Increasing Effectiveness of U.S. Counterintelligence: Domestic and International Micro-Restructuring Initiatives to Mitigate

Ferguson, Cody J.

Monterey, California: Naval Postgraduate School

NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

INCREASING EFFECTIVENESS OF U.S. COUNTERINTELLIGENCE: DOMESTIC AND INTERNATIONAL MICRO-RESTRUCTURING INITIATIVES TO MITIGATE CYBERESPIONAGE

by

Cody J. Ferguson

June 2012

Thesis Advisor:	Thomas Bruneau
Co-Advisor:	Andrew Singer

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE		Form Approved OMB No. 0704–0188

1. AGENCY USE ONLY *(Leave blank)*	2. REPORT DATE June 2012	3. REPORT TYPE AND DATES COVERED Master's Thesis

4. TITLE AND SUBTITLE Increasing Effectiveness of U.S. Counterintelligence: Domestic and International Micro-Restructuring Initiatives to Mitigate Cyberespionage	5. FUNDING NUMBERS
6. AUTHOR Cody J. Ferguson	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943–5000	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A	10. SPONSORING/MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government. IRB Protocol number _____N/A_____.

12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited	12b. DISTRIBUTION CODE

13. ABSTRACT

Cyberespionage is a prolific threat that undermines the power projection capacity of the United States through reduced economic prowess and a narrowing of the technical advantage employed by the American military. International attempts to limit hostile cyber activity through the development of institutions, normative patterns of behavior, or assimilation of existing laws do not provide the American national security decision maker with a timely or effective solution to address these threats. Unfortunately, the stove-piped, redundant and inefficient nature of the U.S. counterintelligence community does not deliver a viable alternative to mitigating cyberespionage in an effective manner. Instituting a domestic and international micro-restructuring approach within the Department of Defense (DoD) addresses the need for increased effectiveness within an environment of fiscal responsibility. Domestic restructuring places emphasis on developing a forcing mechanism that compels the DoD counterintelligence services to develop joint approaches for combating cyberespionage by directly addressing the needs of the Combatant Commands. International restructuring places an emphasis on expanding cybersecurity cooperation to like-minded nations and specifically explores the opportunity and challenges for increased cyber cooperation with Taiwan. This approach recognizes that Taiwan and the United States are both negatively affected from hostile cyber activity derived from within the People's Republic of China.

14. SUBJECT TERMS Counterintelligence, Reform, Restructuring, Effectiveness, Counterespionage, Counter-espionage, Cyberespionage, Cyber-espionage, Cybersecurity, Cyber-security, Cyberattack, Cyber-attack, Taiwan, Naval Criminal Investigative Service, NCIS, Air Force Office of Special Investigations, AFOSI, Law Enforcement, Micro-restructuring	15. NUMBER OF PAGES 137
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	Unclassified	Unclassified	UU

NSN 7540–01–280–5500 Standard Form 298 (Rev. 2–89)
Prescribed by ANSI Std. 239–18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

INCREASING EFFECTIVENESS OF U.S. COUNTERINTELLIGENCE: DOMESTIC AND INTERNATIONAL MICRO-RESTRUCTURING INITIATIVES TO MITIGATE CYBERESPIONAGE

Cody J. Ferguson
Civilian, Department of the Navy
B.A., Pacific Lutheran University, 2001

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF ARTS IN INTERNATIONAL SECURITY STUDIES (DEFENSE DECISION MAKING AND PLANNING)

from the

NAVAL POSTGRADUATE SCHOOL
June 2012

Author: Cody J. Ferguson

Approved by: Dr. Thomas C. Bruneau
Thesis Advisor

RADM Andrew M. Singer (Retired)
Thesis Co-Advisor

Dr. Daniel J. Moran
Chair, School of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Cyberespionage is a prolific threat that undermines the power projection capacity of the United States through reduced economic prowess and a narrowing of the technical advantage employed by the American military. International attempts to limit hostile cyber activity through the development of institutions, normative patterns of behavior, or assimilation of existing laws do not provide the American national security decision maker with a timely or effective solution to address these threats. Unfortunately, the stove-piped, redundant and inefficient nature of the U.S. counterintelligence community does not provide a viable alternative to mitigating cyberespionage in an effective manner. Instituting a domestic and international micro-restructuring approach within the Department of Defense (DoD) addresses the need for increased effectiveness within an environment of fiscal responsibility. Domestic restructuring places emphasis on developing a forcing mechanism that compels the DoD counterintelligence services to develop joint approaches for combating cyberespionage by directly addressing the needs of the Combatant Commands. International restructuring places an emphasis on expanding cybersecurity cooperation to like-minded nations, and specifically explores the opportunity and challenges for increased cyber cooperation with Taiwan. This approach recognizes that Taiwan and the United States are both negatively affected from hostile cyber activity derived from within the People's Republic of China.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

AFOSI	Air Force Office of Special Investigations
APT	Advanced Persistent Threat
AIT	American Institute of Taiwan
AOR	Area of Responsibility
AUSCANNZUKUS, or the Five Eyes	Australia, Canada, New Zealand, United Kingdom and United States
CIA	Central Intelligence Agency
CIB	Criminal Investigation Bureau
COCOM	Combatant Command
CCDR	Combatant Commanders
CCICA	Command Counterintelligence Coordination Authority
CNA	Computer Network Attack
CND	Computer Network Defense
CNE	Computer Network Exploitation
CCDCE	Cooperative Cyber Defense Center of Excellence
CI	Counterintelligence
CIFA	Counterintelligence Field Activity
CCP	Chinese Communist Party
CMR	Civil-Military Relations
CIU	Crimecrime Investigation Unit, Taiwan
DCHC	Defense Counterintelligence and Human Intelligence Center
DIA	Defense Intelligence Agency
DCO	Defensive Cyberspace Operations
DoD	Department of Defense
DHS	Department of Homeland Security

DDOS	Distributed Denial of Service
DEA	Drug Enforcement Administration
FBI	Federal Bureau of Investigation
FCA	Field Counterintelligence Activity
FCC	Fleet Cyber Command
FIS	Foreign Intelligence Service
FMS	Foreign Military Sales
GSD	General Staff Department
GWN	Goldwater-Nichols Defense Reorganization Act of 1986
GAO	Government Accountability Office
HUMINT	Human intelligence
ISB	Information Support Base
IC	Intelligence Community
ICIB	International Criminal Investigations Brigade, Taiwan
IPv6	Internet Protocol Version 6
JCIU	Joint Counterintelligence Unit
JCC	Joint Cyber Center
JOA	Joint Operations Area
JPL	Jet Propulsion Laboratory
KMT	Kuomintang
LOAC	Law of Armed Conflict
MOU	Memorandum of Understanding
MJIB	Ministry of Justice Investigation Bureau, Taiwan
MND	Ministry of National Defense, Taiwan
NASA	National Aeronautics and Space Administration

NCIWG	National Cyber Counterintelligence Working Group
NCIX	National Counterintelligence Executive
NIS	National Intelligence Strategy
NPA	National Police Agency, Taiwan
NRO	National Reconnaissance Office
NSA	National Security Agency
NSB	National Security Bureau, Taiwan
NCIS	Naval Criminal Investigative Service
OCO	Offensive Cyberspace Operations
OFCO	Offensive Counterintelligence Operations
ONCIX	Office of the National Counterintelligence Executive
OSD	Office of the Secretary of Defense
PACOM	Pacific Command
PLA	People's Liberation Army
PRC	People's Republic of China
Taiwan	Republic of China
PDPA	Personal Data Protection Act, Taiwan
RSA	RSA Technologies
SCID	Strategic Counterintelligence Directorate
TDY	Temporary Duty Assignment
UN	United Nations
USCI	United States Counterintelligence
USCYBERCOM	United States Cyber Command

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

For my family…in one way or another, this is all for you.

I am greatly appreciative to my past and current management at NCIS for giving me the opportunity to gain the professional and personal growth that accompanies this degree. I would also like to thank my thesis advisors for their direction and guidance throughout this process, to the gifted professionals within OSD Policy who have supported my research in this field and to those at AIT who assisted in making my trip to Taiwan a reality. This product and my personal knowledge benefited greatly from your assistance.

THIS PAGE INTENTIONALLY LEFT BLANK

I. THESIS INTRODUCTION

A. RESEARCH QUESTION

> How can restructured domestic and international partnerships focused towards mitigating the national cyberthreat improve effectiveness within the U.S. counterintelligence enterprise?

The wording of this research question correctly suggests that increasing effectiveness within the U.S. counterintelligence enterprise is the goal. Addressing the national cyberthreat by restructuring domestic and international partnerships therefore becomes a tool to address this goal. Domestically, research will focus on combining capabilities of Department of Defense (DoD) counterintelligence elements and comparing them to efforts currently underway in other branches of government as a means to increase effectiveness in combating the cyberthreat. Internationally, a comparative approach will be used that focuses on the development of liaison relationships between DoD law enforcement counterintelligence units and traditional and non-traditional partners; namely, the traditional Australian, British and American trifecta validated against an expanded cyber cooperation posture with Taiwan.

B. METHODS AND SOURCES

This thesis will include both an international relations theory and comparative case study approach to introduce a framework by which the national security decision maker can level judgments about increasing effectiveness of counterintelligence to mitigate the cyberespionage threat. This analysis has been juxtaposed with direct consultations with key international and domestic policy experts who collectively present a decision making model for restructured effectiveness of counterintelligence to combat the totality of the national cyberthreat. These leaders include decision makers within the U.S. counterintelligence community (USCI), DoD and the Taiwanese government. Moreover, consultation with these individuals was intended to provide a working framework by which the larger issue of effectiveness could be addressed; as such, the need for specific identification is not only unnecessary, but would otherwise obfuscate the structure of the model they have indirectly provided. Concern over this sourcing issue

is not confined strictly to the protection of identity, but also to the unintended parallels the reader could draw from analyzing the institutions that these individuals represent.

Analysis of U.S.-Taiwan cooperation clearly includes the political complexities of U.S. policy regarding the People's Republic of China (PRC). While a detailed analysis of these complexities is outside the scope of this thesis, a study of U.S.-Taiwan military to military relations will provide the context for increasing cooperation into other areas. Consultation with personnel within the Office of the Secretary of Defense (OSD) for Policy has provided amplifying details regarding the political complexities that could arise from increased liaison between the U.S.-Taiwan. This consultation has taken place via e-mail and personal meetings in Washington D.C.

Additional context is necessary to detail the complex and disjointed nature of the U.S. counterintelligence community. This context shows the need for reorganization and proves that large-scale, top-down reorganization has been and will continue to be unsuccessful at developing a robust national CI institution. Relying on previous scholarship to support the micro-restructuring of Naval Criminal Investigation Service (NCIS) and Air Force Office of Special Investigations (AFOSI), this thesis will study the feasibility of merging capabilities toward the single non-geographic mission set of cybersecurity. In doing so, it provides recommendations that remove redundancies and streamline capabilities. Analysis of these redundancies was obtained from published reports and statements from U.S. leaders as they addressed the issues surrounding the U.S. counterintelligence community's attempt to deal with the cyberespionage threat.

C. A WORKING LEXICON

This thesis uses the term "hostile cyber activity" as an all-inclusive phrase used to describe any event conducted in cyberspace that opposes the state's ability to maintain a monopoly on power within its borders. This includes cyberattack for a political or entertainment purpose, all forms of cybercrime, the preemptive use of cyberweapons in a military conflict and cyberespionage.

In addition, this thesis makes use of the language currently accepted by the cyberspace operations community as advanced by U.S. Cyber Command (USCYBERCOM). The most frequently used terms of the USCYBERCOM lexicon used in this report are:

- Cyberspace: A global domain within the information environment consisting of the interdependent network of information technology infrastructures and associated data that includes the Internet, telecommunications networks, computer systems and the processors and controls that make these elements function.[1]
- Computer Network Attack (CNA): Offensive cyberspace operations that are specifically intended to deny or manipulate information or infrastructure in cyberspace.[2]
- Defensive Cyberspace Operations (DCO): Attempts to direct and synchronize cyberspace actions to detect, analyze, counter and mitigate cyberthreats and vulnerabilities.[3]
- Offensive Cyberspace Operations (OCO): Attempts or actions conducted that seeks to create enabling or attack effects in cyberspace or to actively defend information networks.[4]
- Cyberwarfare: The inherently military use of cyberspace as intended to support a combatant commander's military objectives.[5] Such actions can include CNA, DCO and OCO.

D. INTRODUCTION OF THESIS CONCEPT

1. The Intended Audience

Counterintelligence is an often misunderstood and misrepresented field within the national security establishment. This is in part due to the classified nature of the work, a combination of sub-disciplines within the field and a culture of secrecy among those who practice its craft. These factors have generally produced limited information by which the national decision maker or scholar can build a holistic understanding of the role that

[1] United States Cyber Command, "The USCC Cyber Lexicon: A Language to Support the Development of Cyber Capabilities, and the Planning and Execution of Military Cyberspace Operations," Version 4.1, Pre-Decisional Draft (30 March 2011), 7.

[2] Ibid., 8.

[3] Ibid., 11.

[4] Ibid., 12.

[5] Ibid., 5.

counterintelligence plays in providing for the national interest. As such, matters relating to the structure and function of the counterintelligence institution are generally left for bureaucratic insiders to debate on their own. Improving the decision maker's ability to adequately judge counterintelligence effectiveness requires a more robust literature in the unclassified realm. Through such a literature, the role of counterintelligence in safeguarding the competitive advantage of the United States in both economic and military matters can be more adequately explored. This thesis therefore seeks to stimulate and contribute to a more robust dialogue regarding the impact and importance of counterintelligence for the academic, professional and decision making audience.

2. The Lack of a Definitive Literature

A significant factor in the lack of a robust counterintelligence literature is based on the premise that the current literature is broad in scope, but limited in quality. This is primarily due to the complexity of the counterintelligence discipline juxtaposed to its classified standing. The complex nature of the counterintelligence field has produced a body of literature that is filled with inaccuracies, misconceptions and scant professional discourse. Sherman Kent addressed the lack of literature in the field of intelligence more than half a century ago, "[a]s long as this discipline [counterintelligence] lacks a literature, its method, its vocabulary, its body of doctrine and even its fundamental theory runs the risk of never reaching full maturity."[6] His claims ring true for the field of counterintelligence today.

The literature review conducted for this thesis sought to navigate the broad scope of the counterintelligence mission and placed boundaries around those aspects of the discipline that do not address the thesis topic. Essentially, this constraint restricts the restructuring debate to topics that produce the *unity of effort* required by the 2005 National Counterintelligence Strategy.[7] The concept of *unity of effort* is just as strong today as it was in 2005, yet it was left out of the preceding 2008 and 2009 National

[6] Sherman Kent, "The Need for an Intelligence Literature," *Studies in Intelligence* (Washington, DC: Center for the Study of Intelligence, fall 1955), 3.

[7] Office of the National Counterintelligence Executive, "The National Counterintelligence Strategy of the United States of America 2005," 4.

Counterintelligence Strategies.[8] In an environment of fiscal restraint and a pervasive cybersecurity threat, *unity of effort* within the counterintelligence enterprise is as fundamentally important as it has ever been.

3. The Need for Structural Reform

Furthering the need for a more robust unclassified literature is the general lack of effectiveness across the counterintelligence enterprise. The U.S. counterintelligence community has been described as fractured, myopic and marginally effective.[9] The stove-pipes created from a national intelligence community comprised of seventeen members, each with separate and distinct counterintelligence authorities, remains the largest burden to effective mitigation of adversarial intelligence threats in the United States.[10] The establishment of the National Counterintelligence Executive (NCIX) demonstrated recognition on the part of the national security decision maker to create efficiencies and address effectiveness within the counterintelligence community. However, the prevalence of the individual agency structures that initially produced such stove-pipes has limited the NCIX from accomplishing its lofty objective. This failure underscores the need for a bottom-up approach to restructuring vice the additional bureaucratic layering and top-down approach that has already been found lacking.

Effective restructuring at the micro-level is more likely to produce efficiencies that can be replicated throughout the counterintelligence community. A counterintelligence system restructured to develop integrated partnerships within USCI, while leveraging the knowledge gained through international partnerships, can remove a degree of the barriers that prevent counterintelligence from effectively safeguarding the national interest. The study of this approach necessitates a singular mission that is not limited to geographic jurisdictions or one that is otherwise marred by complicated

---

[8] See Office of the National Counterintelligence Executive, "The National Counterintelligence Strategy of the United States of America 2008"; and Office of the National Counterintelligence Executive, "The National Counterintelligence Strategy of the United States of America 2009."

[9] U.S. Congress, "Chapter Eleven Counterintelligence," The Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction (31 March 2005), 485.

[10] Joel Brenner, "Strategic Counterintelligence," *American Bar Association: Standing Committee on Law and National Security* (The University Club, Washington, DC: 29 March 2007), 30; Joel Brenner, "*Joel Brenner, of Counsel: Biography*," Cooley LLP (2011), <http://www.cooley.com/jbrenner>.

domestic law enforcement, intelligence and military counterintelligence guidelines. The national cyberthreat, is such, a transnational mission and the study of its mitigation provides a concentrated area of study though which such micro-restructuring initiatives can be explored.

A counterintelligence system restructured to develop integrated partnerships within USCI, while leveraging the knowledge gained through international partnerships, removes some of the barriers that prevent counterintelligence from effectively safeguarding the national interest. Using the national cyberthreat as the catalyst to explore such structural changes is the foundation of this report. In an effort to maintain academic integrity, this thesis explores both the nature of and the proposed solutions for current cybersecurity challenges. In doing so, it attempts to provide a rigorous analysis of the various options available to the national security decision maker.

E. A MODEL FOR INTELLIGENCE REFORM

The study of intelligence reform—of which counterintelligence is a critical component—necessitates a conceptual model that provides structure to a subject that is complex, opaque and bound in secrecy. The model chosen for this thesis borrows aspects of New Institutionalism and combines them with several key tenants from the study of Civil-Military Relations (CMR), namely, the two aspects of effectiveness in achieving roles and missions and efficiency.[11] This overarching model of intelligence reform was proposed by Thomas Burneau and Steven Boraz in their book *Reforming Intelligence*. They note that "intelligence has specific roles and missions, the study of which establishes a way to analyze intelligence community structures and their implications for democratic civilian control and effectiveness."[12] This statement places an emphasis on understanding the roles and missions of intelligence in an effort to analyze effectiveness. Applied to counterintelligence, this approach necessitates an exploration of the roles and missions that are vital to counterintelligence, specifically, as they relate to cyberespionage mitigation.

---

[11] Thomas Bruneau and Steven Boraz, *Reforming Intelligence: Obstacles to Democratic Control and Effectiveness* (Austin, TX: University of Texas Press, 2007), 4.

[12] Ibid., 2.

While the evaluation of roles and missions is critical for any meaningful analysis of effectiveness, there is also a structural need to analyze how these roles and mission are derived. The New Institutionalist model fills this need and therefore becomes the second component of Bruneau and Boraz's method to evaluate intelligence reform. The collection of analytic concepts known as *New Institutionalism* places an emphasis on the importance that institutions have upon how actors manage power within society.[13] In doing so, the model assumes that individuals are rational self-interested maximizers and that their institutions matter.[14] Defining *institution*, as referenced by this approach, is crucial for understanding how this analysis translates to counterintelligence reform.

This thesis uses the Institutionalist definition of *institution* as the formal and informal procedures, routines, norms, or conventions embedded within the structure of a polity or political unit.[15] This understanding of *institution* used to evaluate the effectiveness of counterintelligence places an emphasis on the culture and norms that the actors within the discipline use as a means to delegate power and authority in the fulfillment of their mission objectives. In fact, "the creation and implementation of institutions are all about power"[16] and New Institutionalism is primarily concerned with the manner in which power is distributed within any given institution.

Amy Zegart, in her book *Flawed by Design*, utilizes a New Institutionalist framework to evaluate the initial design of the U.S. national security system as a means to stress the importance of creating effective bureaucratic structures during initial agency development. Zegart uses the model to describe a U.S. intelligence community that is hindered by ineffective design and built to resist major overhaul.[17] These factors contribute to an overall lack of effectiveness within the intelligence community and difficulty in producing adequate reform. Zegart's analysis applied to the topic at hand

---

13 Bruneau and Boraz, *Reforming Intelligence*, 3.

14 Amy Zegart, *Flawed by Design: The Evolution of the CIA, JCS, and NSC* (Stanford University Press, 1999), 210.

15 Peter Hall and Rosemary Taylor, "Political Science and the Three New Institutionalisms," *Political Studies*, vol. 44 (1996), 938.

16 Bruneau and Boraz, *Reforming Intelligence*, 4.

17 Zegart, *Flawed by Design*, 223, 227.

places an emphasis on the difficulty of macro-level reform within the USCI and the need to create an understanding of the actors that form the rules of the game and how the rules will be implemented.[18]

Addressing reform within the national security apparatus of an established democracy typically focuses on increasing efficiency and effectiveness vice democratic civilian control. As this thesis deals with the U.S. counterintelligence community, it will focus primarily on effectiveness in the completion of goals and objectives and efficiency, as it becomes a significant issue for maintaining effectiveness within an environment of fiscal restraint. This approach, supplemented with a New Institutionalist model that demonstrates the complications involved in major reform, will provide the analytic framework by which this thesis will evaluate counterintelligence restructuring options.

F. LITERATURE REVIEW

The main problem associated with this research lies with the general paradox that exists when studying intelligence within a democratic system; primarily, that the secretive nature of intelligence conflicts with a democratic system that demands transparency.[19] This challenge is not new to the study of intelligence, but it makes the evidentiary needs of this thesis more complicated in an unclassified format. That said, there are significant unclassified contemporary and historical materials that deal with the structure and function of the Intelligence Community (IC) in the United States.

1. Problems within the Counterintelligence Enterprise

The literature addressing effectiveness in U.S. counterintelligence is decades old. Geschwind (1963) called for a restructuring of USCI in order to address a system that was decentralized, subordinate and ineffective.[20] He described a 1960s USCI apparatus that was so fragmented it was unable to even comprehend its own "aggregate inability" to affect the threat posed by Communist secret services.[21] In dealing with the same issue

18 Bruneau and Boraz, *Reforming Intelligence*, 4.

19 Ibid., 17.

20 Geschwind, C. N. "Wanted: An Integrated Counter-intelligence," *Studies in Intelligence 7*, no. 3 (summer 1963), 15–37.

21 Ibid., 15.

several years later, Matschulat (1969) called for a cohesive and coordinated effort from the counterintelligence community to mitigate Soviet Intelligence from enabling communist forces in Vietnam.[22] According to Matschulat, coordination translated to increased response capacity in the defeat of a foreign intelligence threat, namely, through increased cooperation among the military counterintelligence elements and those of the intelligence community. In addition to calls for greater cooperation, Matschulat also referred to the tendency of USCI to derive its structure and function from the activities of the chief adversary vice any other factor.[23] If this holds true today, what structure and functions has the counterintelligence community developed to effectively combat the national cyberthreat? The exploration of this question will take place in Chapter IV of this thesis.

2. Definitional Problems of Counterintelligence

Review of the literature on counterintelligence points to an abundance of information that defines the defensive mission of counterintelligence. Bruneau and Boraz (2006) offer a succinct definition of counterintelligence that has been generally accepted within the scholarly community as "the protection of the state and its secrets against other states or organizations."[24] A virtual cornucopia of literature defines how this goal of counterintelligence is executed, but the preponderance of this literature deals with defensive counterintelligence activities. Defensive activities are those that dissuade, investigate, analyze, or harden targets to prevent a Foreign Intelligence Service (FIS) from committing espionage.

A cross section of these defensive works includes descriptions by Churchill and Wall (2001)[25] of FBI investigations into dissident groups ranging from communist sympathizers in the 1950s to the solidarity movement in the 1980s. Contemporary

---

[22] Austin Matschulat, "Coordination and Cooperation in Counterintelligence," *Studies in Intelligence 13*, no. 2 (spring 1969), 25–36.

[23] Ibid., 1.

[24] Thomas Bruneau and Steven Boraz, "Democracy and Effectiveness," *Journal of Democracy 17*, no. 3 (July 2006), 30.

[25] Ward Churchill and Jim Vander Wall, *The Cointelpro Papers: Documents from the FBI's Secret Wars Against Dissent in the United States* (Boston: South End Press, November 2001), 1–500.

investigative literature includes Masco (2002)[26] and Goodman (2005)[27] who deal with the political sensitivities of counterespionage investigations. Additionally, a large grouping of case studies has been published that detail the espionage investigations of Jonathan Pollard, Robert Hanssen, Aldrich Ames *and* Ana Montes, to name but a few. These defense-centric works dominate proactive writings within counterintelligence literature. In doing do, they substantially reduce the range of professional discourse regarding the role of counterintelligence in protecting the national interest.

For the dialogue on counterintelligence to be complete, it cannot be viewed by the scholar, professional, or national security decision maker as simply a reactive effort to uncover the damage done by FIS penetrations. The lack of literature dealing with the offensive counterintelligence mission (OFCO), therefore, results in a misinformed understanding of counterintelligence's role for mitigating foreign intelligence threats. The DoD Joint Publication 1–02 (2012) defines two types of OFCO operations as double agent and controlled source operations.[28] However, misunderstandings about OFCO still occur. Illustrating this point was a Defense Intelligence Agency (DIA) briefing, in which an OFCO unit had been stood up within the Defense Counterintelligence and Human Intelligence Center (DCHC). During a question and answer period with the media, such misunderstandings were highlighted when questions were posed about OFCO techniques that included targeted assassination of foreign intelligence officers.[29]

Despite such misunderstandings, there is general consensus within the literature that USCI needs to focus on offensive counterintelligence as a means to mitigate foreign

---

[26] Joseph Masco, "Lie Detectors: On Secrets and Hypersecurity in Los Alamos," *Public Culture 14*, no. 3 (fall 2002), 441–467.

[27] Michael Goodman, "Who Is Trying to Keep What Secret from Whom and Why? MI5-FBI Relations and the Klaus Fuchs Case," *Journal of Cold War Studies 7*, no. 3 (summer 2005), 124–146.

[28] United States Department of Defense, "Joint Publication 1–02: Dictionary of Military and Associated Terms" (Washington D.C.: 15 March 2012), 238.

[29] Defense Intelligence Agency, "Media Roundtable about the Establishment of the Defense Counterintelligence and Human Intelligence Center" (Washington, DC: Federal News Service, 5 August 2008).

intelligence threats. Michelle Van Cleave (2007),[30] the WMD Report (2005),[31] and the National Counterintelligence Strategies of the United States (2005, 2008, 2009)[32] have all called for USCI to place an emphasis on offensive operations. Van Cleave (2005), the former National Counterintelligence Executive from 2003–2006, indicates that such offensive based activities need to take place outside the United States on foreign soil. [33] She also stated, "Ninety percent of our counterintelligence resources are concentrated within the United States. We're playing goal-line defense rather than looking for opportunities to get ahead of the game."[34] She is not alone, the WMD Report (2005)[35] and the DIA DCHC announcement (2008)[36] echo her sentiments. Moreover, the need for increased offensive capacity is not confined only toward the mitigation of traditional threats. Translated toward the evolved cyberespionage threat, Brenner (2011) describes one type of offensive counterintelligence action that would seek to "live inside our adversaries networks before they launch attacks against us."[37] His comments are an adaptation of Lin (2011) who sought to describe a means by which offensive action could support defensive purposes. Lin suggested the early warning of an incoming cyberattack could be developed from living inside advisories networks.[38] Thus, there is consensus

---

30 Michelle Van Cleave, "Counterintelligence and National Strategy," *National Defense University: School for National Security Executive Education* (April 2007), 11.

31 U.S. Congress, "Chapter Eleven Counterintelligence," 487.

32 Office of the National Counterintelligence Executive, "The National Counterintelligence Strategy of the United States of America" (2005); Office of the National Counterintelligence Executive, "The National Counterintelligence Strategy of the United States of America" (2008); Office of the National Counterintelligence Executive, "The National Counterintelligence Strategy of the United States of America" (2009).

33 Michelle Van Cleave, "Foreign Spies Are Serious. Are We?" *The Washington Post* (8 February 2009).

34 Ibid.

35 U.S. Congress, "Chapter Eleven Counterintelligence," 486.

36 Defense Intelligence Agency, "Media Roundtable about the Establishment of the Defense Counterintelligence and Human Intelligence Center."

37 Joel Brenner, *America the Vulnerable: Inside the New Threat Matrix of Digital Espionage, Crime and Warfare* (New York: Penguin Press, 2011), 216.

38 Herbert Lin, "Understanding Cyberattack as an Instrument of U.S. Policy," Presentation at the Council on Foreign Relations (New York City, NY: 9 May 2011), 9, <http://www.cfr.org/content/thinktank/Lin_UnderstandingCyberattack.pdf> (28 May 2012).

regarding the need to generally increase offensive capabilities for a more effective counterintelligence enterprise and as a means to mitigate the cyberespionage threat.

3. The Need to Restructure

a. Contemporary Focus on Fragmentation

Just as past scholars addressed the fragmented state of counterintelligence within the United States, current scholarship agrees that USCI is mired in stove-pipes and too fragmented to be effective. Van Cleave (2007),[39] Brenner (2007),[40] the WMD Report (2005),[41] and Taylor (2007)[42] all echo this sentiment. On the issue of stove-piping, these sources define a USCI enterprise comprised primarily of the three organizations with operational counterintelligence responsibilities; the Central Intelligence Agency (CIA), the Federal Bureau of Investigation (FBI) and the DoD. Brenner (2011) expands the definition of the USCI enterprise to one that comprises all seventeen members of the U.S. intelligence community.[43] His distinction recognizes that all members of the IC have internal defensive authorities to investigate insider threats and to implement security methods to minimize exposure to foreign intelligence services. However, not all IC members have the authority to run offensive operations against a FIS. Expanding the definition of the USCI enterprise in this regard further illuminates the stove-piping issue.

Consolidating opinion regarding a fractured USCI community, the NCIX *Fundamentals of CI Report* (2006) indicated that fragmentation within the counterintelligence community has resulted in duplication of effort, uneven performance in the workplace and unmet training requirements.[44] These symptoms are in agreement

39 Van Cleave, "Counterintelligence and National Strategy," 1.

40 Brenner, "Strategic Counterintelligence," 30.

41 U.S. Congress, "Chapter Eleven Counterintelligence," 485.

42 Stan Taylor, "Definitions and Theories of Counterintelligence," in Loch Johnson, ed., *Strategic Intelligence 4: Counterintelligence and Counterterrorism* (Westport, CT: Praeger Security International, 2007).

43 Brenner, "*Joel Brenner, of Counsel: Biography*."

44 Office of the National Counterintelligence Executive, "Fundamental elements of the Counterintelligence discipline: Universal Counterintelligence Core competencies," vol. 1 (The National Counterintelligence Institute: January 2006), 3.

with other literature that further defines the lack of effectiveness within USCI. Recent scholarship on the topic of restructuring therefore echoes the words written by Geschwind. Van Cleave (2007) issued similar charges for the need to restructure USCI. She calls the adoption of a case-by-case approach for dealing with the foreign intelligence threat and the practice of concentrating counterintelligence resources inside the United States vice engaging FIS abroad as tantamount to "ceding advantage to the enemy."[45]

b. Macro vs. Micro-Restructuring

A professional intelligence community with a long tradition of intelligence work does not guarantee effectiveness.[46] As such, the USCI community has recognized the need to restructure in order to deal with effectiveness; however, a key problem that remains is the divergent viewpoints regarding the method that such restructuring should follow. Large-scale *Goldwater-Nichols style* restructuring has been the favored government reform model. This style of reform is also evident in the National Security Act of 1947, the Intelligence Reform and Terrorism Prevention Act of 2004 (which created the Office of the Director of National Intelligence) and the creation of the Office of the National Counterintelligence Executive (ONCIX), whose mission is to lead an integrated national counterintelligence effort against foreign intelligence threats to the United States.[47]

These major reform efforts have had both intended and unintended consequences. Intended results include increases in capacity and effectiveness, but such reform efforts also lead to the unintentional creation of additional layers of bureaucracy. Generally, major structural reforms have proven to have little effect in addressing a fragmented counterintelligence community. This is due to the fact that counterintelligence at the enterprise level derives its mission priorities from various

---

[45] Van Cleave, "Counterintelligence and National Strategy," 1.

[46] Bruneau and Boraz, *Reforming Intelligence*, 20.

[47] This is the mission statement of the Office of the National Counterintelligence Executive. The ONICX website can be found at, http://www.ncix.gov/about.php (accessed 4/25/12).

government agencies and departments.[48] Thus, counterintelligence—more than perhaps any other government function—remains unaffected by the positive aspects that such reform brings. The New Institutionalist framework used to evaluate this concept indicates that the impetus for large-scale CI reform from both the legislative and executive perspective lacks political support. Counterintelligence's lack of an effective domestic constituency in this regard is a contributing factor for continued fragmentation and subsequent lack of effectiveness.

Even when an exogenous event would otherwise compel reform, such events have little impact on compelling reform within the counterintelligence community. The 9/11 Commission Report included an analysis of the operational and conceptual failings of the IC and counterintelligence community to detect and prevent the September 11, 2001, terrorist attacks.[49] Thus, even when USCI is found negligent, Congress fails to hold the community accountable by mandating a restructuring process to remove stove-pipes or create the *unity of effort* mandated by the 9/11 Commission Report.[50] Additionally, large-scale public espionage cases against spies like Robert Hanssen, Aldrich Ames, John Anthony Walker, etc., do not result in a public outcry for reform. These cases show the lack of constituent interest produces a negligible amount of congressional and executive attention, which reduces action by these leaders to meaningless grand standing in an attempt to appear like statesmen.[51]

The reason for this lack of accountability is twofold. One, there is a general aversion in the United States to a domestic intelligence agency similar to the British MI-5 model, which is seen as incompatible to an American democracy concerned

---

48 Van Cleave, "Foreign Spies Are Serious. Are We?."

49 William Lahneman, "U.S. Intelligence Prior to 9/11 and Obstacles to Reform," in Bruneau and Boraz, *Reforming Intelligence*, 77.

50 House Permanent Select Committee on Intelligence and Senate Select Committee on Intelligence, "Report of the Joint Inquiry into the Terrorist Attacks of September 11, 2001, 107th Congress, 2nd Session" (Washington D.C.: Government Printing Office, December 2002), 399.

51 Zegart, *Flawed by Design*, 215.

with the protection of civil liberties and effective oversight.[52] Secondarily, the congressional action model suggests that Congress has little incentive to tackle issues that do not meet the demands of a particular interest group or those that otherwise directly impact their constituents. While counterintelligence cases may stir the passions of the American populace, they in and of themselves do not represent a specific constituency by which a congressional representative can be held accountable for failing to enact legislation or reform that creates a more effective USCI community.[53]

Large-scale—macro-style—restructuring of government is best described by Locher (2002), which details the last successful major overhaul of the Defense Department under the Goldwater-Nichols Defense Reorganization Act of 1986 (GWN). Locher indicated that such macro-style reform required the perfect alignment of political, media and public support, and that the alignment of these factors normally requires an exogenous event.[54] Zegart (2009) adds an important analysis of restructuring in general as she describes the permanency of intelligence bureaucracies once they have been established, regardless of such an exogenous event.[55] She further adds that even when major reorganizations of national security agencies occur, they have a low success rate for achieving greater effectiveness.[56] This analysis underscores the need for a micro-approach to restructuring. Such an approach was introduced by Bachman (2011) who recommended the integration of DoD OFCO capabilities between NCIS and AFOSI using their relocation to a joint headquarters in Quantico, VA, as a catalyst.[57] Such a recommendation is "micro," in that it does not necessitate congressional approval of large-scale capital investment.

---

52 James Burch, "A Domestic Intelligence Agency for the United States? A Comparative Analysis of Domestic Intelligence Agencies and Their Implications for Homeland Security," *Homeland Security Affairs*, vol. iii, no. 2 (June 2007), 1.

53 Zegart, *Flawed by Design*, 102.

54 James Locher III, *Victory on the Potomac: The Goldwater–Nichols Act Unifies the Pentagon* (College Station: Texas A&M Press, 2002), 15–32.

55 Zegart, *Flawed by Design*, 227.

56 Ibid., 234.

57 Gregory J. Bachman, "Integrating Defense Counterintelligence: A First Step," Georgetown Public Policy Institute: Capstone Paper (Georgetown University, 25 April 2011), 1–29.

G. MICRO-RESTRUCTURING AT THE DOMESTIC LEVEL

The general hypothesis developed to this point places a counterintelligence reform impetus on a micro-restructuring model. Such a model would not require the large-scale political capital needed during a GWN style reorganization and could be interdepartmentally focused. Such restructuring omits the need for Congressional approval and thus circumvents the two reasons for congressional inaction mentioned previously. Accordingly, DoD owns four of the six operational counterintelligence elements within the U.S. government and it has the authority to restructure its own components, as it deems necessary by issuing DoD Directives.

The other hypothesis developed from this research is that within the United States, the mitigation of the cyberthreats—independent of cyberwar—is primarily a law enforcement and security function. This supposition builds upon the decades old understanding of counterintelligence as an inherently governmental function.[58] Brought into the contemporary environment, this understanding appears supported by initiatives lead by the Department of Homeland Security (DHS) for implementing *The National Cybersecurity Strategy* and investigative authority for financially motivated cybercrime with the U.S. Secret Service. While DHS is tasked as the coordination authority for mitigating vulnerability of critical infrastructure inside the United States, the law enforcement role for reducing cyberespionage outside the United States appears limited.

In lieu of a consolidated federal law enforcement response to these activities, USCYBERCOM has largely absorbed the responsibility for mitigating such threats. This is principally due to the co-location of USCYBERCOM with the NSA and a subsequent capacity to mitigate cyberthreats that is unmatched by other agencies in the federal government.[59] This research does not make the claim that USCYBERCOM's role in mitigating such actions is incorrect; rather, it asserts that the mitigation of hostile cyber activity is a young endeavor and as such, addressing cyberespionage outside the United

---

[58] A.C. Wasemiller, "The Anatomy of Counterintelligence," *Studies in Intelligence* 13, no. 1 (winter 1969), 10.

[59] Paul Rosenzweig, "10 Consecutive Principles for Cybersecurity Policy," *The Heritage Foundation Backgrounder*, no. 2513 (Washington, D.C.: 2011).

States should evolve to incorporate the existing authorities that govern espionage writ large. The counterintelligence community must not abandon its responsibility to offensively target such activates outside the United States simply because it does not have the cyber expertise resonant within USCYBERCOM.

Addressing this imbalance indicates that USCYBERCOM—while well suited in the technical realm—does not maintain an optic from which to fully employ a host of offensively derived techniques in the mitigation of espionage. This research therefore, determines that the mitigation of all forms of espionage is an inherently law enforcement and governmental function and one that the USCI enterprise would be more effective at countering through a micro-restructuring approach that places an emphasis on domestic partnerships within DoD. Such partnerships would include increased USCI presence at USCYBERCOM in a fusion center approach to offensively combat cyberespionage by DoD's service counterintelligence components (NCIS, AFOSI, Army CI and DIA DCHC). In turn, the development and sustainment of such relationships would become a force multiplier for USCYBERCOM, as it would enable full spectrum capacity for dealing with cyberespionage and cyberattack within one institution.

H. MICRO-RESTRUCTURING AT THE INTERNATIONAL LEVEL: DOD AND ALLIES

The National Counterintelligence Strategy (2009)[60] specifically addressed the need to integrate counterintelligence with all aspects of cyberspace stating, "we must strengthen collaboration among policy makers, law enforcement, counterintelligence elements, security and other key players across the U.S. government on cyber operations"[61], but this list specifically leaves out international partnerships as an element in combating the cyberthreat. Despite the lack of a current counterintelligence strategy that addresses international cyber cooperation, the 2011 National Security Council *Cyberspace Policy Review* does address the need for international cooperation.

[60] The 2009 strategy document is the most recently published National Counterintelligence Strategy.

[61] National Counterintelligence Strategy of the United States of America 2009, vi.

Furthermore, it specifically advises the United States government to work with international bodies, military allies and intelligence partners who face similar threats.[62]

There is a consensus in the literature regarding the necessity of the international community to cooperate on cybersecurity. This is seen through multinational collaborative events like the semi-annual DHS sponsored *Cyber Storm* exercise[63] and recommendations by Schreier, Weeks and Winkler (2011)[64] for international support in constructing regimes and institutions that develop norms by which cybersecurity can be addressed. Calls for such international regimes have been echoed by international decision makers as well, as was observed at the London Conference on Cyberspace through comments made by British Foreign Secretary William Hague (2011).[65]

It is assessed that increased international cyber engagement is a fundamental method by which to curtail hostile cyber activity. However, the degree of actual cooperation in the international environment appears subject to discussion vice action. Actionable responses for reducing cyberespionage and cyberattack appear limited to traditional allies. In the case of the United States, this level of cooperation became evident in the shaping of the 2012 *Cyber Storm* exercise, which will only include participation from the current cyber trifecta that includes the United States, Australia and the United Kingdom.[66] While there are clearly policy and security concerns in broadening cooperation beyond America's traditional allies, this research seeks to fill a knowledge gap regarding the decision making framework by which national security leaders judge such engagement.

---

[62] National Security Council, "Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure" (2011), 20.

[63] United States Department of Homeland Security, "Cyber Storm III: Final Report," Office of Cybersecurity and Communications National Cybersecurity Division (July 2011), 1–21.

[64] Fred Schreier, Barbara Weekes, Theodor Winkler, "Cybersecurity: The Road Ahead," Geneva Security Forum, Democratic Control of Armed Forces (DCAF) Horizon 2015 Working Paper No. 4 (2011), 1–53.

[65] William Hague, "*London Conference on Cyberspace: Chair's statement*," Foreign and Commonwealth Office (London: February 11, 2011), <http://www.fco.gov.uk/en/news/latest-news/?view=PressS&id=685663282> (1 May 2012).

[66] Consultation with U.S. government official #1 (20 April 2012), regarding the shaping of the 2012 Cyber Storm IV event.

All states share a preponderance of America's vulnerabilities in cyberspace and at times are threatened by the same actors. U.S.-Taiwan cooperation in the cyber arena is particularly well suited to meet the demands of the National Intelligence Strategy as both nations are highly impacted by illicit cyber activity derived within the People's Republic of China (PRC).[67] Furthermore, inside the U.S. government, DoD arguably maintains the best diplomatic channels with the Taiwanese national security establishment. Leveraging these relationships with Taiwan could provide much needed liaison intelligence to counter the cyberthreat under Title 50 (intelligence); but more specifically, this research seeks to determine how this could be accomplished under Title 18 (criminal). Taiwan therefore, becomes a poignant case study by which further international cooperation can be gauged. What would law enforcement liaison and increased cooperation between the United States and Taiwan look like, and what are the political implications by which it would be constrained?

As law enforcement liaison is conducted under Title 18 vice Title 50, the secrecy burdens are lessened. This is not to suggest that information is shared outside DoD's approval channels, but rather and only, that law enforcement liaison is sometimes a more effective means of developing the initial mechanisms needed to explore such issues in larger detail. Restructuring DoD counterintelligence at the international level to leverage Taiwanese resources could provide a significant advantage to the U.S. counterintelligence enterprise and to the DoD. This research seeks to explore those advantages to determine the various issues for and against the development of such partnerships.

I. CONCLUSION

The research conducted for this thesis determined that small ground-up institutional changes within DoD law enforcement counterintelligence organizations can improve the effectiveness of the USCI enterprise as it seeks to combat and ultimately mitigate the national cyberthreat. This research took a dual track approach to derive its final conclusions. One such approach showed that domestic level micro-restructuring focused toward mitigating cyberespionage will streamline resources and produce an

67 Yao-chung Chang, "Cyber Conflict Between Taiwan and China," *Strategic Insights*, vol. 10, no. 1 (spring 2011), 26–35.

effective level of counterintelligence within the Department of Defense. Secondarily, international restructuring placed a focus on developing a closer liaison relationship with Taiwan, principally as it relates to mitigating cyberespionage, but also as it pertains to the larger issue of cybersecurity.

Apart from increasing domestic cooperation among DoD counterintelligence elements to streamline effectiveness, such restructuring also affords the national security apparatus an avenue to address the challenging fiscal environment. The stove-piped nature of counterintelligence in the United States produces redundancy, waste and overlap of mission authorities and financial resources. Unlike the military services, which have the preponderance of their yearly appropriations tied up in weapons and weapons systems, taxpayer dollars spent on counterintelligence is invested primarily in the training and retention of personnel through salaries.

Minimizing the redundancy between agencies—especially those agencies that fall under the same executive department—should therefore be considered a best practice in an era of fiscal restraint and heightened fiscal responsibility. Instituting a micro-restructuring approach for DoD CI agencies is an approach in effective reform that addresses redundancies within the counterintelligence enterprise and improves effectiveness of counterintelligence while adhering to efficiency concerns. Should such a micro-restructuring approach be proven successful, it could pave the way for broader restructuring across the counterintelligence enterprise. Clearly the external threat to American national security from cyberespionage demands nothing less.

II. CYBERESPIONAGE IN THE CONTEXT OF THE CHINESE CYBERTHREAT

A. CHAPTER INTRODUCTION

This chapter seeks to assess the role that cybersecurity plays in the U.S. national security establishment. It begins by exploring the foundation upon which current cyberthreats thrive; including the emerged role that cyberespionage has upon a state's capacity for intelligence collection. Finally, this chapter explores the need for an evolved U.S. counterintelligence enterprise that effectively addresses increased FIS capacity to steal U.S. military technology and commercial secrets.

B. WHAT IS CYBERESPIONAGE AND WHY DOES IT MATTER?

> The American military-industrial complex is the world's fattest espionage target. While the scope and intensity of economic espionage have assumed startling proportions, the "traditional" espionage assault on our national defense establishment dwarfs anything we have ever before experienced.[68]

In the above passage, Joel Brenner, the former National Counterintelligence Executive, is accurate to refer to the "traditional" espionage threat as one directed against the defense establishment. However, in this context the term "traditional" is somewhat misleading. While espionage still traditionally targets the defense establishment, its means of commission are certainly not traditional. The intelligence community assesses that the use of cyber tools to conduct economic espionage has become the preferred method for illicit intelligence collection.[69] This prevalence has likely spread to the collection of sensitive commercial information and technology as well, producing a transformation in the commission of espionage in the modern era. The reason for this is quite clear. Espionage committed electronically is cheap, easy and low risk. [70] These

---

68 Brenner, *America the Vulnerable*, 73.

69 Office of The National Counterintelligence Executive, "Foreign Spies Stealing U.S. Economic Secrets in Cyberspace: Report to Congress on Foreign Economic Collection and Industrial Espionage, 2009–2011" (October 2011), i.

70 Brenner, *America the Vulnerable*, 74.

three factors are embedded within the modern cyber infrastructure and they act in concert to produce a mounting national security vulnerability. This shift is summarized as:

> Information that previously required close-in human intelligence (HUMINT) access, necessitating the long-term development and recruitment of individuals with access to targeted information, is now easily obtained by sending a phishing e-mail to the unsuspecting targets.[71]

In today's information environment, the exfiltration of intelligence that once took years and involved the development of substantial human intelligence networks can be accomplished in a matter of minutes in one download session.[72] Cyberespionage has revolutionized the intelligence collection business and the American counterintelligence enterprise must respond in kind.

In the current cyberspace environment, sophisticated cyber capabilities reside almost exclusively with nation-states.[73] State sponsored hostile cyber activity generally includes support to espionage operations, reconnaissance of military networks using sensors or "sleeper" tools for later use during a conflict, theft of commercial data or intellectual property and sometimes demonstrating capabilities that deter rival states.[74] Instances of these hostile events continue to grow at an alarming rate and each new incident is a lesson in the vulnerability of American power. William Lynn, Assistant Secretary of Defense, while unveiling the *Department of Defense Cyber Strategy*, identified the most prevalent of these hostile cyberthreats as computer network exploitation (CNE). He summarizes CNE as "the [cyber derived] theft of information and intellectual property from government and commercial networks."[75] The most significant

---

[71] Bryan Krekel, Patton Adams, and George Bakos, "Occupying the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage," U.S.-China Economic and Security Review Commission (Northrop Grumman Corporation, 7 March 2011), 107.

[72] James Cartwright, "Hearing on China's Military Modernization and its Impact on the United States and the Asia-Pacific," Testimony before the U.S.-China Economic and Security Review Commission (Washington D.C., 29 March 2007), 7, 105.

[73] William Lynn, "Remarks on the Department of Defense Cyber Strategy," Office of the Assistant Secretary of Defense for Public Affairs (National Defense University, Washington, D.C., 14 July 2011).

[74] Krekel, Adams, and Bakos, "Occupying the Information High Ground," 96.

[75] Lynn, "Remarks on the Department of Defense Cyber Strategy."

cases of CNE to date have included Google's Aurora incident, Titan Rain, Ghost Net, Shady Rat and the RSA-Lockheed Martin incident.

The research contained in this thesis does not attempt to amplify the details of these cases; in fact, much has already been written on their relevance to include the damage they have collectively caused to American national security.[76] Rather, more relevant to this debate is how their combined impact has led U.S. policymakers to make several important judgments. Primarily, that cyberspace presents new and unique challenges to the protection of American economic, industrial and military secrets; and secondarily, "[a] large body of both circumstantial and forensic evidence strongly indicates Chinese state involvement in such activities, whether through the direct actions of state entities or through the actions of third-party groups sponsored by the state."[77] While it is no surprise that cyber powerhouses like China and Russia view themselves as strategic competitors of the United States, they are also the most aggressive collectors of U.S. economic information and technology.[78] The non-traditional use of cyberspace as a new medium in which states can conduct espionage activity prevents a grave challenge to the U.S. counterintelligence community.

C. THE COST OF CYBERESPIONAGE

The true cost of cyberespionage remains elusive—costs measured in terms of economic deprivation and loss of technical military dominance—although it is clear that the transfer of cutting edge military technology to America's adversaries endangers the lives of U.S. military personal and strengthens the resolve of those nations who wish to

---

[76] For reports on these incidents see: Greg Walton, Nart Villenueve, et. al., "Tracking GhostNet: Investigating a Cyber Espionage Network," *Information Warfare Monitor, JR02–2009* (Toronto: Citizen Lab, Munk Centre for International Studies, University of Toronto, 29 March 2009); Allan Paller, "Titan Rain Shows Need for Better Training," *SearchSecurity.com* (13 December 2005); Christopher Drew, "Stolen Data Is Tracked to Hacking at Lockheed Martin" *New York Times* (4 June 2011); Dmitri Alperovitch, "Revealed: Operation Shady RAT," McAfee Corporation (Santa Clara, CA: 2011); Alex Stamos, "'Aurora' Response Recommendations," *iSEC Partners* (17 February 2010).

[77] U.S.-China Economic and Security Review Commission, "2009 Report to Congress of the U.S.-China Economic and Security Review Commission" (Washington D.C.: November, 2009), 167.

[78] Office of The National Counterintelligence Executive, "Foreign Spies Stealing U.S. Economic Secrets in Cyberspace," 4.

thwart American political objectives.[79] The Government Accountability Office (GAO) released a March 2012 report that listed the aggregated year-on-year portfolio value of the top 96 military acquisition programs at $1.58 trillion.[80] When these programs are compromised, their aggregate value drops dramatically as adversary nations are able to develop both countermeasures to these systems—based on knowledge of how they work—and replicate them for use in their own arsenals. These losses produce enormous economic opportunity costs for the United States financially and degrade the technical military advantage they are intended to convey. Raising the political cost for nations that commit cyberespionage therefore becomes a means to curtail such activity while strengthening the American economy and a defense establishment.

In the private sector, the theft of trade secrets from U.S. companies "undermines the corporate sector's ability to create jobs, generate revenues, foster innovation and lay the economic foundation for prosperity and national security."[81] American power has always been the byproduct of a stable and healthy wealth generating capitalist system. In the contemporary environment, the linkage between the private sector and government has officially dissolved as the boundary between economic security and national security has disappeared.[82] Addressing the national security of the United States requires the protection of corporate intellectual property and cutting-edge military technology in the face of cyberespionage threats.

The speed of technical innovation coupled with an increased global reliance upon technology makes threats from cyberspace the most serious contemporary security challenge faced by the state. Cybercriminals, patriotic hackers and even the intelligence establishments of most states have found reduced risk and increased opportunity due to the difficulty of positive attribution. This global challenge requires effective legislation,

---

79 Office of the National Counterintelligence Executive, "Foreign Spies Stealing U.S. Economic Secrets in Cyberspace," 3.

80 Government Accountability Office, "Defense Acquisitions: Assessments of Selected Weapon Programs," Highlights of GAO-12–400-SP a Report to Congressional Committees (March 2012).

81 Office of the National Counterintelligence Executive, "Foreign Spies Stealing U.S. Economic Secrets in Cyberspace," 3.

82 Brenner, *America the Vulnerable*, 76.

international agreements, established norms and enforcement mechanisms to adequately mitigate cybersecurity challenges in the modern world. Of these threats, cyberespionage—as an advanced form of state sponsored cyber intelligence collection—poses a significant threat to the American national security establishment.

Espionage in general reduces the power advantages enjoyed by the United States afforded through its dominance in economic, industrial and advanced military technology. When coupled with the inherent properties of cyberspace such as speed, decreased risk and cost effectiveness, it is easy to see that cyberespionage is a new and all-encompassing threat to American power and way of life.

D. THE THREAT FROM CHINA

Military strategic planners in China have recognized the geopolitical value of cyberpower, specifically as it relates to a new form of warfare. People's Liberation Army (PLA) Air Force Senior Colonels, Wang Xiangsui and Qiao Liang, published a definitive book on the subject of asymmetric warfare, of which they include cyberwarfare as a revolutionizing means of conducting war in the modern era. While their analysis generally includes the ways and means to mitigate U.S. military dominance, it also provides important insight into Chinese decision-making.

Wang and Qiao advocate the development of cyber capabilities that are intended to paralyze and undermine potential adversaries, but not to produce casualties.[83] Their conclusions come from the recognition that American weapon systems are completely reliant on technology, and that cyberweapons can become a cost effective way to equalize a high-tech battlefield environment. In an economic context, their strategic decision to advance the use of cyberweapons is one of necessity rather than choice. They recognize the financial cost of developing new weapon systems constrains China's ability to compete in a high-tech battlespace. Their solution therefore is the development of a

83 Qiao Liang and Wang Xiangsui, *Unrestricted Warfare* (Beijing: PLA Literature and Arts Publishing House, 1999), 29.

robust cyberwarfare capability that not only levels the playing field, but also acts as a deterrent for American decisions to project military power.[84] They write:

> [T]echnological progress has given us the means to strike at the enemy's nerve center directly without harming other things, giving us numerous new options for achieving victory, and all these make people believe the best way to achieve victory is to control, not to kill.[85]

For these Chinese strategic planners, future wars will be network wars. Wars that will likely involve no bloodshed, but be capable of determining the overall victor before kinetic weapons are employed.[86] However, Chinese strategic planning in this regard goes further than just classifying cyberattack as a means to conduct warfare, there is also a clandestine usage argument in their remarks.

For these strategic planners, the battlefield itself is no longer limited strictly to the traditional units of tanks, soldiers and large standing armies. As such, the modern battlefield also includes the cyber infrastructures of an opposing state, infrastructure that can be targeted and destroyed clandestinely if needed. This point is clarified in their own words, "the battlefield is omnipresent. Just think, if it's even possible to start a war in a computer room or stock exchange that will send an enemy country to its doom, then is there non-battlespace anywhere?"[87] While these writings may be intended to mislead as well as deceive the American national security decision maker, it is important to observe that their strategic thinking has been adopted by the current group of power holders in China. Evidence suggests that these decisions makers are primarily concerned with strategy and planning that seeks to neutralize a stronger and more powerful enemy.

A June 2011 article of the CCP newspaper *Youth Daily* (*Qingnian Bao*) notes that "the quantity of military intelligence information obtained over the Internet is large, the classification level is high, the information is timely and the cost is low, intelligence reconnaissance activities that are launched over the Internet are already omnipresent and

---

[84] Qiao and Wang, *Unrestricted Warfare*, 24.

[85] Ibid., 27.

[86] Ibid., 43.

[87] Ibid.

are extremely difficult to defend against."[88] As such, the value of understanding the progression of Chinese decision making with regards to cyberspace lies with the knowledge that Chinese strategy seeks to exploit the weakness inherent within the interconnected networks that drive the modern American military machine. David Shambaugh clarifies this point in his book *Modernizing China's Military*, "PLA strategists are convinced that they must fight the United States in ways that negate comparative American advantages while exploiting relative weaknesses."[89] It is the targeting of American military networks that they seek to exploit as a means to mitigate U.S. military advantage. These networks must therefore be made secure in the effort to assure America's ability to protect its national interest.

E. CHINA'S CYBER CAPACITY BUILDUP: TRANSITIONING FROM THEORY TO CAPABILITY

China's general lack of transparency with its military modernization obfuscates any assessment of its cyberwarfare capabilities. That said, there are certain aspects along the path of China's progression from strategic theory to the development of tangible cyber capacities under the auspices of the PLA that can be explored. PLA units are being trained and mobilized to "expand the types of targets or objectives for armed conflict to command and control systems, communications systems and infrastructure."[90] Strategic theory meets preparation at this juncture, where the PLA cyber units are staffed, trained and mobilized to support the totality of CNE, CND and CNA operations. The PLA unit established to conduct these activates has assumed the name "Online Blue Army."

Analysts are astute to point out that the term "Online Blue Army" was actually derived from a misconception on behalf of the media. In China opposition forces are given the term "Blue Army," and a media reference to a war game involving a cyber-

88 Ye Zheng and Zhao Baoxian, "How Do You Fight a Network War?" *Zhongguo Qingnian Bao* (June 3, 2011).

89 David Shambaugh, "Modernizing China's Military: Progress, Problems, and Prospects" (Berkeley, CA: University of California Press, 2004), 81.

90 Zhao Erquan, "Lun Xinxihua Zhanzheng dui Wuzhang Chongtu fa de Shenyaun Sixiang, " in Liu Jixian and Liu Zheng, eds., *Xin Jishu Geming yu Junshi Fazhi Jian she (The New Technical Revolition and Building Our Military)* (Beijing: Jiefang Jun Chubanshe, 2005), 498–505; as referenced in Larry Wortzel, "China's Approach to Cyber Operations: Implications for the United States," *Testimony Before the Committee on Foreign Affairs, U.S. House of Representatives* (Washington, D.C., 10 March 2010), 6.

opposition force led to the misclassification of the unit as an "Online Blue Army." Independent of the names origin is the fact that this name has come to represent China's CYBERCOM equivalent.[91] With the title well entrenched within the Chinese and Western media, the "Blue Army's" mission has been described as ensuring the security of China's military networks, protecting China's economic development and maintaining social stability.[92] While these acknowledgements confirm the establishment of a PLA cyber component, they do not address the means by which the unit seeks to achieve its goals, or how it is situated within the PLA's command structure.

On July 19, 2010, the PLA General Staff Department (GSD) unveiled the Information Support Base (ISB), which Western analysts have determined to be similar in scope and mission to USCYBERCOM. The ISB has been tasked to deal with cyberthreats and safeguarding China's national security.[93] Further structural revelations have determined the PLA GSD Third Department and Fourth Department to be the two largest players in China's burgeoning cyber infrastructure.[94] Of these two departments, the Third Department has assumed the responsibility for assuring the security of PLA computer systems in order to prevent access to sensitive national security information.[95] Additionally, the Third Department is the PLA's recognized signals intelligence command; and as such, it can be assessed that the Third Department is also responsible for coordinating China's CNE capabilities and its cyberespionage activities.

While the strength of China's cyber command component remains elusive and will most likely remain so as a means to create deterrent value, it is reported that the unit relies on a PLA "cyber militia" that uses private sector experience to improve upon the unit's CNE capabilities.[96] Specifically. this analysis indicates that China's cyber

---

91 Krekel, Adams, and Bakos, "Occupying the Information High Ground," 23.

92 Guo Lei, Gu Caiyu, and Wu Lan, "Why China established 'Online Blue Army'," *People's Daily* (28 June 2011), <http://english.people.com.cn/90001/90780/7423270.html> (13 April 2012).

93 Mark Stokes, Jenny Lin, and Russell Hsiao, "The Chinese People's Liberation Army Signals Intelligence and Cyber Reconnaissance Infrastructure," *Project 249 Institute* (11 November 2011), 2.

94 Ibid.

95 Ibid. 2–3.

96 George Wittman, "China's Cyber Militia," *The American Spectator* (21 October 2011).

command is supplemented by part-time citizens in both the academic and commercial sectors. While the veracity of such an alignment is oblique, it is important to note that China's cyber capabilities are not hindered from a lack of talent or experience. Chinese military experts attempt to obfuscate this fact by indicating that its online military capacity is still in a "fledging state" when compared with those of Western nations.[97] In contrast, a more subjective analysis indicates that China's strategic direction is in favor of offensive cyber capabilities as seen through the development of a military command structure. This points to an offensive cyber capability that is larger and more defined than what the Chinese state is willing to acknowledge.

The People's Republic of China is regarded by many to be a grave threat to the United States with the capability and motivation to collect against the most sensitive and classified of U.S. information and technology.[98] However, it is important to clarify that culpability of the Chinese state in the commission of hostile cyber activities directed against the United States remains unproven. U.S. policy and analysis documents that disclose the Chinese cyberthreat are always astute to address this fact. Yet, the lack of a "smoking gun" does not negate the importance of circumstantial evidence in the production of American policy or an effective counterintelligence structure to investigate, harden against and deter hostile cyber activity derived within the PRC.

F. THE CIRCUMSTANTIAL EVIDENCE, WHAT DOES IT TELL US?

An unsubstantiated U.S. State Department report uncovered in the wake of the Google's Aurora incident claims that the order to initiate the operation was given from within the Standing Committee of the Chinese Communist Party.[99] The evidence for this

---

97 Su Jie, "PLA 'Online Blue Army' gets ready for cyber warfare," *ECNS.cn Online*, (16 January 2012), <http://ecns.cn/2012/01–16/6254.shtml> (18 April 2012).

98 This concept is referenced and repeated in numerous authoritative texts, to include: Clark and Knake, "Cyber War: The Next Threat to National Security and What To Do About It,"; Brenner, *America the Vulnerable: Inside the New Threat Matrix of Digital Espionage, Crime and Warfare*; Office of the National Counterintelligence Executive, *Security Counterintelligence: Foreign Spies Stealing U.S. Economic Secrets in Cyberspace, Report to Congress on Foreign Economic Collection and Industrial Espionage 2009–2011*; and Stokes, Lin, and Hsiao, "The Chinese People's Liberation Army Signals Intelligence and Cyber Reconnaissance Infrastructure."

99 Ellen Nakashima, "Chinese Leaders Ordered Google Hack, U.S. Was Told," *The Washington Post* (5 December 2010).

allegation appears to come from a single source, making it circumstantial at best and false at worst. However, nearly all other incidents that detail public knowledge of Chinese state-directed cyberespionage include similar claims of circumstantial evidence. In February 2012, the National Aeronautics and Space Administration's (NASA) inspector general testified before Congress that in the previous year NASA had sustained 47 Advanced Persistent Threats (APT)—a term used to indicate a level of cyberattack that involves a well-resourced and skilled attacker, the term is usually reserved to indicate state activity—13 of which had successfully compromised NASA networks. The most significant of these attacks were traced back to a Chinese-based Internet Protocol (IP) address and included the penetration of NASA's Jet Propulsion Laboratory (JPL). The attackers gained full access to JPL's computer systems and sensitive user accounts, allowing them full functional control of the network.[100]

In light of the NASA JPL incident, it is important to clarify that circumstantial evidence relying on IP addresses resolving to China do not necessarily prove a meaningful connection to the Chinese government. Rather, more powerful analysis for determining CCP complicity resides with the nature of the information sought from exploitation. This analysis has led an Assistant U.S. Deputy Secretary of Defense to state:

> When looking across the intrusions of the last few years...a great deal of it concerns our most sensitive systems, including aircraft avionics, surveillance technologies, satellite communications systems, and network security protocols. The cyber exploitation being perpetrated against the defense industry cuts across a wide swath of crucial military hardware, extending from missile tracking systems and satellite navigation devices to UAVs and the Joint Strike Fighter.[101]

Circumstantial evidence indicative of Chinese state involvement in the context framed above typically deals with the non-monetary value, or overall lack of a market value, for the secret defense related information stolen during such cyberespionage events.[102] The

---

[100] Paul Martin, "NASA Cybersecurity: An Examination of the Agency's Information Security," Testimony before the Subcommittee on Investigations and Oversight, House Committee on Science, Space, and Technology, U.S. House of Representatives (29 February 2012), 5.

[101] Lynn, "Remarks on the Department of Defense Cyber Strategy."

[102] Krekel, Adams, and Bakos, "Occupying the Information High Ground," 96.

information typically compromised during these intrusions has little underground or criminal market value, as governments tend to be the dominant end-users or benefactors for such secret material and high-tech military grade technology. While this factor does not point empirically to China, it does suggest that a large state or states with significant military capacity is behind such hostile actions. This fact allows for analysis that indicates only a few states have the capacity and motivation to conduct cyberespionage. In other words, not all states have both an ability to implement stolen information into their own military weapon systems and the strategic outlook to produce an asymmetric means to balance against U.S. military dominance.

Circumstantial evidence of state-directed hostile cyber activity seen through this optic predominantly points to China, Russia and Iran as the perpetrators that fit the above referenced model. While such analysis may be significant, it is not sufficient to induce the U.S. decision maker to accurately determine Chinese state involvement or accordingly develop policies that effectively aim to label China as a state sponsor of hostile cyber activity. Thus, a more concise understanding of state involvement is needed with regard to China. Such an understanding is properly attained through analysis of the motivations behind China's current cyber capacity buildup. This examination changes the focus of the culpability debate as it places an imperative on the logical elements for state sponsorship rather than a search for the evidence. There are generally four accepted reasons for states to develop, maintain and utilize an aggressive cyber capability:

1. For deterrent value, by infiltrating and demonstrating a capability to exploit the vulnerabilities of another state's critical infrastructure.[103]
2. For cyberespionage, aimed at producing classified plans or technology that makes it possible for states to advance their military development at increased speed.[104]
3. For cyberespionage, to make economic gains through industrial espionage. This provides an economic advantage for the state's commercial interests as they compete in the global economic system.[105]

[103] Magnus Hjortdal, "China's Use of Cyber Warfare: Espionage Meets Strategic Deterrence," Journal of Strategic Security, vol. 4, no. 2 (2011), 3; Wortzel, "China's Approach to Cyber Operations: Implications for the United States," 4–5.

[104] Ibid.

[105] Ibid.

4. For cyberwarfare, to degrade or paralyze an adversary's military capacity.[106]

Looking at China's cyber capacity build-up through the lens of these four reasons leads to a logical conclusion that it is in China's best interest to develop hostile cyber capabilities.

Within international relations parlance, there is a generally accepted observance that China employs a defensive realist security strategy.[107] China's adherence to this model of international engagement necessitates that it refrain from offensive realist strategies, or those strategies that place an imperative on the accumulation of power at the cost of decreased relations with neighboring countries or cooperation in international agreements. China's path toward defensive realism is dictated in part by its geographic location and the realization that if it were to choose offensive policies, its neighbors would easily be able to develop balance of power alliances to constrain PRC actions.[108]

Thus, while China is forced to follow defensive realist polices that place a greater need for it to participate constructively in multilateral organizations, the development of offensive cyber capabilities does not jeopardize its defensive realist position. In other words, cyberpower remains a tool by which the Chinese state can maintain both a defensive realist posture while developing a strong offensive capability. Cyberpower's non-attribution quality makes this possible. China's position is strengthened by this aspect of cyberpower, for it does not truly have to demonstrate offensive capability but rather only the semblance of one. In this respect, Chinese involvement in hostile cyber activities simply becomes the rational expression of its security strategy.

G. BREAKING DOWN CHINA'S CYBER CAPACITY: A CLOSER LOOK AT THE FOUR REASONS THAT STATES DEVELOP OFFENSIVE CYBER CAPABILITIES

Looking closer at each of the four reasons that states develop aggressive cyber capabilities from the perspective of China's national decision makers provides insight into the PRC's cyber capacity. China appears mainly concerned with minimizing political

106 Ibid.; Wortzel, "China's Approach to Cyber Operations," 6.

107 Robert Ross and Zhu Feng, *China's Ascent: Power, Security, and the Future of International Politics* (New York: Cornell University Press, 2008), 154.

108 Ibid., 157.

and military pressure from the United States.[109] Developing and demonstrating a cyber capability to affect the critical infrastructure of the United States at a time of China's choosing is thus a successful deterrent to American action. This forces U.S. decision makers to question Chinese capabilities and weigh the risk of their action against the possibility that China could shut down key elements of the nation's critical infrastructure via cyberattack. However, for this capacity to be an effective deterrent it must be demonstrated with results that not only prove the vulnerability of American infrastructure, but also provide suspicion of Chinese state involvement. In other words, a clandestine capability alone would not be a deterrent; the capacity must be demonstrated and tied to the Chinese government at least through speculation. Is there evidence that this has occurred?

In 2009, investigation revealed that an APT had installed software programs onto the cyber network that controls the U.S. electric grid. [110] The action proved significant for inducing U.S. decision makers to suspect that foreign states may have placed undetected backdoor control mechanisms within U.S. infrastructure networks. In this instance, the need to prove a capability to actually shut down the electric grid became minimized strictly by creating the perception that it might be possible. The 2009 investigation into the electric grid network penetration prompted Joel Brenner, the National Counterintelligence Executive, to state, "we have seen Chinese network operations inside certain [elements] of our electricity grids."[111] These attacks point to a state sponsor and moreover, they appear intended to convey a deterrent effect on the use of American power. As such, the reason for China to conduct hostile cyber activities in support of the first reason listed above is quite clear; it creates an added capacity to deter American hegemonic pressure.

---

[109] Hjortdal, "China's Use of Cyber Warfare: Espionage Meets Strategic Deterrence," 4.

[110] Siobhan Gorman, "Electricity Grid in U.S. Penetrated by Spies," *Wall Street Journal* (8 April 2009); "Cyber spies assault U.S. power grid," *Jane's Intelligence Digest* (5 May 2009), 1.

[111] Joel Brenner, "Business Strategies in Cybersecurity and Counterintelligence: Remarks by the National Counterintelligence Executive," Applied Research Laboratories (University of Texas at Austin, 3 April 2009), 3.

The second reason, using cyberespionage to gain military or technical information, can be seen in similar fashion. China's military capabilities remain behind those of the West and will remain so for the foreseeable future.[112] China realizes that it cannot outspend or out-innovate the United States when it comes to developing and fielding the military technology. Gaining access to such technology through espionage is therefore a force multiplier for China's military modernization efforts, especially as cyberespionage has proven to be more effective, more affordable and less risky than traditional collection methods.[113] Evidence that supports this supposition points to the October 2011 case involving RSA Security (RSA is a global leader in the development and service of high-end network encryption devices). In March 2011, RSA had its systems hacked and encryption algorithm stolen for its remote access authentication token. Both the RSA executive chairman and the analysts who have looked into the incident generally agree that the attack was state sponsored.[114] RSA's clients include Fortune 500 companies, government agencies and major defense contractors.

The RSA breach consequently resulted in a cyberespionage exploitation attempt of Lockheed Martin's secure network. This brought about speculation that the company's secret data, which includes information on the F-22 and F-35 Joint Strike Fighter, was compromised. Lockheed denied publically that any damage was done or information pilfered.[115] However, it is known definitive that the attack on Lockheed and RSA was a multi-stage cyberespionage operation that included intense planning, reconnaissance and operational knowledge. [116] In addition to its complexity, the information sought pertained strictly to defense-related intellectual property on Lockheed's two fifth-

112 Hjortdal, "China's Use of Cyber Warfare: Espionage Meets Strategic Deterrence," 4.

113 Brenner, *America the Vulnerable*, 74.

114 John Leyden, "RSA Defends Handling of Two-Pronged SecurId Breach," *The Register* (11 October 2011).

115 Jim Wolf, "Lockheed Martin hacked using RSA keys: Data Breach at the Pentagon's Largest Supplier," *ITNEWS* (30 May 2011).

116 Christopher Drew and John Markoff, "Data Breach at Security Firm Linked to Attack on Lockheed Martin" *New York Times* (27 May 2011).

generation fighters.[117] Such information points most decisively to state involvement. Only a handful of states have the capacity or intent to capitalize on such information.

The third reason, involving cyberespionage for economic gain, can also be supported with analysis and case study. China's general technological competency still lags behind the United States, which gives it an increased incentive to engage in industrial espionage to gain greater economic advantage.[118] This is especially true given that the legitimacy of the Chinese Community Party (CCP) is increasingly tied to its ability to produce year-after-year economic growth. Even as the CCP attempts to develop other factors upon which to build legitimacy—namely societal stability and national unity—the true underpinning of legitimacy remains unimpeded economic growth.[119] This is evidenced by the manifestation of social unrest in China whenever the economy lags and through the large capital requirements needed to support national unity programs like the hosting of the 2008 Olympic Games. Economic growth alone and the maintenance of it, provides an abundance of incentive for the Chinese government, companies and sovereign investment funds to partake in economic espionage on a global scale. The transferral of this imperative to the cyberdomain is summarized as follows:

> During peacetime, computer network exploitation has likely become a cornerstone of PLA and civilian intelligence collection operations…[t]he apparent expansion of China's computer network exploitation (CNE) activities to support espionage has opened rich veins of previously inaccessible information that can be mined both in support of national security concerns and, more significantly, for national economic development.[120]

The fourth reason, developing a capacity to degrade the superior combat forces of a Western advisory (in effect to level the playing field), has already been explored through analysis of Wang and Qiao's strategic and doctrinal suggestions. However, it is important to note how these strategic decisions have affected China's modern military

---

[117] Drew and Markoff, "Data Breach at Security Firm Linked to Attack on Lockheed Martin."

[118] Hjortdal, "China's Use of Cyber Warfare: Espionage Meets Strategic Deterrence," 4.

[119] Office of the Secretary of Defense, "Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2011," (2011), 1.

[120] Krekel, Adams, and Bakos, "Occupying the Information High Ground," 107.

build-up in terms of a real capacity. The creation of a Chinese Blue Army and the development of a command unit similar in scope and mission to USCYBERCOM, is the manifestation of Wang and Qiao's strategic thinking in terms. The creation of an online army in this capacity is tantamount to the continued observance of balance of power strategy that has summarized Chinese foreign policy throughout modern history.[121] In the context of its own security and the unipolar world order, China's balance of power strategy cannot seek to traditionally balance with another state against U.S. cyberwarfare capabilities. As such, China seeks to balance American dominance of cyberspace with a buildup of its own cyberwarfare capability. In this process, China and the U.S. usher in a security dilemma with regard to cyberspace. The cyber capacity developments from both sides indicate any military conflict between the United States and China would include hostile cyber activates during all phases of the conflict.

H. CONCLUSION

Discovering evidence of Chinese state involvement within the various instances of hostile cyber activity directed at the United States is not necessary to determine the courses of action available to the U.S. decision maker with regard to bolstering America's cyber defense and offensive capabilities. Several defensive initiatives are already in the works, to include the deployment of robust intrusion detection systems like EINSTEIN 2 and EINSTEIN 3 (systems established by DHS to monitor network activity on government computers and provide real-time alerts on unauthorized access and malicious activity).[122] However, in a rapidly changing environment like cybersecurity, defensive systems alone are not adequate to effectively protect against or deter

121 Professor Nan Li at the U.S. Naval War College lays out the foundation of Chinese foreign policy as a continual progression of balance of power policies. His evidence for this is in regard to the transformation of the People's Liberation Army from a force structured to fight a "people's war" to a modern fighting force focused on "local limited wars under high tech conditions." This transition reflects a continuous trend on China's part to balance against the dominant threat and to structure the PLA according to their perceived threat. See Nan Li, "The PLA's Evolving War fighting Doctrine, Strategy, and Tactics, 1985–1995: A Chinese Perspective," in David Shambaugh and Richard Yang, eds., *China's Military in Transition*, (Oxford: Clarendon Press, 1997), 179–199.

122 Kim Zetter, "U.S. Declassified Part of Secret Cybersecurity Plan," *Wired* (2 March 2010).

cyberthreats. The national decision maker is consequently faced with the need to develop effective defensive alternatives, and such methods include expanded offensive capabilities.

Unfortunately, both offensive and defensive capabilities take time to develop. General Keith Alexander, Commander U.S. CYBERCOM, addressed this concept with Congress in 2010:

> In the cyberdomain, however, we are just beginning to craft new doctrine and tactics, techniques, and procedures…we are developing doctrine for a pro-active, agile cyber force that can "maneuver" in cyberspace at the speed of the Internet; and we are looking at the ways in which adversaries might seek to exploit our weaknesses.[123]

Addressing the timely development of proactive-offensive capacities can generally include greater integration of offensive counterintelligence capabilities that are currently available to the strategic decision maker. In fact, the concept of a government-wide cyber counterintelligence plan was addressed by President Obama's Comprehensive National Cybersecurity Initiative.[124] Addressing this need employs the concept that realigning the U.S. counterintelligence enterprise with authorities and structures to immediately benefit the offensive cyber mission is a crucial first step in addressing a whole of government approach to cybersecurity.

Finally, as a realist actor within the international system, China has much to gain by developing and partaking in cyberespionage, computer network exploitation and the development of a cyberwar capability directed at the United States. In this vein, the U.S. decision maker does not have to wait for a smoking gun of evidence to take steps that will improve upon the defensive and offensive capabilities of the U.S. national security establishment to plan for and mitigate these attacks. A large part of this process is to recognize that the U.S. counterintelligence enterprise has a large role to play in the

---

[123] Keith Alexander, "Testimony of the Commander United States Cyber Command, Before the House Committee on Armed Services Subcommittee on Emerging Threats And Capabilities" (Washington D.C.: United States House of Representatives, 20 March 2012), 12.

[124] Executive Office of the President of the United States, "The Comprehensive National Cybersecurity Initiative," Online Paper (2010), 4, <http://www.whitehouse.gov/sites/default/files/cybersecurity.pdf> (23 February 2012).

development of these capabilities, and that its cyber elements need to be effectively organized to best impact its mission. While the goal of this thesis is to prove that this capability increase is warranted, in an effort to explore the other options available to the decision maker, one must look at the possibility for international agreements to limit the damage to American national security as well. The next chapter is dedicated to an exploration of the international options that are currently on the table.

III. INTERNATIONAL ATTEMPTS TO REGULATE CYBERSPACE: LESSONS FROM ESTONIA

A. CHAPTER INTRODUCTION

This chapter assesses the international community's attempt to regulate cyberspace as a means to limit hostile cyber activity within the international system. It uses the 2007 cyberattack against Estonia to develop a working foundation that will be used to assess the fundamental issues effecting cybersecurity. This foundation is then used to analyze the implications for a variety of international regulatory mechanisms proposed by scholars, international institutions and states. In analyzing these existing and proposed international mechanisms, this chapter determines that effective mitigation is neither guaranteed nor achievable in the short term. As a means to assess the American national security decision maker's options for effective mitigation of the national cyberespionage threat, this chapter concludes after exploring the drawbacks of these proposals and determining the need for more timely and effective measures for cyberthreat mitigation.

B. CYBERSPACE: THE CONTEMPORARY CONTEXT OF CYBERWAR, CYBERATTACK AND STATE RESPONSE

Hostile cyber activities—including cyberattack for political gain, cyberwarfare and cyberespionage—are all threats that jeopardize a states' ability to consolidate power within its own territory or project power beyond its borders. It is imperative that the international community recognize and deal with these threats. This realization stems primarily from the lessons learned in Estonia during the April-May 2007 cyberattack that became known as the first information war in Europe's history.[125] In fact, apart from the *Titan Rain* attacks against the U.S. defense industrial base and NASA in December of 2005, it stands as the quintessential event in posing important political questions about

[125] Stephen Blank, "Web War I: Is Europe's First Information War a New Kind of War?" *Comparative Strategy*, vol. 27 (2008), 227–247.

the larger definition of cyberwar, cyberattack and state-alliance responses to the same. As such, the Estonian cyberattack forces an examination of the current and future structure of the international cyberdomain.

This chapter uses the Estonian case to deal with the fundamental questions that this event imposed; namely, the use of the cyberattack as a tool of political influence, the challenge with state attribution and the changes to state behavior that have occurred as a result. While previous chapters dealt principally with the cyberthreat emanating from major state actors like China, the Estonian case provides a different geographic area of study that yields similar results. The fundamental issues that affect the United States with regard to cyberespionage crosscut all geographic domains.

C. ESTONIA CASE BACKGROUND

In April 2007, the city government of Tallinn, Estonia, announced plans to remove a Soviet military statue from the city's center to a military graveyard on its outskirts. The statue was initially erected to honor Soviet soldiers who died during World War II. As such, to the majority of Estonia's population, the statute had become a symbol of Soviet annexation and occupation.[126] Conversely, for Estonia's one-quarter ethnic Russian population, its removal was an insult. In Russia, an outcry of nationalistic fever resulted in demonstrations and the targeting of the Estonian government. Russian language websites encouraged protesting and Internet activism. On April 25, the first of three waves of cyberattacks commenced in what some have called a "politically motivated cyber-riot."[127] These cyberattacks were primarily comprised of unsophisticated Distributed Denial of Service (DDOS) tools employing botnets to flood and disrupt service to the cyber infrastructure of the Estonian government, media and banking sectors. This was the largest DDOS attack ever seen in Estonia and as one of the most wired nations in Europe, the rest of Europe took particular interest in the

126 Roland Heickero, "Emerging Cyberthreats and Russian Views on Information Warfare and Information Operations," *Swedish Defense Research Agency* (March 2010), 39.

127 Gadi Evron, "Authoritatively, Who Was Behind The Estonian Attacks," *Security Dark Reading* (17 March 2009).

vulnerability of the Estonian infrastructure to cyberattack.[128] Thus, although the attack itself was labeled unsophisticated, its ability to disrupt civil society demonstrated to the international community the severity of the cyberthreat to the global order.

D. DIFFICULTY OF STATE ATTRIBUTION

In the wake of a hostile cyber activity, one goal for the forensic cyber investigator is to determine the organizations or individuals responsible. In order to conclusively determine these factors, investigators must first obtain evidence from within two subsets of attribution, technical and human attribution. Technical attribution consists of an analysis of a hostile action to classify the malicious cyber tools used and then locate the controlling or initiating cyber node.[129] This includes tying the attack to an IP address or to a specific machine used in the attack. Human attribution builds upon the results of technical attribution to identify the person or organization responsible for the attack.[130] This could include determining the identity of the person who was logged into the machine during the attack period, or identifying the government organization where one or more simultaneous attacks originated. Positive attribution is therefore, the development of conclusive evidence from both technical and human attribution investigations. This is a level of attribution that is rarely achieved in the cyber environment due to the high levels of anonymity built into the structure of the cyber domain.

Adding to the difficulty of attaining positive attribution are impediments with the conversion of technical analysis into identifiable human attribution. In other words, tracing an event back to a specific IP address or machine does not guarantee attribution to a singular human operator. Proving an individual responsible for a hostile cyber activity is complicated due to a variety of effective defense techniques that include evasion, deception and sheer denial.[131] Savvy defense lawyers can easily construct these concepts

---

128 Richard Clarke and Robert Knake, *Cyber War* (New York: Basic Books, 2010), 13–14.

129 Earl Boebert, "A Survey of Challenges in Attribution," in *Proceedings of a Workshop on Deterring Cyberattacks*, National Research Council (The National Academies Press, 2010), 43.

130 Ibid.

131 Boebert, "A Survey of Challenges in Attribution," 49.

into reasonable doubt, which can lead a jury to believe that the individual identified through human attribution was not actually involved in the attack. This defense can be deconstructed in a U.S. court of law with proper evidence, but when attacks originate in a foreign country the issue of human attribution becomes complicated.

In the United States, once a machine has been identified as having participated in an attack through technical attribution, authorities can typically gain access to it. Access then provides an opportunity to determine the presence of malicious code and allows further assessment of the cyber knowledge level of the machine's key operator. These elements can establish human attribution where legal proceedings can hold responsible the perpetrators of cybercrime. However, in an international environment—where jurisdictional and political lines blur—gaining access to a machine for purposes of forensic deconstruction is nearly impossible.[132] Proving state involvement in hostile cyber activities, therefore, becomes a significant hurdle to diplomatic means of curtailing such activity in cyberspace.

The Estonian case provides a working context by which to analyze these difficulties of positive attribution. In the aftermath of the attack, the Estonian foreign minister claimed an investigation had determined a portion of the attack originated from official Russian government IP addresses; yet, their investigation lacked the sufficient human attribution quality needed for positive attribution.[133] The Russian government denied direct involvement in the activity and demanded that such claims be supported with evidence. With only technical attribution, the Estonian claims were incomplete. Furthermore, technical analysis of the attack showed IP addresses emanating from 178 countries and from more than one million computers.[134] The cyberattacker in this case was able to hide within the large volume of cyber activity, gaining a cyber safety-net from positive attribution.

---

[132] Nicholas Cowdery, "Emerging Trends in Cybercrime," paper presented at the 13th Annual International Association of Prosecutors Conference, *New Technologies in Crime and Prosecution: Challenges and Opportunities* (Singapore, 28 August 2008), 4–5.

[133] Arthur Bright, "Estonia accuses Russia of 'cyberattack'," *The Christian Science Monitor* (May 17, 2007), <http://www.csmonitor.com/2007/0517/p99s01-duts.html> (14 February 2012).

[134] Heickero, "Emerging Cyberthreats and Russian Views on Information Warfare and Information Operations," 41.

Circumstantial evidence can assist in determining human attribution, but it can also become mired in a swarm of contradicting variables. This occurred in the Estonian case through anonymous postings on Russian language websites that instructed participants how to run DDOS attacks or lease botnets for use against Estonia.[135] These anonymous postings could not be attributed to either clandestine government units or cyber hacktivists alone. Inconsistent statements made from numerous individuals within Russian state bureaucracies and state-sponsored youth movements effectively manipulated speculation over the origin of the attack.[136] As a result, attempts to prove attribution can became rather meaningless in the larger context, leading the policy maker to searching for additional options.

E. LESSON'S LEARNED FROM THE ESTONIAN INCIDENT

1. Forcing the International Community to Action

The Estonian attack served as a wake-up call for the international community. Although speculation remained regarding attribution, the case proved that state power projection capabilities had changed and that *cyberpower* had arrived. This forced states to reevaluate the means of power projection to include such non-attributable cyber methods that destabilize society, cause economic turmoil and spread distrust of state institutions.[137] In addition, the attack forced the international community to evaluate the definition of "cyberattack." Does such an attack amount to an act of aggression that affords the effected state the right to self-defense in accordance with Chapter VII, Article 51, of the United Nations Charter,[138] or is it something else?

Recognition of this complication by the international community has placed a greater emphasis on the development of a stronger regulations process and the need to

135 Bright, "Estonia accuses Russia of 'cyberattack'."

136 Leaders of *Nashi*, a political youth group started by Russian President Putin to defend the state against fascists, liberals, and oligarch-capitalists, claimed responsibility for the attack.

137 Blank, "Web War I," 230.

138 United Nations, "Charter of the United Nations: Chapter VII," <http://www.un.org/en/documents/charter/chapter7.shtml> (17 March 2011).

reach international consensus on what constitutes a hostile cyberattack.[139] The establishment of the Cooperative Cyber Defense Center of Excellence (CCDCE) in Tallinn, Estonia, is the manifestation of this realization by the European Union. Apart from the creation of a new European institution to deter and address cyber challenges, the incident was valuable in serving as a catalyst for dialogue regarding the institutional changes needed to classify, mitigate and politically address the future of cybersecurity.

The Estonian cyberattack also forced the international community to evaluate the role of cyberpower for state and non-state actors, and it further clarified the centrality of the attribution problem as a fundamental catalyst for cyber conflict.[140] This demonstrated the need for cooperative security reform as a means to limit cyberattack through greater attribution techniques. Positive attribution becomes a clear goal for any state or international security organization wishing to partake in the benefits of an interconnected world while reducing the risk of subversion. Only through positive attribution can cyber-attack become analogues to kinetic attack and subsequently be classified as an act of war. Developing this link should be the goal of cooperative security organizations. Creating this connection would remove the means by which cyberattack is conducted anonymously, thus improving state security in a globally connected world. While this becomes the goal, achieving this end raises questions about the international community's capacity to achieve this level of attribution and even the degree to which such attribution would be desired if it could be attained.

2. Does Attribution Even Matter?

Within the realm of accusations, denials and claims of responsibility, the value of studying the details of the Estonian case lies in its ability to provide a more comprehensive understanding of the difficulty with attributing cyber activities to any one state or state institution. This lack of attribution places an imperative on the aspects of the Estonian attack that were definitive; namely, that the attack was organized, effective and

139 Clarke and Knake , *Cyber War,* 228.

140 Kenneth Lieberthal and Peter Singer, "Cybersecurity and U.S.-China Relations," 21st Century Defense Initiative, John L. Thornton China Center at Brookings (February 2012), 29.

politically motivated.[141] The ability to conduct cyber activities anonymously provides a distinct advantage to the cyberattacker over the cyberdefender. This advantage is magnified due to the low barriers to entry associated with Internet access and the widespread technical knowledge regarding the commission of such actions. The knowledge needed to produce malicious code or software for use in a cyberattack does not necessitate the intensive resources of a state, "brilliance in software development can be found anywhere, and the only physical resources required are a laptop and an Internet connection."[142] Thus, with careful planning almost any state or non-state actor can conduct a cyberattack with a high degree of plausible deniability.[143] This creates a significant problem for the international community and for the national security agencies responsible for mitigating cyberthreats.

Even in cases where both forms of attribution have been determined, taking the evidence to the international community through public disclosure has consequences that may override the decision to take such actions. The attacked state must be mindful that disclosing the methods and means that produced such attribution would consequently provide intelligence to the attacking state regarding how to modify its operations or make them more effective in the future.[144] This would not only strengthen the future capabilities of an adversary to conduct cyberattack, but could also produce political blowback. This is especially true when other factors are present, such as extensive commercial or political ties between states as is the case between the United States and China. In this regard, the complex interdependence between these states does not negate the benefits of clandestine cyber behavior, but it may produce obstacles to attribution out of fear that such public disclosures may damage other critical aspects of the relationship.

---

141 Evron, "Authoritatively, Who Was Behind The Estonian Attacks?"

142 Boebert, "A Survey of Challenges in Attribution," 43.

143 William Owens, Kenneth Dam, and Herbert Lin, "Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities," National Research Council (The National Academies Press, 2009), 141.

144 Wortzel, "China's Approach to Cyber Operations: Implications for the United States," 2.

3. Cyberattack as a Tool for Political Purpose

One key piece of circumstantial evidence presented in the aftermath of the Estonian attack revealed Russian planning and strategy documents that approved cyberattack as an asymmetric implement for achieving the state's political objectives.[145] Cyberattack as a mean to project power was therefore realized and planned for by the Russian government prior to the Estonian attack. In this context, the attack itself may have been the execution of a state policy that involved the use of cyberattack to exercise political influence upon another nation. However, absent an ability to prove Russian state involvement, the importance of this factor becomes the global recognition that cyberattack can be used as a means for the state to project its political will upon another in a non-attributable fashion. This changes the power paradigm through which states have traditionally exerted influence and it adds a new dimension to the study of international relations between states.

Cyberpower is "the ability to use cyberspace to create advantages and influence events in other operational environments and across the instruments of power."[146] Joseph Nye Jr., addresses the growth of power in the cyberdomain as a new and revolutionizing force. Nye clarifies that state use of cyberpower can produce preferential outcomes both *within* and *outside* the cyberdomain.[147] Cyberattack as a tool of political power is therefore two-sided. On one side, it can be used as a clandestine means of influence and intimidation, as seen in the Estonian example. On the other, as seen through the lens of China's strategic military planners (covered in the previous chapter), it can be used to deter military intervention and even mitigate substantial technologically driven military advantages.

---

145 Blank, "Web War I," 231.

146 Daniel Kuehl, "From Cyberspace to Cyberpower: Defining the Problem," in Franklin Kramer, Stuart Starr, and Larry Wentz, eds., *Cyberpower and National Security* (Washington, D.C.: National Defense University, 2009), 38.

147 Joseph Nye, "Cyber Power," *Belfer Center for Science and International Affairs* (Harvard Kennedy School, Cambridge, MA: May, 2010), 3–4.

F. INTERNATIONAL AGREEMENTS THAT REGULATE CYBERSPACE

The current cyber environment has changed the dynamic by which the decision maker must address threats to national security. In the recent past, states could detect, deter and implement advanced early warning systems with technology, or rely on enforceable international agreements that limited state behavior.[148] The contemporary properties of cyberspace—speed, lack of attribution, ease of knowledge and monetary efficiency—have all but erased the traditional political tools used to avert cyberattack. While cybercrime and cyberwarfare do not currently maintain the same destructive properties of past weapons of mass destruction, cyberattack is used with prevailing frequency. The need to counter state-to-state cyberattack therefore appears to necessitate an international solution built upon normative patterns of behavior and international agreements that constrain the state use of cyberweapons for military purposes, while building strong international cooperative mechanisms to effectively investigate and prosecute transnational cybercrime.

While this approach is currently being explored as a means to limit cyberattack, cyberwarfare and cybercrime, it generally omits cyberespionage. It is important to clarify that cyberespionage juxtaposed to these others threats is not considered equivalent and its omission is largely intentional.[149] All states employ intelligence services, and nearly all states use those services to commit espionage on behalf of their own national interest. Cyberespionage is therefore seen as a tacit *quid-pro-quo* in that it serves the interests of individual states while at the same time it jeopardizes the national security of others. As such, states are reluctant to include cyberespionage language in any international mechanism that seeks to limit hostile cyber activity.[150] The United States is principally guilty of this, but it suffers from a duality not shared by most states. While the United States has significant signals intelligence capacity, it also remains the main target for cyberespionage. Other states have an equal amount to gain from cyberespionage, but their

148 See for example the U.S. Defense Support Program (DSP) and the Russian PROGNOZ early warning satellites, both programs monitored the potential launch of Intercontinental Ballistic Missiles (ICBM) and proved to be a valuable accountability mechanisms.

149 Clarke and Knake, *Cyber War*, 236–237.

150 Ibid.

vulnerability to such action is much less. Thus, the lack of cyberespionage language from current international proposals to limit hostile cyber activity leaves the national security policy maker with little confidence that the cyberespionage threat posed to the United States can be curtailed through such liberal or constructivist attempts alone.

G. ATTEMPTS TO PROVIDE INTERNATIONAL REGULATIONS ON CYBERSPACE

The current trend toward development of international treaties, agreements and norms of behavior to restrict nation-state use of cyberspace as a tool of political or military power lacks impact. In 1998, the Russian Federation introduced to the General Assembly of the United Nations a resolution calling for greater international restrictions on cyberspace activities. Resolution 53/70 titled *Developments in the Field of Information and Telecommunications in the Context of International Security* attempted to broaden the context of security and disarmament to the cyberdomain. The United States and several European states generally opposed this resolution due to concern that "such a treaty could be used to limit the freedom of information under the guise of increasing information and telecommunications security."[151] The United States finally signed onto a modified form of the resolution in 2009 after the Russian government strengthened the resolution to address these U.S. concerns.[152] Consequently, the resolution has become a non-binding agreement between signatory states who only agree that further discussion is warranted in an attempt to reach mutual understanding regarding cybersecurity. In this form, the UN resolution is merely a tool to spur further dialogue and the UN itself simply a forum for future cooperative exploration.

On September 14, 2011, an international cyber code of conduct governing information security was developed within the United Nations General Assembly and sent to the general secretary for dissemination. The drafters of this code of conduct, Russia, China, Uzbekistan and Tajikistan, appear to recognize the need for greater

---

151 Tim Maurer, "Cyber Norm Emergence at the United Nations: An Analysis of the UN's Activities Regarding Cyber-Security?" *Discussion Paper 2011–11* (Cambridge, MA: Belfer Center for Science and International Affairs, Harvard Kennedy School, September 2011), 21.

152 Franz-Stefan Gady and Greg Austin, "*Russia, The United States, and Cyber Diplomacy: Opening the Doors*," East West Institute, (New York, 2010), 3.

international engagement on the principles that govern state conduct within cyberspace, but their intentions for leading the effort on a code of conduct to govern behavior in this realm appear questionable. Russia and China both have negative records when it comes to the use of cyberspace to project state power. Russia is generally regarded as the only state to use cyberweapons in a non-war context, as evidenced in the Estonian case. For its part, China has sought to control the distribution of information its citizens receive through cyberspace with the implementation of The Great Firewall. This action limits Internet freedom and allows for the monitoring of dissident activity, both as a means for the state to maintain authoritarian control.[153]

The United States is generally against any such international mechanisms unless they contain within their provisions a section that addresses the need to preserve Internet freedoms.[154] As such, a multilateral code of conduct that addresses the preservation of Internet freedom would appear to garner larger international support and may be the best way to limit the frequency and breadth of cyberattack while establishing international norms that could lead to more binding agreements in the future.

The need for an international regime with strong enforcement protocols has also spurred debate over the creation of a cyberweapons regulatory regime similar to those of the nuclear, chemical and biologic arms control regimes. Applied to cyberwarfare, the purpose of such a regime would be to delegitimize the use of the cyberweapon as an effective tool for achieving military objectives. The United States would appear to be a significant benefactor from the establishment of such a mechanism, due to the increased dependence of American society and the military upon its cyber infrastructure.[155] Yet, even if the United States were willing to lead a regulatory ban on such weapons, it would be nearly impossible to include any verification protocol into its charter.[156] The lack of a verification protocol all but renders a cyber arms control regime ineffective, and in fact

---

153 Wortzel, "China's Approach to Cyber Operations: Implications for the United States," 3.

154 Maurer, "Cyber Norm Emergence at the United Nations," 25.

155 Ownes, Dam, and Lin, "*Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities*," 322.

156 Clarke and Knake, *Cyber War*, 238.

could end up harming the national security of litigious societies when compared with states that have higher tolerance for corruption, like China and Russia.[157]

While the arms control regimes that restrict the use of weapons of mass destruction are generally regarded as successful; these control regimes are based on an accepted set of universally accepted taboos in that their use is morally reprehensible to a preponderance of the global human population. Joseph Nye Jr. points out that these taboos were developed independent of state-state negotiation and were rather the product of independent learning over time.[158] His claim presents both a positive and negative dynamic when analyzing the effectiveness of a cyberweapons control regime.

From a positive standpoint, it suggests that independent learning in the cyberdomain may pave the way for active cyber cooperation at a later date. This is especially true for states like China and Russia, who are realizing an increased difficultly in controlling their own cyber-hacktivists and may therefore, have an expanded need for regulation in the future.[159] However, from a negative perspective, this principle fails to recognize that a large impetus for a state's willingness to join the chemical and biological weapons conventions relied on an accepted understanding that these weapons lack military utility on the battlefield.[160] This lack of utility does not appear to affect cyberweapons, which have been proven effective and efficient tools to support military objectives. Nor does the argument appear to recognize that in some respects, the employment of a cyberweapon to prosecute a military target is in many ways morally superior than destroying the same target with a kinetic weapon. So, while Nye is correct to assert that independent learning may pave the way for future cooperation, the utility of these weapons for military purposes will prevent nations from banning their use through official mechanisms. This analysis determines that limiting the state use of cyberweapons

157 Joseph Nye, "Nuclear lessons for Cyber security?" *Strategic Studies Quarterly* (winter 2001), 34.

158 Nye, "Nuclear lessons for Cyber security," 29.

159 Ibid., 30.

160 Joseph Cirincione, *Bomb Scare: The History and Future of Nuclear Weapons* (New York: Columbia University Press, 2008), 45.

through the development and enforcement of control mechanisms fails to create an incentive for states to ratify any such mechanisms in the near future.

H. CYBERCRIME CONVENTION

The Council of Europe Cyber Convention serves as the only binding cyber-crime regulatory mechanism within the international community.[161] As of June 7, 2012 the convention had 47 state signatories, 34 of whom had ratified the convention through their own governments.[162] The convention carries an accountability provision that includes an *obligation to assist* other member states in the investigation and mitigation of cybercrime emanating from within one's own territory. The convention also carries a promise by signatories to adopt legislation and foster international cooperation within their borders in an effort to develop a common criminal code to address transnational cybercrime.[163] Lastly, the convention has been successful in developing both extradition policies and mutual law enforcement practices among member states.[164] These developments have given a boost to the international community's capacity to regulate cybercrime.

Yet, for all the above mentioned benefits, the convention remains relatively weak. It allows for a member state to decline assistance in the fulfillment of its obligation on fairly broad grounds. Overall, it lacks an enforcement mechanism to ensure member compliance and it does not address a realistic timeline by which members need respond to demands for assistance.[165] As such, the only binding attribute of the convention is in effect the willingness of member states to comply with its provisions. Therefore, the convention's largest contribution to the international community becomes its norm-

---

161 Council of Europe Cybercrime website, "Action Against Economic Crime," <http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/default_en.asp> (4 March 2012).

162 Council of Europe Treaty Office, "Convention on Cybercrime, CETS No.: 185," <http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=8&DF=&CL=ENG> (5 March 2012); The United States ratified the convention on September 29th, 2006.

163 Council of Europe, "Convention on Cybercrime" (Budapest: 23 November 2001), <http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm> (6 March 2012).

164 Owens, Dam, and Lin, "*Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities*," 280.

165 Ibid.

generating potential as participating states develop common approaches toward curtailing the severity of cybercrime through cooperative learning.

I. INTERNATIONAL REGIMES AS AN EFFECTIVE METHOD OF CURTAILING CYBERTHREATS

There are other proposals that seek to limit cybercrime and state sponsored cyberattack through an evolution of currently accepted international laws to better reflect cybersecurity issues. This includes a proposal that calls for an extension of the Law of Armed Conflict (LOAC) to account for the use of information systems.[166] This proposal would render any attack that violates the LOAC by conventional means as a violation of the LOAC if carried out by cyber means.[167] Assimilating the LOAC to cover cyberattack therefore carries a strong enforcement mechanism through the international criminal court system; however, the issue of positive attribution remains.

In this instance, the best scenario to attain a positive development for reducing the risk of hostile cyber activity may be in the state level implementation of a *no first use policy*. Such a policy adheres to the principle that a cyber arms control mechanism should not eliminate state capability—as the other forms of arms control regimes do—and rather that policies should only be implemented that prohibit acts.[168] To make this easier for states to immediately implement, a *no first use* policy does not have to be a multi-lateral agreement. States could choose to follow the path instituted by President Nixon in 1969 when he issued a unilateral policy that the United States would dismantle its bioweapons stockpile and would refrain from their use in warfare.[169] This unilateral declaration later garnered a similar response from the Soviet Union. The later convergence of these unilateral decisions catalyzed the success of the Biological Weapons Convention with support from the international community. This example shows that limiting the damage done from cyberattack is only one component of a successful international treaty

166 Owens, Dam, and Lin, "*Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities*," 322.

167 Davis Brown, "A Proposal for an International Convention to Regulate the Use of Information Systems in Armed Conflict," *Harvard International Law Journal*, vol. 47, no. 1 (winter 2006), 179–221.

168 Clarke and Knake, *Cyber War*, 253.

169 Cirincione, "Bomb Scare," 129–130.

governing cyberspace, establishing norms that reduce the likelihood of attacks are equally important. The path to norm development can start with individual states, yet any of these approaches are absent in the current international security environment.

J. CONCLUSION

As referenced throughout this chapter, the cyberattack on Estonia serves as a fundamental case study for assessing the issues surrounding the state sponsored use of the cyber domain to project power. As such, the Estonian example has derivative lessons that can be applied to any contemporary debate on cybersecurity because it serves as the initial case that extrapolates the issues of cyberpower, attribution and the complexities surrounding the formation of institutions. Principally, the case shows the difficulty with attribution and how an overall lack of accountability has become the main enabler of cyberattack. Efforts to produce an international cyberdomain that includes attribution have become mired in technical challenges, and even if such hurdles were overcome there is speculation regarding the political utility of attribution in state-to-state relations.

The Estonian case has also provided a context to assess the various proposed and in place methods for mitigating hostile cyber activities covered in this chapter; namely, the establishment of cyber norms, international agreements, codes of conduct, ratification or assimilation of laws and attempts to solve the attribution problem. All of these solutions require a significant investment in time and resources before they can become effective. Faced with an existential threat to American national security, national leaders do not have the luxury of adopting solutions that require such investments of time. The national security decision maker thus faces a quandary in responding to hostile threats in cyberspace. Recognizing that the international cyberattacker has an advantage over the state's cyber defenders, the question becomes one of offense or defense and the political risks versus rewards of attribution.

Playing defense alone does not provide a capacity to mitigate threats before they become attacks, and the complexity of human attribution makes political accusations nearly irrelevant. Therefore, increasing the offensive components of the national security establishment to effectively search out, classify, identify and work with international

partners to mitigate both state and non-state threats is an exercise in increasing cyber and state security. The current liberal and constructivist proposals for limiting hostile cyber activity in the international cyberdomain do not afford the U.S. national security decision maker an avenue for addressing the cyberespionage threat in a timely manner. Instituting a proficient defensive and offensive capability within the U.S. counterintelligence community is therefore a means of effectively addressing cyberespionage within the present time limitations. A detailed analysis of what is required to create this capacity is covered in the next chapter.

In 2012, upon giving his recommendations on improving cybersecurity, Dr. Larry Wortzel stated before the House Committee on Foreign Affairs, that "Congress should ensure that the appropriate federal agencies are working with their counterparts in allied and friendly countries to detect and combat malicious cyber activity."[170] This statement recognizes the need to increase cybersecurity effectiveness through the development of international partnerships. However, while there is little ambiguity in his recommendation to "detect" malicious activity, there is great room for interpretation regarding how to effectively "combat" malicious activity, especially as one engages with international partners. Not all international partnerships can be created equal as demonstrated in the vast amounts of security intelligence shared in the intelligence partnership between the allied nations of Australia, Canada, New Zealand, the United Kingdom and the United States (AUSCANNZUKUS, or the Five Eyes). Yet, a focus strictly on improving the cooperative liaison between these countries omits the perceived gains from enhancing cooperation with other friendly nations, such as Taiwan.

[170] Wortzel, "China's Approach to Cyber Operations: Implications for the United States," 7.

IV. DEVELOPING INCREASED CAPACITY TO COUNTER CYBERESPIONAGE: DOMESTIC AND INTERNATIONAL MICRO-RESTRUCTURING EFFORTS

A. INTRODUCTION

> DoD will continue to work with domestic and international allies and partners and invest in advanced capabilities to defend its networks, operational capability, and resiliency in cyberspace.[171]

This chapter explores domestic and international micro-restructuring initiatives that increase capacity to mitigate cyberespionage. From the domestic perspective the chapter will seek to address changes in the structure of DoD Counterintelligence as a means to eliminate stove-pipes, address efficiency and bring DoD CI in line with the Goldwater-Nichols Defense Reorganization Act of 1986. This strategy places an emphasis on developing joint operational counterintelligence support at the COCOM level, principally within each of the CYBERCOM sponsored Joint Cyber Centers (JCC). This approach builds on the success of the joint Strategic Counterintelligence Directorates (SCID)—used effectively to address counterintelligence issues in the contingency environments of Iraq and Afghanistan—to apply the SCID model toward effective mitigation of cyberespionage within the COCOM.

International restructuring addresses a host of U.S. policy documents that emphasize expanding international cyber cooperation to friendly nations and the degree to which such cooperation could include Taiwan. Research conducted in fulfillment of the latter included consultations with Taiwanese national security, DoD Policy and law enforcement professionals to obtain direction for further research. This included on-the-ground research in Taiwan as a means to gain a broad understanding of both the Taiwanese and American perspective for increased cyber cooperation.

171 United States Department of Defense, "Sustaining U.S. Global Leadership: Priorities for the 21st Century Defense" (January 2012), 5.

B. DOMESTIC MICRO-RESTRUCTURING: INCREASING CAPACITY

1. DoD Strategic Initiatives for Developing Domestic Capacity in Cyberspace

In July 2011, DoD released its first strategic policy document regarding defense of its cyber domain. The document listed five strategic initiatives for operating in cyberspace. Two of these initiatives pertain directly to information contained within this thesis. They are listed as:

- Strategic Initiative 2 (SI2): Employ new defense operating concepts to protect DoD networks and systems[172]
- Strategic Initiative 3 (SI3): Partner with other U.S. government departments and agencies and the private sector to enable a whole-of-government cybersecurity strategy.[173]

SI2 deals principally with increases to defensive operations that seek to "form an adaptive and dynamic defense of DoD networks and systems."[174] The document further defined that SI2 will strengthen DoD critical infrastructure by going beyond the current focus on information assurance to include an exploration of "new operating concepts" that have the potential to reduce vulnerabilities.[175] SI2 primarily advocates attaining these objectives through increased integration of cyber technology to harden the target and reduce the risk of insider threats. Additionally, it proposes a shift to "active cyber defense," which seeks to monitor DoD cyber infrastructure in real time to discover, detect, discover, analyze and mitigate threats.[176] From a defensive perspective, these changes are warranted and astute, but the language contained within the report also provides an allowance for the development of increased offensive counterintelligence capabilities as a means to further defend DoD networks. The rest of this chapter will address SI2 in this regard, as it fulfills the development of capacities that seek to form an adaptive and dynamic defense through the development of new operating concepts.

---

172 United States Department of Defense, "Department of Defense Strategy for Operating in Cyberspace" (July 2011), 6.

173 Ibid., 8.

174 Ibid., 6.

175 Ibid.

176 Ibid., 7.

SI3 addresses the need for DoD to continue working closely with interagency partners on new and innovative ways to increase national cybersecurity.[177] This initiative deals primarily with expanded cooperation between DoD and DHS, and the development of programs that protect sensitive information within the Defense Industrial Base. However, similar to SI2, the language included in SI3 provides for further development of cooperation between DoD entities, like DoD CI and external partners that are yet to be developed. This stance on cybersecurity is encouraging as it shows a recognition and desire to develop capacity through non-traditional approaches to partnership development. This concept will likewise be explored throughout the chapter as it pertains to cyberespionage.

2. Addressing Domestic Micro-restructuring

"Creating organizational arrangements in which the analysts and collectors systematically collaborate would improve each of them."
–Joel Brenner, former NCIX

Developing organization arrangements that improve effectiveness is the ultimate means for the elimination of stove-pipes and creating *unity of effort* across the USCI enterprise. While this concept is addressed in numerous CI policy documents, little has been done to change the structure of USCI to achieve these goals. The 2010 Comprehensive National Cybersecurity Initiative references the need for a government-wide cyber counterintelligence plan "to coordinate activities across all Federal Agencies to detect, deter, and mitigate the foreign-sponsored cyberintelligence threat to U.S. and private sector information systems."[178] This language is clear recognition that the USCI enterprise must strive to eliminate stove-pipes and increase effectiveness toward mitigating the cyberespionage threat. While the report recognizes this need, it provides scant direction to the counterintelligence community regarding how to develop such capacity increases. Highlighting this point, the report states:

---

[177] United States Department of Defense, "Department of Defense Strategy for Operating in Cyberspace," 7.

[178] Executive Office of the President of the United States, "The Comprehensive National Cybersecurity Initiative," 4.

> To accomplish these goals, the plan establishes and expands cyber CI education and awareness programs and workforce development to integrate CI into all cyber operations and analysis, increase employee awareness of the cyber CI threat, and increase counterintelligence collaboration across the government.[179]

Educating and increasing employee awareness are the only definitive suggestions contained within this report for establishing a more effective cybercounterintelligence capacity. These solutions are irrelevant to a cross-section of the civil service workforce that is already highly educated toward their professional duties and whose awareness level need only expand to encompass cyberespionage as a prolific threat to national security. The other features contained within the proposal, integrating CI into all aspects of cyber operations and increasing collaboration across the government, is astute; however, accomplishing these tasks without first creating appropriate structure is nearly impossible.

Government bureaucracies have an acute resistance to change and are increasingly more risk averse. This concept has a strong impact on the degree to which cross-cutting collaboration amongst the counterintelligence community can be attained. The New Institutionalist model would suggest the reason for such aversion is that bureaucratic functionaries are seldom motivated to change the structure of organizations in which they personally benefit. After all, the bureaucrat responsible for making the decision to take risk or accept structural change has risen within the very system that needs restructuring. In fact, they are vested in their current structure. This creates a lack of incentive for addressing effectiveness, especially when such increases require macro-level changes. This analysis does not connote a derogatory labeling of the decision maker, rather it is meant to state that bureaucratic parochialism—and the culture of the institution itself—plays a strong role in the decision making process. This has principally been the problem with efforts to create a consolidated Defense Bureau of Investigation, or even the more tangible example of the DoD Counterintelligence Field Activity (CIFA) from 2002–2008. These large restructuring initiatives generally fail due to the New

[179] Executive Office of the President of the United States, "The Comprehensive National Cybersecurity Initiative," 4.

Institutionalist bureaucratic model referenced. With this concept in mind, the next section explores small changes that do not impact upon such decision making factors, and as such could lead to increased counterintelligence effectiveness within the DoD as it pertains to cyberespionage.

a. A Need to Narrow the Focus

The October 2011 NCIX report on cyberespionage lists "improved collaboration" as one method through which the Intelligence Community can respond to the increased cyberespionage threat. Improved collaboration in this regard highlighted the need for a coordinated response at the national level, the result of which was the establishment of the National Cyber Counterintelligence Working Group (NCIWG). This working group, comprised of the sixteen members of the IC and several other federal agencies, meets to build improved collaboration across the enterprise.[180] It is doubtful that top-level government working groups are the answer to eliminating stove-pipes and improving effectiveness within the counterintelligence community. Historic precedent indicates that without an ability to demand compliance or the power to control budgets, such working groups are reduced to venues for individual agencies to consolidate stove-pipes rather than remove barriers.[181]

The NCIX report also calls for improved analysis, collection, offensive operations, training and awareness as ways for the USCI to more adequately address the cyberespionage threat in the United States.[182] In other words, apart from aligning some counterintelligence functions toward combating cyberthreats, the counterintelligence community at large will continue business as usual. This statement may appear anecdotal, but when analyzed without prejudice it begs the question: what has the counterintelligence community been doing if it has not always focused on improving

---

[180] Office of The National Counterintelligence Executive, "Foreign Spies Stealing U.S. Economic Secrets in Cyberspace," A-1.

[181] For Historical examples of this in the counterintelligence world, see information pertaining to the failure of the DoD Counterintelligence Field Activity (CIFA) or remarks by former National Counterintelligence Executives regarding the inability of the NCIX to exercise control over the counterintelligence community.

[182] Ibid.

analysis, collection, offensive operations, training and awareness? The lack of relevant guidance contained within this report is rather absurd and most likely offensive to a counterintelligence community that would like to hear meaningful suggestions for building stronger capacity toward threat mitigation.

How is it that direction from the nation's top counterintelligence office is so watered down? A former director from the same organization, Joel Brenner 2006–2009, had a comment that elucidates this point, "[t]he higher cybersecurity recommendations rise in the bureaucracy, the greater the chance they'll be watered down to achieve consensus, or sidelined. This is why we get continual declarations of urgency but little real progress."[183] Brenner's comment underscores the need to make inter-departmental vice community wide reform decisions, i.e., those that only require a mandate from a single secretary rather than attempts to gain acceptance across departments. The Secretary of Defense Department is uniquely positioned to issue restructuring orders to the counterintelligence units within DoD that comprise the bulk of the government's offensive counterintelligence capacity. Without such direction, individual counterintelligence agencies will continue to plot their own course and subsequently languish from a lack of effective leadership at the national level.

Narrowing the focus of reform to only the DoD OFCO counterintelligence units is therefore an effective means of building a stronger capacity to mitigate cyberespionage. As the DoD is perhaps the most negatively impacted department from all forms of hostile cyber activity, leadership within the department has the most incentive to generate small scale reforms that will truly create *unity of effort*, improve collaboration and increase effectiveness. Without such direction, DoD counterintelligence units will continue to receive a smattering of useless direction that instructs them to improve areas they already focus on, or instructions from a national working group whose directives becomes too watered down to prove effective.

183 Brenner, *America the Vulnerable, 214.*

b. In Violation of Goldwater-Nichols?

> "To the extent that DoD counterintelligence is viewed as a unitary set of missions, functions, and resources, it is a relic of the pre-1986 U.S. military establishment."[184]

If the incentives presented in the previous section do not prove strong enough to induce the DoD decision maker to institute micro-reforms across the DoD counterintelligence enterprise, then perhaps the failure to comply with the Goldwater-Nichols Defense Reorganization Act of 1986 (GWN) produces additional incentive. The Goldwater-Nichols Act reformed the military force structure to place operational control within joint Combatant Commands (COCOMs), addressing a previously demonstrated inability of the military services to effectively conduct joint operations.[185] The statutory changes to Title 10 of the U.S. Code established that operational matters would become the providence of the COCOMs while administrative matters would remain the responsibility of the individual service Secretaries. With only few exceptions "the Secretaries of the military departments shall assign all forces under their jurisdiction to unified and specified combatant commands…to perform missions assigned to those commands."[186] For this reason, operational control of the U.S. Armed Forces now resides within the COCOMs; yet, the DoD CI community completely avoided the main thrust of the Goldwater-Nichols Act.

This avoidance has resulted in a DoD CI community that remains operationally controlled by the separate military departments, not the Combatant Commanders (CCDR). This has left DoD CI in the hands of organizers and trainers and not the planners and operators who are closest to the foreign intelligence challenges facing the DoD.[187] This legacy structure impairs effectiveness as it fails to enact a forcing mechanism or incentive structure for joint operations that support COCOM

---

184 Michael Woods and William King, "An Assessment of the Evolution of Defense Counterintelligence Activities," *Journal of National Security Law & Policy*, vol. 3, no. 169 (2009), 187.

185 William J. Crowe, *The Line of Fire: From Washington to the Gulf, the Politics and Battles of the New Military* (New York: Simon and Schuster, 1993), 146.

186 Title10 USC Section 162 (a)(1).

187 Bachman, "Integrating Defense Counterintelligence," 6.

requirements.[188] This analysis, used to evaluate DoD CI effectiveness at mitigating cyberespionage, indicates that the CCDR has a limited ability to assign joint DoD OFCO resources to mitigate a perceived FIS threat to their cyber infrastructure. This creates a problem for counterintelligence effectiveness as a whole, which translates to an increased vulnerability for the CCDR whose assets are in jeopardy. Thus, rather than tasking CI assets directly, the CCDR must rely on a complex process of DoD CI liaison support to coordinate with the respective CI services. This structure typically includes the assignment of a senior counterintelligence advisor to the CCDR staff, known as a Command Counterintelligence Coordination Authority (CCICA), whose responsibility is to deconflict counterintelligence issues and provide CI expertise to the COCOM.[189] Additionally, the CICCA typically has a staff comprised of analysts and special agents from the various DoD CI services. This structure provides the COCOM without an innate operational capacity as the activities of DoD CI remain under the control of the individual military departments.

(1) Continued Neglect of Goldwater-Nichols. Continued lack of accountability for DoD Counterintelligence to adhere to the joint operational principles mandated by the Goldwater-Nichols Act principally deals with the New Institutionalist concept of culture. As mentioned previously, counterintelligence operates within a vacuum of secrecy. This secrecy has produced very little information for the national security decision maker to gain insight into the structure and function of counterintelligence. Aiding to this dilemma is that intelligence oversight in the United States is a process that focuses primarily on ensuring legality and not effectiveness. Such a focus on propriety seeks to determine that actions are conducted in accordance with U.S. law and that civil liberties and financial resources are not abused.[190] Counterintelligence oversight is expanded slightly, but only as a means to explore "lapses," or the investigation of counterespionage failures that produced the likes of

188 Bachman, "Integrating Defense Counterintelligence," 6.

189 Department of Defense Directive 5240.10, "Counterintelligence in the Combatant Commands and Other DoD Components" (5 October 2011), 8.

190 Mark Lowenthal, *Intelligence: From Secrets to Policy, 4th ed.* (Washington, D.C.: CQ Press, 2009), 202–207.

Aldrich Ames and Robert Hanssen.[191] Evaluating effectiveness is not a significant component of oversight in the United States, primarily because the congressional and executive organs responsible for oversight do not have an optic by which to evaluate counterintelligence effectiveness. The USCI community has therefore sought refuge within its culture of secrecy to avoid scrutiny over effectiveness in the fulfillment of its mission objectives. For DoD CI elements, this has included an ability to continually neglect the joint mandates of the Goldwater-Nichols Act.

While this initial analysis appears to suggest that USCI is complicit in disregarding the mandates of the Goldwater-Nichols Act, further examination indicates that the lack of CI compliance does not reside within its culture of secrecy alone. As mentioned previously, Title 10 of the U.S. Code states that "all forces" shall be assigned to the COCOMs.[192] However, there are also clearly stated statutory exceptions to the general principle of "all forces" to include forces assigned to carry out the functions of the Secretary of a military department.[193] Such functions are generally summarized as those that are associated with the need to organize, train and equip each military service.[194] Yet, another exception maintains that each service Secretary will remain responsible for "the effective supervision and control of the intelligence activities" within their department.[195] Herein lies the ambiguity, Title 10 does not specifically categorize counterintelligence personnel. If counterintelligence personnel are to be categorized as "all forces" then their operational control should lie with the COCOMs; yet, if they are considered a subset of "intelligence activities," then the latter would exempt them from being assigned to Combatant Commands.[196] This second exception is primarily why

191 Lowenthal, *Intelligence: From Secrets to Policy*, 201.

192 Title10 USC Section 162 (a)(1).

193 Woods and King, "An Assessment of the Evolution of Defense Counterintelligence Activities," 190.

194 As defined in the functions of the military departments; see Department of Defense Directive 5100.1, "Functions of the Department of Defense and Its Major Components" (21 December 2010), 25.

195 Title 10 USC Section 3013(c)(7), Section 5013(c)(7), and Section 8013(c)(7).

196 Woods and King, "An Assessment of the Evolution of Defense Counterintelligence Activities," 190.

operational control of above-service intelligence agencies like DIA, NSA and the National Reconnaissance Office (NRO) remain subordinate to the Secretary of Defense vice attached to a specific COCOM.

In all of the these referenced cases the agencies themselves operate under Title 50 intelligence authorities, and their exclusion from an "all forces" status is rarely in contention. However, counterintelligence—as an inherently law enforcement function in the United States—operates under Title 18 authorities and DoD CI elements operate in an awkward hybrid of Title 10 (Military), 18 (Criminal) and 50 (Intelligence) authorities. Subsequently, the statutes themselves provide no clear guidance to DoD CI regarding its alignment with Goldwater-Nichols. This ambiguity is most likely the reason why DoD CI has never been held accountable for not conforming to GWN. Disentangling the legal authorities for DoD CI in this regard may create more questions than answers. As such, in order to better understand where DoD CI truly falls within the joint operational environment, one must analysis the intent of the law rather than its opaque design.

(2) Conforming to Intent. The intent behind the Goldwater-Nichols Defense Reorganization Act was to improve military effectiveness in the wake of perceived national security failures. It is doubtful that the designers intended to create additional bureaucratic obstacles or complex laws for the national security establishment to interpret. Thus, evaluating the degree to which DoD CI is in violation of—or in keeping with—the Defense Reorganization Act places an unnecessary emphasis on an ambiguous legal issue rather than on developing adequate structures that improve effectiveness. In keeping with the spirit of the reorganization effort, an impetus should be placed on the intent behind GWN; thus, changing the debate to focus on effective restructuring. By adhering to intent, the DoD decision maker is left seeking solutions that could increase effectiveness of DoD Counterintelligence. One possible solution would be to place certain offensive elements under the direction of the COCOMs, whether mandated by law or not. Determining the feasibility of this proposal places an emphasis

on the degree to which such restructuring would increase jointness across the DoD CI enterprise while subsequently providing alignment of perceived COCOM threats with capabilities.

c. Building Capacity in Relation to Cyberespionage

The current DoD counterintelligence structure places the Combatant Commander at a distinct disadvantage. The CCDR who determines cyberespionage has adversely affected theater security, combat effectiveness or intelligence systems under their control must engage in a lengthy coordination process to attain operational support from the DoD CI services. As such, the CCDR cannot currently call upon elements within their command to mitigate these threats. This system is not satisfactory, and the CCDR seeks new options to develop a mitigation capacity that can more effectively address such threats.[197] The DoD cyber community has recognized the need to provide the CCDR with timely and accurate support in fulfillment of CND capabilities with the development of a Joint Cyber Center (JCC) within each COCOM. JCCs are operationally controlled by the COCOM but staffed with CYBERCOM personnel. They are responsible for providing direct cyber support to the COCOM, while coordinating their activities with their parent organization. This model places a stronger capacity for CND within the COCOM and develops a strong coordination mechanism for CNA and CNE support through CYBERCOM.[198] However, while the establishment of the JCC improves COCOM capabilities in regard to ensuring network integrity, it currently has no bearing on counterintelligence support. CCDRs require an innate level of counterintelligence support to illuminate operational advantages and to sustain integrity of plans and operations; however, the current structure does not provide this level of support.

The CCDR obtains counterintelligence support—of the defensive or offensive variety—through the J2X and the CCICA. The CCICA, as the senior CI advisor

---

[197] Consultation with a Unified Command J2 (12 May 2012), while discussing the coordination process by which the CCDR gains support to mitigate cyberespionage threats.

[198] Thomas Doscher, "NORAD, USNORTHCOM Joint Cyber Center stands up" (1 May 2012), <http://www.northcom.mil/News/2012/050112.html> (23 May 2012).

and subject matter expert, relays requests for assistance through their staff to the respective DoD CI services. Operational plans are then independently developed within each DoD CI service, tasked to a CI unit for action and then sent back to the CCICA through staff channels for coordination with the COCOM. If the proposed counterintelligence action lies within the continental United States, then the DoD CI service must also coordinate any action with the FBI. This process is complex and does not always adhere to the time demands of the COCOM.[199] Additionally, this process leaves the COCOM without innate counterintelligence support and reliant on the services to fulfill their threat needs. Unfortunately, the services are also being requested to provide support from other COCOMS, or other domestic law enforcement entities, and thus have to weigh their response against their own limited resources.

Changing the structure of this process to adhere with a GWN framework would provide the CCDR with a much needed innate operational counterintelligence function. This would subsequently reduce the redundancy among the services and provide increased efficiency for the use of scarce resources. Attaching a joint cyber-OFCO element to the Joint Cyber Center could provide the increased level of effectiveness required across the enterprise. Similar to the JCC model, the cyber-OFCO unit would be focused on cyberespionage issues that directly affect the COCOM. Their staffing structure would likewise be similar, where operational control resides at the COCOM with administrative control provided by CYBERCOM, in that operational control would reside at the COCOM while staffed independently from NCIS, AFOSI, Army CI and DCHC. The COCOM JCC would therefore have a resident cyber-OFCO joint counterintelligence unit that could respond quickly and effectively to the joint command's perceived cyberespionage threats.

Adding to the feasibility of this approach is a tested and proven model of joint counterintelligence collaboration within the contingency environments of Iraq and Afghanistan. DoD CI elements worked effectively in joint Strategic Counterintelligence

[199] During a consultation with a COCOM N2, the individual commented that timely support is not being met by counterintelligence units. The N2 indicated that requests for counterintelligence support generally takes four months before the COCOM is briefed on a plan of action.

Directorates (SCID) throughout the contingency period. Each SCID maintained an executive agency on a rotational basis, and was traditionally staffed with personnel from the DoD CI elements of NCIS, AFOSI and Army CI.[200] DoD Directive 5240.9 has since replaced the SCID with the Joint Counterintelligence Unit (JCIU), although it functions in similar capacity.[201] JCIUs report to the Theater Commander for operational direction and function autonomously to provide counterintelligence support.

It is important to note that SCIDs were not developed and implemented as the result of a legal interpretation of the Defense Reorganization Act. Rather, the SCID/JCIU concept was established through the recognition of a capability gap coupled with an exigent need to develop a capacity to support the Contingency Commander. This brought out the best in DoD CI as each service put aside bureaucratic parochialism in an effort to develop increased effectiveness. This same capability gap and exigent need are now prevalent in addressing the cyberespionage threat. Replicating the JCIU model within select COCOM JCCs would be a tangible means of prosecuting offensive counterintelligence operations that mitigate cyberespionage.

d. Developing the JCIU Model toward Mitigating Cyberespionage

Opponents to this micro-restructuring model would be correct to point out that current DoD Directive only allows for the formation of JCIUs within environments designated as a Joint Operations Area (JOA).[202] This appears to be a legal obstacle for implementing JCIUs within the COCOM JCCs; however, this does not limit the options available to the DoD decision maker regarding the establishment of an operational CI unit within the JCCs under some other name. In this regard, the JCIU would be seen as a proven model and forcing mechanism that compels the DoD CI services to staff and operate out of joint units. Additionally, speculation would point to an apparent manpower requirement that the services currently cannot afford. Unfortunately, this would most

---

200 Louis Beyer, "Defense Investigators and the War on Terrorism," *The Journal of Public Inquiry* (spring/summer 2006), 6.

201 United States Department of Defense, "Joint Publication 1–02: Dictionary of Military and Associated Terms," 172.

202 Consultation with U.S. law enforcement official (6 June 2012), while discussing the structure of the COCOM J2X and CI effectiveness issues.

likely be used as an excuse by the CI services rather than an actual limitation. Historically, the DoD CI services staffed a multitude of SCIDs within Iraq and Afghanistan. As the United States continues to reduce its presence in these locations, the available CI manpower could be reallocated toward JCIU-like units within the JCCs.

Creating an innate Cyber-OFCO capacity within the COCOM JCCs, directly modeled after the proven SCID/JCIU model, eliminates a great deal of the redundancies and answers concerns over fiscal responsibility. Additionally, creating such a capacity within the COCOMs eliminates the need for some of the CI coordination function with each COCOM. These coordination billets could be reabsorbed by the services or restructured into multiple operational billets within the JCC. The executive agency for each Cyber-OFCO unit would be responsible for conducting coordination directly with the COCOM via the CCICA, while taking the operational imperatives of the CCDR directly back to the Cyber-OFCO unit for execution. Lastly, the DoD CI services would benefit from joint capacity increases in which they no longer develop operations independent of one another, but rather—through joint activities—develop and execute consolidated operations built on each services' own inherent strengths.

3. Domestic Level Restructuring, Conclusion

The current DoD CI structure utilizes an archaic organizational form that creates ineffective and wasteful results. As demonstrated through this analysis, the degree to which the DoD CI services are legally forced to conduct joint operations is immaterial. Rather, what GWN illuminates is that the *intent* for increased effectiveness is an imperative. Over the past 25 years the reorganization benefits provided by GWN has clearly demonstrated that joint capacity development does result in increased effectiveness. The protection of parochial self-interest was just as unacceptable 25 years ago as it is for counterintelligence in the contemporary environment. Combining cyberespionage in a joint Cyber-OFCO unit, similar in structure to the JCIU model but within the JCC of each COCOM, is therefore, a practice in increased effectiveness across the DoD CI enterprise. Implementing this approach adheres to the current impetus for pragmatic and efficient solutions to combat cyberespionage and further fulfills DoD

policy directives that call for greater collaboration. Instituting such a process would provide the CCDR with an increased capability to address cyberthreats to his or her COCOM while ensuring the integrity of the DoD Global Information Grid.

C. INTERNATIONAL MICRO-RESTRUCTURING: INCREASED COOPERATION WITH TAIWAN

> The interdependence of the U.S. Counterintelligence community is also manifest in our relationships with liaison services. We cannot cut off these relationships because of concern about security, but experience has certainly shown that we must calculate the risks involved as realistically as possible. –Austin Matschulat, 1963

While Matschulat's words were meant to describe the importance of DoD CI cooperation with South Vietnam, as a means to develop an increased capacity to mitigate the Soviet intelligence threat, these words are just as relevant today regarding current threats as they were when he wrote them. Expanding this understanding to include cybersecurity capacity development with Taiwan adheres to the principle that liaison relationships can be established for the benefit of CI effectiveness if the risks are calculated in a rational manner. Choosing not to expand these relationships due security concerns alone limits growth and displays a lack of faith in the professional abilities of our USCI professionals to adequate navigate these hurdles.

1. DoD Strategic Initiative for Developing International Capacity in Cyberspace

Leveraging international partners as a means to increase capacity in Cyberspace is echoed by current DoD policy. Strategic Initiative number four of the DoD *Operating in Cyberspace* report specifically provides that the Department of Defense should, "[b]uild robust relationships with U.S. allies and international partners to strengthen collective cybersecurity."[203] The report goes on to suggest a number of tangible benefits to such cooperation:

> The development of international shared situational awareness and warning capabilities will enable collective self-defense and collective

203 United States Department of Defense, "Department of Defense Strategy for Operating in Cyberspace" (July 2011), 9.

> deterrence. By sharing timely indicators about cyber events, threat signatures of malicious code, and information about emerging actors and threats, allies and international partners can increase collective cyber defense.[204]

Increasing collective cyber defense provides both direct and indirect benefit to the United States. From a CI perspective, the direct benefits are those highlighted in the passage above; namely, the sharing of malicious code and information about emerging actors. Indirectly, developing capacity in this regard produces trust and strengthens state-state relations. The resulting interdependence provides states with an increased deterrent capacity and ability to respond to threats with increased effectiveness. Creating this capacity with Taiwan provides the United States with additional capabilities to respond to threats in the Asia Pacific region, while ensuring an increased capacity to mitigate cyberthreats to its own critical infrastructure.

2. Developing Capacity with Taiwan

> A defense of Taiwan against mainland aggression is the one contingency in the western Pacific Ocean in which success for the United States hinges upon the speed of its response and the ability of the military to arrive on station with sufficient force to defend Taiwan adequately.[205]

a. Cyber Cooperation with Taiwan: Historical Perspective

Since 2004, the United States has engaged in policy-level discussions with Taiwan on cybersecurity primarily as a means to support Taiwanese critical infrastructure.[206] The priority placed on cybersecurity and critical infrastructure protection in the ensuing years has varied by and within Taiwanese administrations. Recent national elections saw the moderate Kuomintang (KMT) retain control of both the executive and legislative branches of the Taiwanese government, firmly demonstrating popular support for KMT policies that are summarized as being more conciliatory toward Mainland China. Those polices place a greater emphasis on economic engagement and a

---

[204] United States Department of Defense, "Department of Defense Strategy for Operating in Cyberspace."

[205] Krekel, Adams, and Bakos, "Occupying the Information High Ground," 9.

[206] Consultation with U.S. government official #1 (20 April 2012), regarding history of mil-mil cyber cooperation between the U.S. and Taiwan.

maintenance of the *status quo* vice an agenda for greater international independence.[207] Increased ties with the Chinese mainland, demonstrated through political and economic improvements, has resulted in an apparent downgrading in the level of urgency by which Taiwan seeks to develop cybersecurity cooperation with likeminded nations. This has resulted in a duality of sorts, wherein Taiwan appears mindful of the need for greater engagement, but reluctant to conduct activities that may be translated as antagonistic toward their larger policy goals. This issue most likely has a limiting effect on the development of cooperation for cybersecurity issues between the United States and Taiwan as it lies within the backdrop of any policy-level discussion.

b. Cyber Cooperation with Taiwan: Contemporary Period, Cyber Storm 2012

The 2012 Cyber Storm IV event included a decision to omit foreign observers beyond the traditional U.S. allies of AUSCANNZUKUS. This was a drastic change from previous Cyber Storm events that had grown to include participation from 30 nations.[208] International participation in the 2012 event will be limited as a means to focus on findings developed from previous years and to further develop tangible solutions vice explore strategic problems. While this change precluded foreign participation and observation, it has not ruled out future participation. Rather, this decision expressed a desire by the United States to afford U.S. participants with a maximum ability to work issues independent of competing inputs.[209] As an active global leader in international cybersecurity development, the United States will most likely continue international outreach via the Cyber Storm event once it has taken the time to absorb and implement the lessons learned from previous years.

Regarding Taiwan, there is not a concern by DHS or the State Department with Taiwan's future participation in Cyber Storm, nor is aggravating the PRC a concern

---

[207] James Pomfret and Jonathan Standing, **"**Ma Ying-jeou wins second term in Taiwan election," *National Post* (14 January 2012).

[208] United States Department of Homeland Security, "Cyber Storm III: Final Report," 1–21.

[209] Consultation with U.S. government official #1 (20 April 2012), regarding the decision to limit Cyber Storm IV participation.

or issue that has been expressed by the lead U.S. agencies.[210] International participation in Cyber Storm is the culmination of a developed relationship between the United States and participant nations; it is not the beginning relationship development.[211] As such, it is likely that Taiwan would need to take initial steps through coordination with the American Institute in Taiwan (AIT) prior to inclusion in any Cyber Storm event. Building a stronger Cyber Storm in the future would most likely entertain Taiwanese participation and input once these precursor steps have been met.

c. Legal Concerns: U.S. Law and Titles

There are not currently any insurmountable legal barriers that preclude the United States from cooperating with Taiwan on security matters. Rather, complications include policy and priority issues that lead to engagement with some states over others. As countries experience an increase in the frequency of cyberattack they also gain a better appreciation for the pain of hostile cyber activities. In this context, international law enforcement cooperation has developed quicker than other forms of collaboration. Such cooperation has resulted in increased capacity to conduct cross-border investigations, make arrests and prosecute cyber criminals;[212] however, the mitigation of cyberespionage has generally not been enhanced by these efforts. Mitigating cyberespionage—a crime that generally only affects the state or corporation upon which it is committed—has largely remained outside the confines of state-state cooperation. In addition to these international barriers, the culture of secrecy observed by counterintelligence professionals often prevents increased cooperation between states. The national decision maker is therefore left to seek other avenues of capacity development to improve the mitigation of cyberespionage. This poses an interesting question *vis-à-vis* developing international cooperation: in what areas could U.S.-Taiwan

[210] Consultation with U.S. government official #1 (20 April 2012), regarding the decision to limit Cyber Storm IV participation.

[211] Consultation with U.S. law enforcement official #2 (28 May 2012), while discussing the criteria for international participation in Cyber Storm.

[212] Council of Europe Treaty Office, "Convention on Cybercrime, CETS No.: 185."

cyber cooperation expand, and how would such increases equate to advancements in counterintelligence effectiveness for mitigating cyberespionage?

d. Overall Model for Mil-Mil Cyber Cooperation

Developing a decision-making model to address the larger issue of state-to-state cooperation can also evaluate the initial underpinnings of the question posed above. Within the Department of Defense mil-mil cyber cooperation with any country is assessed on a case-by-case basis. The level of cooperation a state receives from the United States is based primarily on five considerations:

1) Level of Cyber Awareness and Development: Focused on legal structures, organizations and policies that govern cyber activities. Immature capacity in this regard equates to a different level of cooperation from the United States, one that does not include complex arrangements or partnership on cybersecurity issues.[213]

2) Level of Cybersecurity or CND: Focused on the state's capabilities and implementation of a competent cybersecurity and network defense posture. Nations with poor security, immature cyber defense practices or weak capacity to protect their networks obtain a separate level of exchange with U.S. decision makers.[214]

3) Level of Perceived FIS Penetration or Threat: A separate criteria to evaluate the cybersecurity or CND of a candidate state. A country deemed high risk for penetration by a concerned foreign intelligence service becomes a problematic candidate for detailed or sensitive exchange on cybersecurity matters.[215]

4) Intent for Cooperation with the United States: This is used as a means to evaluate the intent by which another state seeks cyber cooperation. This also includes analysis that enhanced capabilities could someday be used against the United States.[216]

5) Benefit for United States: Basic cost benefit formula derived by evaluating cost and time juxtaposed to the benefits received. United States policy experts are in high demand regarding capacity development issues and do not have time or resources to pursue cooperation avenues with unclear benefit to U.S. security.[217]

---

213 Consultation with U.S. government official #1 (20 April 2012), regarding the U.S. decision making process for policy-level discussion and coordination.

214 Ibid.

215 Ibid.

216 Ibid.

217 Ibid.

3. Applying the Model to Taiwan

Using the model referenced in the previous section to determine the feasibility of cyber cooperation with Taiwan provides important inputs to the decision making process. Each of the following five considerations can be assigned a value of low, moderate or high depending on an assessment of supporting evidence for each element. Taken in aggregate form, these values provide overall assessment for the feasibility of increased cyber cooperation with Taiwan and allow a more precise supposition for cybersecurity capacity development as a whole.

a. Assessing Taiwan's Level of Cyber Awareness and Development

(1) Legal Structures. Taiwan has an adequate legal foundation by which to address cybersecurity issues and has developed and implemented effective laws that govern cyberspace. In 2003, the Legislative Yuan enacted a new chapter to Taiwan's Criminal Code that addresses cybercrime (Chapter 36 Articles 358–363). According to an assessment conducted by Microsoft, Taiwan has enacted robust computer security laws that have resulted in favorable alignment with the Council of Europe Convention on Cybercrime. This assessment found that Taiwan's computer security laws are most strongly aligned in the areas of: illegal access, illegal interception, data interference, system interference, misuse of devices, computer-related forgery and computer-related fraud.[218]

Taiwan does not have a standalone cyberespionage statute. Rather, cyberespionage is investigated as violations of Chapter 36 Articles 358 and 359.[219] Article 358 deals with illegal intrusions and can be applied to government, corporate and individuals' computers. Article 359 deals with the unauthorized alteration of computers and likewise can be applied to the same users. Both laws were initially developed in an effort to combat hackers,[220] but have since been assimilated to investigate and prosecute

218 Microsoft Corporation, "Asia Pacific Legislative Analysis: Current and Pending Online Safety and Cybercrime Laws" (17 October 2007), 84.

219 Consultation with Taiwanese law enforcement official #1 and #2 (Taipei, Republic of China: 30 May 2012), regarding application of Taiwanese Law to cyberespionage.

220 Chang Weiping, Chung Wingyan, et. al., "Fighting cybercrime: a review and the Taiwan experience," *Decision Support Systems 41* (2006), 677–678.

cyberespionage cases as violations of Taiwanese law. In addition to these cyber related offenses, additional changes can be brought against individuals involved in cyberespionage under Taiwan's national security laws that regulate standard espionage violations, specifically, Chapter 2 Article 109, which addresses the passage of state secrets to a foreign government.[221] Overall, Taiwan's current criminal statues adequately allow law enforcement the authority to investigate and arrest cyber criminals and to mitigate cyberespionage, which provides an overall high assessment for Taiwan's legal capacity.

(2) Organizations. Cybercrime that involves personal property, identity, e-commerce, prostitution, child pornography and violation of individual liberties are generally investigated by the Criminal Investigation Bureau (CIB) of the National Police Agency (NPA) of Taiwan.[222] When these crimes rise to a threshold that impairs national security they are referred for further investigation to the Ministry of Justice Investigation Bureau (MJIB). This process works similarly to the federal versus local or state level of jurisdiction within the United States, with the MJIB being most analogous to the FBI. National security investigations on behalf of the MJIB typically involve major money-laundering, narcotics, anti-corruption, financial and espionage cases. However, when cyberespionage is determined or alleged to have emanated from another country, then MJIB corroborates in a subordinate capacity with the National Security Bureau (NSB) for further investigation.[223] Cyberespionage in these cases generally includes the theft of intellectual property from Taiwanese corporations or theft of state secrets via cyber means.

Taiwan recognizes that cybercrime is a major threat to domestic and international security. As part of this assessment the government of Taiwan has prioritized the development of its own internal capacity and sought broader engagement with international partners. As part of its domestic efforts, Taiwan established a

---

221 Correspondence with Taiwanese law enforcement official #3 (1 June 2012), regarding the charges levied against individuals arrested for cyberespionage.

222 Weiping Chang, Shihchieh Chou, Chichao Lu, et. al., "Cybercrime & Cybercriminals: An Overview of the Taiwan Experience," *Journal of Computers*, vol. 1, no. 6 (September 2006), 1–2.

223 Consultation with Taiwanese law enforcement official #1 (29 May 2012), while discussion the structure of Taiwanese law enforcement to combat cybercrime.

Crimecrime Investigation Unit (CIU), a division within the MJIB that is responsible for the investigation and coordination of cyber incidents.[224] In 2007, the MJIB established a National Cyber Forensics Laboratory at its Headquarters in Taipei. The CIB of the NPA also established its own cyber lab and a CIU, which is responsible for cybercrimes within their jurisdiction. This development included the placement of a CIU within each county level NPA station.[225] In addition to these structural improvements, the government of Taiwan has assigned special prosecutors within the Ministry of Justice to streamline cybercrime prosecutions for criminal and national security cases.[226]

On the international front, Taiwan has established an International Criminal Investigations Brigade (ICIB) within the CIB. ICIB has become the principal authority for transnational criminal investigations related to Taiwan.[227] Taiwan also participates in Interpol and has participated in the High Technology Crime Investigation Conference hosted by the FBI in Quantico, VA.[228] In 2006, an MJIB delegation of cyber investigators attended a two-day forensic workshop sponsored by the Massachusetts' State Police and the Suffolk County District Attorney's Office.[229] Attendance at this event sought to further develop forensic cyber investigative knowledge and bring best practices back to Taiwan.

Apart from Taiwan's law enforcement efforts to combat cybercrime, its Ministry of National Defense (MND) J6 also plays a central role in cybersecurity.[230] While Taiwan does not have an analog to USCYBERCOM, MND J6 would be its closest comparison. Although little is known about the capacity of this unit,

---

224 Chien Shih Chieh, "An Overview: Anti-Cybercrime Efforts in Taiwan," Naif Arab University for Security Studies (Circa 2007–2008), 3.

225 Chang Weiping, Wingyan Chung, et. al., "Fighting cybercrime: a review and the Taiwan experience," 678.

226 Solin Yen, Souchan Chen, "Planning and Building a Taiwan Cyber Forensic Laboratory," *IEEE A&E Systems Magazine* (September 2007), 17–22.

227 Taiwan Criminal Investigations Bureau, "About CIB: History" (23 December 2009), <http://www.cib.gov.tw/English/about/about01.aspx> (30 May 2012).

228 Correspondence with Taiwanese law enforcement official #3 (30 May 2012), while addressing law enforcement efforts for international cooperation.

229 "EvidentData Hosts Cybercops from Taiwan," *Business Wire* (19 April 2006).

230 Consultation with U.S. government official #4 (28 May 2012), regarding Taiwan MND's role in cybersecurity.

MND J6 employs Taiwan's primary CND capability. Overall, due to Taiwan's substantial level of development for combating cybercrime within its law enforcement and judicial departments, combined with an unknown but established unit to conduct CND within the MND J6, Taiwan's organizational capacity for cybercrime investigation and prosecution is regarded as high.

(3) Policies. Taiwan has instituted a number of polices that have led to an increased capacity to protect state secrets and to harden national security communication infrastructures. The MND utilizes an air-gaped "Intranet" similar in function to DoD's Sipernet[231] and a system of secure voice using an encryption algorithm to ensure voice communication is transported securely between users.[232] Additionally, Taiwan institutes a firm set of policies that regulate the handling of sensitive and classified information.[233] For its attention to security and implementation of hardware and policies that regulate protection of sensitive information, Taiwan constitutes a level policy development and awareness assessed as moderate to high.

b. Assessing Taiwan's Current CND Capacity

The sensitive nature of this subject has made assessment of the Taiwan's government capacity for CND difficult. However, inferences from other areas of Taiwan's CND posture can be made to assess its overall capacity in this regard. These tangential areas include corporate, education and commercial sectors. In April 2010, Taiwan's Legislative Yuan strengthened its information technology laws with passage of a revised Personal Data Protection Act (PDPA). The purpose of the revision was to mandate compliance by corporations and individuals in the handling, collection and safeguarding of personal data.[234] The PDPA created a standardized process in Taiwan

---

231 Consultation with Taiwanese MND official #1 (Washington, D.C.: 18 May 2012), regarding similarities between the U.S. and Taiwanese policies that regulate defense communications.

232 Consultation with U.S. government official #4 (28 May 2012), regarding Taiwan policies for defense communication.

233 See "The Classified National Security and Protection Act" (6 February 2003), which defines classified information handling procedures and punitive measures of lack of compliance, <http://law.moj.gov.tw/Eng/LawClass/LawAll.aspx?PCode=I0060003> (6 June 2012).

234 Benjamin Chiang, "Taiwan's Revised Personal Data Protection Act: The Age of Information Liability Begins," *CommonWealth*, no. 454 (26 August 2010).

for the protection of personal data that compels all industries, universities and commercial entities to pass a certification process in order to remain in compliance with the law.[235] There appears to be a great deal of speculation regarding the enforcement of this law, but the intent behind its implementation signifies the clear understanding of a government that wants Taiwanese corporations and individuals to pay more attention to the defense of information security.

New policies and the passage of laws that strengthen information security governance show a strong understanding of the cybersecurity threat environment in Taiwan. The assessed level of CND support instituted by large Taiwanese corporations is high. However, there appears to be a significant gap between these large entities and companies that constitute the medium to small end of the spectrum. This gap presents a significant problem to Taiwan business development and creates an overall permissive environment for malicious computer activity. Contributing factors for this capability gap mostly includes the high cost of CND implementation due to a minimal presence of domestic technical expertise.[236] Currently, Taiwan has three major deficits in its commercial CND structure that cannot be filled by domestic support alone; they are:

1) Digital Identification Services: E-commerce identification solutions.[237]

2) Insurance Mechanisms: Protection of companies from liability if consumer data is mishandled or breached.[238]

3) Total Solution Providers: Taiwan has a limited amount of companies who can act as total solution providers and a strong demand for such services.[239]

Taiwan needs affordable solutions to address these three problem areas in order to bring its small and medium companies in line with current CND processes. American companies willing to develop services to fulfill these needs would be greatly

---

[235] Consultation with Taiwanese university professor #1 (Taipei, Republic of China: 1 June 2012), regarding the application of PDPA.

[236] Consultation with individuals from a Taiwanese think tank (Taipei, Republic of China: 1 June 2012), as provided in a formal presentation detailing Taiwan's cybersecurity posture and current gaps.

[237] Ibid.

[238] Ibid.

[239] Consultation with individuals from a Taiwanese think tank (Taipei, Republic of China: 1 June 2012).

welcomed in Taiwan.[240] Addressing these areas would provide a significant boost in Taiwan's overall CND posture, and improve its rating. An aggregate assessment of Taiwan's CND capacity thus incorporates an understanding of its current gaps coupled with an assumption that its high capacity to implement legal, organizational and policy initiatives in the protection of its cyber infrastructure (covered previously) determines that Taiwan has developed at least a moderate capacity in the CND arena.

c. Taiwan's Ability to Mitigate FIS Penetration

A series of recent espionage arrests and convictions has produced great concern over Taiwan's level of FIS penetration. In January 2011, Major General Lo Hsien-che was arrested and charged for committing espionage on behalf of the PRC in what has been described as "the most prominent espionage case in Taiwan in decades."[241] Lo was later found guilty and sentenced to life in prison by a Taiwanese military court. Since Lo's arrest, three other Taiwanese have been separately arrested and charged on espionage statues for providing national defense related information to China.[242] These cases signify a high degree of intelligence penetration within Taiwan's national security establishment and China's continued priority to collect C4ISR related information within Taiwan despite improved political relations.[243] The prevalence of these cases reveals a possible increase in the effectiveness of Taiwan's counterintelligence capabilities; however, a consequence of this frequency also depicts a level of PRC intelligence penetration that is most likely deeper than what has been exposed. Taken together, this analysis suggests that Taiwan's level of FIS penetration is high.

This sequence of spy scandals has produced a realization by Taiwan's decision makers that Taiwan needs to improve its counterintelligence efforts to limit the effects of Chinese espionage. President Ma has called for Taiwan to "actively prevent"

---

240 Ibid.

241 Edward Wong, "Taiwan General Charged in Spy Case," *New York Times* (9 February 2011).

242 Peter Enav, "Spies Target Taiwan's U.S.-made defenses," *Army Times* (21 March 2012).

243 Peter Mattis, "Evaluating China's Intelligence Penetration of Taiwan," *The Jamestown Foundation China Brief*, vol. 12, no. 6 (15 March 2012).

Chinese espionage though strengthened defensive counterintelligence efforts.[244] Highlighting these efforts includes new policies that institute travel restrictions for retired National Security Bureau (NSB) personnel wishing to travel to China and the development of reporting requirements for military members who are engaged in romantic relationships with Chinese nationals.[245] In a recent example, a Taiwanese fighter pilot was disciplined for having "improper conduct" with a female reporter from China National Radio. In response to the incident, the MND released a statement saying, "[t]he ministry continues to strengthen its anti-spying mechanism to prevent Chinese communists from prying on our military intelligence."[246] Thus, despite the high level of perceived foreign intelligence penetration, Taiwan appears to be taking action to enhance its counterintelligence efforts and limit its exposure to Chinese espionage.

Exacerbating Taiwan's espionage problem is the ease by which Chinese Intelligence has been able to use ideology to recruit Taiwanese spies. A shared national identity between China and Taiwan indicates that Taiwanese identity politics play a central role in these espionage recruitments. While current polling shows a trend in the growth of an independent Taiwanese identity, [247] the interdependence created from amicable commercial and political policies appears to have produced a mindset for many in Taiwan that China is no longer a grave threat. Enhanced suitability in this context limits Taiwan's ability to mitigate its exposure to espionage from the Chinese mainland despite encouraging signs that the Government of Taiwan is instituting policies and enhancing its counterintelligence capabilities. As such, this analysis concludes that Taiwan's high level of assessed FIS penetration is due to a PRC proclivity to use espionage as a means to gain insight into Taiwanese politics and produce military advantage, coupled with an increased suitability from a shared national identity.

---

244 "Taiwan should boost defences against China Spies," *Sino Daily* (5 August 2011).

245 Joseph Yeh, "NSB chief urges ex-agents to avoid travel to mainland," *The China Post* (9 March 2012).

246 "Taiwan pilot punished for dating Chinese reporter," Hindustan Times (16 May 2012).

247 Chu Yun-han, "Taiwan's National Identity Politics and the Prospect of Cross-Strait Relations," *Asian Survey* 44, no. 4 (July/August 2004), 484–512; Malcolm Cook, "Taiwan's Identity Challenge," *SAIS Review 25*, no. 2 (summer/fall 2005), 83–92.

d. Taiwan's Motivation for Increased Cooperation

It is highly probable that Taiwan would attach more value to political gains from increased cooperation with the United States than they would from tangible defense upgrades. For Taiwan, capability increases often pale in comparison to the political messages that accompany such procurements. In this vein, continued demands for U.S. flag level officer visits, acquisition of F-16 C/D fighter aircraft, or diesel submarines are all viewed for their significant political vice capability enhancement value. In this regard, it is likely that Taiwan would seek a public announcement of increased cyber cooperation as a means to provide a political message to the Chinese mainland. This political message could be intended to deter Chinese cyber aggression while signaling increased ties with the United States. However, such a political message has consequences that could alter the calculus of Taiwan's willingness to engage in bilateral cyber cooperation with the United States altogether.

In the current political environment, a political message signifying increased cyber cooperation with the United States is aggressive and not congruent with the state of conciliatory political discourse between China and Taiwan.[248] As such, it is assessed that although there would be political pressure to publicly announce increased cyber cooperation with the United States to gain deterrent value, such cooperation would be downplayed by the Taiwanese in the current political environment. This is not to assume that Taiwan would always restrain a broadcast of increased CND capabilities. Domestic political pressure could become an important element in such a disclosure if hostile cyber activity emanating from China continues or worsens in the years ahead. Additionally, such announcements could have second and third order effects for other U.S. strategic partners in the region.[249] Thus, while there are tangible benefits for Taiwan to seek greater cyber cooperation with the United States, calculations regarding the public acknowledgment of such increases will most likely remain Taiwan's primary considerations when evaluating increased cyber cooperation with the United States.

---

[248] Paul Mozur and Jenny Hsu, "Taiwan Vote Shows Doubt About China," *The Wall Street Journal* (16 January 2011).

[249] Consultation with U.S. government official #3 (20 April 2012), regarding the political effects of U.S.-Taiwan cyber cooperation on the Pacific region.

e. Benefit for the United States

Determining the benefit for increased cyber cooperation with Taiwan to the United States involves a basic risk vs. reward calculus. As stated previously, at the U.S. policy-decision maker level, cooperation on cybersecurity issues with Taiwan is not constrained by concern over PRC reactions.[250] As such, any reluctance on behalf of the United States is about the balance of risk versus reward. Thus, the same calculus used to evaluate broadened U.S. engagement for any nation also applies to Taiwan.

(1) Reward Analysis. In 2010, while he was still the Secretary of Defense, Robert Gates wrote in *Foreign Affairs* that the United States needs to focus on "building partner capacity," which he defined as "helping other countries defend themselves or, if necessary, fight alongside U.S. forces by providing them with equipment, training, or other forms of security assistance."[251] Building partner capacity with Taiwan proposes that the United States explores how to help Taiwan help itself. In the realm of cybersecurity, developing closer cooperation on cyber issues is therefore, a benefit to the U.S. policy agenda as it supports an increased indigenous capacity for Taiwan to defend against unwanted military, economic and political influence. Furthermore, the United States has a fundamental desire for Taiwan to maintain a capacity to defend itself against kinetic and cyberattack derived from within China.[252] This includes cyber actions that produce political coercion as a means to influence Taiwanese policy. Developing cooperative cybersecurity with Taiwan, therefore fulfills U.S. policy regarding building partner capacity, while at the same time produces a more independent Taiwanese capacity to resist PRC coercion.

There are also non-political rewards for developing a more robust cyber cooperation agenda with Taiwan. Since Taiwan shares many of the same cyberspace threats as the United States, it is reasonable to conclude that their law enforcement and national security apparatus maintains knowledge that could enhance

---

[250] Consultation with U.S. government official #1 (20 April 2012), regarding constraints on U.S. policy.

[251] Robert M. Gates, "Helping Others Defend Themselves: The Future of U.S. Security Assistance," *Foreign Affairs*, vol. 89, no. 3 (May/June 2010), 2.

[252] Consultation with U.S. government official #1 (20 April 2012), regarding U.S. policy goals.

U.S. cybersecurity capabilities. Developing a mutually beneficial relationship with Taiwan in this regard could likely provide a mechanism by which new cyber exploitation tools, zero-day exploits, phishing attempts, computer viruses and even attribution information could be learned by the United States. USCI currently expends a great deal of resources within stove-piped organizations in an attempt to better understand these issues. Enhancing cybersecurity cooperation with Taiwan could enhance counterintelligence effectiveness and address efficiency concerns in a fiscally constrained environment. Regarding the latter, leveraging Taiwanese knowledge becomes a force multiplier, which is an attractive element as USCI agencies weigh effectiveness against limited resources. Given these advantages, the inquiry regarding increased cooperation with Taiwan becomes less about what the United States gains and more about how to balance several inherent risks.

(2) Risks Analysis. The United States benefits from cyber cooperation with Taiwan through an increased ability to fulfill U.S. policy *vis-à-vis* building partner capacity; however, the risk incurred from such development is more opaque. The United States should be concerned about the level of the perceived FIS penetration in Taiwan, and how this equates to increased vulnerability of U.S. plans, intentions and capabilities for building partner capacity. However, if cybersecurity cooperation can be conducted while addressing the FIS concern, then this threat becomes rather subdued. The DoD *Operating in Cyberspace* document indicates that as a means to increase cybersecurity, the DoD will institute best practices of "cyber hygiene," those activities that seek to protect user data and ensure both software and operating systems are up to date.[253] Sharing these best practices with international partners is a simple cooperative step toward building trust and enhancing future cooperation. Helping Taiwan to help itself in this regard is simply the development of standards that would allow Taiwan an ability to more adequately protect their own infrastructure while not providing a capability that—if provided to another nation—would result in increased U.S. vulnerability.

253 United States Department of Defense, "Department of Defense Strategy for Operating in Cyberspace," 6–7.

It is most likely that the United States is more concerned about near-term events than those in the distant future. As such, international cooperation that results in a foreign nation receiving increased capacity is not necessarily weighted against how such increases could be used against the United States in the future. Applied to Taiwan, this analysis indicates small increases that produce better standards of cyber hygiene would not produce concern for how such capacity developments could someday be used against the United States. As such, if initial cyber cooperation is limited, then the threat of China obtaining increased capabilities through subversion or unification should not factor into the decision making process.

This approach toward developing cybersecurity cooperation with Taiwan is a short term trust building exercise that could expand as each partner demonstrates its commitment to enhancing the others cybersecurity posture. If such an expansion were to occur, then increased cooperation would have to be levied against concerns that capacity may be transferred to the PRC. While this concern is important to note, it may not be as large a factor in the decision making process as it first appears. Seen from a similar perspective, this same concern has not stopped the U.S. from engaging in the sale of military equipment and weapons to Taiwan. These sales clearly provide capacity increases to Taiwan that if transferred through subversion or unification, would increase the PRC's capacity as well. Using the foreign military sales angle to shed light on the risk versus reward dynamic for increased cyber cooperation poses an interesting question; is there something inherent in cyberspace that changes the calculus or otherwise prohibits application of the foreign military sales model to cyber cooperation?

Any assessment detailing the continued sale of military weapons and equipment to Taiwan in support of the Taiwan Relations Act of 1979 must include domestic political concerns. While these concerns can be ideological—in that the United States supports democratic nations—the more significant rationale includes the economic benefit to the defense industrial base. As such, congressional representatives whose constituents profit financially from the sale of military goods to Taiwan are likely to press

for continued deals despite the risks involved. Assimilating this dynamic to assess the risks for increased cyber cooperation produces similar but different outcomes.

The primary difference between foreign military sales (FMS) and increased cybersecurity cooperation is that the cyber component has no constituent interest in the United States and thus, lacks a critical component for overriding inherent risk. In addition, the FMS model appears to mitigate risk by selling Taiwan less than cutting-edge military hardware. This is evident in FMS that includes Kidd, vice Arleigh Burke class destroyers and F-16s, vice F-22s. This poses a question regarding the degree to which the United States could provide second rate cyber capability enhancements while it desires first rate information in return. A proper analysis of this question must take into consideration that second rate capability enhancements are most likely not adequate within the current cyber environment. This is due in large part to the speed at which cyberspace technologies advance. Thus, for any degree of substantial capacity enhancement to be meaningful, the United States would likely have to include first rate cyber defense hardware, software and know-how in order maintain a viable level of cooperation. Unlike FMS, overcoming the risks inherent with this level of capability enhancement would not be mitigated by constituent interests. As such, proving the feasibility of cooperation in micro-areas of cyber capacity development would likely need to be attained before cyber cooperation could expand.

4. Increased Cyber Cooperation from the Taiwanese Perspective

Understanding what increased cybersecurity cooperation means from the Taiwanese perspective provides a more solid foundation from which, to amply assess the feasibility of increased cooperation as a whole. Taiwan has signed a number of criminal related Memorandums of Understanding (MOU) with foreign governments in Europe, Asia and the Americas, but these agreements typically only address traditional crimes such as money laundering, human trafficking and child indecency.[254] Taiwan seeks broader international partnerships to address a host of other criminal issues, but it recognizes that its geopolitical situation impedes effectiveness and limits the potential for

[254] Consultation with Taiwanese law enforcement official #1 and #2 (Taipei, Republic of China: 30 May 2012), regarding international cooperation.

expansion. Taiwan's national leaders believe "the lack of formal channels for Taiwan cybercrime investigators to communicate with other countries' law enforcement agencies hinders effective investigation."[255] In an effort to establish a more secure society, Taiwan's purpose for international law enforcement engagement appears geared toward the solidification of relationships, channels or forums through which it can effectively mitigate crime within its own borders.

Taiwan's geopolitical status further prevents basic cooperation in other areas of cybercrime mitigation. While Taiwanese investigators are able to obtain law enforcement related information from foreign Internet companies that maintain offices in Taiwan (Yahoo, Microsoft and Google), they are unable to acquire information when acts are conducted via services that do not have representation in Taiwan (Facebook and Twitter).[256] To counter this deficit, Taiwan maintains liaison relationships with the FBI and U.S. Secret Service, but the closest representatives of these agencies reside in Hong Kong. This geographic separation and the lack of established formal channels has resulted in sporadic and untimely requests for assistance.[257] Taiwan's motivation for increased cyber cooperation therefore, seeks to change this dynamic by establishing formal channels of cooperation through signed MOUs for cybersecurity.

Proposed parameters for such an MOU would include the sharing of cybersecurity information, procedures for effective cybercrime investigation, training of Taiwanese officers by U.S. experts in workshop formats, sharing standard operating procedures and jointly developing best practices.[258] Taiwan is further motived to "establish cooperative platforms" by which direct connections or taskforce style relations can be established.[259] Such information sharing could ultimately include Taiwan providing the United States

---

[255] Chang Weiping, Wingyan Chung, et. al., "Fighting cybercrime: a review and the Taiwan experience," 678.

[256] Consultation with Taiwanese law enforcement official #1 (Taipei, Republic of China: 30 May 2012), regarding Taiwanese capabilities in obtaining support to cyber investigations.

[257] Ibid., regarding the process by which Taiwan obtains American law enforcement assistance.

[258] Consultation with Taiwanese law enforcement official #1 and #2 (Taipei, Republic of China: 30 May 2012), regarding the process by which Taiwan obtains American law enforcement assistance.

[259] Ibid., regarding Taiwan's view of expanded cybersecurity cooperation.

with knowledge of new viruses, zero-day exploits, identification of hacker groups and individual hackers and possibly even attribution of individuals involved in cyberespionage.

5. International Level Restructuring, Conclusion

The quote referenced at the beginning of this chapter by Austin Matschulat in 1969 has profound applications for addressing counterintelligence effectiveness today. As the national security decision maker looks to balance increased effectiveness with the risk that accompanies developing and maintaining international partnerships, it becomes necessary to adopt a responsible strategy to afford the development and maintenance of liaison relationships. For the USCI community historically, it has been easier to avoid such relationships than to seek ways that provide for effective mitigation of risk in the pursuit of added counterintelligence capacity. However, analysis presented in this chapter delineates a path by which the risk of engaging in developing greater cooperation with Taiwan can be minimized in the short term, and possibly even the long term if trust and mutual benefit can be established.

Working to improve Taiwan's cyber hygiene serves as a risk-neutral micro-approach to building cyber cooperation and could serve as an initial step in developing the trust needed for more robust cyber cooperation in the future. Although the United States must balance international cooperation priorities, the national cyberthreat clearly necessities that non-traditional approaches be fully considered and evaluated for potential gains. The model of cyber cooperation presented in this chapter and applied to Taiwan, indicates that Taiwan would be an ideal candidate for increased cooperation if its assessed level of FIS penetration can be mitigated. While this factor is a significant and potentially insurmountable barrier, initial cyber cooperation could be developed that mitigates this threat as a means to develop trust and set a precedent for mutually beneficial exchange. Improving Taiwan's level of awareness through joint exchanges and sharing of cyber hygiene best practices could result in an increased CND capability within Taiwan, which could positively impact its ability to mitigate FIS penetration.

Taiwan's motivation for desiring increased cyber cooperation is apparent. Taiwan seeks political empowerment through publically announced increases in cooperation with the United States on a variety of issues; however, there remains a strong voice within Taiwan's decision making body that such announcements could complicate cross-strait developments.[260] This concern indicates that growing cyber cooperation from the initial cyber hygiene steps proposed in this chapter may encounter political challenges. This concern could produce a need for cyber cooperation to take on a law enforcement or commercial sector undertone in the future, vice an overt U.S. policy one. Movement in this direction would find Taiwan less motivated to seek political gains and more interested in tangible cybersecurity improvements. This would be a positive transformation in Taiwanese strategic thinking as Taiwan has an imperative to develop law enforcement liaison relationships that result in less vulnerability to a variety of transnational crimes. Thus, while Taiwan's motivations are mixed between political and tangible capacity increases, it is likely that both desires can serve U.S. policy and counterintelligence priorities.

The United States ultimately benefits from increased cooperation with Taiwan if the initial phases of cyber cooperation can be developed within a framework that circumvents risk. Developing formal law enforcement channels that institutionalize a process for joint cybersecurity development, information sharing and risk management would provide the United States with a means to fulfill Secretary Gates' concept of developing partner capacity. Secondarily, increasing cyber cooperation with Taiwan affords the United States a political message of its own; namely, that if the PRC cannot adequately curtail cybercrime emanating from within its borders, then U.S. decision makers will be forced to develop cooperative relationships that China believes are contrary to its own interests. Finally, utilizing a micro-approach to set the scene for a larger cooperative relationship with Taiwan could prove valuable as a means to increase counterintelligence effectiveness through the provision of early-warning for new computer viruses, zero-day exploits, exploitation tools and possibly even attribution at

[260] Consultation with individuals from a Taiwanese think tank (Taipei, Republic of China: 1 June 2012), regarding complications from increased U.S.-Taiwan cyber cooperation.

the state or individual level. Arriving at this point is not an overnight process, but the potential gains certainly compel the initiation of these first steps.

THIS PAGE INTENTIONALLY LEFT BLANK

V. CONCLUSION, APPLYING THE FINDINGS

Addressing counterintelligence effectiveness in the United States has long been a neglected topic that has resulted in many misconceptions and few suggestions regarding how to create a unified counterintelligence enterprise. This gap in knowledge has much to do with New Institutionalist concepts that stress the importance of culture and initial agency development. Counterintelligence professionals practice a strict culture of secrecy, and they should, but this concept permeates into other areas of the discipline that do not require such safeguarding. This thesis explored this concept, namely, through the adequate restructuring of counterintelligence toward building a stronger capacity to mitigate cyberespionage. Drawing lessons learned from a case study of the April 2007 cyberattack on Estonia and the international community's ensuing attempts to ensure cyberspace, this thesis developed an initial baseline for addressing the issues of cyberespionage. It has determined that the cyberespionage threat to American national security—explored via cases that targeted the U.S. Department of Defense, defense industrial base and the commercial sector—is prolific and requires immediate attention from the nation's national security establishment.

Mitigating this threat is a significant challenge for today's national security decision maker, especially in light of the fact that the current USCI community is not properly structured. Removing stove-pipes, minimizing redundancies and engaging non-traditional international partners are techniques proposed in this thesis that together constitute micro-level changes for implementation in the short term. These structural changes take into account the current fiscal environment and evolving U.S. policy decision to rebalance toward the Asia-Pacific region.[261] These findings not only provide effectiveness and efficiency alternatives for the current environment, but if proven successful they could institute larger changes for both the U.S. counterintelligence community and provide direction for DoD policy makers. Instituting micro-level structural changes enhances the national security posture of the United States by allowing

[261] Mark Manyin, Stephen Daggett, et. al., "Pivot to the Pacific? The Obama Administration's 'Rebalancing' Toward Asia," *Congressional Research Service*, R42448 (28 March 2012), 1.

additional means for the U.S. military to retain its technological superiority and for U.S. companies to maintain their competitive advantage. Finally, refocusing USCI efforts toward building international partner capacity acts as a force multiplier in combating cybercrime and could produce increased effectiveness for mitigating cyberespionage from an operational and political perspective.

A. NEW INSTITUTIONALISM APPLIED TO COUNTERINTELLIGENCE EFFECTIVENESS

Using a New Institutionalist approach to examine the culture of secrecy surrounding counterintelligence determines that internal agency predilections against intelligence sharing impedes domestic and international cooperation. Nations do not generally like to share intelligence of any sort unless they are close allies and even then, there are strong rules that govern the level and nature of the information shared. There is a rational reason for this as sensitive operations can sometimes be compromised by expanding the circle of knowledge beyond those who need to know. However, operational details notwithstanding, there are areas for intelligence sharing that do not threaten current operations or undermine national policy decisions. In these areas, counterintelligence cooperation should be stressed between like-minded nations where capacity developments can lead to increased effectiveness.

Counterintelligence—as a subset of intelligence—is mostly concerned with the investigation and mitigation of the crime of espionage. A standard technique for reducing crime includes law enforcement liaison between similarly affected nations as a means to develop cooperative techniques and share threat information. However, counterintelligence's culture of secrecy limits the means available for effective reduction of cyberespionage, as it generally prohibits law enforcement liaison between like-minded nations. This analysis does not suggest that operational details need to be shared between nations; after all such sharing could be abused or lead to the divulgence of intelligence sources and methods. Rather, the culture of secrecy unnecessarily prevents cooperation that should be focused on capacity development toward areas of common interest. Capacity building could focus on sharing trend analysis, developing a common threat picture, training or exploring joint defensive means to protect common interests.

Additionally, the counterintelligence culture protects it from oversight controls that should demand accountability for effectiveness. Those who fall outside this subset of government service are rarely given a true optic through which to gauge its effect on national security. Therefore, counterintelligence oversight in the United States becomes a process to ensure the enforcement of rules that protect civil liberties and financial resources from being abused. Neither congressional nor executive oversight is designed to adequately judge the true level of counterintelligence effectiveness,[262] because neither branch of government has the institutional knowledge to properly gauge what effectiveness really looks like. As such, oversight serves an accountability measure to ensure the protection of institutional reputations and observance of U.S. law.

This analysis places an emphasis on the need to create mechanisms through which counterintelligence can prove its value to the national security decision maker and allow for an adequate level of judgment about counterintelligence effectiveness. However, this cannot be achieved without first addressing the structural issues that prevent counterintelligence from becoming an indispensable force for sustaining national security. Creating true *unity of effort* across the USCI enterprise toward mitigating cyberespionage is therefore, a means to accomplish this goal.

Another New Institutionalist problem is that federal employees often face one reform effort after another due to the perceived need of decision makers to start anew with each change of leadership. These reforms often lead to confusion, waste and the setting of priorities that are shifted once political winds change.[263] Taken together, the large *macro-approaches* to reform generally add bureaucratic layers by creating new administrative hurdles. In fact, this onslaught of reform initiatives has contributed to the government's reputation for administrative inertia vice operational effectiveness.[264] The last major overhaul generally regarded as successful was the GWN Act of 1986.

---

262 Lowenthal, *Intelligence: From Secrets to Policy*, 199–213. In this section Lowenthal describes a process of intelligence oversight that does not focus on effectiveness in the fulfillment of mission objectives or the setting of priorities, but rather is concerned with procedure and adherence to U.S. law.

263 Paul Light, "A Government Ill Executed: The decline of the Federal Service and How to Reverse It," (Cambridge, MA: Harvard University Press, 2008), 223.

264 Ibid., 222.

However, opponents of GWN cited concern that an over-centralized bureaucracy would diminish the role of the Service Secretaries and Service Chiefs.[265] While they were proven incorrect, a favorable domestic political climate and a media willing to advance the topic to the American people were important aspects of the reform's success.

These factors are lacking within the USCI reorganization environment today, leaving the decision maker to search for small-scale efforts that can prove successful at improving effectiveness over time. A micro-restructuring model would not require the large-scale political capital demonstrated during GWN and would be based on authorities already within the institutions targeted for reform. Micro-level changes are easier to institute because they typically involve only one or two agencies and when taken together, can result in large-scale capability increases.

B. ADDRESSING THE NEED FOR REFORM WITHIN DEFENSE COUNTERINTELLIGENCE

Various national security policy documents covered in this thesis address the need for increased counterintelligence effectiveness to mitigate cyberespionage. Yet, the stove-piped and parochial nature of counterintelligence in the United States provides no forcing mechanism by which these agencies need comply. The Office of the National Counterintelligence Executive is perhaps the best situated to develop such mechanisms, but current policy generated from this national coordination authority has no real influence. The ONCIX can suggest and even pretend to influence the three core areas of counterintelligence hiring, training and personnel development through career paths, but they have no means to compel the services to actually develop such practices.

The fact of the matter is that without a forcing mechanism, NCIS will continue to hire based on its core mission of civilian law enforcement, AFOSI will look for qualified officers within its ranks and bright enlisted personnel who test well enough to earn the most coveted training in federal law enforcement, and Army CI will continue to buck the trend and utilize a preponderance of military personal to perform the core competencies of CI within its department. This report recognizes that these differences are inadequate

265 Locher, *Victory on the Potomac*, 400–401.

for DoD CI as a whole and that the cultural variance between these organizations prevents the development of a true DoD CI enterprise. As such, a forcing mechanism is needed; developing one within DoD instead of relying on ONCIX to gain the authority necessary to control budgets, hiring practices, training or career paths is the most effective means of producing the *unity of effort* required to mitigate threats to national security.

Furthermore, this thesis recognizes that national security agencies evolve differently than domestic policy departments. Amy Zegart succinctly points out this distinction:

> In domestic policy, interest groups and their legislative supporters take the lead in shaping agency design and operations. The action takes place mostly in Congress. But in national security affairs, presidents and bureaucrats are the primary players, battling over agency structure far away from the capitol steps.[266]

Her distinction rests primarily on the fact that domestic policy has a constituency that law makers must appease, while national security has no such body to represent it. However, cyberespionage changes this dynamic in that it too, has a domestic policy base represented by the corporations whose bottom lines are affected from the loss of proprietary information or strengthened competition based on stolen product designs. Thus, counterintelligence reform intended to increase effectiveness in mitigating the national cyberthreat can act more like a domestic policy organization and less like a national security agency in that it too, has the support of a constituent bases with substantial interest group representation.

Increasing domestic cooperation among DoD counterintelligence is a practice in streamlining effectiveness in a challenging fiscal environment. Minimizing redundancy between agencies should be considered a best practice in an era of fiscal restraint. Micro-restructuring DoD CI by employing the JCIU model within the established COCOM JCCs removes stove-pipes that create redundancy and waste by providing a forcing mechanism that compels DoD CI agencies to work together toward a common goal. Not

266 Zegart, *Flawed by Design*, 123.

only is this level of restructuring easy to accomplish, because it all can take place within a single government department, but it provides an additional tool to the CCDR who desperately needs to address the cyberespionage threat to their commands.

C. ADDRESSING THE THREAT FROM CYBERSPACE

The global community clearly recognizes the criminal, military and intelligence threats posed from increased dependence on cyberspace. This thesis has used the Estonian case to extrapolate the issues of cyberpower, attribution and the complexities surrounding the formation of institutions that seek to prevent cyberattack. Threat mitigation techniques that include the establishment of cyber norms, international agreements, codes of conduct, ratification or assimilation of laws and attempts to solve the attribution problem all require a significant investment in time and resources before they can become effective.

This thesis has determined the difficulty of attribution has become the main enabler of cyberthreats. Even efforts to produce an international cyberdomain that addresses attribution in Internet Protocol Version 6 (IPv6) has been met with complications in its worldwide acceptance and attribution workarounds. IPv6 provides the capability of tracking the activity and location of individual devices on networks; however, privacy concerns have already produced tools to circumvent the added attribution features of this new Internet protocol system.[267] Regulating hostile cyber activity through international political mechanisms or technological improvement alone does not address the current cybersecurity situation. Faced with an existential threat to American national security, national leaders do not have the luxury of adopting solutions that require such investments of time.

Instead, the decision maker must embrace decisions that empower national security elements to offensively target hostile cyber activity in accordance with U.S. law. Reliance on liberal ideals alone to shape international behavior or establish new international regimes to regulate cyberespionage is unlikely to achieve desired results.

[267] Kevin Scott, "The Next Internet Privacy in Internet Protocol Version 6 (IPv6)" SANS Institute Infosec Reading Room (24 March 2004), 8.

When looking at the breadth of the cyberespionage problem with China, key national security advisors have determined that "[t]he potential of cyber space for espionage is so overwhelming that it is unrealistic to seek cooperative agreements to govern this part of the problem."[268] This recognition, while accurate, has unfortunately produced an incorrect policy direction within the current U.S. administration, one that emphasizes defense over offensive. The propensity to embrace defense is clearly expressed in the June 2009 National Cyberspace Policy Review Security:

> Without major advances in the security of these systems or significant change in how they are constructed or operated, it is doubtful that the United States can protect itself from the growing threat of cybercrime and state-sponsored intrusion and operations. Our digital infrastructure has already suffered intrusions that have allowed criminals to steal hundreds of millions of dollars and nation-states and other entities to steal intellectual property and sensitive military information.[269]

This alarmist statement advocates that large structural changes to the Internet or the establishment of new government organizations to regulate and curtail malicious cyber activity are the necessary solutions to mitigate the current challenges in cyberspace. However, such approaches do not take into account fiscal responsibility and they should leave the national security decision maker anxious for alternatives that efficiently utilize taxpayer dollars. Solutions that employ micro-changes to the existing national security infrastructure would be more responsible and could prove more effective in the near term.

1. The Effect of Cyberspace on Espionage

The properties of cyberspace have made cyberespionage cheap, easy and low risk when compared to the investment, payoff and political blowback from traditional human espionage. In this context cyberespionage has become an affordable solution for states looking for asymmetric means to balance power. The prevalence of cyberespionage presents challenges to the conduct of intelligence and counterintelligence, forcing each to change tactics in order to be successful in the current environment. Joel Brenner references the need for change as:

---

[268] Lieberthal and Singer, "Cybersecurity and U.S.-China Relations," 33.

[269] Office of the President of the United States, *National Cyberspace Policy Review*, p. i.

> In an age of mass surveillance and instant electronic storage and retrieval, covert espionage operations will never be the same again. The intelligence business, like everyone else, now operates in a glass house…You'd have to be crazy not to believe that the Pentagon's top-secret system, JWICS, isn't penetrated.[270]

Brenner's alarming words are supported by the current Director of the NSA's Information Assurance Directorate Debora Plunkett, who confirms that threats from cyberspace has fundamentally changed the way the NSA does business, "[t]here is no such thing as 'Secure' anymore...the most sophisticated adversaries are going to go unnoticed on our networks."[271] In light of these assessments the national security establishment and commercial sector need to adapt new techniques and empower old ones. In the current cyber environment speed, not security, will be considered the main defense against cyberespionage.[272] Developing an ability to continuously out-innovate, bring to market and employ products or weapons systems faster than opponents is the only assured way to maintain competitive advantage in both the commercial and defense sectors. However, there is one additional component to producing this advantage, the ability to vigorously employ a capacity to slow down the competition. Making it difficult for the adversary by slowing down their acquisition cycle, becomes one of the primary functions of offensive counterintelligence in the cyber dominated environment.

D. ADDRESSING THE THREAT FROM CHINA

This thesis has determined that as a realist actor within the international system, China has much to gain by partaking in cyberespionage, computer network exploitation and the development of a cyberwarfare capability directed at the United States. A study of China's current military doctrine shows the development of asymmetric capabilities aimed at degrading the technological advantage of a superior advisory. Writings from PLA military officers confirm that developing cyber capacity is recognized as a fundamental means for achieving political and military goals.

---

270 Brenner, *America the Vulnerable*, 86, 163.

271 Jim Wolf, "U.S. Code-Cracking Agency Works as if Compromised," *Reuters* (16 December 2010).

272 Brenner, *America the Vulnerable*, 199.

As such, the U.S. decision maker does not need positive attribution before taking steps that will improve the defensive and offensive capabilities of the national security establishment, to plan for and mitigate attacks derived from within China. A large part of this process is to recognize that USCI has a large role to play in the development of these capabilities and that its cyber elements need to be effectively organized to best impact its mission. This capability increase is not only warranted, but imperative in the current political and strategic environment. However, not all proposals suggest such realist means for combating the cyberthreat from China.

Kenneth Lieberthal and Peter Singer have written of the need for constructive political dialogue with China as a means to establish normative patterns of behavior that will regulate mounting tensions in the U.S.-China relationship over cybersecurity. In doing so, they propose an agenda for cooperation that builds upon a realistic recognition of the difficulties each nation faces as a basis for discussion and eventual exploration of common steps toward the mitigation of hostile cyber activity.[273] Their proposal consistently states that such an agenda would include a "respect that each government will protect its ability to use cyber capabilities to carry out espionage activities and support military activities should they become necessary."[274] This proposal clearly seeks to obfuscate the fact that a suspicion of Chinese state-directed cyberespionage is perhaps one of the leading causes of tension between the two nations. Attempting to isolate espionage from the larger issue is not only inconsistent with seeking to determine a viable solution, but it grossly misrepresents the structural problems that have caused tensions in the first place.

Such liberal idealism will not suffice to address the realist underpinnings of the U.S.-China relationship or create an education of minds and a mutual understanding on cybersecurity issues. However, while their proposed solutions are unlikely to achieve results, the basis for their analysis is reasonable. The fact of the matter is that "the perception is growing at both the popular and elite level in America that the cyberthreat

[273] Liberthal and Singer, "Cybersecurity and U.S.-China Relations," 23.

[274] Ibid.

from China, while multifaceted, has a large government-directed component."[275] In order to mitigate this threat, or to prove its state-sponsored veracity, a forcing mechanism needs to be created that compels DoD CI to develop *unity of effort* to increase effectiveness, derive mitigation techniques and develop intelligence that allows the decision maker a clear understanding of the cyberespionage threat posed from within China. Attribution becomes a key enabler of U.S. policy in this regard and DoD CI is uniquely positioned to answer the attribution question for the policy maker, if provided the resources and structural foundation to be effective.

E. ADDRESSING MICRO-RESTRUCTURING DOMESTICALLY

President Obama's *International Strategy for Cyberspace* document confirms the United States will maintain the right to protect itself against attacks in and through cyberspace. His policy stated, "[w]hen warranted, the United States will respond to hostile acts in cyberspace as we would to any other threat to our country."[276] As such, the United States reserves the right to use all necessary means—diplomatic, informational, military and economic—to limit cyberthreats in accordance with applicable international law.[277] This indicates cyberattacks that cripple the nation's critical infrastructure or military capacity will be treated the same as kinetic attacks that have the same effect. Calculating responses to these events therefore, includes the ways and means used to respond to more traditional strikes.

In similar fashion, attacks that pilfer vast amounts of secret or sensitive data from defense contractors, American corporations, or DoD systems via traditional espionage would be met with swift response from the nation's counterintelligence enterprise. In the cyber realm, assimilating the White House doctrine referenced above necessitates a similar unleashing of the nation's CI enterprise to offensively and defensively mitigate the cyberespionage threat. Joel Brenner said this best in his comment that USCI needs "to

---

[275] Liberthal and Singer, "Cybersecurity and U.S.-China Relations," 3.

[276] Office of the President of the United States, "International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World" (May 2012), 14.

[277] Alexander, "Testimony of the Commander United States Cyber Command, Before the House Committee on Armed Services Subcommittee on Emerging Threats And Capabilities," 7.

live inside our adversaries' networks."[278] His suggestion includes an offensive counterintelligence capability and one in which USCI needs to play an active role in implementing.

This analysis does not intend to identify or exclude other elements of the U.S. government who are currently engaged in offensive CNO, or otherwise define or minimize the authorities of organizations like USCYBERCOM. Rather, it proposes a linkage between the authorities that are traditionally responsible for mitigating espionage activates in the United States under Title 18 with those that have an increased cybersecurity mission to defend the nation under Title 10, i.e., USCYBERCOM. Combining these authorities produces the *unity of effort* required in U.S. policy documents and eliminates waste.

However, instead of attempts to create a true DoD CI enterprise, new stove-pipes are created, as manifest in the recent operational authority vested within DIA DCHC. Time will tell if the new DCHC model will be effective, but it too will encounter profound structural problems due to the manner in which it was established. Zegart refers to initial agency design as a critical juncture in an agency's ability to be effective later in its life cycle. DCHC is likely to have hiring practices that emphasize the need for experienced intelligence personal vice law enforcement. In fact, in the announcement of its offensive mission, DCHC specifically renounced the need for a law enforcement body to fulfill its role, and even went so far as to allude to the failure of CIFA in large part due to the assimilation of a law enforcement mindset and personnel where one was not necessary.[279]

Such wrangling actually detracts from effectiveness in general and limits the ability of decision makers to create a true DoD CI enterprise. There is little debate in the United States about the law enforcement nature of counterintelligence. Attempts to parse this into defensive and offensive semantics do not otherwise take away from the recognized fact that counterintelligence in the United States is an inherently law

[278] Joel Brenner, *America the Vulnerable*, 216.

[279] Defense Intelligence Agency, "Media Roundtable About the Establishment of the Defense Counterintelligence And Human Intelligence Center," 11–12.

enforcement function. The parallel to this in the criminal world is the war on drugs. No one argues that the war on drugs within government is not a law enforcement function. As such, both the offensive and defense means of fighting this war are handled by law enforcement entities, most notably by the DEA. Yet, there is little speculation that DEA offensive operations that seek to identify, penetrate and ultimately mitigate drug cartels should be an intelligence function left solely for the CIA to implement. Rather, DEA's offensive mission continues in the overseas environment, one that it conducts with intentional coordination with the CIA.

In a similar vein, domestic discussions and statements about the law enforcement nature of offensive or defensive counterintelligence also necessitate the need for coordination and cooperation between law enforcement and intelligence. DIA's attempt to restructure and develop another counterintelligence entity without law enforcement authorities not only undermines the charter of counterintelligence in the United States, but it fails to create the initial agency cooperation that is needed in the current environment. Such cooperation is even more critical in an environment of fiscal restraint and when facing a threat as significant as cyberespionage.

F. ADDRESSING MICRO-RESTRUCTURING INTERNATIONALLY

This thesis has analyzed numerous U.S. policy and strategy documents that apply to the current counterintelligence, intelligence and cyberspace environments. Each of these initiatives discusses the need to increase international cooperation to non-traditional allies in an effort to create a more effective national security posture. Evaluating the feasibility of expanding cybersecurity cooperation with Taiwan has determined that there are political and security challenges that must be addressed prior to the development of a robust cooperative relationship. This analysis also suggests that the common cybersecurity threat optic that the United States and Taiwan share compels efforts that seek to build trust and lay the foundation for larger engagement in the future. The DoD has a unique role to play in providing for this initial foundation through its presently established relations with Taiwan's national security establishment.

While the U.S. national security decision maker is not constrained from building partner capacity with Taiwan, the same cannot be said for Taiwan's decision makers who appear concerned over PRC reactions. Ma Ying-jeou, the President of the Republic of China (Taiwan), in a speech he provided virtually to the Center for Strategic Studies in Washington D.C., voiced his political reluctance to exacerbate the PRC. Ma stated:

> For Cross-Strait relations to continue advancing, the U.S. must help Taiwan level the playing field. Negotiating with a giant like the Chinese mainland is not without its risks. The right leverage must be in place, otherwise Taiwan cannot credibly maintain an equal footing at the negotiation table.[280]

Statements like this, along with research conducted during this thesis, make it safe to assume that Taiwan is clearly concerned about jeopardizing conciliatory relations between itself and the PRC. As such, any expansion of the existing U.S.-Taiwan relationship needs to be constructed in a manner that is mindful of this larger issue. USCI appears to have a unique role to play in developing the initial pathways of this capacity, because LE-LE liaison is a non-threatening way to address capability increases. Developing cooperative law enforcement forums, platforms or formally established channels for joint cybercrime investigation is a micro-approach to building trust while adhering to Taiwan's concerns over disrupting the balance of cross-straits relations.

The FMS model indicates that the risk of increasing Taiwanese capabilities is mitigated when there is strong domestic political support in the United States. Cyberespionage also has a degree of this domestic political support as represented by the American corporations who continually have their competitive advantage degraded through cyberespionage. While this domestic political pressure does not relinquish any of the concern that increased Taiwanese capabilities could be siphoned off to the PRC, it does compel the national security decision maker to initiate a dialogue with Taiwanese authorities regarding the initial stages of cooperation. This thesis concludes that initial cooperation could be as benign as helping Taiwan to increase its cyber-hygiene, or linking U.S. cybersecurity companies and insurance provides with Taiwan businesses to

280 Ma Ying-jeou, "Building National Security for the Republic of China," Speech via Videoconference with Center for Strategic and International Studies (Washington, D.C., May 12, 2011), 6.

provide cost effective solutions to cybersecurity issues. These activities are risk neutral and can set the scene for larger capacity development in the future.

If it is later determined that more robust cyber cooperation can be achieved, then it is practical that USCI should play a major role in creating this capacity. While the DoD has firmly established relationships with Taiwan, the FBI would be the ideal candidate to lead a USCI initiative in building cybercrime reduction capacity in Taiwan. DoD CI would certainly play a large role in such an endeavor, but primarily as a means to address cyberespionage. Micro-restructuring in this regard changes the focus of DoD CI toward building partner capacity with Taiwan in a manner that takes into account the present security considerations. By deliberately employing a small capacity building process initially—as a means to build trust and test the political climate for increased cooperation—DoD CI could eventually realize increased effectiveness through shared knowledge of the cybersecurity threats faced by Taiwan.

G. FINAL REMARKS

The current structure of USCI is not properly geared toward the effective mitigation of national security risk. For all the references to a U.S. counterintelligence enterprise, the unsightly reality is that a true USCI enterprise does not exist in the United States today. Rather, individual counterintelligence agencies determine priorities and allocate resources independent from any type of national coordinating authority. This creates a counterintelligence process that is stove-piped, redundant and largely ineffective as each agency advances interests pursuant to their own course of action. As such, descriptions of a U.S. counterintelligence community that is fractured, myopic and marginally effective are unfortunately accurate. Attempts to bring about the *unity of effort* desperately needed within counterintelligence, as referenced in numerous counterintelligence strategy documents, has resulted in the development of large coordination entities absent the forcing mechanisms needed to compel integration.

The establishment of the NCIX and CIFA are the best examples of this, and neither agency was provided the budgetary authority or operational oversight needed to force interagency collaboration, reduce redundancies or address efficiency. When asked

if the U.S. government takes the espionage threat from China seriously, former National Counterintelligence Executive Michael Van Cleave responded:

> I think that we are not presently structured, as a government, to take it seriously enough. We continue to play defense, we continue to wait until the cases manifest themselves here in the United States, and because that is the way we have gone about the counterintelligence business we are behind. (Question: How would you change things?) Someone be assigned the responsibility to identity, assess, and *proactively degrade* foreign intelligence threats against the United States. No one has that job today.[281]

As the former lead authority on USCI structural matters, Van Cleave was uniquely positioned to make such a comment. She calls for a counterintelligence structure that unites the various elements around an offensive mission, a radical concept even today.

The creation of a DoD counterintelligence enterprise should be simple enough. Four operational CI agencies fall under the direction of the Department of Defense, and all four must abide by decisions set forth by the Secretary of Defense. However, different cultures and parochial interests remain the primary obstacles to large-scale reform. In an environment absent the political will or monetary capital needed for macro-level reform, micro-approaches must be developed that establish a level of joint cooperation that increases DoD capacity to more effectively respond to national security threats.

This thesis concludes that cyberespionage is one of the gravest threats facing the national security of the United States. This threat degrades the American economy through the theft of intellectual property and subsequent reduction of American commercial prowess. As such, cyberespionage decreases the true underpinnings of American power and the source of American influence around the world. This threat also substantially reduces the capacity of the American military. Theft of military secrets and technology allows potential advisories to close the technology gap that provides distinct advantage to America's modern fighting force. The result is diminished capacity to project American power and the wasteful expenditure of trillions of dollars in research and development costs.

---

281 Henry Schuster, "Extra: Stopping Chinese espionage" *60 Minutes* (28 February 2010), <http://www.cbsnews.com/video/watch/?id=6252859n&tag=segementExtraScroller;housing> (28 April 2012).

Current international attempts to curtail hostile cyber activity in cyberspace provide no short-term solutions for the national security decision maker who seeks options to address the cyberespionage threat. Recommendations that rely on international mechanisms, institutions or laws take too much time to implement and as such, fail to be effective solutions. Determining a path to increase counterintelligence effectiveness is the most viable solution for mitigating this threat in short order. Developing such a capacity increase around the cyberespionage threat provides a mission oriented approach that could lead to systemic changes in the future.

Utilizing the JCIU model to develop joint operational support for the COCOM within each JCC provides a micro-restructuring solution that allows for the timely and effective mitigation of cyberespionage while at the same time eliminating stove-pipes and producing *unity of effort* within DoD CI. Such developments result in increased efficiency and effectiveness, two large benefits for national security capabilities in a fiscally restrained environment. Additionally, developing an operational cyberespionage mitigation capacity within each COCOM conforms to the intent of GWN without the need for legal interpretations that mandate such compliance. This structural reform can be established by the authorities vested within the Secretary of Defense. This omits many of the complications that would be present in cross-departmental structural reforms and provides a pathway for the alignment of needs with ways and means.

Additional micro-restructuring places an emphasis on the degree to which increased cybersecurity cooperation can be developed with Taiwan. While there are political and security concerns on both the sides of this issue, this thesis has explored the ways in which LE-LE liaison can act in a non-threatening capacity to develop increased cooperation with Taiwan. To maximize effectiveness, this approach could be conducted in parallel with the sharing of best practices of cyber-hygiene. Both initiatives are micro-approaches toward building trust and a mutually beneficial relationship that could one day develop into larger cooperation on cybersecurity issues. The shared cyberthreat environment between Taiwan and the United States should place the development of this

relationship at the forefront of U.S. priorities for international cybersecurity engagement. Taking initial steps to explore this path is a low risk and responsible endeavor in the current threat environment.

Minimizing redundancy between agencies—especially those that fall under the same executive department—should be considered a best practice in an era of fiscal restraint and heightened responsibility. Instituting a micro-restructuring approach for DoD CI agencies is an exercise in effective reform that can be accomplished within the constraints of the current environment. Should such a micro-restructuring approach be proven successful, it could pave the way for broader restructuring and the development of an actual DoD counterintelligence enterprise. Working to develop cooperative capacity with international partners is potentially a force multiplier for DoD CI, if conducted in a manner that minimizes risk and maximizes benefit. Using the national cyberthreat to develop increased counterintelligence effectiveness is a vital step in securing national security and addressing efficiency. Counterintelligence has always played an important role in safeguarding the nation; providing CI with an adequate structure to address contemporary challenges will assure that the United States retains its fundamental elements of national power. The current state of geopolitical affairs requires continued leadership from the United States, empowering it to maintain this role requires the effective mitigation of threats from its counterintelligence establishment.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

Adams, Patton, George Bakos and Bryan Krekel. *Occupying the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage*: Prepared for The U.S.-China Economic and Security Review Commission by the Northrop Grumman Corporation, 2011.

Alexander, Keith. *Testimony of the Commander United States Cyber Command, before the House Committee on Armed Services Subcommittee on Emerging Threats and Capabilities,* 20 March 2012.

Austin, Greg and Franz-Stefan Gady. *Russia, the United States, and Cyber Diplomacy: Opening the Doors*. New York: East West Institute, 2010. http://www.ewi.info/system/files/USRussiaCyber_WEB.pdf.

Bachman, Gregory. "Integrating Defense Counterintelligence: A First Step." Georgetown Public Policy Institute, 2011.

Beyer, Louis. "Defense Investigators and the War on Terrorism." *The Journal of Public Inquiry* (spring/summer, 2006). http://www.ignet.gov/randp/sp06jpi.pdf (23 May 2012).

Blank, Stephen. "Web War I: Is Europe's First Information War a New Kind of War?" *Comparative Strategy* 27, (2008): 227–247.

Boebert, Earl. *A Survey of Challenges in Attribution*: The National Research Council, The National Academies Press, 2010.

Boraz, Steven and Thomas Bruneau. "Democracy and Effectiveness." *Journal of Democracy* 17, no. 3 (2006): 28–42.

Brenner, Joel. *America the Vulnerable: Inside the New Threat Matrix of Digital Espionage, Crime and Warfare*. New York: Penguin Press, 2011.

Bright, Arthur. "Estonia Accuses Russia of 'Cyberattack'." *The Christian Science Monitor,* 17 May 2007. http://www.csmonitor.com/2007/0517/p99s01-duts.htm.

Brown, Davis. "A Proposal for an International Convention to Regulate the use of Information Systems in Armed Conflict." *Harvard International Law Journal* 47, no. 1 (winter, 2006): 179–221.

Burch, James. "A Domestic Intelligence Agency for the United States? A Comparative Analysis of Domestic Intelligence Agencies and their Implications for Homeland Security." *Homeland Security Affairs* III, no. 2 (June, 2007): (30 April 2012).

"Business Strategies in Cybersecurity and Counterintelligence: Remarks by the National Counterintelligence Executive." University of Texas at Austin, Applied Research Laboratories, 3 April 2009. http://www.dni.gov/speeches/20090403_speech.pdf.

Cartwright, James. U.S.-China Economic and Security Review Commission. *Hearing on China's Military Modernization and its Impact on the United States and the Asia-Pacific*, 29 March 2007. http://www.uscc.gov/hearings/2007hearings/transcripts/mar_29_30/mar_29_30_07_trans.pdf.

Chang, Weiping and Shichieh Chou et. al. "Cybercrime & Cybercriminals: An Overview of the Taiwan Experience." *Journal of Computers* 1, no. 6 (September, 2006). http://academypublisher.com/jcp/vol01/no06/jcp01061118.pdf (27 May 2012).

Chang, Weiping and Wingyan Chung et. al. "Fighting Cybercrime: A Review and the Taiwan Experience." *Decision Support Systems 41* (2006). http://www.ai.arizona.edu/intranet/papers/fighting_cybercrime_DSS.pdf (30 May 2012).

Chang, Yao-Chung. "Cyber Conflict between Taiwan and China." *Strategic Insights* 10, no. 1 (spring, 2011): 26–35.

Chen, Souchan and Solin Yen. "Planning and Building a Taiwan Cyber Forensic Laboratory." *IEEE A&E Systems Magazine* (September, 2007): 17–22.

Chiang, Benjamin. "Taiwan's Revised Personal Data Protection Act: The Age of Information Liability Begins." *CommonWealth* no. 454. http://english.cw.com.tw/article.do?action=show&id=12214&offset=0 (26 August 2010).

Chien, Shih Chieh. *An Overview: Anti-Cybercrime Efforts in Taiwan*: Naif Arab University for Security Studies, 2007–2008.

Chu, Yun-han. "Taiwan's National Identity Politics and the Prospect of Cross-Strait Relations." *Asian Survey* 44, no. 4 (July/August, 2004): 484–512.

Churchill, Ward and Jim Vander Wall. *The Cointelpro Papers: Documents from the FBI's Secret Wars Against Dissent in the United States*. Boston: South End Press, 2001.

Cirincione, Joseph. *Bomb Scare: The History and Future of Nuclear Weapons*. New York: Columbia University Press, 2008.

Clark, Richard and Robert Knake. *Cyber War: The Next Threat to National Security and what to do about it*. New York: HarperCollins, 2010.

Cook, Malcom. “Taiwan’s Identity Challenge.” *SAIS Review* 25, no. 2 (summer/fall, 2005): 83–92.

Cowdery, Nicholas. “Emerging Trends in Cybercrime, Paper Presented at the 13th Annual International Association of Prosecutors Conference, New Technologies in Crime and Prosecution: Challenges and Opportunities.” Singapore: 2008.

Crowe, William J. *The Line of Fire: From Washington to the Gulf, the Politics and Battles of the New Military.* New York: Simon and Schuster, 1993.

“Cyber Spies Assault U.S. Power Grid.” *Jane’s Intelligence Digest,* 5 May 2009.

Daggett, Stephen, Ben Dolven, Mark Manyin, and et. al. *Pivot to the Pacific? The Obama Administration’s ‘Rebalancing’ Toward Asia*: Congressional Research Service, 2012. http://www.hsdl.org/?view&did=705063.

Dam, Kenneth, Herbert Lin, and William Owens. *Technology, Policy, Law, and Ethics regarding U.S. Acquisition and use of Cyberattack Capabilities*: The National Academies Press, 2009.

Defense Intelligence Agency. *Media Roundtable about the Establishment of the Defense Counterintelligence and Human Intelligence Center*. Washington: Federal News Service, 2008.

Department of Defense Directive 5100.1. *Functions of the Department of Defense and its Major Components,* 2010. http://www.dtic.mil/whs/directives/corres/pdf/510001p.pdf.

Department of Defense Directive 5240.10. *Counterintelligence in the Combatant Commands and Other DoD Components,* 2011.

Department of Defense Strategy for Operating in Cyberspace, 2011.

Doscher, Thomas. “NORAD, USNORTHCOM Joint Cyber Center Stands Up.” http://www.northcom.mil/News/2012/050112.html (23 May 2012).

Drew, Christopher. “Stolen Data is Tracked to Hacking at Lockheed Martin.” *The New York Times,* 3 June 2011. http://www.nytimes.com/2011/06/04/technology/04security.html.

Drew, Christopher and John Markoff. “Data Breach at Security Firm Linked to Attack on Lockheed Martin.” *The New York Times*, 27 May 2011. http://www.nytimes.com/2011/05/28/business/28hack.html.

Enav, Peter. “Spies Target Taiwan’s U.S.-made Defenses.” *Army Times*, 21 March 2012. http://www.armytimes.com/news/2012/03/ap-china-spies-target-taiwan-us-made-defenses-032112/.

“EvidentData Hosts Cybercops from Taiwan.” *Business Wire,* 19 April 2006. http://findarticles.com/p/articles/mi_m0EIN/is_2006_April_19/ai_n16127160/.

Evron, Gadi. *Authoritatively, Who was Behind the Estonian Attacks* Security Dark Reading. http://www.darkreading.com/blog/227700882/authoritatively-who-was-behind-the-estonian-attacks.html. (2009).

Executive Office of the President of the United States. “The Comprehensive National Cybersecurity Initiative.” The White House. http://www.whitehouse.gov/sites/default/files/cybersecurity.pdf (23 February 2012).

Extra: Stopping Chinese Espionage. Video. Produced by Schuster, Henry. 60 Minutes, 2010. http://www.cbsnews.com/video/watch/?id=6252859n&tag=segementExtraScroller;housing.

Feng, Zhu and Robert Ross. *China’s Ascent: Power, Security, and the Future of International Politics*. New York: Cornell University Press, 2008.

“Foreign Spies Are Serious. Are We?” *The Washington Post*, 8 February 2009. http://www.washingtonpost.com/wp-dyn/content/article/2009/02/06/AR2009020603498.html?sid=ST2009121703759.

Gates, Robert M. “Helping Others Defend Themselves: The Future of U.S. Security Assistance.” *Foreign Affairs* 89, no. 3 (May/June, 2012): 2.

Geschwind, C. N. “Wanted: An Integrated Counter-Intelligence.” *Studies in Intelligence* 7, no. 3 (1963): 15–37.

Goodman, Michael. “Who is Trying to Keep what Secret from Whom and Why? MI5-FBI Relations and the Klaus Fuchs Case.” *Journal of Cold War Studies* 7, no. 3 (summer, 2005): 124–146.

Gorman, Siobhan. “Electricity Grid in U.S. Penetrated by Spies.” *Wall Street Journal,* 8 April 2009. http://online.wsj.com/article/SB123914805204099085.html.

Government Accountability Office. *Defense Acquisitions: Assessments of Selected Weapon Programs*: Highlights of GAO-12–400-SP, a Report to Congressional Committees, 2012. http://www.gao.gov/assets/590/589696.pdf.

Guo, Lei, Caiyu Gu, and Lan Wu. “Why China Established ‘Online Blue Army’.” *People’s Daily Online,* 28 June 2011. http://english.people.com.cn/90001/90780/7423270.html.

Hall, Peter and Rosemary Taylor. “Political Science and the Three New Institutionalisms.” *Political Studies* 44, (1996).

Heickero, Roland. *Emerging Cyberthreats and Russian Views on Information Warfare and Information Operations*: Swedish Defense Research Agency, 2010.

Hjortdal, Magnus. “China’s use of Cyber Warfare: Espionage Meets Strategic Deterrence.” *Journal of Strategic Security* 4, no. 2 (2011): 3.

House Permanent Select Committee on Intelligence and Senate Select Committee on Intelligence. *Report of the Joint Inquiry into the Terrorist Attacks of September 11, 2001, 107th Congress, 2nd Session*. Washington DC: Government Printing Office, 2002.

Hsiao, Russell, Jenny Lin, and Mark Stokes. “The Chinese People’s Liberation Army Signals Intelligence and Cyber Reconnaissance Infrastructure.” 11 November 2011.

Hsu, Jenny and Paul Mozur. “Taiwan Vote shows Doubt about China.” *The Wall Street Journal,* 16 January 2011. http://online.wsj.com/article/SB10001424052970204555904577162143105033610.html.

Kent, Sherman. “The Need for an Intelligence Literature.” *Studies in Intelligence* (1955): 1–11.

King, William and Michael J. Woods. “An Assessment of the Evolution of Defense Counterintelligence Activities.” *Journal of National Security Law & Policy* 3, no. 169 (2009): 187.

Kuehl, Daniel. “From Cyberspace to Cyberpower: Defining the Problem.”In *Cyberpower and National Security,* edited by Kramer, Franklin, Stuart Starr and Larry Wentz, 38. Washington D.C.: National Defense University, 2009.

Leyden, John. “RSA Defends Handling of Two-Pronged SecurId Breach.” *The Register,* 11 October 2011. http://www.theregister.co.uk/2011/10/11/rsa_securid_breach_keynote/.

Li, Nan. “The PLA’s Evolving War Fighting Doctrine, Strategy, and Tactics, 1985–1995: A Chinese Perspective.” In *China’s Military in Transition,* edited by Shambaugh, David and Richard Yang, 179–199. Oxford: Clarendon Press, 1997.

Lieberthal, Kenneth and Peter Singer. *Cybersecurity and U.S.-China Relations*: 21st Century Defense Initiative, John L. Thornton China Center at Brookings, 2012.

Light, Paul. *A Government Ill Executed: The Decline of the Federal Service and how to Reverse it*. Cambridge, MA: Harvard University Press, 2008.

Lin, Herbert. *Understanding Cyberattack as an Instrument of U.S. Policy, Presentation at the Council on Foreign Relations*. New York City: 2011. http://www.cfr.org/content/thinktank/Lin_UnderstandingCyberattack.pdf.

Locher III, James. *Victory on the Potomac: The Goldwater – Nichols Act Unifies the Pentagon* College Station: Texas A & M Press, 2002.

Lowenthal, Mark. *Intelligence: From Secrets to Policy*. 4th ed. Washington DC: CQ Press, 2009.

Lynn, William J. "Remarks on the Department of Defense Cyber Strategy." Office of the Assistant Secretary of Defense for Public Affairs, National Defense University, 14 July 2011. http://www.defense.gov/speeches/speech.aspx?speechid=1593.

Ma, Ying-Jeou. *Building National Security for the Republic of China, Speech Via Videoconference with Center for Strategic and International Studies,* 12 May 2011. http://csis.org/files/attachments/110512_President_Ma_CSIS_0.pdf.

Martin, Paul. *NASA Cybersecurity: An Examination of the Agency's Information Security, Testimony before the Subcommittee on Investigations and Oversight, House Committee on Science, Space, and Technology, U.S. House of Representatives*, 2012. http://oig.nasa.gov/congressional/FINAL_written_statement_for_%20IT_%20hearing_February_26_edit_v2.pdf.

Masco, Joseph. "Lie Detectors: On Secrets and Hypersecurity in Los Alamos." *Public Culture* 14, no. 3 (fall, 2002): 441–467.

Matschulat, Austin. "Coordination and Cooperation in Counterintelligence." *Studies in Intelligence* 13, no. 2 (1969): 25–36.

Mattis, Peter. "Evaluating China's Intelligence Penetration of Taiwan." *The Jamestown Foundation China Brief* 12, no. 6 (March 15, 2012): http://www.jamestown.org/programs/chinabrief/single/?tx_ttnews[tt_news]=39140&tx_ttnews[backPid]=25&cHash=ea6e806f4b7bac89cc7a3bb413c640b3. (23 May 2012).

Maurer, Tim. *Cyber Norm Emergence at the United Nations: An Analysis of the UN's Activities regarding Cyber-Security?* Cambridge, MA: Belfer Center for Science and International Affairs, Harvard Kennedy School, 2011.

Microsoft Corporation. *Asia Pacific Legislative Analysis: Current and Pending Online Safety and Cybercrime Laws*: Microsoft Corporation, 2007. http://www.itu.int/ITU-D/cyb/cybersecurity/docs/microsoft_asia_pacific_legislative_analysis.pdf.

Nakashima, Ellen. "Chinese Leaders Ordered Google Hack, U.S. was Told." *The Washington Post*, 5 December 2010. http://www.washingtonpost.com/wp-dyn/content/article/2010/12/04/AR2010120403347.html.

The National Counterintelligence Strategy of the United States of America 2005, 2005. http://www.ncix.gov/publications/policy/FinalCIStrategyforWebMarch21.pdf.

The National Counterintelligence Strategy of the United States of America 2008, 2008. http://www.ncix.gov/publications/policy/2008_Strategy.pdf.

The National Counterintelligence Strategy of the United States of America 2009, 2009. http://www.ncix.gov/publications/policy/NatlCIStrategy2009.pdf.

National Security Council. *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure*, 2011.

Nye, Joseph. *Cyber Power*. Cambridge, MA: Belfer Center for Science and International Affairs, Harvard Kennedy School, 2010.

"Nuclear Lessons for Cyber Security?" *Strategic Studies Quarterly* (winter, 2001): 34.

Office of the National Counterintelligence Executive. "Fundamental Elements of the Counterintelligence Discipline: Universal Counterintelligence Core Competencies." 1, (January, 2006): 3.

Office of the President of the United States. *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World*, 2012. http://www.whitehouse.gov/sites/default/files/rss_viewer/internationalstrategy_cyberspace.pdf.

Office of the Secretary of Defense. *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2011*: U.S. Department of Defense, 2011. http://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0CFIQFjAA&url=http%3A%2F%2Fwww.defense.gov%2Fpubs%2Fpdfs%2F2011_cmpr_final.pdf&ei=keXLT_mhOaOq2gWvybjaCw&usg=AFQjCNFUNSZXGFGEAd4KTKbA98OKl9X3Hg&sig2=r6x1F1H0xtpUCRNH1nW8Iw.

Pomfret, James and Jonathan Standing. "Ma Ying-Jeou Wins Second Term in Taiwan Election." *National Post*, 14 January 2012. http://news.nationalpost.com/2012/01/14/ma-ying-jeou-wins-second-term-in-taiwan-election/.

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

Reforming Intelligence: Obstacles to Democratic Control and Effectiveness. Austin, TX: University of Texas Press, 2007.

Rosenzweig, Paul. *10 Consecutive Principles for Cybersecurity Policy*: The Heritage Foundation Backgrounder, 2011. http://www.heritage.org/research/reports/2011/01/10-conservative-principles-for-cybersecurity-policy.

Schreier, Fred, Barbara Weekes, and Theodor Winkler. *Cyber Security: The Road Ahead*: Geneva Security Forum, Democratic Control of Armed Forces (DCAF) Horizon 2015 Working Paper No. 4, 2011.

Scott, Kevin. *The Next Internet Privacy in Internet Protocol Version 6 (IPv6)*: SANS Institute Infosec Reading Room, 2004. http://www.sans.org/reading_room/whitepapers/protocols/Internet-privacy-Internet-protocol-version-6-ipv6_1397.

Security Counterintelligence: Foreign Spies Stealing U.S. Economic Secrets in Cyberspace, Report to Congress on Foreign Economic Collection and Industrial Espionage 2009–2011, 2011.

Shambaugh, David. *Modernizing China's Military: Progress, Problems, and Prospects*. Berkeley, CA: University of California Press, 2004.

"Strategic Counterintelligence." Washington D.C., The University Club, 29 March 2007.

Su, Jie. "PLA 'Online Blue Army' Gets Ready for Cyber Warfare." ECNS.cn Online. http://ecns.cn/2012/01–16/6254.shtml (14 April 2012).

Sustaining U.S. Global Leadership: Priorities for the 21st Century Defense, 2012.

"Taiwan Pilot Punished for Dating Chinese Reporter." *Hindustan Times,* 16 May 2012. http://www.hindustantimes.com/world-news/RestOfAsia/Taiwan-pilot-punished-for-dating-Chinese-reporter/Article1–856705.aspx.

"Taiwan 'should Boost Defenses Against China Spies'." *Sino Daily,* 5 August 2011. http://www.sinodaily.com/reports/Taiwan_should_boost_defences_against_China_spies_999.html.

Taylor, Stan. "Definitions and Theories of Counterintelligence." In *Strategic Intelligence 4: Counterintelligence and Counterterrorism* , edited by Johnson, Loch. Westport, CT: Praeger Security International, 2007.

U.S.-China Economic and Security Review Commission. *2009 Report to Congress of the U.S.-China Economic and Security Review Commission*. Washington DC: U.S. Government Printing Office, 2009. http://www.uscc.gov/annual_report/2009/annual_report_full_09.pdf.

United States Congress. *The Commission on the Intelligence Capabilities of the United States regarding Weapons of Mass Destruction*, 2005.

United States Cyber Command. *The USCC Cyber Lexicon: A Language to Support the Development of Cyber Capabilities, and the Planning and Execution of Military Cyberspace Operations*, 2011.

United States Department of Defense. *Joint Publication 1–02: Dictionary of Military and Associated Terms*, 2011. http://www.dtic.mil/doctrine/dod_dictionary.

United States Department of Homeland Security Office of Cybersecurity and Communications National Cyber Security Division. *CYBER STORM III: Final Report*, 2011.

Van Cleave, Michelle. *Counterintelligence and National Strategy*: National Defense University: School for National Security Executive Education, 2007.

Wasemiller, A. C. " the Anatomy of Counterintelligence." *Studies in Intelligence* 13, no. 1 (winter, 1969): 10.

Wittman, George H. "China's Cyber Militia." *The American Spectator,* 21 October 2011. http://spectator.org/archives/2011/10/21/chinas-cyber-militia.

Wolf, Jim. “Lockheed Martin Hacked using RSA Keys: Data Breach at the Pentagon’s Largest Supplier.” ITNEWS Online. http://www.itnews.com.au/News/258910,lockheed-martin-hacked-using-rsa-keys.aspx (7 April 2012).

“U.S. Code-Cracking Agency Works as if Compromised.” *Reuters,* 16 December 2010. http://ca.reuters.com/article/technologyNews/idCATRE6BF6BZ20101216?pageNumber=2&virtualBrandChannel=0&sp=true.

Wong, Edward. “Taiwan General Charged in Spy Case.” *The New York Times,* 9 February 2011. http://www.nytimes.com/2011/02/10/world/asia/10taiwan.html.

Wortzel, Larry. *China’s Approach to Cyber Operations: Implications for the United States, Testimony before the Committee on Foreign Affairs, U.S. House of Representatives*. Washington D.C., 2010.

Ye, Zheng and Baoxian Zhao.”How do You Fight a Network War?” *Zhongguo Qingnian Bao,* 3 June 2011.

Yeh, Joseph. “NSB Chief Urges Ex-Agents to Avoid Travel to Mainland.” *The China Post,* 9 March 2012. http://www.chinapost.com.tw/taiwan/china-taiwan-relations/2012/03/09/334068/NSB-chief.htm.

Zegart, Amy. *Flawed by Design: The Evolution of the CIA, JCS, and NSC* Stanford University Press, 1999.

Zetter, Kim. “U.S. Declassified Part of Secret Cybersecurity Plan.” *Wired,* 2 March 2010. http://www.wired.com/threatlevel/2010/03/us-declassifies-part-of-secret-cybersecurity-plan/.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

3. MaryAnn B. Cummings
   Communications Director, W3628
   Naval Criminal Investigative Service
   Russell-Knox Bdg, Quantico, Virginia

4. Thomas C. Bruneau
   Naval Postgraduate School
   Monterey, California

5. Andrew M. Singer
   Naval Postgraduate School
   Monterey, California

6. Scott E. Jasper
   Naval Postgraduate School
   Monterey, California

7. Tim J. Doorey
   Naval Postgraduate School
   Monterey, California

8. CAPT John B. Stubbs
   NAVINSGEN N2

9. Cody J. Ferguson
   Naval Postgraduate School
   Monterey, California