nuclear and criminal justice deterrence theory than I first envisioned. Cooperation was a fixture in criminal justice deterrence because the population of non-offenders had to agree to mandates of governing bodies. Some non-offenders even cooperate with law enforcement officials by supporting enforcement efforts. Further, offenders often

cooperate by serving as informants and agreeing to plea bargains. Many offenders are reformed and thus cooperate with the laws established by governing bodies after receiving punishment in that they do not commit additional crimes.

Cooperation between the superpowers was a fixture of the Cold War, particularly after the Cuban missile crisis. It became an important component of deterrence as arms control and nonproliferation efforts emerged. Cooperation during the Cold War relied upon what I call strategic cooperation between states and international organizations to forge agreements and treaties. As previously explained, this form of cooperation took place between non-adversaries and adversaries. This informed my decision to incorporate strategic cooperation as an important element in the cyber triad. Additionally, evidence in the cases supported the important role of coordination at the tactical level between states and others during the cyber wars. This factor led to the incorporation of tactical cooperation as an added element of cyber deterrence by cooperation.

The evolution of punishment included attribution and the capacity of society to threaten to punish potential offenders and/or actually punish offenders in criminal justice deterrence theory. These ideas clearly influenced early nuclear deterrence theorists as they formulated punishment as a core component of nuclear deterrence theory. Likewise, denial efforts in both criminal justice and nuclear deterrence theory are quite similar. The idea is to alter the risk calculus of a potential offender or attacker by using barriers such as iron bars and safes in the criminal sense and missile defense, geographic separation of missiles, and mobility in the nuclear deterrence variant.

These core components of deterrence, denial and punishment, with the addition of cooperation as a core component form the triadic framework used in this study. The literature review further helped to define the elements that were most critical to these core components with which to analyze our cases. Regarding denial, the theories preceding cyber deterrence influenced the inclusion of defensive actions and the targets that were attacked.

Exploited and unexploited vulnerabilities were assessed to help develop requirements for the denial component. This approach was necessary given the impossibility of proving the negative associated with deterrence research. In this research, vulnerabilities are crucial because by studying them, we are able to assess what it might have taken in each case to deter cyber war or cyber attacks. Such an approach assists in determining if denial is a basis for cyber deterrence. It is this line of reasoning that prompted the second supporting question above.

Analysis – The Heart of the Study[7]

This section compares and contrasts the only two cases of cyber war, the war between Estonia and Russia in 2007 and the war between Georgia and Russia in 2008. As described above, the framework for this analysis is a triadic construct with denial, punishment, and cooperation as the core components. I suggest a basis for cyber deterrence emerges from each component because of the requirements that were derived from a combination of the literature and the analysis.

[7] The core components and their main elements are in bold font. Sub-elements have been underlined. The reader may note that requirements have been italicized.

This analysis will leave the reader with a top-level sense of the fundamental similarities and differences between these cases that help explain the requirements for a theory of cyber deterrence. See Table 6.1 for a summary of the fundamental similarities and differences that existed between the cases and Table 6.2 for a summary of case-driven requirements for cyber deterrence theory. The **first triadic component explored is denial,** in which four elements were examined: exploited and unexploited vulnerabilities, targets, and defensive actions. By understanding the vulnerabilities that were attacked and those that could have been attacked, we begin to see requirements, which serve as a basis for cyber deterrence by denial.

Exploited vulnerabilities were studied across four areas: Internet dependence, system weaknesses, hardware exploitations, and software exploitations. Here we discover the actual vulnerabilities that formed the basis for the cyber attacks against Estonia as well as other vulnerabilities that could have been exploited. As depicted in Table 6.1, Estonia was heavily dependent upon the Internet with nearly 60 percent of its population having Internet access, in contrast to Georgia, whose Internet usage as a function of population was in the single digits. This would suggest that Estonia's higher usage rate implied a greater vulnerability to attacks on the Internet. However, Georgia was perhaps more vulnerable to cyber attack, because of its small IT structure it was less able to respond. Further, as the case explored in detail, Georgia was highly susceptible to Russian cyber attacks given the Internet routes into the country. This implies

that geographic pathways matter in the cyber domain and that cyber choke points exist and can therefore be exploited.

Deterrence by denial requires that a state possess secure lines of communication to use and defend access to the Internet. Without this measure of security, denial by defensive means is difficult, if not impossible. Because of these choke points and their global dispersion, cooperation in the form of alliances is necessary for all state and non-state actors.

An additional requirement pertaining to Internet dependence relates to denial via cyber defenses as a whole-of-society endeavor. Effective denial requires an approach that provides for the common cyber defense of a state. This means that government, private companies, and individuals must accept policies and technical enhancements to satisfy these ends. This is currently a problem, particularly in the U.S., as governmental denial efforts exclude the U.S. economy. Due to privacy concerns, all participation in U.S. defensive efforts is currently voluntary. This permits companies to "free-wheel," resulting in a dangerous and less secure environment where some employ cyber mercenaries (who are willing to serve the highest bidder) and others languish.

System weaknesses in both Estonia and Georgia permitted attacks on network configurations. This means that hackers were able to "gain improper access" when a resource was not configured appropriately. Examples of this include component flaws that have not been patched, less secure authentication (infrequently changed passwords), and "misconfigured perimeter protection

and/or access control policy."[8] Given the configuration weaknesses exploited in both wars, these somewhat simple-to-alleviate factors that were exploited in Estonia, were exploited again a year later in Georgia. These same factors remain troublesome areas across governmental and corporate IT systems well after the lessons learned from these wars are known.

In contrast to Estonia, Georgia experienced a noticeable surge in Russia's exploitation of specification and design vulnerabilities. These vulnerabilities occur when a "process or component has design flaws," and these flaws are then exploited in "unintended ways to gain access to a system." Examples are insecure communication protocols and flawed coding.[9] Russian attackers apparently learned between the cyber wars because they benefitted from tailoring attacks against Georgia to target process design flaws, which were less evident in the 2007 war. These system weaknesses could perhaps be addressed with technological overhauls; however, this seems infeasible. *A more palatable requirement focuses on the recruitment and retention of properly trained IT professionals (may require institutional/organizational changes), continuous training to reflect the rapid pace of technical evolution, rapid incorporation of shared data on vulnerabilities, enhancement of attention to detail, establishment of a zero-fault mindset with standards and accountability in which employees who cannot follow established protocol are terminated, and implementation of continuous self-inspection/self-assessment processes. Training efforts must*

[8] Terry Fleury, Himanshu Khurana, and Von Welch, "Towards A Taxonomy of Attacks Against Energy Control Systems," in *Proceedings of the IFIP International Congerence on Critical Infrastructure Protection*, 2003, 10-11, http://www.ncsa.illinois.edu/People/hkhurana/IFIP_CIP_08.pdf.
[9] Ibid., 11.

improve to narrow the gap between a basic IT education in the fundamentals and what is necessary to develop relevant technical expertise in "high technology areas such as forensics, embedded systems, and mobile communication" and trade craft specific to cyber operations, "incident response, intelligence gathering, latest hacking tactics, and cyber protection strategies."[10]

As the reader may recall, the explanations of hardware and software exploitations were in-depth, highly technical, and complex in both cases. Both cases were strikingly similar except in one regard, which has minimal theoretical implications. In the Georgia war, Russia's tailoring of flood attacks meant that far fewer zombie computers were needed for the DDoS attacks.

My purpose in examining these exploitations is not to revisit the technical complexity of what took place, nor is it to comment on each type of exploit individually, because the theoretical element crucial in both of these categories of exploitation has more to do with process, practice, and capability than a mastery of the technical aspects. Certainly, a technical mastery of these exploits is required to devise and implement measures to stop them; this is best left to another researcher. That said, it is instructive for this discussion to understand the difference between a flood attack, ping attack, and SQL injection, etc.; this is why this material was addressed in the cases. However, in setting the requirements for deterrence theory, what matters, at a minimum, is that the defender has the

[10] Upasana Gupta, "NSA Launches Cyber Operations Program," *WebGuard*, June 14, 2012, http://web-guard.blogspot.com/2012/06/nsa-launches-cyber-operations-program.html. The shortage of cyber talent is so severe that U.S. government agencies are "poaching security experts from private firms." In many cases, cyber security firms are sending less capable employees to service U.S. government contracts because they are afraid of losing them; see Jim Finkle and Noel Randewich, "Experts Warn of Shortage of U.S. Cyber Pros," *Reuters* (New York, June 13, 2012), http://www.reuters.com/article/2012/06/13/us-media-tech-summit-symantec-idUSBRE85B1E220120613.

capability to recognize that an exploit is under way and then possess the capacity to deny the attacker the benefit of that exploit.

A preferable position would be one in which a defender is able to recognize an exploit before an attacker and thus eliminate the vulnerability, removing any possibility of susceptibility to that particular exploit. Either of these circumstances enhances deterrence by denial if a potential attacker is aware that a targeted actor possesses denial capabilities of this magnitude. As we learned from these cases, particularly from the discussion on unexploited vulnerabilities for which additional thoughts will follow below, if you stop one attack avenue, another will develop.

This suggests that passive defense must be a requirement to deter hardware and software exploitations. Passive defenses block cyber attacks and consist of "firewalls, intrusion detection/prevention systems, patching, and auditing logs."[11] In combination with passive defenses, resilience is a requirement for deterrence by denial.

Resilience, which is the capacity to recover quickly, should serve as the most important requirement in deterring hardware and software exploitations. Technical experts will offer that resilience on this order requires hardware and software re-engineering. However, such a requirement would face a divided technical community, which could paralyze policy makers to inaction. This could occur because there might exist a latent interest in maintaining the cyber security status quo as the world's leading cyber security companies, which are closely

[11] Tiong Pern Wong, "Active Cyber Defense: Enhancing National Cyber Defense" (Naval Postgraduate School, 2011), 19, http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA556635.

aligned with the world's leading cyber powers, are vested in cyber insecurity.[12] This means that a deterrence requirement to stringently engineer hardware and software to minimize exploits, albeit necessary, might face opposition from those that benefit from the existing cyber-industrial complex.

There was not a large distinction between **targets selected for exploitation** by Russian attackers. In both cases, networks and individual users were subject to attack.[13] In the Georgia case, processes appeared to be targeted to a greater degree, which indicated a greater propensity for the tailored nature of the attacks described previously.[14] What we see in the increased focus on tailoring attacks by Russia is a precise effort to attack design flaws in processes.

This means that the attackers adapted in the intervening months between the wars and the defender's efforts did not keep pace. Therefore, this evidence sustains an earlier requirement that defense by denial is a continuous process of evaluating vulnerabilities and potential vulnerabilities and repairing them without delay. Fulfilling this requirement is necessary to protect the categories of targets that were attacked (networks, processes, and users) while best ensuring that attacks against additional target categories not attacked (systems and data) are

[12] The cyber security industry is a global multi-billion dollar enterprise, which profits greatly from the status quo. Governmental efforts to address cyber security concerns that threaten the existing business models of the more powerful companies are likely to face stiff resistance from this lobby unless the sources of lost revenue are replaced.
[13] Fleury, Khurana, and Welch, "Towards A Taxonomy of Attacks Against Energy Control Systems," 9. Networks are made up of the "computers, switches, hubs, etc. connected either via wires or wirelessly." In attacking a network, the malicious actor seeks to "make communications among the computers and switches difficult or impossible." A user is a person with "authorized access to a system." In attacking a user, the perpetrator generally seeks to "illicitly gain information from the user for later use," for example, gaining access to the user's password.
[14] Ibid. A process is an application or "program running on a computational device."

equally deterred.[15] *In addition to the passive defense measures mentioned above, an important requirement for this aspect of denial is the use of cyber red teams. This requirement would establish a dedicated core of IT professionals who constantly test IT security to determine vulnerabilities before they are discovered by potential attackers.*[16]

Defensive actions in both cases were ad hoc, reactive, and required cooperation to stave off the attacks. In Estonia, near-immediate collaboration offered research and investigative capabilities, which helped filter traffic and complicate attackers' techniques until the attacks subsided. In Georgia, cooperation featured prominently, and while there were some technical responses, the core of Georgia's defensive strategy centered on website relocation to other countries that were not under attack and, in some circumstances, the use of a self-blockade. In both cases, one may argue that the defenders prevailed as the attacks ceased in a matter of days. However, this would ignore the circumstantial evidence that the attackers quit on their terms. In both cases, Russian attackers adjusted to every defensive move until it appeared their political objectives were satisfied.

---

[15] Ibid. Data are defined as "information suitable for processing by humans or machines," while systems are made up of "one or more connected components that can perform substantial computations." In short, a system is a computer. In both cases, data and individual computers were not targeted. I interpreted efforts to steal passwords that involved a user's computer as an attack on that user and not on the computer. I suspect that access to additional (classified) information on these attacks would likely yield some examples of malicious activity in all five target categories that have been used in this study: network, process, system, data, and user. Any minor oversights in this area will have no bearing on the requirements for deterrence that emerged from the study.

[16] Red teams were a prominent fixture of U.S. deterrence efforts during the Cold War. These small groups of experts adopted the role of potential adversaries to stress U.S. nuclear war plans as part of a continuous planning process.

I was unable to determine the extent to which the attainment of the attacker's objectives or the utility of the defense prevailed in either case. Perhaps it was, to some degree, a function of both. Regardless, we should consider the defenders' actions juxtaposed with the exploited vulnerabilities (as well as vulnerabilities that were available but unexploited in contrast to available defensive capabilities) to consider how these events shaped the necessary requirements for deterrence by denial. Many of the above recommendations hold true for this category of assessment, yet one key addition comes into focus. The ad hoc and reactive nature of the defensive response will invite an attack as long as the aggressor can obtain his or her goals. This suggests that a priori coordination is required between aligned states prior to cyber war. These arrangements and the ensuing training and exercises that will take place communicate an added measure of preparation and prevention that may alter a potential attacker's decision calculus.

One controversial, yet potentially circumstance-altering requirement moves the defender beyond the reliance upon passive defenses and cooperative-driven reactive measures – an aggressive pursuit of active defense capabilities. Active defenses pursue attackers as an immediate response to a cyber attack. The use of active defenses should be a complement to their passive counterparts, not a substitution.[17] Active defenses are a requirement in a well-rounded denial approach as they significantly elevate risks in what is tantamount to a "whack-a-mole" game.

[17] Wong, "Active Cyber Defense: Enhancing National Cyber Defense," 30.

Theoretically, a defender can reasonably anticipate additional pressure on an attacker's risk calculus if the potential for immediate redress is anticipated.[18] Typologies of active cyber defense can include cyber exploitation, counterattack, preemptive strikes, and preventive strikes.[19] These methods could be used in combination. For example, a state may respond to a cyber attack with a combination of exploitation and counterattack by using an intrusion detection system and trace-back technology to locate an attacker and then disrupt the attack. Governments and non-state actors have been using this method on the Internet for more than a decade.[20]

The legal ramifications of using active defenses have not been resolved domestically or internationally, yet the practice continues to gain traction. Increasingly, private companies in the U.S. are conducting reprisals that "range from modest steps to distract and delay a hacker to more controversial measures."

---

[18] The "pressure on an attacker's risk calculus" is also a part of punishment. With punishment, we know that attribution is necessary, yet often difficult; however, by employing active defenses a defender may benefit from the effect of the potential of punishment-like effects on the attacker's decision-making process without the difficulties associated with an overt punishment approach. In short, active cyber defense is an immediate form of retaliation.

[19] Ibid., 19–27. By using **cyber exploitation**, IP trace-back difficulties may be avoided. "After obtaining the last IP address of the computer used by the attacker (based on results from forensics and log audits), the computer could be exploited or 'hacked back.' After gaining access, in-depth analysis could determine the next system in the chain. By repeating the process, the attack path could be identified, eventually leading to the computer used for the attack." See David Wheeler and Gregory Larsen, "Techniques for Cyber Attack Attribution," Institute For Defense Analyses, October 2003, 23. With a **cyber counter attack**, the "equivalent would be to counter hack the attacker responsible for the cyber attack, instead of relying on more passive means such as a perimeter firewall or an intrusion prevention system to filter or block the attacks." See Siobhan Gorman and Julian Barnes, "Cyber Combat: Act of War," *Wall Street Journal*, 31 May 2011. By using **preemptive cyber strikes** in the cyber domain, a state conducts an "attack on a system or network in anticipation of that system or networking conducting an attack on your system." See "Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyber Attack Capabilities," 149. With **preventive cyber strikes**, a cyber attack may be "launched against a hostile actor (both state and non-state) to prevent the latter from acquiring any cyber [or other] offensive capability"; see pages 26-27. Wong uses the Stuxnet attack on Iran as an example.

[20] Jay P. Kesan and Carol M. Hayes, *Thinking Through Active Defense in Cyberspace*, Illinois Public Law and Legal Theory Research Papers Series (University of Illinois College of Law, November 2010), 328, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1691207.

In some cases, private companies have hired private contractors or cyber mercenaries to hack their attackers even when these actions "could violate laws in the U.S. or other countries."[21]

Unexploited vulnerabilities provide us insight into avenues for attack that could have been used but were not. It is impossible to determine precise reasons why these avenues were not pursued by attackers. However, the mere existence of these vulnerabilities is an important factor in deterrence by denial for several reasons. First, to deter by denial it is as crucial to prevent or defend against both exploited and unexploited vulnerabilities. Second, because of changing technology, evolving malware, and the sheer number of attack avenues maintaining a successful defensive position is demanding and requires advanced planning and continuous attention – factors that are necessary to incorporate into one's denial operations.

In the six months leading up to each case studied, several thousand new software vulnerabilities were discovered. With only a handful of known vulnerabilities used in the attacks, the potential for the use of other attack options was likely present. However, given the attackers' success, it appears they selected their avenues of attack well. In both cases, attackers exploited vulnerabilities in Internet-facing sites and client-side software.

Two important differences were observed between the cases. First, the piracy rate in Georgia was nearly double that of Estonia. Because pirated software is not routinely updated with security patches, Georgia was far more

[21] Joseph Menn, "Hacked Companies Fight Back with Controversial Steps," *Reuters*, June 18, 2012, http://www.reuters.com/article/2012/06/18/us-media-tech-summit-cyber-strikeback-idUSBRE85G07S20120618.

susceptible to vulnerabilities emerging from these security lapses. Of perhaps greater note, there was a significant development as a result of the Estonia war in that many older vulnerabilities were resolved by Georgia's IT professionals. This forced Russian attackers to concentrate more on social engineering and email malware to exploit networks and users.

From these circumstances, two requirements for deterrence arise. *First, and in sync with the other requirements mentioned above, is the need for enhanced detection and monitoring in conjunction with active defense.* A prevailing view is emerging in which "many large security providers no longer preach that keeping the enemy out is paramount ... they adopt the more recent line taken by the Pentagon, which is to assume that hackers have gotten inside and will again."[22] This approach has led to a revision of mainstream advice that now focuses on "trying to detect suspicious activity as quickly as possible in order to shut it down."[23] Vigorously protecting against attack from previously unexploited vulnerabilities via active defense offers several benefits that include helping with attribution, instilling a fear of retaliation (which may deter), and potentially preempting imminent attacks.[24]

The second requirement evolving from unexploited vulnerabilities in these cases creates the need for states to either find on their own or purchase zero-day vulnerabilities. This requirement establishes a continuous process in which governments develop their own capabilities to perform this function (tools and

[22] Joseph Menn, "US Firms Deploy Hacking 'Strike Back' Technology," *iTnews*, June 18, 2012, http://www.itnews.com.au/News/305296,us-firms-deploy-hacking-strike-back-technology.aspx.
[23] Ibid.
[24] Tiong Pern Wong, "Active Cyber Defense: Enhancing National Cyber Defense" (Naval Postgraduate School, 2011), 43, http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA556635.

trained professionals) or participate in a market-based system that already exists; see Figure 6.1. This market has emerged after the 2007 cyber war and exploded since 2010. Prior to 2007, hackers discovered and published vulnerabilities for bragging rights among their peers.[25]

In recent years, private companies have begun to sell vulnerabilities to governments, "who buy vulnerabilities with the intent of keeping them secret so they [governments] can exploit them."[26] In the past vulnerabilities were publicly disclosed and patched, which made states and non-state actors more secure. In this new vulnerabilities-market, unexploited vulnerabilities are "remaining secret and unpatched."[27]

Figure 6.1: Price List on Zero-day Exploits[28]

ADOBE READER	$5,000–$30,000
MAC OSX	$20,000–$50,000
ANDROID	$30,000–$60,000
FLASH OR JAVA BROWSER PLUG-INS	$40,000–$100,000
MICROSOFT WORD	$50,000–$100,000
WINDOWS	$60,000–$120,000
FIREFOX OR SAFARI	$60,000–$150,000
CHROME OR INTERNET EXPLORER	$80,000–$200,000
IOS	$100,000–$250,000

[25] Bruce Schneier, "The Vulnerabilities Market and the Future of Security," *Forbes*, May 30, 2012, http://www.forbes.com/sites/bruceschneier/2012/05/30/the-vulnerabilities-market-and-the-future-of-security/.
[26] Ibid.
[27] Ibid. Schneier reported that within the NSA, there was traditionally a debate "between the COMSEC (communications security) side of the NSA and the SIGINT (signals intelligence) side. If they found a flaw in a popular cryptographic algorithm, they could either use that knowledge to fix the algorithm and make everyone's communications more secure, or they could exploit the flaw to eavesdrop on others, while at the same time allowing even the people they wanted to protect to remain vulnerable." He noted that this debate continued through several decades, but "by 2000, the COMSEC side had largely won, but things flipped completely around after 9/11."
[28] Andy Greenberg, "Shopping For Zero-Days: A Price List For Hackers' Secret Software Exploits - Forbes," *Forbes*, March 23, 2012, http://www.forbes.com/sites/andygreenberg/2012/03/23/shopping-for-zero-days-an-price-list-for-hackers-secret-software-exploits/.

The **second triadic component explored is punishment** in which two elements were examined: attribution and offensive/retaliatory means. The Estonia and Georgia cases offer insight into capabilities that may be needed for punishment to serve as a basis for cyber deterrence. Pursuing punishment is a necessary component of cyber deterrence but a state embarking on this path incurs a measure of risk that should be factored at the outset. We must think of cyber deterrence as framed by criminal justice more so than nuclear deterrence. This is the proper frame of reference as cyber deterrence, when it eventually exists, will fail – and likely with great consequence. However, in response to such failures in future cyber crises, deterrence will be reset until it invariably fails again (and again).

Thus, in this sense, we are not facing a new deterrence norm. Nuclear deterrence is a theoretical exception in that any use (any failure) is not acceptable. Again, to the contrary, with cyber war, we expect the first and future iterations of cyber deterrence to fail in a fashion similar to criminal justice deterrence.[29] With this frame of reference, we prepare both to deter and for that deterrence to fail – this is the path forward for cyber deterrence. Although this study posits that a

[29] Criminal deterrence will sometimes succeed and at other times fail. In criminal deterrence theory, most actors are either deterred or uninterested in initiating malicious behavior. A broad acceptance of norms helps explain these phenomena; however, others are not deterred by these norms – they may be deterred by defensive measures such as locking doors. When criminal acts are committed, the offending actors must be brought to justice and punished, which helps to deter others. Similarly, I anticipate that emerging cyber norms will deter most actors; however, as argued elsewhere in this study, denial and punishment approaches hold relevance (as does cooperation). The deterrence dynamic in its cyber iteration more closely follows that of criminal justice because the stakes are currently lower than those associated with nuclear deterrence. This will remain the case until actors are able to achieve nuclear-type effects with cyber weapons. At that time, a failure of cyber deterrence will equate to a failure of nuclear deterrence. If these events should unfold, as I suspect they will, the triadic construct of the model offered in this research will remain valid. However, emphasis would shift from cooperation to punishment between states that possess cyber capabilities with this level of destructive potential.

combination of denial and cooperation offers the strongest basis for cyber deterrence, we must not omit the value of punishment for some categories of actors. To do so is to our detriment and will likely result in more future cyber wars than may otherwise be the case.

Attribution is necessary to threaten to punish or actually punish an attacker. Both cases demonstrated that attribution is possible, although in each case, attribution occurred after the cessation of open hostilities. This fact should have no bearing on the utility of attribution and hence punishment as a core component of the triadic concept. Also in both cases, aside from the identified perpetrators, alleged perpetrators and the links that connected these actors were strikingly similar. The one main difference occurred in the larger amount of data implicating Russian organized crime in the Georgian attacks.

Although attribution is possible, states may have valid reasons for not wanting to attribute attacks because this could result in internal or external pressure to pursue unwanted retaliatory action. Despite such fear, retaliatory means should be developed and sufficiently, yet not needlessly, exposed so that targeted aggressors may be fearful of these capabilities.[30] A further insight relating to attribution that we learned from these cases is that actors' capabilities matter.

We observed that the actors in these cases had differing capabilities, kinetically and non-kinetically. This suggests the importance of a requirement to

[30] Transparency does not have to mean full disclosure of one's retaliatory capability. An opponent only need believe the credibility of one's promise of a threat, which is a function of capability and will.

tailor cyber deterrence for differing classes of actors.[31] It mattered that Russia was a nuclear power with overwhelming conventional superiority over Estonia and Georgia.

Retaliatory means are a critical component of punishment. Because of the drastic mismatch in kinetic capabilities between the attacker and defenders, it is quite telling to consider that given certain attribution, what capabilities would Estonia or Georgia have had to possess to exploit available vulnerabilities to punish their Russian attackers? Kinetically, we know that Georgia ranked 88th globally and Estonia 126th. Unfortunately, I was unable to assess the cyber capabilities of either state. However, given the advanced IT structure of Estonia, one would think the capability might be present from which to build offensive cyber forces.

What is known is that Estonia, despite being the most wired nation in Europe, mounted no cyber counteroffensive. Georgia, on the other hand, managed a feeble cyber counterattack with virtually no impact. Therefore, the evidence suggests that neither Estonia nor Georgia possessed offensive capabilities in any form with which to retaliate, leaving Russia virtually unscathed. This means that even though attribution proved possible, albeit belatedly, neither state possessed the capability to deter Russia by punishment.

From these cases, a striking requirement springs forward. *Cyber deterrence must be tailored for two classes of state and non-state actors: nuclear powers and/or conventional peers, and all other states and non-state actors.*

[31] This idea builds upon the work of Keith Payne, Elaine Bunn, and Geoffrey French on tailoring, which is discussed in previous chapters.

Kinetic power matters and until such time that the imperative to preserve one's interests, whether it be with a nuclear-tipped ICBM or the barrel of a loaded rifle, is superseded by nonkinetic power – the ability to apply that force is a major factor in determining retaliatory potential. This can be interpreted in several ways; however, the result is the same. Kinetic superiority as a function of retaliatory capability is a potent component of deterrence whether non-kinetic cyberoffensive means exist or not.

The retaliatory element of cyber deterrence can take the form of kinetic or non-kinetic capabilities. In circumstances where an actor enjoys non-kinetic superiority, that actor holds an advantage unless his opponent is kinetically superior and inclined to use those forces. This implies, with regards to offensive weapons, that a crisis can escalate beyond cyber war to a general war in which cyber attacks are a key component.[32] *This analysis leads to a second requirement for this element: Developing retaliatory cyberoffensive capabilities that can hold at risk the nuclear and conventional capabilities of a state could potentially position a state or non-state actor (perhaps a single individual) to deter by punishment a current superpower and all classes of actors with less kinetic and/or non-kinetic offensive capabilities.*

The combination of denial and **cooperation, the third triadic component,** offers the strongest basis for cyber deterrence. The potential for escalation is too great, and disparities in both kinetic and non-kinetic capabilities suggest that a combination of these components warrants merit as we compile

[32] An added danger inherent in offensive cyber capabilities is that once used, the originator could experience a boomerang effect with unintended consequences. Offensive cyber weapons, more so than most kinetic weapons, can be captured, re-engineered, and re-deployed against the originator.

requirements to develop a theory of cyber deterrence. The cases examined the most relevant **cooperative relationships** by considering those between and among non-adversaries and adversaries.

The cases were similar in that cooperative responses were largely ad hoc. Estonia relied upon its domestic IT social network and a small number of international experts that, by chance, happened to be in Estonia when the war began. Estonia is a member of NATO; however, beyond sending one observer (belatedly), the alliance was useless during the war. It is an important factor that NATO did not perceive the cyber war against one of its members as an armed attack, which would have invoked an Article 5 response. Several years later, policy actions undertaken by NATO in response to the cyber wars indicate that the alliance favors Article 4 instead.

Although Estonia awakened the world to the potential that could befall any state due to cyber war, the forthcoming actions from NATO, the EU, and the UN were not helpful to Georgia the following year. While Georgia benefitted from the assistance of CERT teams from Estonia, Poland, and France, there was no international framework beyond the Convention on Cybercrime. Georgia, of course, was not a member of NATO or the EU. These international organizations since have neither defined cyber war nor determined conditions that warrant intervention in response to cyber attacks on member states.

Georgia did manage to take advantage of a private relationship in which a U.S. citizen, born in Georgia, used his company to host critical Georgian websites. Although Poland offered the same opportunity, the U.S. effort did not

have the permission or support of the U.S. government. After the Georgian websites were relocated to the U.S., the cyber attacks continued. Thus, the cyber war widened, this time without incident; however, the nature of the domain and the dearth of international norms of behavior could have a less fortunate outcome in future cyber wars.

These circumstances suggest a useful requirement for deterrence by cooperation is to establish a priori relationships between non-adversaries. Tactical-level cooperation in which states with shared interest also share information and capabilities is essential to fulfilling this requirement. Both of these cases show us that cooperation, which is both ad hoc and post hoc is too little, too late. We take from these cases a lesson that needs to be remembered: Just-in-time cyber support is a poor substitute for advanced planning and preparation.

Cooperation involving both adversaries and non-adversaries is inherent in customary international law, such as the Law of War. This has not been updated to reflect the technological changes unleashed by the digital era. The global community of nations would benefit from pledges and agreements in the short term and treaties in the longer term. Before states can achieve formal agreements, adversaries and non-adversaries must establish an appreciation for common norms. Frankly, norms relating to cyber war were not present during these cases, and minimal progress has emerged since. The likely reasons for this influence the practical application of achieving cyber deterrence by cooperation in a profound manner.

For norms to develop and cyber agreements to follow, there first has to be a willingness by those that possess the greatest measure of power (in terms of kinetic and non-kinetic capabilities and economic means) to either yield that power, exchange it for another form of power, or acquiesce for a greater good. Because the security dilemma is alive and well in the cyber domain, a rational actor would never make such a choice without receiving something in return – it would be foolish.

Our theory may recognize norm formation and agreements as elements of a cooperative component; however, the practical circumstances suggest that despite a powerful state's advantage of possessing offensive and defensive capabilities as valuable enforcement mechanisms – cooperation as a function of deterrence must be tailorable to account for the security dilemma as well as the reasons that were discussed in the punishment component above. *Therefore, a requirement for cooperation in its strategic (norm-developing) form is to develop a limited set of norms that prohibit the most harmful cyber attacks from which to forge an international agreement.*[33]

Table 6.1: Summary of Case Analysis

Triadic Component	**Element Examined**		**Estonia**	**Georgia**
Denial	Exploited Vulnerabilities	*Internet Dependence*	- 100% government business online - Most wired country in Europe - 57% population have access	- 7% population have access - Dependent on Russia and others for access - Small IT structure, only 5 providers
		System Weaknesses	- Configuration	- Configuration - Specification
		Hardware Exploitations	- Flood attacks	- Flood attacks - Tailored
		Software	- Flood attacks	- Flood attacks were

[33] Nigel Chamberlain, "Cyber Warfare and NATO," *NATO Watch*, June 14, 2012, http://www.natowatch.org/node/723.

Triadic Component	Element Examined		Estonia	Georgia
		Exploitations	- Ping attacks - SQL injection	tailored - Ping attacks - SQL injection
	Targets		- Networks - Users	- Networks - Processes - Users
	Defensive Actions		- Research and investigations - Collaboration to filter traffic - SQUID	- Technical responses - Cyber counteroffensive - Self-blockade - Website relocation
	Unexploited Vulnerabilities		- 3,400 new software vulnerabilities early '07 - Internet-facing sites - Client-side software - 51% piracy rate - Social engineering - Email malware - Dynamic malware development	- 2,500 new software vulnerabilities early '08 - Internet-facing sites - Client-side software - 95% piracy rate - Social engineering efforts increased (fcn of '07 war) - Email malware increased (fcn of '07 war) - Dynamic malware development
Punishment	Attribution/Origin	*Identified Perpetrators*	- Ethnic Russian student in Estonia - Nashe youth group	- Cyber militia - RS organized crime
		Alleged Perpetrators	- Russian government	- RBN - Russian government
		Connecting Links	- Three-tier structure: RS-Nashe-Org. Crime	- Three-tier structure: RS-Cyber Militia-Org. Crime
	Retaliatory Means		- Non-nuclear state - Ranked 126th globally/minimal kinetic capability - Cyber capability unknown	- Non-nuclear - Ranked 88th globally/little kinetic capability - Cyber capability unknown
Cooperation	Cooperative Relationships	Non-adversaries	- Domestic IT social network - NATO member - NATO sent 1 observer - Three int'l vetted experts	- CERT-EE - CERT-PL - CERT-FR - Tulip Systems (U.S. company) - No int'l agreement - Not a EU or NATO member
		Adversaries	- Law of War is dated - 2001 CoC provided for mutual assistance - Direct int'l regimes offered little help - Indirect int'l regimes offered no help	- Law of War is dated - 2001 CoC provided for mutual assistance - Direct int'l regimes offered little help - Indirect int'l regimes offered no help

Table 6.2: Summary of Case-driven Requirements

Triadic Component	Element Examined		Requirements
Denial	Exploited Vulnerabilities	*Internet Dependence*	- Secure lines of communication to counter cyber choke points - Whole-of-society approach to provide for a common cyber defense
		System Weaknesses	- Recruit and retain properly trained IT professionals - Narrow the gap between a basic IT education and necessary cyber operations trade craft skills - Continuous training to reflect rapid pace of technical evolution - Rapid incorporation of shared data on vulnerabilities - Establish zero-fault mindset with rigorous standards and accountability - Implement continuous self-inspection/assessment processes
		Hardware Exploitations	- Continuously evolve passive defenses: firewalls, intrusion detection and prevention, patching, log auditing - Engineer resilience into new hardware and software
		Software Exploitations	
	Targets		- Use cyber red teams to constantly stress IT systems for vulnerabilities
	Defensive Actions		- Develop and deploy active defense capabilities (cyber exploitation, counter attack, preemptive strikes, and preventive strikes)
	Unexploited Vulnerabilities		- Enhanced detection and monitoring in conjunction with active defense - Develop capacity to find or purchase zero-day vulnerabilities
Punishment	Attribution/Origin	*Identified Perpetrators*	- Tailor cyber deterrence for two classes of state and non-state actors: nuclear powers and/or conventional peers, and all other states and non-state actors
		Alleged Perpetrators	
		Connecting Links	
	Retaliatory Means		- Developing retaliatory cyber offensive capabilities that can hold at risk the nuclear and conventional capabilities of a state could potentially position a state or non-state actor (perhaps a single individual) to deter by punishment a current superpower and all classes of actors with less kinetic and/or non-kinetic offensive capabilities
Cooperation	Cooperative Relationships	Non-adversaries	- Establish a priori relationships between non-adversaries
		Adversaries	- Develop a limited set of norms that prohibit the most harmful cyber attacks from which to forge an international agreement

The Hypotheses Revisited

This research offered four hypotheses, which are presented in Table 6.3 with overarching empirical results. These hypotheses, informed by basic

deterrence, criminal justice deterrence, and nuclear deterrence theories, are rooted in a critical question regarding the cyber domain. How is deterrence possible if attribution, offensive capabilities, defensive capabilities, or cooperative relationships are either missing from or inadequate to deter a malicious actor?

What I discovered in analyzing and evaluating the cases and synthesizing this with the literature is that we are left with neither a full accounting of what is possible nor an accounting of what is not possible. Instead, the research indicates the presence of a middle ground, where cyber deterrence becomes conditional and/or variable in its effectiveness based on attention or inattention to the triadic components, all of which are captured by the hypotheses.

In each instance, the cases revealed evidence supporting the hypotheses; however, I must confess, in an effort to understand the nuances embedded in the elements supporting these core deterrence components, other questions and challenges arose. Regarding the **attribution-focused hypothesis**, we learned that attribution was possible in both cases. Therefore, a punishment strategy is possible in cyber deterrence. This satisfies theoretical demands; however, I remain troubled by the fact that attribution in both cases occurred after the cessation of hostilities. This fact leaves open two possibilities. First, one may argue that the potential of attribution, even if it is belated, may alter a potential attacker's decision calculus and thus deter an attack. A second possibility exists in that a potential attacker may need only a brief period to achieve his objectives, and thus the delayed attribution is less a factor, if any at all.

Despite these differences, I have determined that in the cyber domain, it remains a theoretically sound principle that to punish or threaten to punish a party, it is first necessary to identify that party. Therefore, attribution must be a component of any cyber deterrence-by-punishment approach. Any time delay associated with attribution while possibly a factor with denial efforts is of little consequence to one's punishment calculus.

In considering the **offensive capability-centric hypothesis,** we learned that neither Estonia nor Georgia possessed the kinetic or non-kinetic capabilities to hold the attackers' interests at risk. Had either state possessed a larger measure of these capabilities, we still do not know if they would have been able to deter Russia, but the possibility to do so would have existed. The operative word is *possibility*. We know from the literature that despite the findings in cyber deterrence theory to punish a known actor, the capacity to do so must exist.

The **third hypothesis focused on deterrence by denial**. We learned from the cases that the pool of exploited and unexploited vulnerabilities continuously expands. This means that an actor requires a robust capacity to field denial capabilities that includes responding to this steady stream of malicious enhancements. We saw that within both cases, the basis for deterrence by denial resided in efforts to counter both exploited and unexploited vulnerabilities. A denial approach that also incorporates resilience with hardening offers a better opportunity for deterrence by denial as it introduces the potential of futility into the attackers' decision calculus.

The **fourth hypothesis introduced cyber deterrence through cooperative relationships**. What we learned from the cases is that cooperative relationships should be viewed through two lenses: one non-adversarial, the other adversarial. I introduced the concept of tactical cooperation, which includes domestic and international approaches to information sharing and incident response, as a means to categorize efforts that allies or friendly states engage in to protect shared interests. Strategic cooperation is necessary between states that are adversaries as well as non-adversaries to develop norms in order to reach agreements. What we have learned is that cooperation in both its tactical and strategic forms is a necessary component of cyber deterrence and that either advance the potential for deterring cyber warfare. However, I found that a combination of denial and cooperation offers the greatest potential in deterring cyber war between the more powerful kinetic and non-kinetic states.

Table 6.3: Hypotheses and Results

Hypotheses	Empirical Result
If attribution is present in cyber deterrence strategy, then credible deterrence of states and/or non-state actors through a punishment strategy is possible.	Attribution was possible in both cases. The fact that it occurred after the cessation of hostilities and in the absence of international agreements that define or prohibit cyber war and cyber attacks is less a factor. It remains an integral theoretical aspect of cyber deterrence that the identity of an attacker must be known before that party may be held at risk.
If the offensive capability to hold at risk what an actor values is present in cyber deterrence strategy, then credible deterrence of states and/or non-state actors through a punishment regime is possible.	In both cases, defenders did not have the non-kinetic or kinetic capacity to hold the aggressor's interests at risk. However, the possibility to deter lies in the possession of offensive capabilities, which is a crucial element in cyber deterrence by punishment.
If a state's cyber vulnerabilities are protected by defensive capabilities from cyber aggression by states and/or non-state actors, then credible cyber deterrence by denial is possible.	The pool of exploited and unexploited vulnerabilities continuously expands. This requires robust capacity to field denial capabilities and respond to the steady stream of malicious enhancements. By countering these vulnerabilities with defensive measures, the prospect of deterring cyber war is possible.

If a state's cyber infrastructure is protected by cooperative relationships between non-adversaries and adversaries, then credible cyber deterrence by cooperation is possible.	Cooperative relationships should be viewed through two prisms: tactical and strategic. Cooperation is a necessary component of cyber deterrence; however, it is most effective when used in combination with denial efforts.

A Theory of Cyber Deterrence

A plethora of scholarly work exists on what cyber deterrence is and is not, but no concise theory has been offered until now. Of the literature used in this research and other sources reviewed but not referenced, no scholar was observed to have said, "The following is my theory of cyber deterrence..." Certainly, scholars have debated the requirements that might constitute such a theory; they have at length discussed how such requirements might be formulated and why or why not they are valid; and some have offered comprehensive frameworks. Given all this attention, I do not know why a concise theory has not been formally presented – perhaps it is the fear of being wrong. On the other hand, maybe it is "more scholarly" to hedge, but this does not help address the serious problems actors face in the cyber domain that an accepted theory of cyber deterrence may be able to address.

Near the outset of this research, two prominent cyber scholars told me that by 2010 there was nothing left to be said or written about cyber deterrence. They were correct in that I did find a lot of information on cyber deterrence, but again, there was no presentation of a concise theory. As I have studied this topic, I have learned that an assembly of ideas does not constitute a theory. Putting the word *theory* in the title of a book or article does not take the place of actually offering a theory.

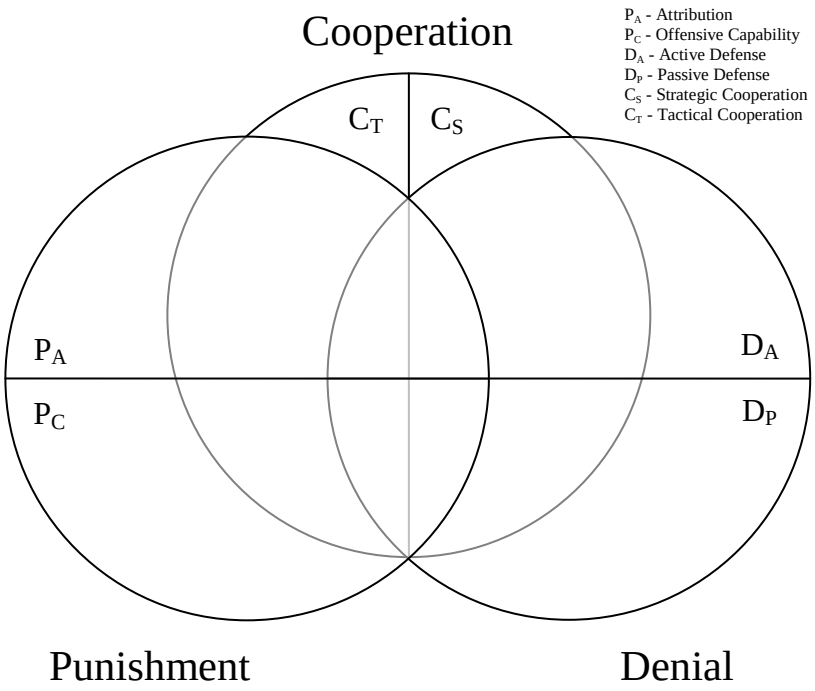
What follows is a theory – accept it or improve it; convince policy makers to use it or a better version in developing budgets to realize the needed capabilities to organize, equip, and train forces accordingly – let us use this or a better theory to shape policy and procurement. The cyber domain and operational practices have matured such that now we have enough information to develop and use a theory of cyber deterrence to inform strategy and policy so as not to suffer from its absence.

I propose the following theory of cyber deterrence, which is based upon a triadic concept formed by an interwoven relationship between denial, punishment, and cooperation (see Figure 6.2). Denial is a function of active defense (D_A) and passive defense (D_P). Both active and passive defenses featured prominently as requirements that emerged from the case studies. To successfully employ these defensive variants, actors must possess secure cyber lines of communication, a whole-of-society approach to cyber security, security specialists trained and equipped with enhanced detection and monitoring capabilities to confront continuously evolving vulnerabilities, and the wherewithal to find or buy zero-day vulnerabilities using any necessary means.

Punishment is a function of attribution (P_A) and offensive capabilities or retaliatory means (P_C). We know from the case studies that attribution was possible; however, the retaliatory means did not exist in these cases to deter Russia. Yet from the literature, we know that with attribution it is possible to deter an actor if the capability (and will) is present. The cases indicated the value

of tailoring in designing cyber deterrence theory to account for escalation that could occur between peer kinetic powers engaged in a cyber war.

Figure 6.2: A Theory of Cyber Deterrence



Cooperation is a function of cooperative relationships between non-adversaries and adversaries. Tactical cooperation (C_T) occurs when actors that are non-adversaries establish relationships to mutually satisfy shared interests and objectives. The case studies demonstrated that tactical cooperation should be a priori and not post hoc. Strategic cooperation (C_S) occurs between and among non-adversaries and adversaries, whereby the advantage of mutually beneficial interaction for all actors exists in developing norms as a prerequisite for reaching international agreements governing cyber war.[34]

[34] In referring to cooperation between adversaries, I also include the interaction that may or may not occur between each of the adversaries and respective allies.

In this theory, Actor A in response to known and unknown vulnerabilities employs passive and active defensive measures to counter a potential action by Actor B with consequences that prevent, or deter, Actor B from taking the proscribed action. Actors can be nation-states, groups other than states, or single individuals. Credible cyber deterrence requires Actor A's passive and active defenses be believable by Actor B. This is achieved through Actor B's experience and overt communication between Actor B and other actors considering potential action against Actor A.

Actor A must exhibit the capability for passive and active defenses to be considered credible. Additionally, Actor A's specific active defense capability does not have to be transparent as Actor B needs only to appreciate that credible active defenses are present for deterrence to occur.

The capabilities of Actor A may be offensive such that they inflict cost in that benefits are denied to Actor B. Actor A's use of offensive cyber capabilities to threaten or if necessary punish Actor B are necessary and productive aspects of a deterrence-by-punishment approach. Cyber offensive capabilities are useful when the identity of an egregious actor is a known factor thus promoting the utility of threat issuance or punishment in the failure of deterrence.

Actor A may employ cooperation in response to known and/or unknown vulnerabilities. In its strategic form, cooperation employs the stages of norm cultivation[35] to strengthen and develop regimes and institutions to create pledges,

[35] Martha Finnemore, "Cultivating International Cyber Norms," in *America's Cyber Future* (Center for a New American Security, 2011). Finnemore presented the states of norm cultivation, which include norm articulation and promulgation; norm dissemination; and norm internalization, institutionalization, and enforcement. I suggest that while difficult, it may be possible to

agreements, or treaties to counter a potential action by Actor B with consequences that prevent, or deter, Actor B from taking the proscribed action. New and enhanced cyber institutions and legal regimes as a component of an overarching and long-term cooperative approach may serve to deter state actors and their agents. In its tactical form, cooperative relationships formed and exercised prior to crises may provide a deterrence effect, as Actor A in conjunction with Actor C may either undertake preparation or create an impression that such preparations exist to negate or diminish malicious actions planned by Actor B.

Tailoring Cyber Deterrence Theory

Nuclear and peer conventional powers should be approached differently from others because of the potential for escalation. I recommend a softer approach for peers or near-peers and a no-nonsense, hard approach for others. An approach of this nature permits the deterring state to factor in economic or other interdependencies as well as the capacity to over time move actors from one approach to the other as capabilities rise and fall.

The combination of requirements that emerge from studying deterrence literature and from examining the two cases of cyber war leads me to argue that the cyber deterrence theory introduced above requires further refinement. There should be a variant that is tailored to deter cyber war between nuclear and conventional peers. A second iteration would then address cyber war between lesser powers or between a kinetically powerful and non-powerful state (as in the 2007 and 2008 cyber wars).

---

delegitimize the tools of offensive cyber war through the emergence of norms similar to those developed over time to address chemical, biological, and nuclear weapons.

I suggest that refining the theory of cyber deterrence into hard and soft variants serves this purpose. Scholars who have written extensively on the concepts of hard power and soft power inform the characterizations of what I call *hard cyber deterrence* and *soft cyber deterrence*. Nye wrote that *hard power* rested upon "inducements ('carrots') or threats ('sticks')."[36] Campbell and O'Hanlon defined hard power as the "application of military power to meet national ends – that is, the deployment of ground troops, naval assets, and precision munitions to secure a vital national objective."[37] Hard power thus provides the tools to threaten and if necessary punish as called for in nuclear deterrence. Is this too dangerous a game to play between nuclear powers that may be in the midst of a cyber war? I suggest this is the case.

We know that the value of inducements should be considered because of the research of George and Smoke, who wrote, "Theory needs to give as much attention to the role of 'inducement' or 'promise' as to that of threat."[38] They argued for a "wider theory" which they suggested could be "called 'deterrence,' or 'influence theory' of which 'deterrence' would be one portion."[39] Inspired by their idea, I propose the development of a "wider" theory of tailorable cyber deterrence that includes both threat and inducement based approaches to the extent that escalation is not induced – while, of course, remaining within an accepted understanding of what constitutes cyber deterrence theory.

---

[36] Joseph S. Nye, *Power in the Global Information Age: From Realism to Globalization* (London: Routledge, 2004), 5.
[37] Michael E. O'Hanlon and Kurt M. Campbell, *Hard Power: The New Politics of National Security* (New York: Basic Books, 2006), 7.
[38] Alexander L. George and Richard Smoke, *Deterrence in American Foreign Policy: Theory and Practice* (New York: Columbia University Press, 1974), 81.
[39] Ibid., 81.

Nye defined *soft power* as exploiting a nation's "broad appeal of cultural, ideological, and institutional factors" to realize national objectives.[40] He further suggested that the value in soft power lay in "getting others to want the outcomes that you want" to co-opt people instead of coercing.[41] Nye illustrated in Table 6.4 that cyber power could produce hard and soft power effects both within the cyber domain and through others.[42]

Table 6.4: Physical and Virtual Dimensions of Cyber Power[43]

TARGETS OF CYBER POWER		
	WITHIN CYBERSPACE	OUTSIDE CYBERSPACE
Information instruments	Hard: Launch denial of service attacks. Soft: Set norms and standards.	Hard: Attack SCADA systems. Soft: Initiate public diplomacy campaign to sway opinion.
Physical instruments	Hard: Enforce governmental control over companies. Soft: Introduce software to help human rights activists.	Hard: Destroy routers or cut cables. Soft: Stage protests to name and shame cyber providers.

I learned from George and Smoke that "deterrence should be viewed not as self-contained strategy, but as an integral part of a broader, multifaceted influence process."[44] This served to further enforce the usefulness of migrating the ideas supporting hard and soft power to influence the emergence of a theory of cyber deterrence, which I further refine into *hard cyber deterrence* and *soft cyber deterrence*. As tangential evidence to the utility of this approach, the Air Force Research Laboratory (AFRL) investigated *hard deterrence* in reference to terrorism and determined that the "ability to defend against a tactical attack is

[40] Nye, *Power in the Global Information Age*, 38.
[41] Ibid., 5.
[42] Joseph S. Nye, Jr., "Power and National Security in Cyberspace," 8. Nye defines *cyber power* as "the ability to obtain preferred outcomes through the use of the electronically interconnected information resources of the cyber domain."
[43] Ibid., 10.
[44] George and Smoke, *Deterrence in American Foreign Policy*, 591.

basically built on hard deterrence actions, such as posting guards and flying CAPs, which in turn are made relevant by detection."[45] The AFRL study defined soft deterrence as the "'hearts and minds' aspect of antiterrorism,"[46] while Jaishankar characterized *soft deterrence* as "deterrence based on the calculation that the human and economic, essentially non-military, costs of initiating a conventional war outweigh any potential military gains."[47]

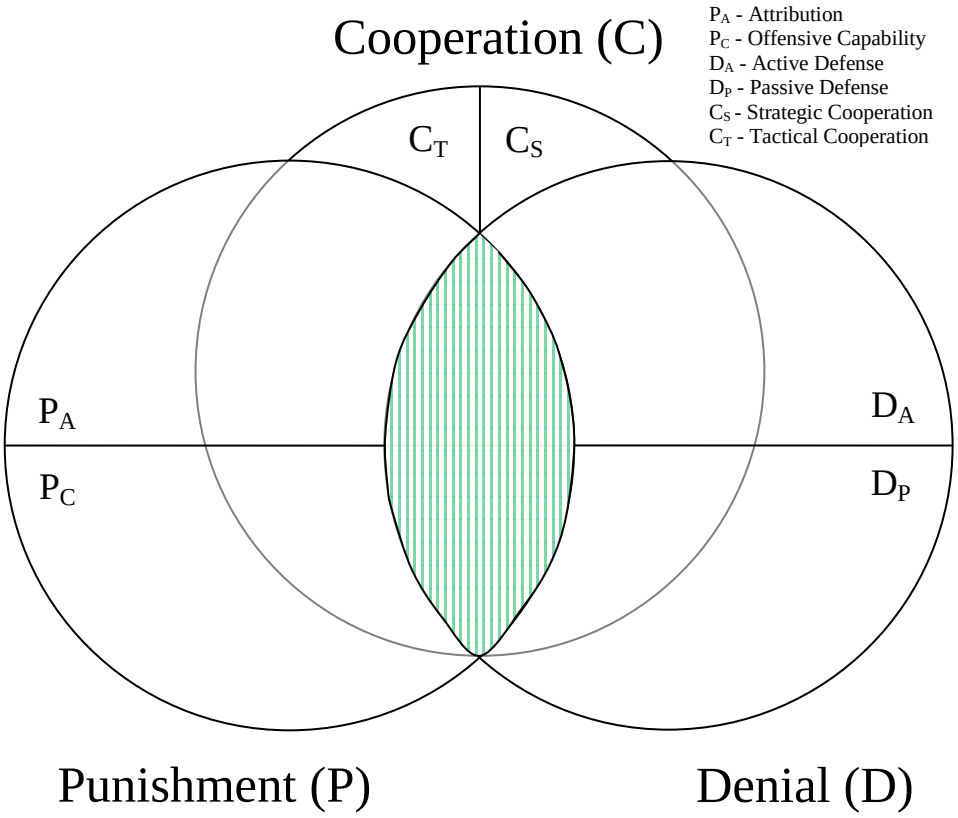
These previous treatments of hard and soft power/deterrence inspire the following definitions of hard and soft cyber deterrence. ***Hard cyber deterrence*** is based upon a calculation that rests upon the offensive capacity to bolster threats and issue punishments and/or the defensive capacity to field passive and active defenses against state or non-state actors who seek to gain military, economic, and informational advantage through cyber war or cyber attack. Hard deterrence in this framework considers known offensive and defensive capabilities and relies upon them in combination with cooperative relationships to form a basis for effective cyber deterrence.

Hard cyber deterrence is therefore a function of $P_A + P_C + C_T + C_S + D_A + D_P$ (see the vertical lines that represent the intersection of P + D + C in Figure 6.3). There is little concern that by using this variant the threat or use of punishment to deter cyber war will escalate into a kinetic war. Hard deterrence rests upon the offensive capacity to bolster threats and issue punishments and/or

[45] David O. Ross and Robinson C. Ihle, "Successfully Managing Insurgencies and Terrorism Effectively (SMITE)", March 2011, 16, http://webcache.googleusercontent.com/search?q=cache:lFoaQr5dhkgJ:www.dtic.mil/cgi-bin/GetTRDoc%3FLocation%3DU2%26doc%3DGetTRDoc.pdf%26AD%3DADA540778+%22hard+deterrence%22+definition&cd=11&hl=en&ct=clnk&gl=us.
[46] Ibid., 19.
[47] D. Jaishankar, "'Soft Deterrence' and the Future of Nuclear Disarmament," *CLAWS Journal*, no. Summer 2008 (n.d.): 222.

the defensive capacity to field passive and active defenses against state or non-state actors who seek to gain military, economic, and informational advantage through cyber war in conjunction with tactical and strategic cooperation.

Figure 6.3: Hard Cyber Deterrence



As previously mentioned, cyber deterrence by punishment may undermine the deterrence calculus for kinetic war between nuclear and conventional peer states. ***Soft cyber deterrence*** recognizes this potential and therefore emphasizes components of cyber deterrence theory based upon the calculation that the diplomatic and economic costs of initiating cyber war or escalating from cyber to kinetic war outweigh any potential military or informational gains.

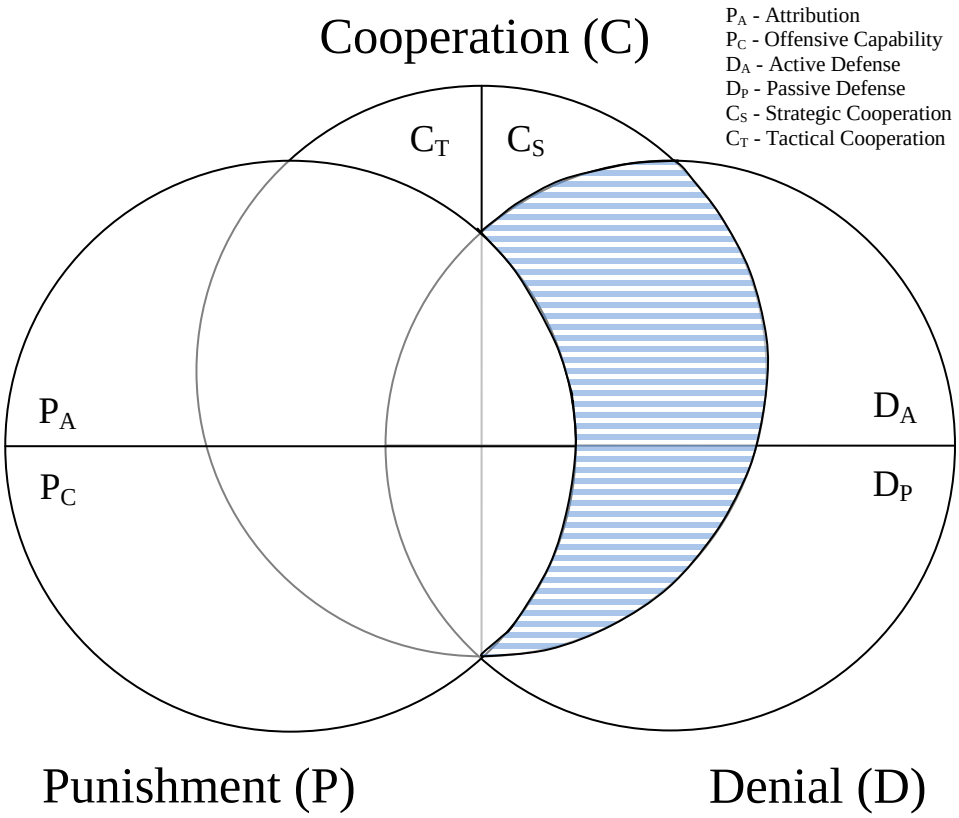
Soft deterrence is a function of $C_S + D_A + D_P - P$; see the horizontal lines that represent the intersection of the applicable elements of denial and cooperation

(less punishment) in Figure 6.4. In this construct, the denial elements of passive and active defenses are fielded as previously described. It should be noted that a peer state may find its risk calculations dramatically influenced by the prospect of active defenses. This is because active defenses used in this manner offer similar benefits to those of offensive capabilities without the need for attribution and a potentially a conscious decision to respond.

Strategic cooperation is based upon norm emergence and the potential to create agreements or bolster international institutions and regimes, particularly those associated with international customary law such as the law of war. The necessary conditions to realize soft cyber deterrence are extant in international regimes and institutions and the supportive national entities that create and reinforce these regimes and institutions. We know that these efforts are long-term in nature and they take years, if not decades, to come to fruition.

Before these types of cooperative efforts can take place, countries like the U.S., which currently enjoy a competitive advantage in the cyber domain, must either lose that advantage or come to a realization that the current path of permitting the intelligence apparatus to control the cyber domain is a path to disaster. In the interim, adoption of a softer approach to cyber deterrence between kinetic powers may both help deter cyber war and, should that deterrence fail, help contain the cyber war from escalating to kinetic war.

Figure 6.4: Soft Cyber Deterrence



Implications for the Future

In reflecting upon the implications of this research, I am drawn to first consider what **a world without cyber deterrence** would look like in ten, twenty, or fifty years. We have a clue as to how this would unfold because to date we have not had a geopolitical climate in which cyber deterrence existed. By simply looking around at the current security environment, we may imagine international and domestic implications.

Internationally, we have two cyber wars. Since these wars, which occurred in 2007–2008, there has been a tremendous movement among many states to organize cyber military forces and to develop cyberoffensive forces. This portends great danger of an eventual major power confrontation in cyber

space that could escalate into a kinetic war. In an international environment in which the largest nuclear powers routinely and freely steal each other's governmental and corporate secrets at an unprecedented level in human history, how safe and secure are we if these current circumstances begin to result in regional or global shifts in power and influence?

Domestically, the populations of many western (and eastern) states are faced with the potential of a continuous erosion of domestic civil liberties. In the future, who will deter nations such as the U.S., China, and Russia from exploiting their own populations by using the cyber domain? When will these new capabilities lead to first civil cyber war or cyber revolution?[48]

The implications of **creating conditions to pursue cyber-related agreements** and potentially treaties that could emerge from the cooperative component of deterrence in the proposed theory are profound. These may prove to be as fundamental to domestic and they are to international concerns. Might the soft deterrence aspects proposed in this research help establish the theoretical groundwork for future treaties fifty years hence? I do not know; however, in response I ask, were those who envisioned the biological and chemical weapons conventions seventy-five years ago, or those who first saw the need for nuclear nonproliferation fifty years ago, any less bold? However, we must acknowledge that the U.S. and other major powers will likely remain reluctant to relinquish

[48] Some may argue that the use of social networking in the 2011 Arab Spring uprising constituted an example of a quasi-cyber revolution.

offensive cyber weapons; therefore, a traditional arms control approach may never work.[49]

The implications for multi-billion-dollar budgets in times of economic duress for **organizing and equipping future forces** based on the demands of the cyber domain, the proposed cyber deterrence theory, and current and emerging global security climate must not be understated. I suggest many states are far from prepared. Current organizational structures and acquisition programs of record may suggest that some states are figuratively still "buying buggy whips" decades after horse-drawn carriages are no longer in use.

By this, I am referring to states that are slow to re-organize, re-arm, and re-train for new security environments. For example, in a future cyber war, even should it escalate to kinetic war, of what value is a complex Napoleonic structure or stealthy short-range attack aircraft in an environment with minimal capacity for forward basing when opposed to a flatter organization or perhaps no organization at all across great distances in which the target is information and no longer military forces or lawfully targeted components of civilian populations? States that waste scarce resources over concerns about developing capabilities to fight the next big war just as the last one, albeit in a different place, may create domestic jobs or validate dated professional experience in the short term; however, in the long term, this practice risks lives, national treasure, and the potential for victory.

[49] Until nations such as the U.S., China, and Russia experience grievous cyber harm, they will not be anxious to relinquish their power to wage cyber war or conduct effective cyber attacks.

The implications of the proposed theory of cyber deterrence as they relate to organization and force structure suggest that the U.S. combatant command structure and many current capabilities are too cumbersome, expensive, and unnecessary. In modern war, the services should be warfighters, and there should be an emphasis on rapid (meaning near instantaneous) global reaction when needed by cyber, space, and air power forces with short response naval and ground special forces at the ready.[50]

The implications of **an emerging cyber arms race and an alarming militarization of the cyber domain** suggest the existence of a cyber security dilemma. The increasing quest for states to develop cyberoffensive capabilities creates conditions for instability in the cyber domain and, absent cyber deterrence, may result in an accidental cyber conflict or war. Prudence and adherence to the proposed cyber deterrence theory may calm the existing climate of cyber insecurity between states.[51]

The **potential for non-state actors, perhaps a single individual to execute state-like cyber attacks,** has implications for the manner in which states employ deterrence strategies. When employing nuclear or conventional arms, it is mostly about the hardware. In the cyber domain, attacks are as much art and imagination as skill. Our side may lose if we do not find and develop these people. They may not look like us, they may not want to follow our rules, and

[50] I envision a large strategic reserve of ground forces and secure nuclear capabilities as a vital component of the nation's deterrence posture.

[51] While the triadic construct of denial, cooperation, and punishment should remain constant, the emphasis upon and relationship between these components (and subcomponents) can be expected to evolve because cyber deterrence is situationally specific. As we have learned from the case studies, due to evolving technologies and constantly emerging vulnerabilities we know that what works today will likely not work tomorrow without adjustments on the part of the defender.

they may reject our somewhat meaningless certifications. We should be forewarned that without them, we may suffer or even lose.

The final implication I offer relates to the inability to recognize and adapt to a potential problem in the future because the status quo is highly beneficial. To protect this status quo, the U.S. and other states have **criminalized cyber attacks instead of pursuing meaningful avenues to confront the growing threat of more damaging cyber attacks and the potential for more cyber wars,** which could result in an unintended escalation into kinetic war. The short-term objective is to protect an advantage in cyber capabilities for as long as possible. The potential for disaster exists as this does more long-term harm than good – particularly as it emboldens potential adversaries.

Recommendations for Future Research

In the course of this study, several areas for additional research have emerged. First, there is a pressing need for research to deter cybercrime, cyber attacks below the threshold of cyber war, and cyber espionage. All were originally included in this research; however, the scope became too large to examine these in concert with cyber war. I suggest that the proposed theory of cyber deterrence may serve as an ideal starting point from which to pursue these topics.

Next, I observed a gap in U.S. policy and scholarly literature relating to cyber deterrence. It appeared that between the March 2003 U.S. invasion of Iraq and 2006 there was very little added to the public domain on this topic. Anecdotally, this may be explained by focus on higher priorities such as the

ongoing wars in Afghanistan and Iraq. However, in this period, several cyber events should have alarmed policy makers that cyber deterrence needed a strong look. This does not appear to have taken place in the presence of serious cyber threats, which suggests that research to ask why may prove valuable.

Lastly, the proposed theory of cyber deterrence was developed by assessing vulnerabilities that were exploited or available for exploitation in the cases and enduring lessons from deterrence literature. This theory needs to be vigorously stressed to improve it where warranted, and it requires validation by others against the existing cases of cyber war or others that may emerge. For example, as of this writing, the U.S. and Israel have been engaged in a prolonged series of cyber attacks on Iran's nuclear infrastructure using Stuxnet. Unsupported claims suggest these actors may be responsible for the Flame virus attacks on Iran as well. Should the U.S.-Iran cyber confrontation reach the level of a cyber war, this would be an ideal case for an independent validation of the cyber deterrence theory.

Conclusions

Initially, I began this study in search of an alternative theory of cyber deterrence. I rapidly discovered that despite robust literature on the topic, there was no theory of cyber deterrence. I was surprised to review much well-thought-out analysis and commentary of what might comprise such a theory as well as insightful frameworks, but no one has offered a theory, until now. The realization that there was no theory of cyber deterrence placed me on a path that led to a

realization I had not anticipated – how can something fail that did not exist in the first place?

This caused me to re-focus on an entirely different challenge from that envisioned. Instead of struggling to prove a negative by asking how cyber deterrence failed in Estonia and Georgia, I was left to figure out how the circumstances of these cyber wars might inform a theory of cyber deterrence. With the guidance of my dissertation chair, who devised the approach I used, the research path was established.

Exploited and unexploited vulnerabilities were closely analyzed to help inform the requirements for cyber deterrence by denial. This permitted us to reverse engineer what actually occurred to design a theory that may prove more relevant to deterring cyber war. In the course of the case studies, we learned that cooperation appears to play a larger role in cyber deterrence than perhaps earlier forms of deterrence theory. This inspired a theory of cyber deterrence based upon denial, punishment, and cooperation.

I offer six conclusions based on this research (see Table 6.5). First, **attribution matters – it is not an insurmountable challenge**. Once attribution is obtained, it matters little if the threat or act of punishment is in the form of cyber non-kinetic or kinetic means. What retains importance in our theory is that the classic requirements of punishment are as valid as ever. If you identify an aggressor and possess the capability in conjunction with credibility, transparency, and willingness – cyber deterrence by punishment is possible.

Next, **smaller states can potentially deter larger states from initiating a cyber war** or mitigating the damage once one starts.[52] To do so they need robust denial capabilities and cooperation, particularly in the form of alliances with organizations of states (or other capable actors) that will come to their aid. Smaller states with less potent capabilities will not deter a larger more capable state with a threat of punishment. Although it may change, at this point, kinetic offensive capabilities still trump cyber capabilities – more capable adversaries always have an option to escalate. This means that a cyber war could evolve into a broader conventional war or conceivably a nuclear exchange, which severely discredits the potential of less powerful states to deter those more capable.

Third, **cyber vulnerabilities can be mitigated, but it is not easy** because this requires a continuous process of evaluation and the capacity to deliver a timely response. This provides a basis for deterrence by denial. Fourth, and closely related, **denial by deterrence can prevent an attacker from succeeding**. Actors should incorporate the capacity to rapidly respond to evolutions in hardware and software and resiliency to instill a sense of futility in the attacker.

Fifth, **cooperative relationships are essential in cyber deterrence**. They must be realized in conjunction with the application of denial capabilities.

---

[52] One could argue that proportional deterrence is as relevant in cyber as it is in nuclear deterrence but it would be premature. For example, France with less offensive nuclear capability might have deterred a larger nuclear power such as the former Soviet Union during the Cold war. Thinking about this dynamic in cyber deterrence, one could argue that a smaller state with modest cyber offensive capability could deter a larger state with robust cyber offensive capability. This is perhaps the case; however, in circumstances where the smaller state is over-matched in conventional or nuclear capability the threat of escalation reduces, if not eliminates, the smaller states deterrence posture. Proportional deterrence in the nuclear sense will not translate to cyber deterrence theory until offensive cyber capabilities exist that can create nuclear-type weapons effects. At that time, proportional cyber deterrence will be possible as a smaller state with such cyber capabilities, albeit lesser in quantity could deter a larger state with these same offensive cyber weapons in larger quantity and quality.

Cooperation in the absence of robust denial capabilities is fruitless in the tactical sense. However, over a prolonged period, strategic cooperation may help develop norms, which foster agreements that assist in deterring cyber aggression.

Lastly, **cyber deterrence must be tailorable** as a function of a state's kinetic capabilities. Nuclear capable and conventionally superior states require a different approach in deterring each other than in their efforts to deter less capable state and non-state actors. Because of the potential for escalation, cyber deterrence between powerful states must focus on cooperation and denial to the exclusion of punishment. Until the potential damage from a cyber offensive strike exceeds that of a conventional or nuclear exchange, the threat of a cyber offensive strike or counterstrike is pointless. The potential reward does not justify the risk.

Table 6.5: Conclusions

Six Conclusions
1. Attribution matters – it is not an insurmountable challenge.
2. Smaller states can potentially deter larger states from initiating a cyber war.
3. Cyber vulnerability can be mitigated, but it is not easy.
4. Denial by deterrence can prevent an attacker from succeeding.
5. Cooperative relationships are essential in cyber deterrence.
6. Cyber deterrence must be tailorable to account for actor's capabilities.

These conclusions, mined from case analysis and the literature, helped in the development of a theory of cyber deterrence. Now policy makers, scholars, and others have access to a theory that explains what could be done to deter future cyber wars based on cyber wars that have already taken place. However, we know that theory generally follows practice and is slow to gain appreciation. Acceptance of a theory such as the one proposed is usually driven by a crisis or other immediate need. It is my hope that given the global cyber security climate

that we do not have to experience a cyber crisis, a "cyber Pearl Harbor," to unite policy makers and practitioners on an important and practical approach to deterring cyber wars in the future.

This is important because the ongoing race to construct offensive cyber arsenals places the U.S. and other powerful states in a less secure position. It took years for more than a couple of nations to develop nuclear offensive capability. The pace for other actors to copy and perhaps improve offensive cyber weapons is greatly accelerated. For example, the capability to replicate the 2010 Stuxnet attacks on Iran by the U.S. and Israel are already a part of the arsenals of others. Complex cyber attacks, like Stuxnet, "can be replicated by merely competent programmers, instead of requiring innovative hacker elites" – "it is as if with every bomb dropped, the blueprints for how to make it immediately follow."[53]

In this unpredictable environment, the U.S., Russia, China, and other powerful states have more to lose than to gain given the importance of the cyber domain to global economic interdependence. The safest approach for powerful states is to "direct cyber research at purely defensive applications" and aggressively pursue strategic cooperation[54] by exercising soft cyber deterrence theory in peer interactions.

[53] "Cyber Wars."
[54] Ibid.

Glossary

ABM	Anti-ballistic missile
ATCA	Asymmetric Threats Contingency Alliance
ATLAS	Active Threat Level Analysis System
BMD	Ballistic missile defense
BPA	Basic Principles Agreement
BPS	Bits per second
BSA	Business Software Alliance
C&C Server	Command and Control Server
C2W	Command and Control Warfare
C4ISR	Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance
CCD COE	Cooperative Cyber Defense Center of Excellence
CDL	Cyber Defense League
CDU	Cyber Defense Unit
CERT	Computer Emergency Response Team
CERT-EE	Computer Emergency Response Team – Estonia
CERT-FR	Computer Emergency Response Team – France
CERT-PL	Computer Emergency Response Team – Poland
CIIP	Critical Information Infrastructure Protection
CIS	Commonwealth of Independent States
CJCS	Chairman of the Joint Chiefs of Staff
CMS	Content management system
CNE	Computer network exploitation
CNO	Computer network operations

CPU	Central processing unit
CSS	Cyber security strategy
CVSS	Common Vulnerability Scoring System
DDoS	Distributed denial of service
DNS	Domain name system
DoD	Department of Defense
DoS	Denial of service
DV	Dependent variable
EIC	Estonian Informatics Centre
ENISA	European Network and Information Security Agency
EU	European Union
EW	Electronic warfare
FOC	Full operating capacity
GB	Gigabyte
HLS	Homeland Security
HSPD	Homeland Security Presidential Directive
IA	Information assurance
ICBM	Intercontinental ballistic missile
ICMP	Internet control message protocol
IO	Information operations
IT	Information technology
IP	Internet protocol
IRBM	Intermediate range ballistic missile
ISP	Internet service provider
IV	Independent variable

IW	Information warfare
JCS	Joint Chiefs of Staff
JP	Joint Publication
KPPS	Thousand packets per second
LOAC	Law of Armed Conflict
MAD	Mutual assured destruction
MB	Megabyte
MBPS	Megabits per second
MFA	Ministry of Foreign Affairs
MILDEC	Military deception
MPPS	Million packets per second
NATO	North Atlantic Treaty Organization
NCIRC	NATO Computer Incident Response Capability
NMS	National Military Strategy
NSA	National Security Agency
NSC	National Security Council
NSS	National Security Strategy
NRC	National Resource Council
NVD	National Vulnerability Database
OPSEC	Operations security
OSCE	Organization for Security and Co-operation in Europe
PC	Personal computer
PDD	Presidential Decision Directive
PDoS	Permanent denial of service
PPS	Packets per second

PSYOP	Psychological operations
PTBT	Partial Test Ban Treaty
QDR	Quadrennial Defense Review
RAM	Rational actor model
RBN	Russian Business Network
RDBMS	Relational Database Management Systems
SALT	Strategic Arms Limitations Talk
SANS Institute	SysAdmin, Audit, Network, Security
SDI	Strategic Defense Initiative
SIGINT	Signals intelligence
SIW	Strategic information warfare
SQL	Structured query language
TB	Terabyte
TCP	Transmission control protocol
UAV	Unmanned aerial vehicle
UDP	User datagram protocol
UN	United Nations
URL	Uniform Resource Locator
U.S.	United States
US-CCU	U.S. Cyber Consequences Unit
USCYBERCOM	U.S. Cyber Command
USSTRATCOM	U.S. Strategic Command
USSR	Union of Soviet Socialist Republics
WMD	Weapon of mass destruction
WWII	World War II

XSS	Cross-site scripting

Bibliography

08 Piracy Study. Business Software Alliance, May 2008. http://global.bsa.org/globalpiracy2008/studies/globalpiracy2008.pdf.

"2007 Cyber Attack on Estonia Launched by Kremlin-backed Youth Group." *Homeland Security News Wire*, March 13, 2009. http://www.homelandsecuritynewswire.com/2007-cyber-attack-estonia-launched-kremlin-backed-youth-group.

2007 Global Software Piracy Study. Business Software Alliance, May 2008. http://global.bsa.org/idcglobalstudy2007/studies/summaryfindings_globalstudy07.pdf.

"4 Steps to Defeat a DDoS Attack on Your Organisation." *The Data Chain*, n.d. http://www.thedatachain.com/articles/2011/8/4_steps_to_defeat_a_ddos_attack_on_your_organisation.

"A Digital Agenda for Europe." European Commission, May 19, 2012. http://ec.europa.eu/information_society/digital-agenda/documents/digital-agenda-communication-en.pdf.

A Preliminary Report on the Cyber Norms Workshop. Cambridge, MA: Massachusetts Institute of Technology, October 2011. http://ecir.mit.edu/events/conferences/184-cyber-norms-conference.

Adair, Stephen. "Georgian Attacks: Remember Estonia?" *Shadowserver*, August 13, 2008. http://www.shadowserver.org/wiki/pmwiki.php/Calendar/20080906.

———. "Georgian Websites Under Attack - DDoS and Defacement." *Shadowserver*, August 11, 2008. http://www.shadowserver.org/wiki/pmwiki.php/Calendar/20080906.

———. "The Website for the President of Georgia Under Attack - Politically Motivated?" *Shadowserver*, July 20, 2008. http://www.shadowserver.org/wiki/pmwiki.php/Calendar/20080720.

Air, Space, & Cyberspace Power in the 21st Century. The Institute for Foreign Policy Analysis, Inc., 2010.

Allison, Graham T. *Essence of Decision: Explaining the Cuban Missile Crisis*. 2nd. ed. New York: Longman, 1999.

Alperovitch, Dmitri. "Towards Establishment of Cyberspace Deterrence Strategy." In *3rd International Conference on Cyber Conflict*, 87– 94. Tallinn, Estonia, 2011. http://www.ccdcoe.org/publications/2011proceedings/TowardsEstablishmentOfCyberstapeDeterrenceStrategy-Alperovitch.pdf.

Andenaes, Johannes. *Punishment and Deterrence*. Ann Arbor: University of Michigan Press, 1974.

———. "General Prevention – Illusion or Reality?" *Journal of Criminal Law, Criminology and Police Science* 43 (1952): 176-198.

Appel, James B., and Neil J. Peterson. "What's Wrong with Punishment." *Journal of Criminal Law, Criminology and Police Science* 56 (1965): 450.

Armin, Jart. “RBN-Georgia Cyberwarfare-Continuation...” *Russian Business Network (RBN)*, August 2008. http://rbnexploit.blogspot.com/2008/08/rbn-georgia-cyberwarfare-continuation.html.

Arnold, Chloe. “Russian Group’s Claims Reopen Debate on Estonian Cyberattacks.” *RadioFreeEurope/RadioLiberty*, March 30, 2009, sec. Features. http://www.rferl.org/content/Russian_Groups_Claims_Reopen_Debate_On_Estonian_Cyberattacks_/1564694.html.

“Avoiding Social Engineering and Phishing Attacks.” *United States Computer Emergency Readiness Team*, October 22, 2009. http://www.us-cert.gov/cas/tips/ST04-014.html.

Ball, John C. “The Deterrence Concept in Criminology and Law.” *Journal of Criminal Law, Criminology and Police Science* 46 (1955): 347–354.

Barnett, Roger W. “Information Operations, Deterrence, and the Use of Force.” *Naval War College Review* 50, no. 2 (1998): 7–19.

Beccaria, Cesare. *On Crimes and Punishments*. Translated by Henry Paolucci. The Bobbs-Merrill Company, Inc., 1963. http://www.questia.com/PM.qst?a=o&d=9061406#.

Becker, Gary S. “Crime and Punishment: An Economic Approach.” *Journal of Political Economy* 76, no. 2 (March 1, 1968): 169–217.

“Behind the Estonia Cyberattacks.” *RadioFreeEurope/RadioLiberty*, March 6, 2009. http://www.rferl.org/content/Behind_The_Estonia_Cyberattacks/1505613.html.

Beidleman, Scott W. *Defining and Deterring Cyber War*. Carlisle Barracks, PA: U.S. Army War College, June 1, 2009. http://www.hsdl.org/?view&did=28659.

Ben-Porat, Udi, Anat Bremler-Barr, and Hanoch Levy. “Evaluating the Vulnerability of Network Mechanisms to Sophisticated DDoS Attacks.” In *INFOCOM 2008. The 27th Conference on Computer Communications. IEEE*, 11, 2008.

Bentham, Jeremy. *An Introduction to the Principles of Morals and Legislation*. Oxford: Clarendon Press, 1996.

Billo, Charlies G., and Welton Chang. *Cyber Warfare: An Analysis of the Means and Motivations of Selected Nation States*. Institute for Security Technology Studies at Dartmouth College, December 2004. http://www.ists.dartmouth.edu/docs/cyberwarfare.pdf.

Blank, Stephen. “Can Information Warfare Be Deterred?” *Defense Analysis* 17, no. 2 (August 2001): 121–138.

Bodeau, Deborah J., and Richard Graubart. *Cyber Resiliency Engineering Framework*. MITRE, September 2011. http://www.mitre.org/work/tech_papers/2012/11_4436/11_4436.pdf.

Brodie, Bernard. *The Absolute Weapon*. New York: Harcourt, Brace and company, 1946.

Bumgarner, John, and Scott Borg. *Overview by the US-CCU of the Cyber Campaign Against Georgia in August of 2008*. U.S. Cyber Consequences

Unit, August 2009. http://www.registan.net/wp-content/uploads/2009/08/US-CCU-Georgia-Cyber-Campaign-Overview.pdf.
Bunn, M.E. “Can Deterrence Be Tailored?” *Strategic Forum*, no. 225 (January 2007): 8.
Carr, Jeff. *Russia/Georgia Cyber War - Findings and Analysis*. Project Grey Goose, October 17, 2008. http://www.scribd.com/doc/6967393/Project-Grey-Goose-Phase-I-Report.
Carr, Jeffrey. *Inside Cyber Warfare*. 1st ed. Sebastopol, CA: O’Reilly Media, 2010.
Cavelty, Myriam Dunn. “Critical Information Infrastructure Vulnerabilities, Threats and Responses.” *ICTs and International Security* Three (2007): 15–33.
CCD COE. “Cyber Defense,” n.d. http://www.ccdcoe.org/.
“CERT-EU,” n.d. http://cert.europa.eu/cert/plainedition/en/cert_about.html.
CERT-EU, “RFC 2350.” October 25, 2011. http://cert.europa.eu/static/RFC2350/RFC2350_CERT-EU_v1_0.pdf.
“Cesare Lombroso.” *Jewish Virtual Library*, 2008. http://www.jewishvirtuallibrary.org/jsource/judaica/ejud_0002_0013_0_12733.html.
Chairman of the Joint Chiefs of Staff. *The National Military Strategy for Cyberspace Operations*. Washington, D.C.: Joint Chiefs of Staff, December 2006.
———. *The National Military Strategy of the United States of America*. Washington, D.C.: Joint Chiefs of Staff, 2004. http://www.defense.gov/news/Mar2005/d20050318nms.pdf.
———. *The National Military Strategy of the United States of America*. Washington, D.C.: Joint Chiefs of Staff, February 2011.
Chamberlain, Nigel. “Cyber Warfare and NATO.” *NATO Watch*, June 14, 2012. http://www.natowatch.org/node/723.
Charlton, Michael. *From Deterrence to Defence: The Inside Story of Strategic Policy*. Cambridge, MA: Harvard University Press, 1987.
Chayes, Abram, and Antonia Handler Chayes. *The New Sovereignty: Compliance with International Regulatory Agreements*. Cambridge, MA: Harvard University Press, 1995.
Cimbala, Stephen J. *Strategy After Deterrence*. New York: Praeger, 1991.
“Cisco IOS TCP Connection Reset Denial of Service Vulnerability.” *Secunia Stay Secure*, n.d. http://secunia.com/advisories/11440/.
Clark, David D., and Susan Landau. “Untangling Attribution.” In *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy*, 25–40. Washington, D.C.: The National Academies Press, 2010. http://www.nap.edu/catalog.php?record_id=12997#toc.
Clarke, Richard A. *Cyber War: The Next Threat to National Security and What to Do About It*. 1st ed. New York: Ecco, 2010.

Clarke, Ronald V. “Situational Crime Prevention.” In *Building a Safer Society: Strategic Approaches to Crime Prevention*, 91–150. Crime and Justice v. 19. Chicago: University of Chicago Press, 1995.

———. *Situational Crime Prevention: Successful Case Studies*. 2nd ed. Criminal Justice Press, 1997.

Common Application Security Vulnerabilities. DAS EISPD - Enterprise Security Office, April 8, 2008. http://www.oregon.gov/DAS/EISPD/ESO/docs/ESO_App_Sec_Vulns.pdf?ga=t.

“Common Vulnerabilities and Exposures (CVE),” n.d. http://cve.mitre.org/.

“Convention on Cybercrime: Member States,” May 23, 2012. http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=ENG.

Cooper, Jeffrey R. *New Approaches to Cyber-Deterrence: Initial Thoughts on a New Framework*. SAIC, December 29, 2009. http://www.americanbar.org/content/dam/aba/migrated/2011_build/law_national_security/new_approaches_to_cyber_deterrence.authcheckdam.pdf.

Corbin, Kenneth. *Lessons from the Russia-Georgia Cyberwar*. United Kingdom: The Institute of Communications Studies, University of Leeds, n.d. http://ics-www.leeds.ac.uk/papers/vp01.cfm?outfit=gdr&folder=442&paper=750.

Corrin, Amber. “NATO Cyber Defense Lags.” *Federal Computer Week*, February 2, 2012. http://fcw.com/articles/2012/02/02/nato-cyber-defense-lagging.aspx.

“Coulomb Force.” *Britannica Online Encyclopedia*, n.d. http://www.britannica.com/EBchecked/topic/140084/Coulomb-force.

Council of Europe. “Convention on Cybercrime,” November 23, 2001. http://conventions.coe.int/Treaty/en/Treaties/html/185.htm.

Critical Infrastructure Protection: Challenges for Selected Agencies and Industry Sectors. Report to the Committee on Energy and Commerce, House of Representatives. Washington, D.C.: General Accounting Office, February 2003. http://www.gao.gov/new.items/d03233.pdf.

Cullen, Francis T. *Correctional Theory: Context and Consequences*. Thousand Oaks, CA: SAGE, 2012.

Cusson, Maurice. “Situational Deterrence: Fear During the Criminal Event.” *Crime Prevention Studies* 1 (1993): 55–68.

“Cyber Wars.” *ChicagoTribune.com*, June 24, 2012. http://www.chicagotribune.com/news/opinion/editorials/ct-edit-cyber-0624-jm-20120624,0,1667062.story.

“Cybercrime: a Threat to Democracy, Human Rights and the Rule of Law.” *Council of Europe*, n.d. http://www.coe.int/web/coe-portal/what-we-do/rule-of-law/cybercrime.

Czosseck, Christian, and Karlis Podins. *An Usage-centric Botnet Taxonomy*. Tallinn, Estonia, n.d. http://www.ccdcoe.org/articles/2011/Czosseck_Podins_An_Usage-Centric_Botnet_Taxonomy.PDF.

Danchev, Dancho. “Coordinated Russia Vs Georgia Cyber Attack in Progress.” *ZDNet*, August 11, 2008. http://www.zdnet.com/blog/security/coordinated-russia-vs-georgia-cyber-attack-in-progress/1670.

———. “DDoS Attack Graphs from Russia Vs Georgia’s Cyberattacks.” *Dancho Danchev’s Blog - Mind Streams of Information Security Knowledge*, October 15, 2008. http://ddanchev.blogspot.com/2008/10/ddos-attack-graphs-from-russia-vs.html.

———. “Georgia President’s Web Site Under DDoS Attack from Russian Hackers.” *ZDNet*, July 22, 2008. http://www.zdnet.com/blog/security/georgia-presidents-web-site-under-ddos-attack-from-russian-hackers/1533.

———. “The Russia Vs Georgia Cyber Attack.” *Dancho Danchev’s Blog - Mind Streams of Information Security Knowledge*, August 11, 2008. http://ddanchev.blogspot.com/2008/08/russia-vs-georgia-cyber-attack.html.

———. “Who’s Behind the Georgia Cyber Attacks?” *Dancho Danchev’s Blog - Mind Streams of Information Security Knowledge*, August 14, 2008. http://ddanchev.blogspot.com/2008/08/whos-behind-georgia-cyber-attacks.html.

Davis, Joshua. “Hackers Take Down the Most Wired Country in Europe.” *Wired Magazine*, August 21, 2007. http://www.wired.com/politics/security/magazine/15-09/ff_estonia?currentPage=all.

Department of Defense. *Department of Defense Cyberspace Policy Report - A Report to Congress Pursuant to the National Defense Authorization Act for Fiscal Year 2011, Section 934*. Washington, D.C.: Department of Defense, November 2011. http://www.washingtonpost.com/wp-srv/world/documents/cyberspace-policy-report.html.

———. *Department of Defense Strategy for Operating in Cyberspace*. Washington, D.C.: Department of Defense, July 2011. http://www.defense.gov/home/features/2011/0411_cyberstrategy/docs/DoD_Strategy_for_Operating_in_Cyberspace_July_2011.pdf.

———. *Deterrence Operations Joint Operating Concept*. Washington, D.C.: Department of Defense, December 2006.

———. *Quadrennial Defense Review Report*. Washington, D.C.: Department of Defense, February 6, 2006.

———. *Quadrennial Defense Review Report*. Washington, D.C.: Department of Defense, February 2010.

Department of Homeland Security. *National Cyber Incident Response Plan - Interim Version*. Washington, D.C.: Department of Homeland Security, September 2010. http://www.federalnewsradio.com/pdfs/NCIRP_Interim_Version_September_2010.pdf.

van Dijk, Jan J.M., and Jaap de Waard. “A Two-Dimensional Typology of Crime Prevention Projects; With a Bibliography.” *Criminal Justice Abstracts* 23, no. 3 (September 1991): 483–503.

Dogrul, Murat, Adil Aslan, and Eyyup Celik. “Developing an International Cooperation on Cyber Defense and Deterrence Against Cyber Terrorism.” In *3rd International Conference on Cyber Conflict*, 29–43, 2011. http://www.ccdcoe.org/publications/2011proceedings/DevelopingAnInternationalCooperation...-M.%20Dogrul-Aslan-Celik.pdf.

Dougherty, James E., and Robert L. Pfaltzgraff. *Contending Theories of International Relations: A Comprehensive Survey*. New York: Longman, 2001.

Elder, Miriam. “Polishing Putin: Hacked Emails Suggest Dirty Tricks by Russian Youth Group.” *The Guardian*, February 7, 2012. http://www.guardian.co.uk/world/2012/feb/07/putin-hacked-emails-russian-nashi.

Engsberg, Mark. “An Introduction to Sources for Treaty Research.” *Hauser Global Law Program*, March 2006. http://www.nyulawglobal.org/Globalex/Treaty_Research.htm#_B._Treaties_and_International Agree.

“ENISA - Securing Europe’s Information Society — ENISA,” n.d. http://www.enisa.europa.eu/.

“Estonia Hit by ‘Moscow Cyber War.’” *BBC*, May 17, 2007, sec. Europe. http://news.bbc.co.uk/2/hi/europe/6665145.stm.

“European Defence Information - Estonia.” *Armedforces*, 2012. http://www.armedforces.co.uk/Europeandefence/edcountries/countryestonia.htm.

“European Union (EU) Forms CERT Group to Fight Cyber Attacks.” *International ICT Policies and Strategies*, June 18, 2011. http://ictps.blogspot.com/2011/06/european-union-eu-forms-cert-group-to.html.

“European Union Needs Common Cyber Policy.” *Estonian Ministry of Foreign Affairs*, March 22, 2012. http://www.vm.ee/?q=en/node/14012.

Van Evera, Stephen. *Guide to Methods for Students of Political Science*. Ithaca: Cornell University Press, 1997.

Finkle, Jim, and Noel Randewich. “Experts Warn of Shortage of U.S. Cyber Pros.” *Reuters*. New York, June 13, 2012. http://www.reuters.com/article/2012/06/13/us-media-tech-summit-symantec-idUSBRE85B1E220120613.

Finn, Peter. “Cyber Assaults on Estonia Typify a New Battle Tactic.” *The Washington Post*, May 19, 2007. http://www.washingtonpost.com/wp-dyn/content/article/2007/05/18/AR2007051802122_pf.html.

Finnegan, Daniel. “Cyber Attacks: History and Scenarios,” United States Naval Academy, 2011.

Finnemore, Martha. “Cultivating International Cyber Norms.” In *America’s Cyber Future*, 89–102. Center for a New American Security, 2011.

Fleury, Terry, Himanshu Khurana, and Von Welch. “Towards a Taxonomy of Attacks Against Energy Control Systems.” In *Proceedings of the IFIP International Congerence on Critical Infrastructure Protection*, 2003. http://www.ncsa.illinois.edu/People/hkhurana/IFIP_CIP_08.pdf.

Foucault, Michel. *Discipline and Punish: The Birth of the Prison*. 1st American ed. New York: Pantheon Books, 1977.

Freedman, Lawrence. *Deterrence*. Malden, MA: Polity Press, 2004.

———. *The Evolution of Nuclear Strategy*. Vol. 3. Basingstoke, Hampshire England; New York: Palgrave Macmillan, 2003.

French, G.S. *Building a Deterrence Policy Against Strategic Information Warfare*. DTIC Document, 2002. http://www.dodccrp.org/events/2002_CCRTS/Tracks/pdf/061.PDF.

“Further Escalation in the Estonian Relationship.” *InfoNIAC.com*, May 4, 2007. http://www.infoniac.com/breaking/chronology-of-the-events-in-tallinn-estonia.html.

Garthoff, Raymond L. *Détente and Confrontation: American-Soviet Relations from Nixon to Reagan*. Brookings Institution Press, 1985.

Geers, Kenneth. *Strategic Cyber Security*. NATO Cooperative Cyber Defence Centre of Excellence, June 2011. http://www.ccdcoe.org/publications/books/Strategic_Cyber_Security_K_Geers.PDF.

George, Alexander L., and Richard Smoke. *Deterrence in American Foreign Policy: Theory and Practice*. New York: Columbia University Press, 1974.

“Georgia Hackers Strike Apart from Russian Military.” *The Washington Times*, August 19, 2008. http://www.washingtontimes.com/news/2008/aug/19/georgia-hackers-strike-apart-from-russian-military/.

“Georgia Military Strength.” *Global Firepower*, n.d. http://www.globalfirepower.com/country-military-strength-detail.asp?country_id=Georgia.

Gibbs, J.P. “Assessing the Deterrence Doctrine: A Challenge for the Social and Behavioral Sciences.” *American Behavioral Scientist* 22, no. 6 (July 1, 1979): 653–677.

Gibbs, Jack P. *Crime, Punishment, and Deterrence*. New York: Elsevier, 1975.

Gillin, John Lewis. *Criminology and Penology*. New York, London: The Century Co., 1926.

Gilling, Daniel. *Crime Prevention: Theory, Policy, and Politics*. London: UCL Press, 1997.

Glaser, Charles L. *Deterrence of Cyber Attacks and US National Security*. The George Washington University, 2011. http://www.cspri.seas.gwu.edu/Seminar%20Abstracts%20and%20Papers/2011-5%20Cyber%20Deterrence%20and%20Security%20Glaser.pdf.

Goldsmith, Jack. “Cybersecurity Treaties: A Skeptical View.” *Hoover Institution*, 2011. http://www.scribd.com/doc/57295186/Cybersecurity-Treaties-A-Skeptical-View-by-Jack-Goldsmith.

Goodman, Will. “Cyber Deterrence: Tougher in Theory Than in Practice?” *Strategic Studies Quarterly* 4, no. 3 (Fall 2010).

Government of Georgia. *Basic Facts: Consequences of Russian Aggression in Georgia*. Russian Invasion of Georgia. Government of Georgia, August 5, 2009. http://georgiaupdate.gov.ge/en/doc/10006881/Microsoft%20Word%20-%20CYBERWAR%20short%20version_111008.pdf.

———. *Chronology of Russian Aggression in Georgia*. Georgia Update - Backgrounders. Government of Georgia, June 19, 2009. http://georgiaupdate.gov.ge/en/doc/10006881/Microsoft%20Word%20-%20CYBERWAR%20short%20version_111008.pdf.

———. *Russian Cyberwar on Georgia*. Russian Invasion of Georgia. Government of Georgia, November 10, 2008. http://georgiaupdate.gov.ge/en/doc/10006881/Microsoft%20Word%20-%20CYBERWAR%20short%20version_111008.pdf.

Gray, Colin S. *Maintaining Effective Deterrence*. Carlisle Barracks, PA: Strategic Studies Institute, U.S. Army War College, 2003.

Green, Philip. *Deadly Logic: The Theory of Nuclear Deterrence*. Columbus: Ohio State University Press, 1966.

Greenberg, Andy. “Shopping For Zero-Days: A Price List For Hackers’ Secret Software Exploits - Forbes.” *Forbes*, March 23, 2012. http://www.forbes.com/sites/andygreenberg/2012/03/23/shopping-for-zero-days-an-price-list-for-hackers-secret-software-exploits/.

Gupta, Upasana. “NSA Launches Cyber Operations Program.” *WebGuard*, June 14, 2012. http://web-guard.blogspot.com/2012/06/nsa-launches-cyber-operations-program.html.

Harknett, Richard J., John P. Callaghan, and Rudi Kauffman. “Leaving Deterrence Behind: War-Fighting and National Cybersecurity.” *Journal of Homeland Security and Emergency Management* 7, no. 1 (January 1, 2010).

Harknett, Richard J. “Information Warfare and Deterrence.” *Parameters* (1996): 93–107.

Hathaway, Oona A., Rebecca Crootof, Philip Levitz, Haley Nix, Aileen Nowlan, William Perdue, and Julia Spiegel. “The Law of Cyber-Attack.” *California Law Review* (2012): 76.

Hayes, Richard E., and Gary F. Wheatley. *Information Warfare and Deterrence*. National Defense University, 1996.

Von Hentig, Hans. “Limits of Deterrence.” *Journal of the American Institute of Criminal Law and Criminology* 29, no. 4 (1938): 555–561.

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

Hughes, Gordon. *Understanding Crime Prevention: Social Control, Risk, and Later Modernity*. Buckingham: Open University Press, 1998.

Huth, Paul, and Bruce Russett. “Testing Deterrence Theory: Rigor Makes a Difference.” *World Politics* 42, no. 4 (July 1, 1990): 466–501.

“ICMP.” *Wedpodeia*, n.d. http://www.webopedia.com/TERM/I/ICMP.html.

IFPA-Fletcher Conference, and Fletcher School of Law and Diplomacy. *Nuclear & Non-Nuclear Forces in Twenty-First-Century Deterrence: Final Report*. Cambridge, MA: Institute for Foreign Policy Analysis, 2006.

"IT Security Threat Summary for H1 2007: Social Engineering, Bank Scams, Cyber War and Mobile Spyware," n.d. http://www.f-secure.com/export/sites/fs_global_site/2007/1/WrapUp_H1_2007.pdf.

Jaishankar, D. "'Soft Deterrence' and the Future of Nuclear Disarmament." *CLAWS Journal*, Summer 2008 (n.d.).

Jeffery, C.R. "Criminal Behavior and Learning Theory." *Journal of Criminal Law, Criminology and Police Science* 56 (1965): 294–300.

Jervis, Robert, Richard Ned Lebow, and Janice Gross Stein. *Psychology and Deterrence*. Baltimore, MD: Johns Hopkins University Press, 1985.

Jervis, Robert. "Review: Deterrence Theory Revisited; Deterrence in American Foreign Policy: Theory and Practice." *World Politics* 31, no. 2 (January 1979): 289–324.

Johnson, L. Scott. "Toward a Functional Model of Information Warfare." *Central Intelligence Agency*, June 27, 2008. https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/97unclass/warfare.html.

Johnson, Mike. "Georgian Websites Under Attack - Don't Believe the Hype." *Shadowserver*, n.d. http://www.shadowserver.org/wiki/pmwiki.php/Calendar/20080906.

Joint Chiefs of Staff. "Joint Publication 3-13: Information Operations." Joint Chiefs of Staff, February 13, 2006.

"Joint Publication 1-02, Department of Defense Dictionary of Military and Associated Terms." U.S. Department of Defense, September 8, 2010. http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf.

Jones, Roy E. *Nuclear Deterrence: A Short Political Analysis*. London: Routledge & K. Paul, 1968.

Joseph S. Nye, Jr. *Cyber Power*. Harvard Kennedy School: Belfer Center for Science and International Affairs, May 2010. http://belfercenter.ksg.harvard.edu/files/cyber-power.pdf.

———. "Nuclear Lessons for Cyber Security." *Strategic Studies Quarterly* 5, no. 4 (2011): 18–38.

———. "Power and National Security in Cyberspace." In *America's Cyber Future: Security and Prosperity in the Information Age*, II:7–23. Center for a New American Security, 2011.

Käärman, Lembe. *X-Road Regulations*. mandator, December 19, 2006. http://ftp.ria.ee/pub/x-tee/doc/X-Road_regulations.pdf.

Kaeo, Merike. "Cyber Attacks on Estonia Short Synopsis," n.d. http://www.doubleshotsecurity.com/pdf/NANOG-eesti.pdf.

Kahn, Herman. *On Thermonuclear War*. Princeton, N.J.: Princeton University Press, 1960.

Kanet, Roger E., and Edward A. Kolodziej, eds. *The Cold War as Cooperation*. Baltimore: Johns Hopkins University Press, 1991.

Kastenberg, Joshua E. “Non-intervention and Neutrality in Cyberspace: An Emerging Principle in the National Practice of International Law,” 2009. http://findarticles.com/p/articles/mi_m6007/is_64/ai_n42124170/pg_12/.

Kennedy, David M. *Deterrence and Crime Prevention: Reconsidering the Prospect of Sanction*. Routledge Studies in Crime and Economics; vol. 2. London: Routledge, 2009.

Kerner, Sean Michael. “Estonia Under Russian Cyber Attack?” *InternetNews*, May 18, 2007. http://www.internetnews.com/security/article.php/3678606/Estonia+Under+Russian+Cyber+Attack.htm.

Kesan, Jay P., and Carol M. Hayes. *Thinking Through Active Defense in Cyberspace*. Illinois Public Law and Legal Theory Research Papers Series. University of Illinois College of Law, November 2010. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1691207.

Khachane, Atul. “How to Prevent HTTP Flood Attack from Your Dedicated Server.” *Web Hosting Issues*, August 24, 2010. http://webhostingissues.blogspot.com/2010/08/how-to-prevent-http-flood-attack-for.html.

Kissinger, Henry A. “Force and Diplomacy in the Nuclear Age.” *Foreign Affairs* 34, no. 3 (April 1, 1956): 349–366.

Korns, Stephen W. “Botnets Outmaneuvered: Georgia’s Cyberstrategy Disproves Cyberspace Carpet-bombing Theory.” *Armed Forces Journal* (n.d.). http://www.armedforcesjournal.com/2009/01/3801084/.

Krebs, Brian. “Report: Russian Hacker Forums Fueled Georgia Cyber Attacks.” *Washington Post*, October 16, 2008. http://voices.washingtonpost.com/securityfix/2008/10/report_russian_hacker_forums_f.html.

Kugler, Richard L. “Deterrence of Cyber Attacks.” In *Cyberpower and National Security*. 1st ed. Washington, D.C.: National Defense University Press, 2009.

Laasme, Häly. “Estonia: Cyber Window into the Future of NATO.” *Joint Force Quarterly*, no. 63 (2011): 58–63.

Landler, Mark, and John Markoff. “Digital Fears Emerge After Data Siege in Estonia.” *The New York Times*, May 29, 2007, sec. Technology. http://www.nytimes.com/2007/05/29/technology/29estonia.html.

Lefon, Rip Carroll. “Georgia and the Roki Tunnel.” *Bring the Heat, Bring the Stupid*, August 20, 2008. http://xbradtc.wordpress.com/2008/08/20/georgia-and-the-roki-tunnel/.

Lettow, Paul Vorbeck. *Ronald Reagan and His Quest to Abolish Nuclear Weapons*. 1st ed. New York: Random House, 2005.

Lewis, J.A. *Thresholds for Cyberwar*. Center for Strategic and International Studies, September 2010. http://csis.org/files/publication/101001_ieee_insert.pdf.

Lewis, James A. *A Note of the Laws of War in Cyberspace*. Center for Strategic and International Studies, April 2010.

http://csis.org/files/publication/100425_Laws%20of%20War%20Applicable%20to%20Cyber%20Conflict.pdf.
———. *Cyber Attacks Explained*. Washington, D.C.: Center for Strategic and International Studies, June 15, 2007. http://csis.org/files/media/csis/pubs/070615_cyber_attacks.pdf.
Lewis, James Andrew. *Fog of Cyberwar: Discouraging Deterrence*. Switzerland: International Relations and Security Network, 2009. http://www.isn.ethz.ch/isn/Current-Affairs/Special-Reports/The-Fog-of-Cyberwar/Deterrence/.
Libicki, Martin C. *Defending Cyberspace and Other Metaphors*. National Defense University, 1997. http://www.hsdl.org/?view&did=446854.
Libicki, Martin C., and Project Air Force. *Cyberdeterrence and Cyberwar*. Santa Monica, CA: Rand, 2009.
Lipson, Howard F. *Tracking and Tracing Cyber-Attacks: Technical Challenges and Global Policy Issues*. CERT Coordination Center, November 2002. http://www.sei.cmu.edu/reports/02sr009.pdf.
"Lisbon Summit Declaration: Issued by the Heads of State and Government Participating in the Meeting of the North Atlantic Council in Lisbon." *NATO*, November 20, 2010. http://www.nato.int/cps/en/natolive/official_texts_68828.htm.
Lombroso, Cesare. "Criminal Man," 1911. http://www.gutenberg.org/files/29895/29895-h/29895-h.htm.
Ma, Jason. "Information Operations to Play a Major Role in Deterrence Posture." *Inside Missile Defense*, December 10, 2003.
Martel, William C. "Deterrence and Alternative Images of Nuclear Possession." In *The Absolute Weapon Revisited: Nuclear Arms and the Emerging International Order*, 213–234. Ann Arbor: University of Michigan Press, 1998.
May, Ernest R., and National Security Council. *American Cold War Strategy: Interpreting NSC 68*. Boston: Bedford Books of St. Martin's Press, 1993.
McDonough, David S. "Tailored Deterrence: The 'New Triad' and the Tailoring of Nuclear Superiority." Canadian International Council, March 2009. http://www.canadianinternationalcouncil.org/download/resourcece/archives/strategicd~2/sd_no8_200.
McGhee, Joshua. "NATO and Cyber Defense: A Brief Overview and Recent Events." *Center for Strategic & International Studies*, July 8, 2011. http://csis.org/blog/nato-and-cyber-defense-brief-overview-and-recent-events.
McNeil, Jeff J. "Maturing International Cooperation to Address The Cyberspace Attack Attribution Problem." *ProQuest Dissertation & Theses*, May 2010.
"Megabytes, Gigabytes, Terabytes ... What Are They?" *What's A Byte?*, n.d. http://www.whatsabyte.com/.
Melchiorre, Mike, and Kenny Piccari. "The South Ossetia War," n.d. http://www.slideshare.net/guestb3370d/the-south-ossetia-war.

Menn, Joseph. “Hacked Companies Fight Back with Controversial Steps.” *Reuters*, June 18, 2012. http://www.reuters.com/article/2012/06/18/us-media-tech-summit-cyber-strikeback-idUSBRE85G07S20120618.

———. “US Firms Deploy Hacking ‘Strike Back’ Technology.” *iTnews*, June 18, 2012. http://www.itnews.com.au/News/305296,us-firms-deploy-hacking-strike-back-technology.aspx.

Michael, Alex. *Cyber Probing: The Politicisation of Virtual Attack*. Defence Academy of the United Kingdom, December 2010. http://www.voltairenet.org/IMG/pdf/Cyber_Probing.pdf.

Microsoft Security Intelligence Report: January Through June 2007. Microsoft Corporation, 2007.

Microsoft Security Intelligence Report: January Through June 2008. Microsoft Corporation, 2008.

“Military Statistics - Armed Forces Personnel by Country.” *NationMaster*, 2002 2001. http://www.nationmaster.com/graph/mil_arm_for_per-military-armed-forces-personnel.

Mitchell, Bradley. “Ping.” *Wireless/Networking*, n.d. ttp://compnetworking.about.com/od/network_ping/g/what-is-a-ping.htm.

———. “UDP.” *Wireless/Networking*, n.d. ttp://compnetworking.about.com/od/networkprotocolsip/g/udp-user-datagram-protocol.htm.

———. “What Is a DNS Server?” *About.com Wireless / Networking*, n.d. http://compnetworking.about.com/od/dns_domainnamesystem/f/dns_servers.htm.

Moore, Ryan J. “Prospects for Cyber Deterrence.” 2008.

Mora, Edwin. “Panetta Warns of Cyber Pearl Harbor: ‘The Capability to Paralyze This Country Is There Now.’” *CNS News*, June 13, 2012. http://cnsnews.com/news/article/panetta-warns-cyber-pearl-harbor-capability-paralyze-country-there-now.

Morgan, Patrick M. *Deterrence Now*. Cambridge, UK: Cambridge University Press, 2003.

Morgan, Patrick M. “Applicability of Traditional Deterrence Concepts and Theory to the Cyber Realm.” In *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy*, 55–76. Washington, D.C.: National Academy of Sciences, 2010. http://www.nap.edu/catalog.php?record_id=12997#toc.

Morozov, Evgeny. “An Army of Ones and Zeroes.” *Slate*, August 14, 2008. http://www.slate.com/articles/technology/technology/2008/08/an_army_of_ones_and_zeroes.html.

Nagin, Daniel. “Deterrence: Scaring Offenders Straight.” In *Correctional Theory: Context and Consequences*. SAGE, 2011. http://books.google.com/books?id=_dkMQVFmOFgC&pg=PA67&lpg=PA67&dq=nagin+deterrence%22scaring+offenders+straight%22&source=bl&ots=63AZMq2uhe&sig=lLh587P49j2hGFvGWiW0N35Snec&hl=en&sa=X&ei=BC8IT6XpDMHY0QHVm6XHAg&ved=0CDwQ6AEwBA#v=

onepage&q=nagin%20deterrence%22scaring%20offenders%20straight%22&f=false.
Nagorski, Andrew, ed. *Global Cyber Deterrence: Views from China, the U.S., Russia, India, and Norway*. EastWest Institute, 2010. http://www.ewi.info/system/files/CyberDeterrenceWeb.pdf.
"Nation's Cyber Strategy Is 'Broken,' USCYBERCOM Commander Says." *Defense Systems*, September 14, 2011. http://www.defensesystems.com/Articles/2011/09/14/AGG-USCYBERCOM-Alexander-cyber-strategy-broken.aspx.
National Research Council (U.S.). *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities*. Washington, D.C.: National Academies Press, 2009.
"National Security Agency/Central Security Service", n.d. http://www.nsa.gov/.
NATO Public Diplomacy Division. "Defending the Networks: The NATO Policy on Cyber Defence." 2011. http://www.nato.int/nato_static/assets/pdf/pdf_2011_09/20111004_110914-policy-cyberdefence.pdf.
"NATO - The North Atlantic Treaty." *NATO*, April 4, 1949. http://www.nato.int/cps/en/natolive/official_texts_17120.htm.
Nazario, Jose, and Andre M. DiMino. "An In-depth Look at the Georgia-Russia Cyber Conflict of 2008," n.d. http://www.shadowserver.org/wiki/uploads/Shadowserver/BTF8_RU_GE_DDOS.pdf.
Nazario, Jose. *Estonian DDoS Attacks – A Summary to Date*. DDoS and Security Reports. Arbor Networks Security, May 17, 2007. http://ddos.arbornetworks.com/2007/05/estonian-ddos-attacks-a-summary-to-date/.
———. "Georgia DDoS Attacks - A Quick Summary of Observations." DDoS and Security Reports: The Arbor Networks Security Blog. *Arborsert*, August 12, 2008. http://ddos.arbornetworks.com/2008/08/georgia-ddos-attacks-a-quick-summary-of-observations/.
———. "Political DDoS: Estonia and Beyond," presented at USENIX Security, 2008. http://static.usenix.org/events/sec08/tech/slides/nazario-slides.pdf.
———. "Politically Motivated Denial of Service Attacks." In *The Virtual Battlefield: Perspectives on Cyber Warfare*. Amsterdam: Ios Press, 2009.
"Nino Doijashvili." *Manta*, n.d. http://www.manta.com/g/mm7g533/nino-doijashvili.
Nitze, Paul H. "Atoms, Strategy and Policy." *Foreign Affairs* 34, no. 2 (January 1, 1956): 187–198.
Nye, Joseph S. *Power in the Global Information Age: From Realism to Globalization*. London: Routledge, 2004.
O'Hanlon, Michael E., and Kurt M. Campbell. *Hard Power: The New Politics of National Security*. New York: Basic Books, 2006.
Office of Homeland Security. *National Strategy For Homeland Security*. Washington, D.C.: The White House, July 2002.

Oorn, Reet. "'Cyber War' and Estonia: Legal Aspects." In *Information Technology in Public Administration of Estonia - Yearbook 2007*, 74–75. Tallinn, Estonia: Ministry of Economic Affairs and Communications, 2008. http://www.riso.ee/en/files/IT_yearbook_2007_final.pdf.

Ottis, Rain. "A Systematic Approach to Offensive Volunteer Cyber Militia". Tallinn Technical University, n.d. http://digi.lib.ttu.ee/i/?585.

———. "Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective." In *Proceedings of the 7th European Conference on Information Warfare and Security*, 163–168. Plymouth: Academic Publishing Limited, 2008.

"Packet." *Wireless/Networking*, n.d. http://compnetworking.about.com/od/networkprotocols/l/bldef_packet.htm.

Paloma, Jay. "What Is a UDP Flood Attack?" *Security Is a State of Mind*, November 14, 2005. ttp://msforums.ph/blogs/jpaloma/archive/2005/11/14/85576.aspx.

Paternoster, Raymond. "How Much Do We Really Know About Criminal Deterrence?" *Journal of Criminal Law and Criminology* 100, no. 3 (2010): 37.

Payne, Keith B. *Deterrence in the Second Nuclear Age*. Lexington, KY: University Press of Kentucky, 1996.

———. *The Great American Gamble: Deterrence Theory and Practice From the Cold War to the Twenty-first Century*. Fairfax, VA: National Institute Press, 2008.

Phillips, Steve. *Heinemann Advanced History: Cold War in Europe and Asia*. Heinemann Secondary Education, 2001.

Poulsen, Kevin. "'We Traced the Cyberwar — It's Coming From Inside the Country!'" *Wired*, January 24, 2008. http://www.wired.com/threatlevel/2008/01/we-traced-the-c/#previouspost.

Preatoni, Roberto. "The Lessons We Are NOT Going to Learn." Mi2g. *The Digital Bending of Estonia on Its Physical Knees - The Lessons We Are NOT Going to Learn*, June 2, 2007. http://www.mi2g.com/cgi/mi2g/frameset.php?pageid=http%3A//www.mi2g.com/cgi/mi2g/media.php.

"Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy." *The National Academies Press*, 2010. http://www.nap.edu/catalog.php?record_id=12997#toc.

Rattray, Gregory J. *Strategic Warfare in Cyberspace*. Cambridge, MA: MIT Press, 2001.

Raustiala, Kal. "Form and Substance in International Agreements." *American Journal of International Law* 99, no. 3 (July 2005): 581–614.

"RBN - Georgia Cyberwarfare - Attribution & Spam Botnets." *Russian Business Network (RBN)*, August 2008. http://rbnexploit.blogspot.com/2008/08/rbn-georgia-cyberwarfare-attribution.html.

"Regions and Territories: Abkhazia." *BBC*, March 12, 2012, sec. Europe. http://news.bbc.co.uk/2/hi/europe/3261059.stm.

Rhoads, Christopher. “Cyber Attack Vexes Estonia, Poses Debate.” *The Wall Street Journal*, May 18, 2007. http://online.wsj.com/article/SB117944513189906904-__3K97ags67ztibp8vLGPd70WXE_20070616.html.

“RIA Novosti Hit by Cyber-attacks as Conflict with Georgia Rages.” *RIA Novosti*, August 10, 2008. http://en.rian.ru/russia/20080810/115936419.html.

Richards, Jason. “Denial-of-Service: The Estonian Cyberwar and Its Implications for U.S. National Security.” *International Affairs Review*, n.d. http://www.iar-gwu.org/node/65.

Rid, Thomas. “Cyber War Will Not Take Place.” *Journal of Strategic Studies* (October 5, 2011): 1–28.

———. “Think Again: Cyberwar.” *Foreign Policy*, April 2012. http://www.foreignpolicy.com/articles/2012/02/27/cyberwar.

Rios, Billy K. “Sun Tzu Was a Hacker: An Examination of the Tactics and Operations from a Real World Cyber Attack.” In *The Virtual Battlefield: Perspectives on Cyber Warfare*. Amsterdam: Ios Press, 2009.

Rob, John. “When Bots Attack.” *Wired Magazine*, September 2007. http://www.wired.com/images/press/pdf/webwarone.pdf.

Ross, David O., and Robinson C. Ihle. “Successfully Managing Insurgencies and Terrorism Effectively (SMITE),” March 2011.

“Russia Conducts Cyber Attacks Against Georgia.” *Agence France-Presse*, August 20, 2008. http://technaute.cyberpresse.ca/nouvelles/internet/200808/13/01-19650-la-russie-mene-des-cyber-attaques-contre-la-georgie.php.

“Russia Military Strength.” *Global Firepower*, July 1, 2011. http://www.globalfirepower.com/country-military-strength-detail.asp?country_id=Russia.

Ruus, Kertu. “Cyber War I: Estonia Attacked from Russia.” *European Affairs* 9, no. 1 (Winter/Spring 2008).

Sachs, Marcus. “MPack Analysis.” *ISC Diary*, June 20, 2007. http://isc.sans.edu/diary.html?storyid=3015.

Sanger, David E. *Confront and Conceal: Obama’s Secret Wars and Surprising Use of American Power*. Crown, 2012.

Schelling, Thomas C. *Arms and Influence*. New Haven: Yale University Press, 1966.

———. *The Strategy of Conflict*. Cambridge, MA: Harvard University Press, 1960.

Schlesinger, James R. “Schlesinger’s Limited Nuclear Options.” *Air Force-Magazine.com* 89, no. 2 (February 2006): 3 Nov 09.

Schneier, Bruce. “The Vulnerabilities Market and the Future of Security.” *Forbes*, May 30, 2012. http://www.forbes.com/sites/bruceschneier/2012/05/30/the-vulnerabilities-market-and-the-future-of-security/.

“Science and Politics as Criminologists’ Vocations.” In *Contemporary Masters in Criminology/Edited by Joan McCordand John H. Laub*, 293–302. Plenum Series in Crime and Justice. New York: Plenum Press, 1995.

"Search Security." *TechTarget*, n.d. http://searchsecurity.techtarget.com/definition/distributed-denial-of-service-attack.

"Security Experts Admit China Stole Secret Fighter Jet Plans | The Australian." *CYBER SECURITY Forum Initiative - CSFI*, March 12, 2012.

Security, Estonia. Jane's Sentinel Security Assessment - Central Europe and the Baltic States. Jane's Information Group, June 16, 2010. http://jmsa.janes.com.

Shachtman, Noah. "'Cyberwar' Panic Over; Estonia Asks for Russian Help to Find Hackers." *Wired*, June 7, 2007. http://www.wired.com/dangerroom/2007/06/cyberwar_panic_/#previouspost.

———. "Estonia, Google Help 'Cyberlocked' Georgia (Updated)." *Wired*, August 11, 2008. http://www.wired.com/dangerroom/2008/08/civilge-the-geo/#previouspost.

Shackelford, Scott J. "From Nuclear War to Net War: Analogizing Cyber Attacks in International Law." *Berkeley Journal of International Law* 27, no. 1 (2009): 192–251.

Sharma, Amit. "Cyber Wars: A Paradigm Shift from Means to Ends." In *The Virtual Battlefield: Perspectives on Cyber Warfare*, 3–17. Amsterdam: Ios Press, 2009.

Snyder, Glenn Herald. *Deterrence and Defense*. Princeton, N.J.: Princeton University Press, 1961.

Socor, Vladimir. "'Nashi' Foray into Georgia Stopped in Time." *Eurasia Daily Monitor* 6, no. 74 (April 17, 2009).

"Spear Phishers." *The Federal Bureau of Investigation*, April 1, 2009. http://www.fbi.gov/news/stories/2009/april/spearphishing_040109.

"SQL Injection 2.0." *Computerdoctors*, n.d. http://www.mauskar.com/index.php/browse-news/11-news/40-sql-injection-20.

"SQL Injection Definition from PC Magazine Encyclopedia", n.d. http://www.pcmag.com/encyclopedia_term/0%2C2542%2Ct%3DSQL+injection&i%3D61172%2C00.asp#fbid=w_NKHxQxur_.

"SQL Injection Tutorial: Learn About SQL Injection Vulnerabilities and Prevention." *Veracode*, n.d. http://www.veracode.com/security/sql-injection.

Staff Writers. "Russia Lowers Official Death Toll from Georgia Conflict." *Space War*, September 11, 2008.

Statement of General Keith B. Alexander. Washington, D.C.: House Committee on Armed Services, n.d.

Stiennon, Richard. *Surviving Cyberwar*. Lanham, MD: Government Institutes, 2010.

STRATFOR. "Georgia, Russia: The Cyberwarfare Angle." *STRATFOR Global Intelligence*, August 12, 2008. http://www.stratfor.com/analysis/georgia_russia_cyberwarfare_angle.

"Stratgic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organisation." NATO, 2010. http://www.nato.int/lisbon2010/strategic-concept-2010-eng.pdf.
Summerfield, Morgan. "Evolution of Deterrence Crime Theory." *Associated Content*, May 18, 2006. http://www.associatedcontent.com/article/32600/evolution_of_deterrence_crime_theory.html?cat=37.
Sutherland, Edwin H. "Criminology," 1924. http://www.questia.com/PM.qst?a=o&d=27947981.
"TCP (Transmission Control Protocol)." *Search Networking*, March 15, 2012. http://searchnetworking.techtarget.com/definition/TCP.
"The Council of Europe in Brief." *Council of Europe*, n.d. http://www.coe.int/aboutCoe/index.asp?page=nepasconfondre&l=en.
"The Tech Terms Computer Dictionary," n.d. http://www.techterms.com/.
"The Top Cyber Security Risks." *Sans*, September 2009. http://www.sans.org/top-cyber-security-risks/.
The White House. *A National Security Strategy for A Global Age*. Washington, D.C.: The White House, December 2000.
———. *A National Security Strategy for a New Century*. Washington, D.C.: The White House, May 1997.
———. *A National Security Strategy for a New Century*. Washington, D.C.: The White House, October 1998.
———. *A National Security Strategy of Engagement and Enlargement*. Washington, D.C.: The White House, February 1995.
———. *Critical Foundations: Protecting America's Infrastructures, The Report of the President's Commission on Critical Infrastructure Protection*. Washington, D.C., October 1997. http://www.fas.org/sgp/library/pccip.pdf.
———. *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure*. The White House, May 2009.
———. *Homeland Security Presidential Directive-7*. Washington, D.C.: The White House, December 17, 2003. http://www.dhs.gov/xabout/laws/gc_1214597989952.shtm#1.
———. *International Strategy for Cyberspace - Prosperity, Security, and Openness in a Networked World*. Washington, D.C.: The White House, May 2011. http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.
———. *National Plan for Information Systems Protection: An Invitation to a Dialogue*. Washington, D.C., 2000.
———. *National Security Strategy*. Washington, D.C.: The White House, May 2010. http://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf.
———. *National Security Strategy of the United States*. Washington, D.C.: United States White House Office, March 2006.

———. “Presidential Decision Directive/NSC-63”. The White House, May 22, 1998. http://www.fas.org/irp/offdocs/pdd/pdd-63.htm.
———. “Remarks by the President on Securing Our Nation’s Cyber Infrastructure,” May 29, 2009. http://www.whitehouse.gov/the-press-office/remarks-president-securing-our-nations-cyber-infrastructure.
———. *The Comprehensive National Cybersecurity Initiative*. Washington, D.C.: The White House, March 2010.
———. *The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*. Washington, D.C.: The White House, February 2003.
———. *The National Strategy to Secure Cyberspace*. The White House, February 2003.
———. *Toward Deterrence in the Cyber Dimension: Report to the President’s Commission on Critical Infrastructure Protection*. The White House, 1997.
Thilek. “Estonia Cyber Attacks 2007,” December 28, 2009. http://meeting.afrinic.net/afrinic-11/slides/aaf/Estonia_cyber_attacks_2007_latest.pdf.
Thomas, T.L. “Deterring Information Warfare: A New Strategic Challenge.” *Parameters* 26, no. 4 (1996): 81–91.
Thomas, Timothy L. “Nation-state Cyber Strategies: Examples from China and Russia.” In *Cyberpower and National Security*. 1st ed. Washington, D.C.: National Defense University Press, 2009.
Thomson, Iain. “Russia ‘Hired Botnets’ for Estonia Cyber-war.” *V3*, May 31, 2007. http://www.v3.co.uk/v3-uk/news/1974750/russia-hired-botnets-estonia-cyber-war.
Tikk, Eneken, Kadri Kaska, Kristel Runnimeri, Mari Kert, Anna-Maria Taliharm, and Liis Vihul. *Cyber Attacks Against Georgia: Legal Lessons Identified*. Tallinn, Estonia: CCDCOE, November 2008. http://www.carlisle.army.mil/DIME/documents/Georgia%201%200.pdf.
Tikk, Eneken, Kadri Kaska, and Liis Vihul. *International Cyber Incidents: Legal Considerations*. Tallinn, Estonia: Cooperative Cyber Defence Centre of Excellence (CCD COE, 2010. http://www.ccdcoe.org/publications/books/legalconsiderations.pdf.
Toby, Jackson. “Is Punishment Necessary.” *Journal of Criminal Law, Criminology and Police Science* 55 (1964): 332–337.
Tonry, Michael H. *The Handbook of Crime & Punishment*. New York: Oxford University Press, 1998.
Traynor, Ian. “Russia Accused of Unleashing Cyberwar to Disable Estonia.” *Guardian*. Brussels, Belgium, May 16, 2007. http://www.guardian.co.uk/world/2007/may/17/topstories3.russia.
“U.S. Objectives With Respect to the USSR to Counter Soviet Threats to U.S. Security”, n.d.
“United States Cyber Command.” *United States Strategic Command*, n.d. http://www.stratcom.mil/.

"United States Strategic Command." *United States Strategic Command*, n.d. http://www.stratcom.mil/.

Vernetti, Gianmaria. *The Power of Networking: An Insight on the Russian Business Network*. The International Network of Civil Society Organizations for the Social Struggle Against Transational Organized Crime, July 1, 2010. http://flarenetwork.org/report/enquiries/article/the_power_of_networking_an_insight_on_the_russian_business_network.htm.

Viira, Toomas. "Cyber Attacks Against Estonia - Overview and Conclusions." In *Information Technology in Public Administration of Estonia - Yearbook 2007*, 71–73. Tallinn, Estonia: Ministry of Economic Affairs and Communications, 2008. http://www.riso.ee/en/files/IT_yearbook_2007_final.pdf.

Wasserstrom, R. "War, Nuclear War, and Nuclear Deterrence: Some Conceptual and Moral Issues." *Ethics* 95, no. 3 (1985): 424–444.

Waxman, Matthew C. "Cyber-Attacks and the Use of Force." *Yale Journal of International Law. LexisNexis Academic*, Summer 2011.

Webster's New World College Dictionary. Vol. 4. Foster City, CA, 2001.

Weis, Robin Tim. "Can NATO Adapt to Cyber Warfare?" *FrumForum*, November 29, 2011. http://www.frumforum.com/can-nato-adapt-to-cyber-warfare.

"What Is a Database." *Database Designs*, n.d. http://www.database-designs.com/DatabaseDefinition.html.

"What Is An IP Address." *What Is My IP .com*, n.d. http://www.whatismyip.com/faq/what-is-an-ip-address.asp.

"What Is Backdoor?" *Webopedia Computer Dictionary*, n.d. http://www.webopedia.com/TERM/B/backdoor.html.

"What Is Client-side?" *Webopedia Computer Dictionary*, n.d. http://www.webopedia.com/TERM/C/client_side.html.

Wingfield, Thomas C. "International Law and Information Operations." In *Cyberpower and National Security*. 1st ed. Washington, D.C.: National Defense University Press, 2009.

Wohlstetter, Albert. "The Delicate Balance of Terror." *Foreign Affairs* 37, no. 2 (January 1, 1959): 211–234.

Wolfgang, Marvin E. "The Just Deserts vs. the Medical Model." In *Contemporary Masters in Criminology/Edited by Joan McCord and John H. Laub*, 279–291. Plenum Series in Crime and Justice. New York: Plenum Press, 1995.

Wong, Tiong Pern. "Active Cyber Defense: Enhancing National Cyber Defense". Naval Postgraduate School, 2011. http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA556635.

Worden, S.P., and R.R Correll. *Responsive Space and Strategic Information*. National Defense University: DTIC Document, 2004.

X. "The Sources of Soviet Conduct." *Foreign Affairs* 25, no. 4 (July 1947): 566–582.

"X-Road e-Government Interoperability Framework," Tallinn, Estonia, 2011. http://www.cyber.ee/home/information-systems/X-Road_factsheet_2011.pdf.

"XSS Definition from PC Magazine Encyclopedia", n.d. http://www.pcmag.com/encyclopedia_term/0,2542,t=XSS&i=57401,00.asp#fbid=w_NKHxQxur_.

Yannakogeorgos, Panayotis. "Thought Leader Perspective: Dr. Panayotis Yannakogeorgos," August 25, 2011. http://www.nsci-va.org/SeniorLeaderPerspectives/2011-08-25-CyberPro-Pano%20Yannakogeorgos.pdf.

Zmijewski, Earl. "Georgia Clings to the Net." *Renesys*, August 10, 2008. http://www.renesys.com/blog/2008/08/georgia_clings_to_the_net.shtml.

Annex: A

Table A.1: Fleury et al's Taxonomy Applied to IVs

Attack			**Vulnerability**
Attribution (IV)	Offensive (IV) – Defensive (IV)		
Origin	*Action*	*Target*	*Vulnerability*
Local	Probe	Network	Configuration
Remote	Scan	Process	Specification
	Flood	System	Implementation
	Authenticate	Data	
	Bypass	User	
	Spoof		
	Eavesdrop		
	Misdirect		
	Read/Copy		
	Terminate		
	Execute		
	Modify		
	Delete		

Fleury et al's Taxonomy[1]

1) Attack
   a) Origin: location of attacker with respect to target
      i) Local: attack originates local to the target
      ii) Remote: originates outside the target site
   b) Action: activity the attack is performing on the target
      i) Probe: determine characteristics of a system
      ii) Scan: attempts to access targets sequentially to determine specific characteristics
      iii) Flood: repeatedly accessing or overloading the target's capacity, possibly disabling the target
      iv) Authenticate: attempt to perform unauthorized authentication as a valid user or process to access a target
      v) Bypass: use alternative method to access the target, bypassing standard access protocols
      vi) Spoof: attempt to assume the appearance of a different entity in the system to access the target
      vii) Eavesdrop: listen to a data stream and extract information
      viii) Misdirect: intercept proper communication channels and output bogus information

[1] Fleury, Khurana, and Welch, "Towards A Taxonomy of Attacks Against Energy Control Systems," 7–9. Fleury et al's Attack-Vulnerability-Damage (AVD) model has been adopted and as the taxonomy through which vulnerabilities across the cases to cyber offensive operations will be assessed. The "Damage" portion of the taxonomy has been omitted as this is less relevant to examination. These terms and definitions in this annex have been drawn in total from the Attack-Vulnerability-Damage (AVD) model.

ix) Read/Copy: In a “read” attack, the data would be read by a human, a “copy” attack duplicates the original data source for later processing
x) Terminate: stop a running process
xi) Execute: run a possibly malicious process on the target
xii) Modify: change the contents of the target
xiii) Delete: remove data from the target or make data impossible to retrieve

c) Target: describes the resource that is being attacked
   i) Network: consists of computers, switches, hubs, etc. connected via wires or wirelessly
   ii) Process: a program running of a computational device, may consist of the actual program as well as any data being accessed by the process
   iii) System: one or more connected components that can perform substantial computations
   iv) Data: consists of information suitable for processing by humans or machines. Data can refer to a single resource such as a file stored on a hard drive or the transmission of such data across a communications network.
   v) User: someone with authorized access to a system

2) Vulnerability: describes why an attack can be successful. The vulnerability does not specify the actual target that is vulnerable, but rather the weakness in the system than can be exploited
   a) Configuration: When a resource is improperly configured, a hacker can gain improper access.
   b) Specification: When a process or component has design flaws, these flaws can be used in unintended ways to gain access to the system.
   c) Implementation: Even when the design of a hardware or software system is correct, the implementation of the system may still be incorrect. This can lead to security holes.

Annex: B

Background of the Estonian Crisis

At the end of World War II (WWII), the Soviet Union and then Russia occupied Estonia from 1944 to 1991. The roots of the 2007 crisis stemmed from misperceptions surrounding Estonia's independence from Russia in 1991. Estonia considered independence, which Russia supported as did the Soviet Union, a return to its pre-WWII status. However, there remained a difference of opinion between Estonia and Russia in one important regard. Estonia held that its independence continued unabated from the pre-WWII era although it had been lost for a period because of its annexation by the Soviet Union. The Russian view was more conservative.

During the forty-seven-year Russian occupation, many Russians moved to Estonia to pursue economic opportunities and a greater quality of life. When the Soviet Union collapsed in 1989, ethnic Russians made up approximately 40 percent of Estonia's population of 1.3 million people. Unlike Latvia and Lithuania, which offered citizenship to their populations when the Union of Soviet Socialist Republics (USSR) dissolved, Estonia pursued a different path that contributed to dissent among ethnic Russians. The Estonian government continued to consider all non-ethnic Estonians foreigners. This meant that ethnic Russians desiring citizenship had to participate in a naturalization process, which further contributed to internal political instability.[2]

[2] Richards, "Denial-of-Service: The Estonian Cyberwar and Its Implications for U.S. National Security."

Despite political instability among its population, Estonian society was homogeneous in one regard – it was one of the world's first cyber societies. In the period leading to the 2007 cyber attacks, 98 percent of Estonians conducted their banking online and the majority of Estonians received their news online. The year after the attacks, 88 percent filed their income taxes online.

The Estonian government at all levels and the private sector heavily depended upon the Internet to function. For example, the government held paperless cabinet meetings, courts and law enforcement agencies relied upon a paperless e-case system, elections were computerized (although there is a paper option), doctors depended upon a national system to review medical records, and schools used an e-school system to communicate daily assignments and grades to students and parents.[3] It was the combination of this reliance upon the Internet to conduct public and private business with the undercurrent of political instability that made this crisis possible: The first created vulnerability, while the second led to the spark that ignited the situation.

Estonia – The Situation

The catalyst for the Estonia cyber war occurred on April 27, 2007 due to the government's relocation of the "Unknown Soldier," a Soviet WWII memorial in Tallinn.[4] The Estonian government debated the relocation for several years and ultimately decided to move the statue for domestic political reasons. This act angered Russia and many ethnic Russians living in Estonia.

[3] Ottis, "A Systematic Approach to Offensive Volunteer Cyber Militia," 183. Ottis defined a cyber society as one that is "based on ubiquitous computing and that a loss of these computer services directly affects the normal existence of [a] society." See page 182.
[4] The Tallinn statue is also commonly referred to as the "Bronze Soldier."

The Unknown Soldier statue, dedicated in 1947, stood over a site that included the interred remains of fourteen WWII Soviet soldiers.[5] For the Estonians, the statue was a constant reminder of foreign occupation. During the earlier years, they called it the "Unknown Rapist." In time, Estonians tolerated the memorial because the Russian Diaspora needed a location to "commemorate their fallen."[6]

Much of the tension arising from the relocation decision stemmed from the differing identities that Estonians and ethnic Russians placed on the statue. For ethnic Russians, including families of WWII veterans, the statue represented a liberator, while the Estonians identified it with an oppressor.[7] In the years immediately preceding the 2007 cyber attacks, the statue had "become a focal point of tension between pro-Kremlin and Estonian nationalist movements."[8] To diffuse this situation, the Estonian government decided to relocate the statue from a busy traffic intersection and to re-inter the remains in a military cemetery in Tallinn.[9]

Workers began to relocate the statue on April 26, 2007. Peaceful protests began during the day; however, in the evening hours, the crowd became larger and more violent. The protesters fought with police for a few hours before some

[5] *Security, Estonia*, Jane's Sentinel Security Assessment - Central Europe and the Baltic States (Jane's Information Group, June 16, 2010), http://jmsa.janes.com.
[6] Ruus, "Cyber War I: Estonia Attacked from Russia."
[7] Ottis, "Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective."
[8] Ibid.
[9] Ibid.

in their midst began to loot stores in the area around the original statue site. By the time dawn approached on April 27, the police had restored calm.[10]

On the 27th, protestors reemerged, but the clashes with police were much smaller than the previous day, yet still violent. During the rioting, six police officers and forty-four protestors were injured, and a 20-year-old man died from a stab wound.[11] In reflecting on the events of April 26–27, Heli Tiirmaa-Klaar, Estonian "cyber Tsar," recalled that his government was preoccupied with the immediate crisis surrounding the statue's relocation and were not concerned with "some geek coming and saying, 'Do you know we are under cyber attack as well?'"[12]

Domestic and international media coverage on the events of April 26 inflamed popular sentiment in Russia and further incited Estonia's ethnic-Russian community. The Russian media reported on the "police violence against peaceful protesters" with no attention to the precipitating actions of protestors. The nature of this reporting helped explain why many Russians felt compelled to participate in cyber attacks on Estonia.[13]

These events alarmed Hillar Aarelaid, director of Estonia's Computer Emergency Response Team (CERT), who knew from experience that "if there are

---

[10] Ibid.
[11] "Further Escalation in the Estonian Relationship," *InfoNIAC.com*, May 4, 2007, http://www.infoniac.com/breaking/chronology-of-the-events-in-tallinn-estonia.html. It was reported that the stabbing victim did not receive care for an hour, which contributed to his death.
[12] Michael, *Cyber Probing: The Politicisation of Virtual Attack*, 13.
[13] Ottis, "Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective," 163–168. Russian reporting fueled many angry articles and statements. Pro-Kremlin youth were incited to hold protests at Estonian embassy in Moscow, and on May 2, the Estonian ambassador was physically assaulted.

fights on the street, there are going to be fights on the Internet."[14] His fears were realized on April 27, 2007, when an Estonian government official discovered that Estonia was under cyber attack. These attacks continued for twenty-two days.

[14] Landler and Markoff, "Digital Fears Emerge After Data Siege in Estonia."

Annex: C

Background of the Georgian Crisis

Georgia first declared its independence from Russia in 1918 during the fog and friction of the Russian Revolution, which began in 1917. In 1921, several years after the revolution ended, the Red Army successfully invaded Georgia. Georgia remained a part of USSR until its collapse in 1991 when Georgia declared its independence for a second time.[15]

The collapse of the USSR also led to the rise of a separatist movement in South Ossetia. The 70,000 people in this region were not ethnic Georgians and spoke a different language. As South Ossetians "always felt more affinity with Russia than with Georgia," the demise of the Soviet Union fueled their effort to escape Georgian rule in the 1991–1992 war.[16]

Because of the 1991–1992 Georgian-Ossetian war, South Ossetia gained de facto independence from Georgia; however, "it remained commonly recognized by the international community as an integral part of Georgia." An Organization for Security and Co-operation in Europe (OSCE) peacekeeping force made up of Russian, Georgian, and South Ossentians under Russian command patrolled the region since its formation in 1992. The dispute remained unresolved from its origin through the eve of the 2008 war. Tensions continued

[15] Clarke, *Cyber War*, 17.
[16] Tikk et al., *Cyber Attacks Against Georgia: Legal Lessons Identified*, 32. South Ossetia is a "territory of about 4,000 sq km2 about 100 km north of the Georgian capital Tbilisi, on the southern slopes of the Caucasus Mountains." The people of this area share a strong bond with those of North Ossetia, which is on the Russian side of the border.

to grow due in part to lack of cooperation between these peacekeeping troops and their sponsoring governments.[17]

These tensions came to a head in early 2008 as conflict grew between Georgia and Russia over Abkhazia and South Ossetia.[18] Georgia considered these regions "breakaway territories," while Russia continued its long pattern of goading these regions to pursue independence.[19] Two events in March 2008 set the stage for impending armed conflict. First, on March 6 Russia withdrew from a 1996 Commonwealth of Independent States (CIS) agreement that prohibited it from having a relationship with Abkhazia. Second, on March 21 the Russian Duma decreed that the Russian government should "actively defend the rights of Russian citizens living in Abkhazia and South Ossetia and discuss the recognition [of] the independence of these breakaway territories."[20]

Within weeks, on April 16, 2008, Russian President Vladimir Putin "issued a decree instructing the Russian government to establish direct relations with the de facto authorities of Abkhazia and South Ossetia."[21] Through the remainder of April, the Russian peacekeeping contingent deployed to the Georgian-Abkhazian conflict zone increased in size. Between May and July,

---

[17] Tikk et al., *Cyber Attacks Against Georgia: Legal Lessons Identified*, 4.
[18] "Regions and Territories: Abkhazia," *BBC*, March 12, 2012, sec. Europe, http://news.bbc.co.uk/2/hi/europe/3261059.stm. Georgia considered Abkhazia a breakaway territory since Abkhazia declared independence in 1999. Abkhazia is in the "north-western corner of Georgia with the Black Sea to the south-west and the Caucasus mountains and Russia to the north-east."
[19] Stiennon, *Surviving Cyberwar*, 96.
[20] Government of Georgia, *Chronology of Russian Aggression in Georgia*, Georgia Update - Backgrounders (Government of Georgia, June 19, 2009), 4, http://georgiaupdate.gov.ge/en/doc/10006881/Microsoft%20Word%20-%20CYBERWAR%20short%20version_111008.pdf.
[21] Ibid.

Russian armaments and troops deployed to the region and Russia began to establish additional checkpoints at strategic choke points.[22]

The exact circumstances remain unclear due to differing versions of what occurred to start the war. It is widely held that in late July 2008, South Ossetia "provoked a conflict with Georgia by staging a series of missile raids on Georgian villages."[23] In response to these missile raids, Georgia bombarded Tskhinvali, the South Ossetian capital. From these events, the situation, as described in the next section, emerged.[24]

Georgia – The Situation

Throughout July, tensions continued to rise as additional Russian forces deployed to the region. The first cyber attack occurred on July 19, 2008, when a DDoS attack struck the website of the President of Georgia, Mikheil Saakashvili.[25] The situation on the ground began to deteriorate rapidly a little more than a week later with three separate attacks by South Ossetian irregular forces on July 29.

- At 10:00, South Ossetian de facto regime irregular forces opened fire at members of the Joint Peacekeeping Forces and an OSCE observer group moving near village Andzisi, Tskhinvali district.
- At 16:00, South Ossetian de facto regime irregular forces shelled the central government controlled villages in Big Liakhvi valley for 40 minutes, using mortars and grenade launchers.
- At 22:00, South Ossetian de facto regime irregular forces shelled the Georgian peacekeeping checkpoint on Sarabuki

[22] Ibid, 4–7. On April 20, 2008 a Russian fighter shot down a Georgian UAV (Unmanned Aerial Vehicle).
[23] Clarke, *Cyber War*, 18.
[24] Ibid.
[25] Government of Georgia, *Chronology of Russian Aggression in Georgia*, 7. Saakashvili's website was www.president.gov.ge.

> heights with 100mm and 120mm artillery. This was the first time such large caliber artillery was used since the hostilities in the 1990s.[26]

Late in the evening on August 1, South Ossetian irregular forces used heavy mortars and cannons to shell seven Georgian villages. This intense attack continued through the night resulting injuries to one police officer and six civilians.[27] Beginning the morning of August 2 and continuing through the August 6, Russia imbedded media with additional troops that continued to arrive to the region.[28]

After months of building tension, the prospects of a wider Russia-Georgia war loomed on August 7, 2008.[29] While Georgia pointed to the earlier South Ossetian irregular force missile attack on its villages as the catalyst for the war, Russia countered that Georgia's response had killed some of its peacekeeping troops, which necessitated a counter-response. In isolating the causal factor, Stiennon noted that Georgia was the first to deploy forces into South Ossetia; only afterwards did Russia insert troops into the region through the Roki Tunnel and use air strikes to attack Georgia.[30, 31]

Early on August 7, Georgia's Ministry of Foreign Affairs released a statement that Russia had raided the Tskhinvali Region in South Ossetia and were continuing to invade Georgia through the Roki Tunnel. Within the same timeframe, at 10:42 Eduard Kokoity, head of South Ossetian proxy authorities,

---

[26] Ibid.
[27] Ibid, 7–8.
[28] Ibid, 8–10.
[29] Hollis, "Cyberwar Case Study: Georgia 2008," 1.
[30] Stiennon, *Surviving Cyberwar*, 97.
[31] Rip Carroll Lefon, "Georgia and the Roki Tunnel." The Roki Tunnel "goes from North Ossetia to South Ossetia and is the only real road connection between them"; thus, this is the main avenue of access for Russia into South Ossetia.

stated that he would "wipe" Georgian forces out if they did not immediately withdraw from South Ossetia. Within minutes, at 11:00, South Ossetian irregulars started to shell Georgian positions and the ensuing military exchange continued through the afternoon and into early evening. At 19:10, Georgian President Saakashvili "confirmed a unilateral ceasefire and called the Russian authorities and de facto regimes for negotiations." The ceasefire was short-lived, and within hours fighting resumed.[32]

Late on the evening of August 7 a "cyber attack was launched against Georgia's governmental and civilian internet facilities."[33] These cyber attacks preceded a Russian air, ground, and naval attack. At 00:15 on August 8, Georgia launched a ground attack backed with artillery against South Ossetian forces. Russia immediately "responded, and the war was in full force. [34] Russia attacked Georgia in retaliation for Georgia's attack on South Ossetia.[35]

The war lasted for five days. At 12:40 on August 12, Russian President Dimitry Medvedev "announced that he had ordered an end to the military operation in Georgia." Although Russian military attacks continued through the afternoon and into the evening, a ceasefire "successfully brokered by President Nicolas Sarkozy between [the] Presidents of Georgia and Russia" led to the cessation of hostilities.[36] This war was not without consequence as the fighting

[32] Government of Georgia, *Chronology of Russian Aggression in Georgia*, 10–12.
[33] Ibid. At the outset of this cyber attack, "a large number of Georgia's Internet servers were seized and placed under external control."
[34] Government of Georgia, *Chronology of Russian Aggression in Georgia*, 13–14.
[35] Tikk et al., *Cyber Attacks Against Georgia: Legal Lessons Identified*, 4–5.
[36] Government of Georgia, *Chronology of Russian Aggression in Georgia*, 19–20.

claimed 161 members of Georgia's military forces and 224 civilians,[37] the Russians had sixty-six soldiers killed in action[38] with 283 missing, and South Ossetia experienced 150 combat fatalities.[39]

The Sarkozy ceasefire held, and from August 13 onward, the Russian occupation continued. On August 28, the Georgian Parliament declared the Russian armed forces on its soil as "occupational forces" and decreed that South Ossetia and Abkhazia were "Russian-occupied territories."[40] In the course of the short war, Georgia "lost control over 189 villages" over which it had previously administered.[41] Russia moved quickly to recognize South Ossetia and Abkhazia and on September 17, Russian president Dimitry Medvedev "signed the treaties of 'friendship, cooperation and mutual assistance' with the de facto authorities" of these former Georgian regions.[42]

Four principal factors explain Russia's rapid defeat of Georgia:[43]

- Georgia's tactical military defeat at the battle of Tskhinvali
- Georgia's operational defeat via Russia's uncontested invasion of the western part of Georgia
- Russia's unchallenged naval blockade of Georgia
- Georgia's difficulty getting their media message out to the world, which led to its strategic defeat in the war

---

[37] Government of Georgia, *Basic Facts: Consequences of Russian Aggression in Georgia*, Russian Invasion of Georgia (Government of Georgia, August 5, 2009), http://georgiaupdate.gov.ge/en/doc/10006881/Microsoft%20Word%20-%20CYBERWAR%20short%20version_111008.pdf. The number of Internally Displaced People (IDP) was large as 127,000 were displaced in the "immediate aftermath of war"; however, 100,000 of these were able to return home shortly after the war.
[38] Staff Writers, "Russia Lowers Official Death Toll from Georgia Conflict," *Space War*, September 11, 2008, Russia lowers official death toll from Georgia conflict.
[39] Mike Melchiorre and Kenny Piccari, "The South Ossetia War", n.d., http://www.slideshare.net/guestb3370d/the-south-ossetia-war.
[40] Government of Georgia, *Chronology of Russian Aggression in Georgia*, 30.
[41] Ibid, 31.
[42] Ibid, 35.
[43] Hollis, "Cyberwar Case Study: Georgia 2008," 1. Georgia was defeated in the "only large-scale major ground combat of the war (battle for the town of Tskhinvali)" because "mechanized Russian military and Ossetian militia forces" outclassed its "more lightly armed" forces.

This fourth factor explained the rationale for Russia's cyber campaign goal, which "fit neatly into the invasion plan."[44]

The major period of cyber attacks began within hours of the Russian military invasion and with few exceptions ended immediately after military operations ceased. Cyber attackers targeted "nearly all [the sites] that would produce benefits for the Russian military."[45] The cyber attacks beginning on August 7 represent the "first case in which an international political and military conflict was accompanied – or even preceded – by a coordinated cyber offensive."[46]

[44] Bumgarner and Borg, *Overview by the US-CCU of the Cyber Campaign Against Georgia in August of 2008*, 6.
[45] Ibid. Georgian news media and communications facilities were not attacked by the Russian military and thus avoided physical destruction, "presumably because they were being effectively shut down by cyber attacks."
[46] Tikk et al., *Cyber Attacks Against Georgia: Legal Lessons Identified*, 4–5.