

REPORT DOCUMENTATION PAGE		FORM APPROVED - - - OMB NO. 0704-0188	
PUBLIC REPORTING BURDEN FOR THIS COLLECTION OF INFORMATION IS ESTIMATED TO AVERAGE 1 HOUR PER RESPONSE, INCLUDING THE TIME FOR REVIEWING INSTRUCTIONS, SEARCHING EXISTING DATA SOURCES, GATHERING AND MAINTAINING THE DATA NEEDED, AND COMPLETING AND REVIEWING THE COLLECTION OF INFORMATION. SEND COMMENTS REGARDING THIS BURDEN ESTIMATE OR ANY OTHER ASPECT OF THIS COLLECTION OF INFORMATION, INCLUDING SUGGESTIONS FOR REDUCING THIS BURDEN, TO WASHINGTON HEADQUARTERS SERVICES, DIRECTORATE FOR INFORMATION OPERATIONS AND REPORTS, 1215 JEFFERSON DAVIS HIGHWAY, SUITE 1204, ARLINGTON, VA 22202-4302, AND TO THE OFFICE OF MANAGEMENT AND BUDGET, PAPERWORK REDUCTION PROJECT (0704-0188) WASHINGTON, DC 20503			
1. AGENCY USE ONLY (LEAVE BLANK)	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED <i>STUDENT RESEARCH PAPER</i>	
4. TITLE AND SUBTITLE <i>CYBER CRIME AND HOW IT AFFECTS DIME</i>		5. FUNDING NUMBERS <i>N/A</i>	
6. AUTHOR(S) <i>Skipper, Steven B.</i>			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) <i>USMC COMMAND AND STAFF COLLEGE 2076 SOUTH STREET, MCCDC, QUANTICO, VA 22134-5068</i>		8. PERFORMING ORGANIZATION REPORT NUMBER <i>NONE</i>	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) <i>SAME AS #7.</i>		10. SPONSORING/MONITORING AGENCY REPORT NUMBER: <i>NONE</i>	
11. SUPPLEMENTARY NOTES <i>NONE</i>			
12A. DISTRIBUTION/AVAILABILITY STATEMENT <i>NO RESTRICTIONS</i>		12B. DISTRIBUTION CODE <i>N/A</i>	
ABSTRACT (MAXIMUM 200 WORDS) Cyber and the instruments of national power (DIME) do not intersect in today's scholarly analysis; as such, responding to these threats does not have a clear cut solution. Cyber has unhinged DIME and has unleashed—and will continue to do so—many unforeseen realities of national-level consequence. While much has been written about these two topics independent of one another, the inextricable relationship between DIME and cyber has not been examined. Cyber has fundamentally altered the way we process and store data – offering both positive and negative outcomes. Regardless of the most sophisticated network security measures, information existing within this domain remains at risk and accessible to nefarious actors. In today's ubiquitous information age, we need to rethink how DIME is employed.			
14. SUBJECT TERMS (KEY WORDS ON WHICH TO PERFORM SEARCH) <i>Cyber, Instruments of National Power; National Security, DIME, Stuxnet, Operation Buckshot Yankee, Sony, JP Morgan</i>		15. NUMBER OF PAGES: 37	
		16. PRICE CODE: N/A	
17. SECURITY CLASSIFICATION OF REPORT <i>UNCLASSIFIED</i>	18. SECURITY CLASSIFICATION OF THIS PAGE: <i>UNCLASSIFIED</i>	19. SECURITY CLASSIFICATION OF ABSTRACT <i>UNCLASSIFIED</i>	20. LIMITATION OF ABSTRACT

*United States Marine Corps
Command and Staff College
Marine Corps University
2076 South Street
Marine Corps Combat Development Command
Quantico, Virginia 22134-5068*

MASTER OF MILITARY STUDIES

TITLE:

Cyber Threats: Past, Present, and Future
Cyber Crime and How it Affects DIME

SUBMITTED IN PARTIAL FULFILLMENT
OF THE REQUIREMENTS FOR THE DEGREE OF
MASTER OF MILITARY STUDIES

AUTHOR:

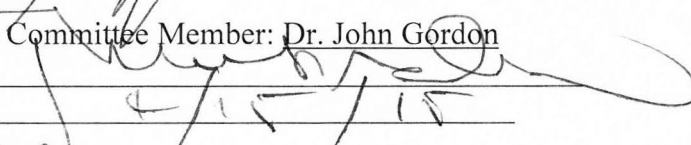
Major Steven B. Skipper

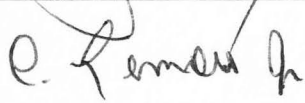
AY 14-15

Mentor and Oral Defense Committee Member: Dr. Matthew J. Flynn

Approved: 
Date: 4/15/15

Oral Defense Committee Member: Dr. John Gordon

Approved: 
Date: 4/15/15


4/15/15
Lt Col USMC

DISCLAIMER

THE OPINIONS AND CONCLUSIONS EXPRESSED HEREIN ARE THOSE OF THE INDIVIDUAL STUDENT AUTHOR AND DO NOT NECESSARILY REPRESENT THE VIEWS OF EITHER THE MARINE CORPS COMMAND AND STAFF COLLEGE OR ANY OTHER GOVERNMENTAL AGENCY. REFERENCES TO THIS STUDY SHOULD INCLUDE THE FOREGOING STATEMENT.

QUOTATION FROM, ABSTRACTION FROM, OR REPRODUCTION OF ALL OR ANY PART OF THIS DOCUMENT IS PERMITTED PROVIDED PROPER ACKNOWLEDGEMENT IS MADE.

Table of Contents

1. Preface.....	4
2. Executive Summary	5
3. Introduction.....	6
4. Background and Literature Review	7
5. Defining the Problem.....	12
6. National Security Strategy	13
7. Diplomatic, Informational, Military, and Economic (DIME).....	14
8. The Hacker Effect	17
9. Military Insider Threats	18
10. Corporate Insider Threats	19
11. Rise of Non-State Actors	20
12. Influence of State Actors	21
13. Operation Buckshot Yankee	22
14. Stuxnet	24
15. JP Morgan Chase	25
16. Sony	26
17. Conclusion	27
18. Endnotes.....	32
19. Bibliography	35

Preface

Cyber and the instruments of national power (DIME) do not intersect in today's scholarly analysis; as such, responding to these threats does not have a clear cut solution. Cyber has unhinged DIME and has unleashed—and will continue to do so—many unforeseen realities of national-level consequence. While much has been written about these two topics independent of one another, the inextricable relationship between DIME and cyber has not been examined. Cyber has fundamentally altered the way we process and store data – offering both positive and negative outcomes. Regardless of the most sophisticated network security measures, information existing within this domain remains at risk and accessible to nefarious actors. In today's ubiquitous information age, we need to rethink how DIME is employed.

I would like to extend my deepest gratitude to my wife, Ginger, and children, Harris, Isabelle, and Jack for their support and patience displayed throughout the research and writing process. Lastly, I would like to offer my genuine appreciation to my research advisor, Dr. Matthew Flynn, for his unwavering encouragement and support.

Executive Summary

Title: The Realities of Cyber Threats: Cyber Crime and How it Affects DIME

Author: Major Steven B. Skipper, United States Air Force

Thesis: This study presents the thesis that network attacks affecting civil and military entities continue to threaten the United States' DIME construct and its broader national security.

Discussion: Quietly emerging from the Silicon Valley, stretching its tentacles from the west coast to the east coast, the Internet revolutionized the information technology world like nothing else before it. In the beginning the network, known as ARPANET during early development, originally consisted of four key nodes, primarily used by both academic and government entities. As this western concept grew in popularity and functionality, the collection of a few nodes eventually and exponentially increased, and encompassed the preponderance of the globe. The growth and utility of this capability paradigmatically changed how the United States managed and processed information, specifically data relative to diplomatic, informational, military, and economic (DIME) imperatives.

Introduction

The Internet, unwittingly, and its incomparable processing capability provided the US with unprecedented capabilities to apply DIME across the international landscape. Over the last few decades, the US increased its dependency on the Internet and closely tethered information technologies. Consequently, as reliance on this system of networks grew, so did the number of those desiring to attack it and invariably place the DIME approach to US commitments overseas at risk. These threats have the potential to unfavorably affect the US. Regardless of global power status, adversaries use the Internet in attempts to weaken the nation's ability to project its foreign policy framework by concurrently eroding information, military, and economic capacities within US borders. Similar to the ancient Pithos, opened by the Greek goddess Pandora, containing worry, sickness, and death among other attributes, the Internet cannot and should not be placed back into its primordial and protected configuration.¹ The intent of this study is not to recite the Internet's exhaustive evolution, advocate for restriction, or categorically resolve DIME and national security issues; rather, this writing evaluates how unscrupulous hackers, whether state or non-state actors, and insider threats endanger the US' security equilibrium. To this end, and to understand the significance and prevalence of challenges occurring within the cyber domain, this study presents the thesis that state actors, non-state actors, hackers, and insiders leveraging the Internet to conduct nefarious network operations impact the United States' DIME construct and its broader national security. Does addressing threats now emanating via the Internet mean diplomacy matters most, or perhaps economics? Perhaps the threats in this new domain are unique in terms of information as a standalone threat basis? And given the nature of these challenges, how does one employ a military response in a domain that appears to be devoid of traditional military understanding? Yet, should adversaries

succeed in continuing their attacks and by default weakening this useful construct, US efforts abroad will become all the more difficult.

Background and Literature Review

Many books and articles have been written about the relationship between cyber and those who maliciously use the domain to create non-kinetic effects through the network. Accounts of intrusions and doomsday scenarios captured in these writings consist of cyber activities ranging from rudimentary web page vandalism to full-scale cyber war. Despite the monolithic amount of research and analysis occurring over the last two decades in the spheres of academia and think tanks, scholars and experts remain deeply concerned about the ability of the United States to achieve hegemony status in the cyber domain. What is absent from much of the dialogue, however, is not the idea of a world-ending cyber conflict, that fear is present, but the thorough consideration of how cyber threats influence the DIME model and weaken US national security – a holistic view of the intersection of DIME and the cyber domain.

The founders' vision and intent relative to designing the Internet was not necessarily to produce an unwieldy network of networks fraught with pervasive security and protection challenges, but to develop an open, innovative, and effective communication medium to essentially improve communication capabilities. The Internet Society, created by developers of the Internet, most notably Vint Cerf and Robert Kahn, is an organization dedicated to preserving Internet's voluminous history. More importantly, however, the organization's introduction of a web-based forum serves as a professional, yet collaborative, environment for scientists and engineers to share scholarly-based ideas, publish intellectual articles, and ultimately foster a domain unencumbered by overly restrictive policies and oversight.²

Perhaps, similar to the founders' early conceptualization and the Internet Society's continued network expansion, the overarching intent is to continue advancing the legacy of liberated cyber access and not necessarily focus on narrowing the design-security vulnerability chasm that continues to plague systems and software applications. Today, the precipitous growth and interconnectedness of networks, to include an ever-increasing number of computing devices tethered to the Internet, represent a large attack surface for those desiring to adversely affect international stability which requires a holistic alliance to improve security. In this example, the challenge becomes how do we improve security when the creators of the Internet remain rightfully focused on growing this capability but mysteriously are reticent in the realm of improving security?

"Cyberwar Case Study: Georgia 2008," authored by Dave Hollis, provides valuable insight into the Russian-Georgian war where the relationship between a state actor, Russia, and a group of hackers within its borders become inextricably linked in combat by conducting both kinetic and non-kinetic strikes against Georgia. While this action was obviously not conducted against the United States, the notion of states coordinating with hackers creates operational and tactical effectiveness certainly worthy of global acknowledgement. As outlined by Hollis, the essence of this state-versus-state engagement encompassed all DIME attributes where Russian hackers clearly dominated the military and information realms.³ However, he did not properly amplify the diplomatic erosion and economic impact that affected Georgian society. In his view, "The Russian-Georgian War in August of 2008 represented a long history of geostrategic conflict between the two nations and was based on many complex factors: geopolitical, legal, cultural, and economic."⁴ Differences throughout history represent antecedents leading to conflict, but the diplomatic and economic impacts created by patriotic hackers associated with

the Russian-Georgian War working inside the network unveil a narrative requiring further examination.

Jon R. Lindsay, author of “Stuxnet and the Limits of Cyber Warfare,” offers a riveting view into how a computer worm crosses international borders and creates cataclysmic physical damage within Iran’s nuclear complex. Lindsay offers that the Stuxnet malware program exhibited unprecedented scientific engineering, delivered crippling effects within Iran’s networks supporting uranium enrichment, and delayed further nuclear processing capabilities for the foreseeable future. Further, he states that the Stuxnet example does not singularly provide lesser actors who release malware with disproportionate advantages in cyber.⁵ While his analysis regarding the technical complexity and engineering success of Stuxnet is well-articulated, Lindsay fails to elaborate on how subversive cyber activities may create unpredictable secondary and tertiary effects, thereby jeopardizing national security for other sovereign nations. For example, Iran’s erroneous attribution of Stuxnet to a nation other than the US (e.g., Israel, Saudi Arabia, etc.) may have created unpredictable and unintended cascading effects.

Operation Buckshot Yankee serves as the US’ response to what many intelligence officials view as a Russian state-on-state, surprise cyber-attack against US Central Command (CENTCOM), and more broadly, the US. The event occurred when a service member inserted a thumb-drive into a classified laptop. Once successfully attached to the computer, malware spread throughout CENTCOM’s unclassified and classified networks, thereby extracting files and distributing them to foreign systems. The breach and subsequent siphoning off of classified information by Russian entities led to a loss of weapons data, military operational planning, and surveillance information.⁶ Beyond the details provided by Deputy Secretary of Defense William Lynn and other cyber security experts, opposing viewpoints relative to events leading up to and

during Operation Buckshot Yankee are not available. This low-scale malware event not only obtained sensitive military data, it categorically changed how government entities processed and shared data, which required a complete network and end-user equipment overhaul. More importantly, the Russian actors drove the US to establish a new organization, US Cyber Command (CYBERCOM), thereby representing another government organization requiring significant funding and sustainment costs. Hardening US networks and equipment represents much needed reform. However, the most telling development in this narrative consists of two facts; the damage resulting from information theft, whether it is knowing weapon capabilities or operational planning concepts, remains unknown, at least at the unclassified level; the gravity of Russia's actions compelled the US to establish CYBERCOM and stretch its economic and military resources, all of which may or may not increase national security but also reveals how other nations affect America's interests at a time and place of their choosing.

"Is the Cyber Threat Overblown?" authored by Stephen M. Walt, the Robert and Renée Belfer professor of International Relations at Harvard University, rightfully identifies the US' effort recently applied toward safeguarding cyberspace, but states that actions over the last several years merely served as an opportunity to incite fear and panic in the American public and therefore fence funding to bolster government coffers. Walt mentions that US networks are mostly secure from bad actors while cyber threats remain rather nebulous.⁷ He fails to acknowledge or describe significant and covert operations that state and non-state actors conducted within the cyber domain. As such, I would offer that the Russian-Georgian War, Stuxnet, and Buckshot Yankee, to name a few, unequivocally weaken Walt's argument. These events represent classic threats to national security that have specifically affected information sovereignty, military operations, and financial systems.

“Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World,” edited by Derek Reveron and published in 2012, contains a collection of writings authored by scholars, strategy analysts and Chief Information Officers. The publication offers in-depth analysis encompassing an evaluation of cyber activities and vulnerable attack vectors that continue to threaten America’s peace and prosperity. According to Reveron, state actors, non-state actors, hackers, and insiders represent the greatest danger to the US’ military operations, financial systems, and critical infrastructures, among other platforms.⁸ While Reveron’s impressive assemblage of writings comprehensively describes perils of cyberspace and reactions to threats, it does not clearly enumerate quantifiable results and subsequent levels of success brought by the bevy of investments applied toward the cyber domain.

The same can be said when looking to evaluate recent cyber attacks on corporations. Both JP Morgan Chase and Sony Entertainment have been recent victims of cyber attacks, and when looking at these two cases and similar such attacks, the problem of calibrating DIME and national security again comes into focus for two reasons. One, how should the US government respond to a cyber attack against a private entity, if at all? And, just as important, there are few sources available to evaluate these attacks: a few press releases, some coverage in the press. This shortcoming makes a complete understanding of these cyber events impossible at that time. However, they are included in this study because those attacks underscore the difficulty of classifying these attacks, and therefore, indicate the impact on the DIME model.

The Internet represents a force multiplier unlike any other innovation and has paradigmatically changed the way in which the world communicates. The inherent openness of networks and the prevalence of information propagate democratic values across the globe. Also, the collection of networks serves as low-entry attack vectors for adversaries to conduct non-

kinetic attacks. However, all nations and their respective citizens may not be internally prepared to embrace or incorporate what many view as westernized ideals; in turn, uprisings occur which often result in the US providing humanitarian aid, military equipment, or a combination thereof. The Internet offers tremendous benefit but it also presents numerous challenges that require alliances between computer scientist, commercial entities, and government agencies to successfully shape the future of cyber. It also requires a close look at the DIME model, something essentially only tangentially referenced in the literature, when it comes to the fore of the analysis at all.

Defining the Problem

The world of cyberspace is a fascinating domain open to the global community. As the founders devised the concept of the Internet, they could not have envisioned the Internet in its current configuration, a seemingly endless collection of networks and closely associated systems literally webbing the world. Further, they did not predict how it would become such a ubiquitous province for enabling the processing and storing of information affecting all aspects of human existence – both positive and negative.

The genesis of today's Internet and the subsequent and precipitous increase in the number networks that quickly surfaced thereafter to create today's cyber domain were born from what began as a rather rudimentary, closed network devised by scholars and government entities alike. In addition to academic experimentations during 1969 with an interconnected network of a few computers, the Department of Defense (DoD) and its Advanced Research Projects Agency (ARPA) offered innovative insight and contract funding which contributed immensely to the development of the first Internet, ARPANET.⁹

The concept of near real-time communications across considerable distances represented a very powerful capability which fundamentally revolutionized the way the world collected, processed, and stored information. In the view of several engineers who contributed to the Internet's advancement, file sharing and electronic messaging represented the most profound capability during the network's initial conception. Other electronic features such as vocal messaging were considered, but the ability to connect multiple networks irrespective of architecture configuration served as the paramount concept.¹⁰ In light of the distributed nature of commercial entities and government agencies, the ability to exchange electronic messages and share files represented efficiency in communication. The advent of the Internet supported effective and efficient communication amongst various entities. Further, the interconnectedness and intermeshing of numerous networks, both commercial and government, throughout the world-wide web provided an expansive attack surface for unscrupulous state and non-state actors to inflict incalculable harm through the network.¹¹ The scope and size of the world wide web is extraordinary. Over 2 billion users leverage the Internet on a daily basis to conduct day-to-day activities.¹² To this end, considering the magnitude of network endpoints, the ability for military and civil entities to properly manage and secure their respective warfighting systems and commercial networks remains rather daunting. While the Internet represents an extremely popular western concept, arising threats are universal and thereby originate from various points across the globe.

National Security Strategy

To achieve its objectives associated with global democracy and peace, and as indelibly outlined in the National Security Strategy (NSS), the United States has a self-imposed obligation to effectively communicate with nations and their respective governments throughout the world.

An inextricable relationship amongst the Internet and national security began during the Clinton administration. The US government, numerous private corporations, and millions of people traverse the same wireless and fiber pathways every second of every day. Therefore, the world of cyber, an extremely powerful and ubiquitous network of networks, is owned by a multitude of entities which share the risks and rewards of operating in this domain.¹³

In today's highly technological society, the US harnesses the cyberspace domain to prosecute its daily agenda consisting of vital national security interests. In fact, the notion of securing this dynamic sphere serves as one of the United States' concerns discussed in the document. As briefly highlighted in the NSS, similar to antecedents supporting other sensitive military enterprises, the writing emphasizes the importance and critical nature of protecting the Global Information Grid (GIG). Specifically, the networks of interconnected networks remain precariously fragile and susceptible to infiltration as the US, both military and civil counterparts, depends on its dominant processing capabilities.¹⁴ To understand the gravity and importance associated with America's national security, an evaluation of its components require examination.

DIME

The basic idea of national security alludes to the preservation of freedom and prosperity for America. It underscores and validates principles associated with the government's foreign policy objectives. According to Joint Publication 1-02, Department of Defense Dictionary of Military and Associated Terms, "national security represents a collective term encompassing both national defense and foreign relations of the United States with the purpose of gaining: A military or defense advantage over any foreign nation or group of nations; a favorable foreign

relations position; or a defense posture capable of successfully resisting hostile or destructive action from within or without, overt or covert.”¹⁵

How does this narrative of unscrupulous network users operating within the cyber domain, a complex configuration of interconnected, globalized networks, affect America’s national security imperatives relative to the DIME model? For context, a review of DIME is helpful to understand foreign policy and national security imperatives. The 1960s Cold War period marked the development and categorization of the US’ instruments of power (i.e., diplomatic, informational, military, and economic), which are commonly referred to as DIME. The concept served as a framework that directly correlated to various federal government departments. Since the inception of DIME, the Department of State, Department of Defense, US Agency for International Development, and other agencies have aligned their expertise and capabilities to most effectively support foreign engagement decisions.¹⁶

The diplomatic instrument represents global interactions among various nations’ diplomats to secure peace and preserve democratic interests that benefit the global populace. Examples of the informational instrument exist in the context of information exchange or bilateral collection between the US and other countries, which serves as an opportunity for America to build relationships and foster alliances through communication. A costly option, both in financial and human terms, refers to a military response. This instrument is generally considered a hard power decision and most notably has kinetic response connotations aimed toward impairing or breaking the enemy’s will to fight. Lastly, the economic instrument consists of applying or lifting sanctions, creating trade embargoes, imposing export and import restrictions, and providing or withdrawing foreign monetary assistance. The DIME model

remains as a relevant concept leveraged by the US to achieve foreign policy objectives, secure its vital interests, protect its national security, and ultimately maintain global stability.

The Internet both supports and threatens DIME and its closely tethered relationship to national security. It most notably represents a valuable way for nations to quickly exchange information. Therefore, it is plausible to argue that global connectivity fosters US democratic interests and promotes DIME. The precipitous increase in technology (i.e., mobile devices, internet modernization, etc.), rapid availability of information, and increasing globalization create an international landscape that supports DIME and has all of the hallmarks to categorically improve diplomatic relations across the globe.¹⁷ While the openness, accessibility, and expediency of communication exchanges occurring through the Internet provide substantial benefit, these factors also bring unexpected threats. Recent releases of government classified information by Julian Assange and his WikiLeaks empire pose significant risks to those entities sharing sensitive information through cyberspace. To leverage the power of networks and nurture future electronic diplomacy exchanges, additional advancements in technology, to include international policy agreements, will need to occur.¹⁸ In the absence of secure and reliable networks, the nation and its ability to effectively and securely adjudicate matters of strategic importance will be at risk. People, primarily hackers and insiders, serve as the predominant cyber domain threat; moreover, the increasing rise in state and non-state actors represents a significant risk to data security and network exploitation.¹⁹ The DIME construct remains as a valuable way to pursue US interests globally and cyber realities are helping to reinforce that importance.

The Hacker Effect

For many years, the practice of hacking information systems has existed in various forms, ultimately becoming more sophisticated through time. As defined by Merriam-Webster, hackers “[S]ecretly gain access to a computer system in order to get information, cause damage, etc.”²⁰ Hacking networked systems does not always equate to subversive acts by unscrupulous users releasing malicious viruses. A community of coders performing legitimate actions to benefit a greater good exists as well. White-hat hackers generally are known for their ability and willingness to identify software weaknesses and to inform the respective entity, usually a corporation, of the findings. These individuals are also known as ethical hackers. Conversely, black-hat hackers aggressively exploit system vulnerabilities to achieve personal satisfaction, which includes and is not limited to cyber vandalism, system access denial, and information theft. Another emerging hacker group is known as hacktivists. Those functioning in this capacity meld nefarious hacking activities resident within the black-hat sphere with efforts to advance a particular agenda, whether activities are motivated by politics, human rights, or religion, among others. It is important to note that the notion of illicitly affecting communications transpired prior to the advent of the first networked system. The first documented system-hacking event began with Nevil Maskelyne’s wireless Morse code interception and message override which occurred in the early 19th century.²¹ This early act of covertly affecting a communications system, although rather benign at the time, ignited the notion of hacking activities. In the decades to follow, as technologies advanced so did the tactics, technics, and procedures (TTPs) associated with system attacks. However, these seemingly endless methodologies to steal data and impair systems would not emerge on a large scale until the creation of the Internet and its associated networks.

Military Insider Threats

Converse to network attacks occurring from external sources, threats to the US national security interests emerge from within organizations as well. Over the last several years, high-profile insider data theft incidents have had profound impact on the American ability to control information and maintain favorable diplomacy with other nations. The case of US Army Private Bradley Manning exhibited how his act of “cyber rebellion” led to the release of the “Afghanistan War Logs,” which consisted of several thousand classified diplomatic cables, official memoranda, and videos of battlefield footage to WikiLeaks, an aggressive freelance distributor of secret information.²²

This particular dissemination of highly sensitive information by Private Bradley Manning has the propensity to unfavorably and indelibly impair years of partnership and alliance development with foreign nations, not to mention the operational security, personal safety, and well-being of those within government agencies and military organizations. The extraordinary electronic transfer of classified information from Manning to WikiLeaks led to a massive reconfiguration of personnel throughout foreign government agencies, specifically the reassignment and firing of personnel, to include removal of US diplomats from several countries.²³

Manning’s leak of information not only affected internal government operations, it spilled over into the international community. Perhaps WikiLeaks is best known for the way it altered the Middle Eastern political landscape, beginning specifically with Tunisia. Many international relations scholars and American government officials are rather confident that diplomatic cables released to WikiLeaks served as the impetus for Arab Spring uprisings occurring across the globe – specifically in Muslim communities. Moreover, and equally disconcerting, was the cascading

impact of relations that occurred between other countries, as the cables contained information relative to covert operations not known by allies.²⁴

Military and corporate entities apply significant portions of their respective budgets to secure networks from outside attacks. Although a complete solution to eliminate insider threats does not and most likely will not exist, implementing measures to reduce data theft incidents and preserve sensitive information requires a proactive approach.

Corporate Insider Threats

From a civil perspective, insider threats are equally damaging not only to the respective corporation but to America's interests as well. For example, Edward Snowden, a Booz Allen Hamilton employee, working as a contractor while supporting the National Security Agency, electronically transferred massive amounts of the DoD's surveillance data to WikiLeaks for public distribution. Snowden's divulgence of classified surveillance programs affected the nation's security and diplomacy, while DoD entities scrutinized Booz Allen Hamilton's corporate credibility and employee screening process. James Clapper, director of the Office of National Intelligence, recently appointed William Evanina to the National Counterintelligence Executive position. In this capacity, Evanina has the responsibility of monitoring attempts of foreign nations to steal data, assessing the nation's security posture following information leaks, specifically those of Snowden and, perhaps most importantly, overhauling measures required to adjudicate and analyze security clearances.²⁵ In spite of DoD's efforts to galvanize its information security, the question arises as to the methods corporations employ to ensure prospective employees meet clearance standards commensurate with information processed in DoD agencies. While it is important to understand actions taken by DoD to mitigate insider threats relative to contractor personnel, employee clearance screening processes conducted by

civil counterparts remain questionable. The US Investigations Services (USIS), a primary government contracted corporation used by Booz Allen Hamilton, won two, five-year contracts to conduct background investigations and provide support services. In the wake of the Snowden case, lawmakers reviewed the contracts awarded to USIS and determined that a conflict of interest existed as the company provided both background checks and essentially audited its own work product.²⁶ In this particular case, the affiliation between Booz Allen Hamilton and the National Security Agency became a strained relationship and presents a unique and complex conundrum, as the arrangement involves hiring decisions by a civil entity, Booz Allen Hamilton, that affected a major National Security Agency program. Irrespective of opinions relative to government-sponsored surveillance programs, this example of intertwined civil-military agencies reveals how the lack of information control and erroneously vetted corporate employees create grave threats to the US' information, diplomacy and national security. Also, it reveals how threats to DIME may very well emerge from external corporate contractors embedded within government-military agencies. In this particular example, breach of data led to release of top secret domestic surveillance programs information along with data relative to the Informational (surveillance data) aspect of DIME which led to and has the propensity to create diplomatic upheaval. How does the US curtail or prevent future data breaches? Or, did the Snowden case uncover an unethical practice by the US government? Perhaps the government's reaction and wide-sweeping surveillance changes will improve diplomacy and domestic policy.

Rise of the Non-State Actors

The most pervasive external threats to the cyber domain are non-state actors (NSA) who operate covertly to access networks and databases throughout the world. To provide adequate context for this particular segment of the analysis, it is appropriate to define the NSA concept.

According to the Oxford English Dictionary, non-state actors are “individuals or organizations that have significant political influence but are not allied to any particular country or state.”²⁷ The Russian-Georgian War serves as an example of NSAs supporting the advancement of a nation-state’s agenda. Cyber-savvy non-state actors carry out hacking operations that negatively affect economic, civil, and military operations. Malicious activity conducted by NSA groups, to include terrorist organizations, organized crime coteries, and lone wolf proxies, in cyberspace have the propensity to affect numerous principles of vital concern identified in the US’ National Security Strategy (i.e., economic prosperity, global peace, and national security, etc).²⁸ The Russian-Georgian conflict exhibited how a nation-state leveraged a segment of its civilian populace to orchestrate non-kinetic operations against another country. Prior to Russia conducting kinetic operations, a robust group of pro-Russian hacktivists launched their own form of cyber sorties and attacked Georgian networks which significantly impaired the nation’s ability to communicate and effectively respond to Russian aggression.²⁹ This narrative highlights how NSAs have the propensity to deliver impacts beyond their borders and in support of a nation-state’s end state. The ubiquitous nature of the Internet provides non-state actors with a conduit to covertly hack networks, collect information, and exploit civil and military organizations.

Influence of State Actors

Similar to the NSA contingent, state actors (SA) represent a significant and formidable threat to the network security environment. Not to the astonishment of many, the most influential and capable nations with the ability to launch cyber-oriented attacks are Russia, Iran, and China, while the US remains the most powerful, yet most targeted country.³⁰ Comparative to armed conflict across barren battlefields, and somewhat converse to the untethered NSA-type TTP construct, the bespoken nations, over the course of a couple of decades, have primarily

directed cyber aggression toward the US' government-level entities. Recently, however, state actors from foreign nations have begun to focus attacks on segments of the US' industrial base. China serves as the most prevalent violator of information and trade secret theft, which affects the financial security of corporate entities and thereby impacts the US' economic sovereignty.³¹ Although subdued in its cyber posture following the Stuxnet fallout, Iran has exhibited signs of a recent resurgence in this domain. Iran's precipitous increase in cyber capabilities over the last few years has ignited international alarm. Also, these improvements changed the way in which the US, Israel, and other western nations devised strategies to counter Iran's newly developed abilities.³² Russia serves as another vaunted member of the powerful, global cyber community. The nation's government, a late adopter of advanced technology, does not directly leverage its resources to adversely affect other nations' network processing functions. Moreover, Russian authorities use capabilities resident within the country's vast hacking community to attack information systems.³³ Russia's hybrid approach to information warfare, a globally recognized nation commissioning NSAs, specifically hackers, to conduct illicit network operations, uncloaks the difficulty associated with attributing responsibility toward the post-cold war country. The absence of a quantitatively known aggressor creates suspicion and has the propensity to further strain tenuous foreign diplomacy relations.

Operation Buckshot Yankee

One of the early and most notable network attacks affecting the US DoD network, believed by many experts to have originated from within Russia, affected the United States Central Command cyber operations. In 2008, the DoD launched Operation Buckshot Yankee in response to a malicious software (malware) known as Agent.btz which affected both unclassified and classified government network systems. The network crippling malware did not originate

from within the network but was introduced externally through the insertion of a USB drive into a classified military laptop located in the Middle East.³⁴ This attack on the DoD network created deep concerns for the US government. The network breach enabled transfer of sensitive and classified files to unknown locations, which may have included unscrupulous state and non-state actors.³⁵

Shocked and stunned by the unexpected thumb drive network attack vector, the DoD partnered with industry experts to not only eliminate the Malware present on numerous systems, it also realized the need for a long-term and enduring process to proactively mitigate future data exfiltration attempts. The DoD desperately reached out to McAfee, a prominent network security firm, to assist with hardening the GIG. In the interim, DoD responded by directing all government components to discontinue use of removable media (i.e., USB, portable hard drives, etc). The enduring counter measure implemented deactivated media ports down to the individual desktop level, and eventually led government officials to disable CD/DVD drives as well.³⁶ The protection efforts by McAfee not only restricted access to data transfer programs, it also enabled respective customers (e.g., DoD) to have an improved ability to account for devices connected to the network which represented a challenge during the initial phases of Operation Buckshot Yankee. Following the restriction of portable media, many in DoD viewed these cyber security initiatives as draconian and reactionary. Nonetheless, the inability to access media ports and use disc drives altered the way in which DoD components and associated entities operated on a day-to-day basis. Although implementing this initiative reduced the amount of data breaches, the Manning and Snowden examples reveal that a no-fail solution exists.

While some analysts contend that Russia orchestrated the network infiltration operation, government authorities have not publicly revealed the attack source. Following the events

leading up to Operation Buckshot Yankee, the US federal government charged the Secretary of Defense with establishing what would eventually become US Cyber Command. In response to Operation Buckshot Yankee, the US Secretary of Defense, Robert Gates, endorsed a memorandum on 23 June, 2009, directing the establishment of USCYBERCOM. As directed by Secretary Gates, the new command focuses on developing proficiency in offensively operating in and protecting the cyber domain, which includes building and strengthening foreign alliances.³⁷ The necessary establishment of USCYBERCOM fundamentally has altered the manner in which military components operated on and within the GIG. Unlike network operations prior to Operation Buckshot Yankee where technicians served as the “keeper of the keys,” the world of cyber now captured attention at the four-star level and thereby ushered in a new operational domain requiring high-level oversight and stricter government control.³⁸ While the network intrusion changed the Pentagon’s perspective relative to confronting adversaries in a uncharted arena, senior administration officials also noted the grave impact that cyber may have on other national interests outlined in the NSS. In his cyber strategy, William Lynn, Deputy Secretary of Defense, specifically states that no aspect of the nation’s security is immune to network attacks. He further notes that the US financial province, among other interests, remains at risk.³⁹

Stuxnet

In July, 2010, the Stuxnet malware attack against Iran’s nuclear complex exemplified a paradigmatic shift in how a state entity, using intricate software coding, attacked a specified target and created physical destruction. Most analysts’ findings indicate that the US created and released Stuxnet for the intended purpose of degrading Iran’s nuclear program; however, similar to the worm’s complex design and unique capabilities, full attribution to a specific nation-state

remains opaque. The idea that the Stuxnet virus succeeded in accomplishing its covert objectives captivated researchers. The degree of interest associated with this unforeseen malware event compelled Symantec, a world-renowned corporation that produces advanced anti-virus software, to conduct in-depth analysis of the virus and publically publish the results – a rare response indeed. As noted in the report, those who engineered Stuxnet intended to precisely attack and destroy equipment managing production of Iran’s uranium. Notably, the network and computers connected to the centrifuge control systems were not adversely affected by the virus.⁴⁰ The multi-role nature of Stuxnet represented an equally fascinating storyline. The virus had the ability to copy itself, identify networked and stand-alone systems, perform configuration changes, and maintain a furtive presence within Iran’s extensive nuclear computing complex for an extended period without detection. All of these characteristics reveal the way in which advancements in malware have the propensity to affect national security for industrialized nations.⁴¹ Opposite to researchers’ eagerness to explore and release details of the virus, Iran maintained a reticent position relative to Stuxnet’s impact to its nuclear enrichment program. Although the nature of this act was unprecedented, a cyber attack against a recognized government or corporate entity typically elicits a strong response describing the scope, scale, and source. Iran chose to remain silent regarding the Stuxnet event for several reasons ranging from efforts to maintain nation-state pride to the country’s inability to identify source of malware.⁴² Once blueprints for malicious software (e.g., Stuxnet) become available to those beyond the secretive sphere of original code designers, the probability for attacks against other nations’ sensitive infrastructure increases significantly.

JP Morgan Chase

In August, 2014, JP Morgan Chase, a globally known financial institution, became a victim of a massive data heist. According to reports, approximately 76 million accounts were pilfered by a cyber espionage attack on the banking and brokerage firm in one of the largest data theft events affecting a financial institution. While mass withdrawals against banking and investment accounts have not occurred, the monolithic loss of data has the propensity to affect the economic condition of consumers, businesses, and the broader US government.⁴³ As reflected throughout history, a loss of trust and confidence in the financial sector, especially banking institutions, potentially creates turbulence on Wall Street which transcends to the Federal Reserve and thereby impacts corporate and government operations. As noted by the Federal Reserve, an abundance of stressors (e.g., loss of confidence in financial institutions) resident in the banking sector creates economic calamities which significantly impair the distribution of credit to consumers and corporations. In turn, a bleak financial outlook and subsequent spending lethargy equate to a precipitous increase in jobless rates which generate amplifying effects across the economic spectrum.⁴⁴ What is most disconcerting about this particular data breach, beyond initial warnings to change passwords, is the fact that JP Morgan Chase did not follow-up with its customers to provide further fidelity and reassurances regarding loss of data.

Sony

In December, 2014, North Korea's cyber attack against Sony led to the cancellation of the world-wide release of "The Interview," a comedy movie depicting the assassination of North Korea's leader, Kim Jong Un. Historically, Hollywood satire has not led to political manipulation, economic impact against corporations, and resultant suppression of US citizens' rights. North Korea's overwhelming influence in and through the Internet compelled one of the

world's largest and highly successful media production corporations to acquiesce and summarily abandon distribution to the broader theater enterprise. Following the attack, President Obama described the event as “cyber vandalism” that led to heavy financial losses but would not categorize the act of aggression as an incident reaching declaration of war. He further indicated that Sony erred in its decision to cancel the film and should have consulted with him before anyone else.⁴⁵ President Obama's comments reveal a peculiar narrative for two reasons. First, the Federal Bureau of Investigation (FBI) conducted a thorough investigation and attributed the attack to North Korea. Notwithstanding unproven theories and cogent speculations from other investigative agencies, the FBI, in this particular case, served as the foremost authority and advised Sony officials accordingly. Secondly, if a corporation follows the nationally-prescribed reporting process, what more can the president of the US do that exceeds the capabilities of those trained and equipped to conduct federally-sanctioned investigations? Considering President Obama's reaction, coupled with North Korea's outward threats, aggression, acts, and ultimate victory against Sony, a new frontier in cyber has been unveiled that remains unaccounted for in today's DIME – global headlines read, “North Korea Uses Cyber to Defeat Sony! Who is Next?”

Conclusion

The intermeshing and hostile actions by state actors, non-state actors, hackers, and insiders existent within the cyber domain create significant and prevalent challenges for the United States' DIME construct and its broader national security – the ever-growing intersection of DIME principles and cyber complexities. The essence of the US' national security safeguards freedom and prosperity for America, DIME highlights and validates doctrinal concepts associated with the government's foreign policy objectives, particularly as they relate to whole of

government matters. To achieve ideals associated with global democracy and peace, and as ineradicably bounded in the NSS, the United States has a chosen commitment to maintain effective dialogue with nations and their respective governments across the globe. Should threatening entities continue to create desired effects through cyber to weaken this useful construct, US efforts abroad will become all the more difficult to successfully execute and shape.

Opposite to the predictability associated with kinetic attacks from known aggressors, the non-kinetic and pervasive nature of cyber has provided capabilities to those entities across the entire threat spectrum, even though those adversaries remain conventionally unequal to US power. When working independent from larger, organized groups, efforts by black-hat hackers and hacktivists pose, for the most part, a negligible threat to the US and its broader interests. As members of these influential spheres begin to rally at the behest of a prominent authority or government (e.g., Russian-Georgian War), they harness the strength of many who share a common purpose and serve in a non-state actor capacity – using their talents and abilities to create desired non-kinetic effects on behalf of a nation-state. Russia and China, and to some degree Iran, represent the most formidable state actor threat. While these nations have historically leveraged NSAs to conduct operations against the US through the Internet, they possess their own capabilities to create desired outcomes. Regardless of the actor, attribution makes identifying the source of attack exceedingly difficult.

Similar to issues associated with assigning responsibility to a specific actor, identifying insider threats, whether military members or government contractors, before information is copied and distributed presents challenges as well. Based on their access to sensitive government information, insiders have the ability to negatively affect all aspects of DIME. As identified and extrapolated in the Manning and Snowden examples, identifying an insider threat

prior to his or her actions is nearly impossible. Once insiders acquire data and release it to another source, the national security implications are widespread which create dire secondary and tertiary effects across the DIME construct. A perfect solution to this problem does not exist; however, maintaining a need-to-know security posture, limiting access to sensitive information, and implementing controls to reduce data copying will aid in proactively securing sensitive information.

Evaluating various actors TTPs in the cyber domain and identifying their impact to whole of government operations remain an ongoing endeavor. As highlighted in the case studies, Operation Buckshot Yankee, Stuxnet, JP Morgan Chase, and Sony, threats to the US' ability to address diplomacy matters, leverage information operations, employ military capabilities, and thrive economically at home and abroad remains at risk. Operation Buckshot Yankee revealed vulnerabilities prevalent in the military's information technology infrastructure, which exposed both hardware and software weaknesses. Today's technologies continue to advance and improve their security features but the adversary's TTPs rapidly evolve in concert with innovative developments – bad actors maintain an advantage in this area. Stuxnet unveiled an unprecedented capability associated with malware where physical destruction of Iran's nuclear enrichment equipment occurred and severely limited production capabilities. The obvious concern here is that once a nation-state displays a new capability, other nations have the tendency to replicate it. The ability of Stuxnet to deliver kinetic-based effects through a multitude of networks without employing military forces or equipment should evoke concern for all sovereign nations. If the US has the ability to launch such cyber weapons, what prevents other technologically astute countries from attacking each other? Similar to the military's nuclear deterrence program, does the notion of mutually assured destruction through the Internet

encourage an equal level of restraint? These questions are difficult to answer but they reveal the realities and challenges that the Internet has created for the world to acknowledge. JP Morgan Chase's unprecedented data breach uncloaked persistent cyber attacks occurring against corporations. The amount of information and sources available to further analyze this particular attack are rather thin which thereby leaves questions regarding the true impact consumers and businesses incur. When corporations experience data theft should more information be available to the public? Do we let private business resolve these problems alone or does the government need to intervene to ensure the economy does not severely shift based on loss of public confidence? Considering the frequency and ubiquity of corporate information theft, perhaps corporations and society as a whole have become immune to such narratives and categorize the practice as a cost of conducting business. Besides, once data departs the trusted boundaries of financial institutions, there are no measures available to retrieve stolen information and erase associated files from the perpetrators' systems – comprised data does not necessarily expire. Similarly, when a nation-state directly and overtly attacks a corporate entity and creates significant financial harm, how should the US respond? Following North Korea's attack on Sony, a considerable amount of confusion ensued, stretching from the Oval Office to the thinly-walled cubicles at Sony. Corporations are not equipped to adequately defend themselves against such formidable aggressors and quickly acquiesce to limit as much damage as possible – the essence of a Clausewitzian-type scenario unfolding in present-day politics.

DIME is still a valid concept but suspicion is that because of cyber, information warfare will dominate. Is there too much "M" in DIME? How should the military respond when elicited actors attack US networks on a daily basis? Does the US quietly respond against the aggressor? Given the reliance on "I" in DIME that would appear to fit how one addresses threats on the

Internet, should the US place a higher level of importance on this particular instrument of power? The precipitous growth in how information influences and shapes perception certainly points toward increased significance, especially as it undergirds the US' ability to pursue diplomacy. Cyber challenges of today are informational realities; perhaps we are now in a perilous position where information is emphasized too heavily. Last, perhaps cyber has elevated the Internet to the preeminent economic engine, and therefore elevated the "E" in DIME as most important. For the linchpin of US policy to date to remain a cornerstone of national security evaluation, considerable thought is needed to get the DIME construct in alignment and therefore have it remain a viable model.

Cyber and DIME do not intersect in today's scholarly analysis; as such, responding to these threats does not have a clear cut solution. Similar to Pandora's Box, cyber has unhinged DIME and has unleashed—and will continue to do so—many unforeseen realities of national-level consequence. In today's ubiquitous information age, we need to rethink how DIME is employed. As a recommendation, the Department of Homeland Security as the lead agency and a consortium of corporations should form an alliance to combat cyber threats – a unified whole-of-government approach that supports the NSS. This partnership leverages unique expertise resident in industry and aligns with the government's executive-level ability to respond proportionally to acts of cyber aggression that threaten the US' vital national interests. Lastly, to form an effective and enduring process beyond America's borders, the US' needs to intensify its foreign policy initiatives relative to developing and strengthening cyber-oriented treaties which will bolster the nation's international approach to addressing a pervasively global issue. Should these two steps be taken, the military's role in cyber will be relegated to where it has traditionally been most utilized by US decision makers, and that is a last resort when seeking to best

implement US policy. Given the cyber lens, DIME can finally yield a fruitful approach to achieving security aims with a balanced calibration of its essential elements of state power.

Endnotes

¹ Jenifer Neils, "The Girl in the *Pithos*: Hesiod's *Elpis*," in *Periklean Athens and its Legacy. Problems and Perspective*, eds. J. M. Barringer and J. M. Hurwit (Austin: University of Texas Press), 2005, 37–38.

² Barry M. Leiner, Vinton G. Cerf, David D. Clark, Robert E. Kahn, Leonard Kleinrock, Daniel C. Lynch, Jon Postel, Larry G. Roberts, Stephen Wolff <http://www.internetsociety.org/internet/what-internet/history-internet/brief-history-internet#References>.

³ Hollis, David M. "Cyber War Case Study, Georgia 2008." *Small Wars Journal*. January 6, 2011, 10.

⁴ Hollis, David M. "Cyber War Case Study, Georgia 2008." *Small Wars Journal*. January 6, 2011, 10.

⁵ Lindsay, Jon R. "Stuxnet and the Limits of Cyber Warfare," *Security Studies*, Vol. 22, No. 3 2013, 365-404.

⁶ William J. Lynn, "Defending a New Domain: The Pentagon's Cyber Strategy," *Foreign Affairs*, September/October 2010.

⁷ Stephen M. Walt, "Is the Cyber Threat Overblown?" *Foreign Policy*, March 30, 2010, <http://foreignpolicy.com/2010/03/30/is-the-cyber-threat-overblown>.

⁸ Derek S. Reveron, *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World*. (Washington DC: Georgetown University Press), 2013, 3.

⁹ Vinton G. Cerf, "The Day the Internet Age Began," *Nature*, October 29, 2009, 1202.

¹⁰ Vinton G. Cerf, "The Day the Internet Age Began," *Nature*, October 29, 2009, 1202.

¹¹ Roland Heickero, *Dark Sides of the Internet: On Cyber Threats and Information Warfare*. (Frankfurt: Peter Lang), 2012, 11-12.

¹² Paul Rosenzweig, *Cyber Warfare: How Conflicts in Cyberspace Are Challenging America and Changing the World*. (Santa Barbara: Praeger), 2013, 24.

¹³ Derek S. Reveron, *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World*. (Washington DC: Georgetown University Press), 2013, 6-7.

¹⁴ The White House, National Security Strategy, 2010, 17-

18. http://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf

¹⁵ Joint Publication 1-02, *Department of Defense Dictionary of Military and Associated Terms*, 2010, 170.

¹⁶ D. Robert Worley, *Orchestrating the Instruments of Power: A Critical Examination of the U.S. National Security System*. (Washington DC: Johns Hopkins University), 2012, 6.

¹⁷ Daryl Copeland, *The Oxford Handbook of Modern Diplomacy*, eds. Andrew F. Cooper, Jorge Heine, and Ramesh Thakur (United Kingdom: Oxford University Press, 2013), 464-465.

¹⁸ Daryl Copeland, *The Oxford Handbook of Modern Diplomacy*, eds. Andrew F. Cooper, Jorge Heine, and Ramesh Thakur (United Kingdom: Oxford University Press, 2013), 464-465.

¹⁹ Derek S. Reveron, *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World*. (Washington DC: Georgetown University Press), 2013, 3.

- ²⁰ Webster-Merriam Dictionary, s.v. “hacker,” accessed Jan 10, 2015, <http://www.merriam-webster.com>.
- ²¹ Paul Mark, “Dot-dash-diss: The gentleman hacker's 1903 lulz,” December 27, 2011, <http://www.newscientist.com/article/mg21228440.700-dotdashdiss-the-gentleman-hackers-1903-lulz.html?full=true#.VLGA7k5CM8>.
- ²² Yangara Sangarasivam, “Cyber Rebellion: Bradley Manning, WikiLeaks, and the Struggle to Break the Power of Secrecy in the Global War on Terror,” *Perspectives on Global Development & Technology*, 2013.
- ²³ David Leigh and Luke Harding, *WikiLeaks: The Inside Story of Julian Assange and Wikileaks*, (New York: Public Affairs), 2011, 224-226.
- ²⁴ Judy Bachrach, “WikiHistory: Did the Leaks Inspire the Arab Spring?” *World Affairs Journal*, July/August 2011.
- ²⁵ Charles S. Clark, “Meet the Man Who’s Gauging the Damage From Snowden,” *Government Executive*, August 15, 2014. <http://www.govexec.com/management/2014/08/meet-man-whos-gauging-damage-snowden/91595>.
- ²⁶ Dion Nissenbaum, “Government Seeks to Replace Firm That Vetted Snowden, Navy Shooter,” *Wall Street Journal*, September 20, 2013. <http://www.wsj.com/articles/SB10001424127887324807704579087601389468282>
- ²⁷ Oxford English Dictionary, s.v. “non-state actors,” accessed Jan 10, 2015, <http://www.oed.com>.
- ²⁸ James Jay Carafano, “Fighting on the cyber battlefield: Weak states and non-state actors pose threats,” *The Heritage Foundation*, November 8, 2013. <http://www.heritage.org/research/commentary/2013/11/fighting-on-the-cyber-battlefield-weak-states-and-nonstate-actors-pose-threats>.
- ²⁹ Hollis, David M. “Cyber War Case Study, Georgia 2008.” *Small Wars Journal*. January 6, 2011, 8.
- ³⁰ Derek S. Reveron, *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World*. (Washington DC: Georgetown University Press), 2013, 144-145.
- ³¹ Paul Rosenzweig, *Cyber Warfare: How Conflicts in Cyberspace Are Challenging America and Changing the World*. (Santa Barbara: Praeger), 2013, 95.
- ³² Gabi Siboni and Sami Kronenfeld, “Developments in Iranian Cyber Warfare, 2013-2014,” *The Institute for National Security Studies*, <http://www.inss.org.il/index.aspx?id=4538&articleid=6809>, April 4, 2014.
- ³³ Nikolas K. Gvosdev, *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World*, ed. Derek Reveron (Washington DC: Georgetown University Press, 2013), 180-181.
- ³⁴ Ellen Nakashima, “Cyber-intruder sparks response, debate,” *Washington Post.com*, December 6, 2011, http://www.washingtonpost.com/national/national-security/cyber-intruder-sparks-response-debate/2011/12/06/gIQAxLuFgO_story.html
- ³⁵ William J. Lynn, “Defending a New Domain: The Pentagon’s Cyber Strategy,” *Foreign Affairs*, September/October 2010.
- ³⁶ Ben Iannotta, “Plugging the WikiLeaks,” *C4ISR*, January 1, 2011, 30.
- ³⁷ Tom Burghardt, “The Launching of U.S. Cyber Command: Offensive Operations in Cyberspace,” *Global Research*, July 1, 2009. <http://www.globalresearch.ca/the-launching-of-u-s-cyber-command-cybercom/14186>.

³⁸ Noah Shachtman, "Insiders Doubt 2008 Pentagon Hack Was Foreign Spy Attack," *The Brookings Institute*, August 25, 2010. <http://www.brookings.edu/research/opinions/2010/08/25-pentagon-worm-shachtman>.

³⁹ William J. Lynn, "Defending a New Domain: The Pentagon's Cyber Strategy," *Foreign Affairs*, September/October 2010.

⁴⁰ Gary D. Brown, "Why Iran Didn't Admit Stuxnet Was an Attack," *Joint Force Quarterly*, 4th Quarter 2011.

⁴¹ Paulo Shakarian, "Stuxnet: Cyberwar Revolution in Military Affairs," *Small Wars Journal*, April 2011, 8-9.

⁴² Gary D. Brown, "Why Iran Didn't Admit Stuxnet Was an Attack," *Joint Force Quarterly*, 4th Quarter 2011.

⁴³ Emily Glaser and Danny Yadron, "J.P. Morgan Says About 76 Million Households Affected by Cyber Breach," <http://www.wsj.com/articles/j-p-morgan-says-about-76-million-households-affected-by-cyber-breach-1412283372>.

⁴⁴ Federal Reserve. "Frequently Asked Questions," <http://www.federalreserve.gov/faqs/why-did-the-Federal-Reserve-lend-to-banks-and-other-financial-institutions-during-the-financial-crisis.htm>.

⁴⁵ Jethro Mullen, "North Korea and the Sony Hack: The War of Words Escalates," <http://www.cnn.com/2014/12/22/world/asia/north-korea-us-sony-hack-who-says-what/index.html>.

Bibliography

- Bachrach, Judy. "WikiHistory: Did the Leaks Inspire the Arab Spring?" *World Affairs Journal*, (July-August 2011): <http://www.worldaffairsjournal.org/article/wikihistory-did-leaks-inspire-arab-spring>.
- Barringer, Judith and Jeffrey Hurwit, eds. *Periklean Athens and its Legacy: Problems and Perspectives*. Austin: University of Texas Press, 2007.
- Brown, Gary D. "Why Iran Didn't Admit Stuxnet Was an Attack." *Joint Force Quarterly*, Issue 63, 4th Quarter, 2011.
- Burghardt, Tom. "The Launching of U.S. Cyber Command: Offensive Operations in Cyberspace." *Global Research*, (July 1, 2009): <http://www.globalresearch.ca/the-launching-of-u-s-cyber-command-cybercom/14186>.
- Carafano, James Jay. "Fighting on the Cyber Battlefield: Weak States and Non-State Actors Pose Threats." *The Heritage Foundation*, (November 8, 2013): <http://www.heritage.org/research/commentary/2013/11/fighting-on-the-cyber-battlefield-weak-states-and-nonstate-actors-pose-threats>.
- Cerf, Vinton G. "The Day the Internet Age Began." *Nature*. October 29, 2009. <http://www.nature.com/nature/journal/v461/n7268/full/4611202a.html>.
- Clark, Charles S. "Meet the Man Who's Gauging the Damage From Snowden." *Government Executive*, (August 15, 2014): <http://www.govexec.com/management/2014/08/meet-man-whos-gauging-damage-snowden/91595>.
- Cooper, Andrew Fenton, Jorge Heine, and Ramesh Chandra Thakur. *The Oxford Handbook of Modern Diplomacy*. Oxford, U.K.: Oxford University Press, 2013.
- Copeland, Daryl. *The Oxford Handbook of Modern Diplomacy*, eds. Andrew F. Cooper, Jorge Heine, and Ramesh Thakur, (United Kingdom: Oxford University Press, 2013).
- Federal Reserve. "Frequently Asked Questions." <http://www.federalreserve.gov/faqs/why-did-the-Federal-Reserve-lend-to-banks-and-other-financial-institutions-during-the-financial-crisis.htm>.
- Glaser, Emily and Danny Yadron. "J.P. Morgan Says About 76 Million Households Affected by Cyber Breach." *Wall Street Journal*, (October 2, 2014): <http://www.wsj.com/articles/j-p-morgan-says-about-76-million-households-affected-by-cyber-breach-1412283372>.
- Heickerö, Roland. *The Dark Sides of the Internet: On Cyber Threats and Information Warfare*. Frankfurt am Main: Germany, 2013.

Hollis, David M. "Cyber War Case Study, Georgia 2008." *Small Wars Journal*. January 6, 2011.

Iannotta, Ben. "Plugging the WikiLeaks." January 4, 2011.
<http://archive.defensenews.com/article/20110104/C4ISR02/101040306/Plugging-WikiLeaks>.

Joint Publication 1-02, *Department of Defense Dictionary of Military and Associated Terms*. 2010.

Leigh, David and Luke Harding. *Wikileaks: Inside Julian Assange's War on Secrecy*. New York: Public Affairs, 2011.

Leiner, Barry M., et al. "The Past and Future History of the Internet." *Association for Computing Machinery, Communications of the ACM*, Vol. 40 No. 2, 1997.

Lindsay, Jon R. "Stuxnet and the Limits of Cyber Warfare." *Security Studies*. Vol. 22, No. 3 (2013).

Lynn, William. "Defending a New Domain: The Pentagon's Cyber Strategy." *Foreign Affairs*. (September/October 2010).

Mark, Paul. "Dot-dash-diss: The gentleman hacker's 1903 lulz." December 27, 2011. <http://www.newscientist.com/article/mg21228440.700-dotdashdiss-the-gentleman-hackers-1903-lulz.html?full=true#.VLGA7k5CM8>.

Mullen, Jethro. "North Korea and the Sony Hack: The War of Words Escalates." *CNN.com*. December 22, 2014. <http://www.cnn.com/2014/12/22/world/asia/north-korea-us-sony-hack-who-says-what/index.html>.

Nakashima, Ellen. "Cyber-intruder sparks response, debate." *Washington Post.com*. December 6, 2011. http://www.washingtonpost.com/national/national-security/cyber-intruder-sparks-response-debate/2011/12/06/gIQAxLuFgO_story.html.

Nissenbaum, Dion. "Government Seeks to Replace Firm That Vetted Snowden, Navy Shooter," *Wall Street Journal.com*. September 20, 2013.
<http://www.wsj.com/articles/SB10001424127887324807704579087601389468282>.

Oxford English Dictionary, s.v. "non-state actors," accessed Jan 10, 2015, <http://www.oed.com>.

Reveron, Derek S. *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World*. Washington, DC: Georgetown University Press, 2012.

- Rosenzweig, Paul. *Cyber Warfare: How Conflicts in Cyberspace are Challenging America and Changing the World*. Santa Barbara, CA: Praeger, 2013.
- Sangarasivam, Yangara. "Cyber Rebellion: Bradley Manning, WikiLeaks, and the Struggle to Break the Power of Secrecy in the Global War on Terror." *Perspectives on Global Development & Technology*. 2013.
- Shachtman, Noah. "Insiders Doubt 2008 Pentagon Hack Was Foreign Spy Attack." *The Brookings Institute*. August 25, 2010. <http://www.brookings.edu/research/opinions/2010/08/25-pentagon-worm-shachtman>.
- Shakarian, Paul. "Stuxnet: Cyber Revolution in Military Affairs." *Small Wars Journal*, April 15, 2011.
- Siboni, Gabi and Sami Kronenfeld. "Developments in Iranian Cyber Warfare, 2013-2014." *The Institute for National Security Studies*. April 4, 2014. <http://www.inss.org.il/index.aspx?id=4538&articleid=6809>.
- The White House, National Security Strategy, 2010. http://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf.
- Walt, Stephen M. "Is the Cyber Threat Overblown?" *Foreign Policy*. March 30, 2010. <http://foreignpolicy.com/2010/03/30/is-the-cyber-threat-overblown>.
- Webster-Merriam Dictionary, s.v. "hacker," accessed Jan 10, 2015, <http://www.merriam-webster.com>.
- Worley, D. Robert. *Orchestrating the Instruments of Power: A Critical Examination of the U.S. National Security System*. Raleigh: Lulu Press, 2012.