2017-03

Three if by internet: exploring the utility of a hacker militia

O'Loughlin, Matthew S.

Monterey, California: Naval Postgraduate School

NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

THREE IF BY INTERNET: EXPLORING THE UTILITY OF A HACKER MILITIA

by

Matthew S. O'Loughlin

March 2017

Thesis Advisor: Leo Blanken
Co-Advisor: Zachary Davis

Approved for public release. Distribution is unlimited.

THIS PAGE INTENTIONALLY LEFT BLANK

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 instruction, 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** March 2017	**3. REPORT TYPE AND DATES COVERED** Master's thesis	
4. TITLE AND SUBTITLE THREE IF BY INTERNET: EXPLORING THE UTILITY OF A HACKER MILITIA		**5. FUNDING NUMBERS**	
6. AUTHOR(S) Matthew S. O'Loughlin			
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 number ____N/A____.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release. Distribution is unlimited.		**12b. DISTRIBUTION CODE**	

13. ABSTRACT (maximum 200 words)

Recent cyber exploits have highlighted the ever-growing complexity of the threats challenging our national security today. The surge of cyberattacks against both U.S. and allied targets has rapidly increased due to technological convergence and the accessibility of cyber tools that once were the sole domain of highly skilled hackers. The potential consequences of cyberattacks on national critical infrastructure, illustrated by state-sponsored encroachments of sovereignty in the cyber realm, underscore a growing list of "cross-domain" capabilities. The significant destructive potential of non-state actors in the cyber realm, however, pales in comparison with the sophistication, number, and consequence of those originating from China and Russia.

Understanding the tools of these new adversaries and leveraging emerging technologies to combat them asymmetrically in the digital environment may provide the foundation for forging a new kind of strategy based on partnerships, in which civilian technologists and government leaders unite against malicious cyber actors with the potential to inflict destabilizing effects worldwide. Collaborative efforts are already underway in government, private industry, and the civilian population. This thesis examines how the U.S. government might effectively incorporate unconventional cyber entities to help improve national cybersecurity via nontraditional means.

14. SUBJECT TERMS counterproliferation, collaboration, militia, national defense, unconventional, asymmetric battlespace, hacking, hacktivists, cyber space			**15. NUMBER OF PAGES** 81
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** 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.

THREE IF BY INTERNET: EXPLORING THE UTILITY OF A HACKER MILITIA

Matthew S. O'Loughlin
Lieutenant, United States Navy
B.S., United States Coast Guard Academy, 2008

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN DEFENSE ANALYSIS

from the

NAVAL POSTGRADUATE SCHOOL
March 2017

Approved by: Leo Blanken
Thesis Advisor

Zachary Davis, Ph.D.
Co-Advisor

John Arquilla, Ph.D.
Chair, Department of Defense Analysis

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Recent cyber exploits have highlighted the ever-growing complexity of the threats challenging our national security today. The surge of cyberattacks against both U.S. and allied targets has rapidly increased due to technological convergence and the accessibility of cyber tools that once were the sole domain of highly skilled hackers. The potential consequences of cyberattacks on national critical infrastructure, illustrated by state-sponsored encroachments of sovereignty in the cyber realm, underscore a growing list of "cross-domain" capabilities. The significant destructive potential of non-state actors in the cyber realm, however, pales in comparison with the sophistication, number, and consequence of those originating from China and Russia.

Understanding the tools of these new adversaries and leveraging emerging technologies to combat them asymmetrically in the digital environment may provide the foundation for forging a new kind of strategy based on partnerships, in which civilian technologists and government leaders unite against malicious cyber actors with the potential to inflict destabilizing effects worldwide. Collaborative efforts are already underway in government, private industry, and the civilian population. This thesis examines how the U.S. government might effectively incorporate unconventional cyber entities to help improve national cybersecurity via nontraditional means.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

AV	Area of Vulnerability
CNAP	Combined National Action Plan
CYBERCOM	U.S. Cyber Command
DDoS	Denial-of-Service
ICS-CERT	Industrial Control Systems Cyber Emergency Response Team
IOT	Internet of Things
IW	Irregular Warfare
S&T	Science and Technology
SOCOM	U.S. Special Operations Command
TDF	Territorial Defense Forces
USG	U.S. Government

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

To my thesis advisors, Dr. Leo Blanken and Dr. Zachary Davis, thank you for your support and thought-provoking discourse throughout this journey. The opportunities you provided me throughout this past year and a half have truly expanded my capacity and perspective.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION AND BACKGROUND

Our problems are man-made.
Therefore, they can be solved by man.

—President John F. Kennedy, 1963[1]

When America has been threatened in the past, the U.S. government has relied upon the civilian and private-industrial sectors for specific expertise and engineering capacity to improve military capabilities. In other words, the national security establishment frequently taps into civilian resources and expertise, but in turn absorbs those factors into its internal organizations and processes. It may be time to look yet again at this traditional paradigm of national security. As cyber capabilities continue to complicate the conflict space, the necessity of civilian and private-sector technology experts is not lessening; in fact, with the advent of cyberwarfare, they are in even greater demand. It may be time to rethink how societal cyber communities may assist in national security.

Observers of the hacker community have explored the question of hackers assisting the national security apparatus in combating this emerging threat.[2] These "hacktivists" could conceivably augment ongoing national security efforts in some form of a "hacker militia" that would utilize their pre-existing skill sets to bridge identified strategic and operational gaps that exist throughout the U.S. government, and are particularly problematic within Special Operations Command (SOCOM) and U.S. Cyber Command (CYBERCOM). This study offers a framework for enlisting the untapped potential of the hacker community to improve the cyber capacity of both national security entities.

[1] John F. Kennedy, "American University Speech" (speech, American University, Washington, DC, June 10, 1963). http://www.pbs.org/wgbh/americanexperience/features/primary-resources/jfk-university/.

[2] I am The Cavalry, "Overview of The Cavalry," accessed July 5, 2016. https://www.iamthecavalry.org/about/overview/.

A. THE PROBLEM

> Today, regional powers such as Russia, China, India, Indonesia, Brazil, Nigeria, South Africa, Turkey, and Iran assert growing power and influence…Sub-state actors (e.g., clans, tribes, ethnic and religious minorities) seek greater autonomy from the central government. The complex nature of the future operating environment will often render traditional applications of the diplomatic and economic instruments ineffective.
>
> —General Joseph Votel, 2016[3]

Offensive cyber threats from alleged state sponsors such as China and Russia have exposed operational and strategic gaps for the national security apparatus. Former Commander of SOCOM, General Joseph Votel says the "gray zone" is "characterized by intense political, economic, informational, and military competition more fervent in nature than normal steady-state diplomacy, yet short of conventional war."[4] In such forms of conflict, all tools of state—and societal—power are at play.

The emerging cyber conflict space perfectly aligns with Votel's concerns. Exploitable vulnerabilities in this interconnected world range from individuals' identities to power grids and the facilities that house weapons of mass destruction to elections. According to the Department of Homeland Security's Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), "in the first half of Fiscal Year 2015 (October 2014 through April 2015), ICS-CERT responded to 108 cyber incidents impacting critical infrastructure in the United States. As in previous years, the energy sector continues to lead all others with the most reported incidents."[5] In an interconnected world, corporations are legitimate hacking targets; consider the cyber hacks of Sony, Target, and the most recent distributed denial-of-service (DDoS) attacks that significantly interrupted services and operating speeds "to dozens of sites, including Twitter, Netflix, Spotify, and

---

[3] Joseph L. Votel et al., "Unconventional Warfare in the Gray Zone," *Joint Force Quarterly* 80 (1st Quarter 2016): 105.

[4] Ibid., 102.

[5] Department of Homeland Security, "Incident Response Activity." *ICS-CERT Monitor* (May/June 2015). https://ics-cert.us-cert.gov/sites/default/files/Monitors/ICS-CERT_Monitor_May-Jun2015.pdf.

Airbnb, for millions of Americans," as *TIME* magazine reported.[6] Looking at these numbers, the immediacy of the threat is readily apparent—and growing.[7]

SOCOM should look at all avenues to develop capacity to respond in the cyber gray zone. As the government embraced private sectors in the past, the proposition of engaging volunteer hacktivists to leverage their pre-existing skill sets to counter the threat of future cyber-attacks justifies serious consideration.

B. PURPOSE AND SCOPE

The purpose and scope of this thesis is to assess, analyze, and eventually develop a method to determine how the U.S. government might effectively mobilize and leverage existing human capital from the hacker community to improve the capacity to defend and appropriately respond to cyberattacks. The scope focuses on the utility of militias, and assesses the conditions under which they can be fruitfully engaged in this realm. Further investigation explores the utility of the hacker community and their ability to effectively counter cyber threats, thereby complementing the ongoing efforts by the national security apparatus. Can the U.S. government improve national cyber security and effectively bridge the existing operational and strategic gaps within SOCOM and CYBERCOM, with unconventional cyber entities via nontraditional means?

C. EXISTING RESEARCH ON "STATE-SOCIETY" RELATIONSHIP FOR NATIONAL SECURITY

The United States has grappled with maintaining an interdependent relationship between the government and the private sectors since the creation of America. Governments have always been "confronted with the interrelation of commercial, financial, and industrial strength on the one hand, and political and military strength on

[6] Haley Sweetland Edwards and Matt Vella, "A Shocking Internet Attack Shows America's Vulnerability," *TIME*, October 27, 2016. http://time.com/4547329/a-shocking-internet-attack-shows-americas-vulnerability/.

[7] Lee Rainie, Janna Anderson, and Jennifer Connolly, "Cyber Attacks Likely to Increase," Pew Research Center, October 29, 2014. http://www.pewinternet.org/2014/10/29/cyber-attacks-likely-to-increase/.

the other"[8] and have struggled to balance on the one hand the control offered by mercantilist policies, and on the other the economic benefits that come from liberalism. The political economy aspects of grand strategy, in fact, should be predicated on these basic questions of how (and how much) societal resources and processes need to be funneled into national security.[9] How are the dynamics of state-society relationships changing? First, the information age may be making the traditional structures of government unable to meet the demands of a rapidly evolving and ambiguous threat environment. Second, if this is the case, then pre-existing societal human capital—such as hackers—may be tapped into directly, rather than being processed and absorbed into (or generated within) the traditional national security apparatus. Finally, the special operations forces (SOF) community may be a uniquely evolved "touch point" to engage and manage such societal assets in the service of protecting the nation.

Writing a decade ago, Blanken and Goldman suggested that "we are situated precisely at the transition between the industrial and information ages, the ability to adapt is critical."[10] Their argument appears accurate, as the last ten years has seen a tremendous turn from the industrial age to the accelerated power and vulnerability of the information age. The number of devices connected devices to the Internet of Things (IoT), for example, continues to grow exponentially. This single concept embodies the changing way in which the strategic environment is moving beyond the traditional battlespace. Jacob Morgan explains IoT as follows:

> Simply put, this is the concept of basically connecting any device with an on and off switch to the Internet (and/or to each other). This includes everything from cellphones, coffee makers, washing machines, headphones, lamps, wearable devices and almost anything else you can think of. This also applies to components of machines, for example a jet engine of an airplane or the drill of an oil rig. As I mentioned, if it has an on and off switch then chances are it can be a part of the IoT. The analyst

[8] Edward Mead Earle, "Adam Smith, Alexander Hamitlon, and Friedrich List: The Economic Foundations of Military Power" in Peter Paret, ed., *Makers of Modern Strategy: From Machiavelli to the Nuclear Age* (Princeton: Princeton University Press, 1986), 217.

[9] Kevin Narizny. The Political Economy of Grand Strategy (Ithaca: Cornell University Press, 2007).

[10] Emily O. Goldman and Leo J. Blanken, "The Economic Foundations of Military Power" (University of Pittsburgh, Matthew B. Ridgway Working Paper #2006-12, 2006), 2.

> firm Gartner says that by 2020 there will be over 26 billion connected devices.[11]

The IoT will disturb the state's pursuit of traditional industrial power because information power, on account of globalization, is manifested at a much faster rate than industry and manufacturing capacity.[12]

As the IOT grows, the U.S. government (USG) will need to reevaluate the hierarchical organizational structure of the entities tasked with defending and responding to cyber threats. To underscore the speed at which the government must be able to adapt, I will explore Moore's Law. Moore's Law was an attempt by Gordon E. Moore in 1970 to predict the exponential growth in the world of digital electronics. Moore predicted that "processor speeds, or overall processing power for computers, will double every two years."[13] Taking a moment to reflect on the technological advances humanity has made over the past 30 years lends some validity to his projection. Given this change of pace, the access to information technology will increase. And with this proliferation of access, Blanken and Goldman suggest, "The information revolution has diffused and redistributed power to traditionally weaker actors."[14] And it is these weaker actors who will utilize cyberattacks as their preferred strategy against stronger actors, thereby exacerbating ongoing cyber security efforts of the USG.[15]

Advances in technology and information systems within the government, financial, and economic sectors have significantly stimulated these sectors' operating capacity in this ever more interconnected and globalized world. With the many opportunities that these innovative systems provide come a wide array of vulnerabilities. Blanken and Goldman, suggest "Information-dependent societies are also more vulnerable to the infiltration of computer networks, databases, and the media, and to

---

[11] Jacob Morgan, "A Simple Explanation of 'the Internet of Things,'" *Forbes*, May 13, 2014, http://www.forbes.com/sites/jacobmorgan/2014/05/13/simple-explanation-internet-things-that-anyone-can-understand/#158dadb86828.

[12] Goldman and Blanken, "The Economic Foundations of Military Power," 11.

[13] "Moore's Law," accessed March 15, 2016, http://www.mooreslaw.org/.

[14] Goldman and Blanken, "The Economic Foundations of Military Power," 6.

[15] Matt Bishop and Emily Goldman, *The Strategy and Tactics of Information Warfare*, 121.

physical as well as cyberattacks on the very linkages upon which modern societies rely to function: communication, financial transaction, transportation, and energy resource networks."[16] The sheer number of cyberattacks against USG and private sector enterprises exhibit how the U.S. is one of these information-dependent societies. Specific examples include a 2014 case brought before the U.S. Department of Justice that "indicted five Chinese military hackers for computer hacking, economic espionage and other offenses directed at six American victims in the U.S. nuclear power, metals and solar products industries."[17] North Korea's 2014 cyberattack of Sony Pictures Entertainment is another violation which exposed "executives' embarrassing emails, salary information and more."[18] Furthermore, the Central Intelligence Agency, in December of 2016, "concluded in a secret assessment that Russia intervened in the 2016 election to help Donald Trump with the presidency, rather than to just undermine confidence in the U.S. electoral system."[19] The ambiguity surrounding each of the aforementioned cases only points to the need for an overhaul of the USG entities tasked with defending against and responding to challenges from within the gray zone. The private sector's effective use of horizontal organizational models could prove to be a beneficial example of how America can maintain an advantage over her enemies. The vertical organizational construct of the majority of USG entities, will make it difficult for the United States and her allies to maintain the initiative against sophisticated asymmetric cyber threats from state and non-state actors who possess information technology that once required national infrastructure and funding to procure.[20]

---

[16] Goldman and Blanken, "The Economic Foundations of Military Power," 6.

[17] Office of Public Affairs, "U.S. Charges Five Chinese Military Hackers for Cyber Espionage against U.S. Corporations and a Labor Organization for Commercial Advantage," Department of Justice, May 19, 2014. https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor.

[18] Zeke J. Miller, "U.S. Sanctions North Korea over Sony Hack," *TIME*, January 2, 2015. http://time.com/3652479/sony-hack-north-korea-the-interview-obama-sanctions/.

[19] Adam Entous, Ellen Nakashima, and Greg Miller, "Secret CIA Assessment Says Russia Was Trying to Help Trump Win White House," *Washington Post*, December 9, 2016. https://www.washingtonpost.com/world/national-security/obama-orders-review-of-russian-hacking-during-presidential-campaign/2016/12/09/31d6b300-be2a-11e6-94ac-3d324840106c_story.html?utm_term=.323e1594995f .

[20] Matt Butler, "Rapid Delivery of Cyber Capabilities: Evaluation of the Requirement for a Rapid Cyber Acquisition Process" (graduate research project, Air Force Institute of Technology, 2012), 1.

According to a 2015 SOCOM white paper, "Not every non-state [or state] actor in the gray zone deserves significant attention, and a useful benchmark for concern is when belligerent ambitions and operational reach become transnational."[21] However, when one actor violates the sovereignty of another within the realm of technology or within an information systems platform, it is deemed an act of cyber warfare.[22] Cyber warfare is a signature example of a Gray Zone challenge. Coffman et al. argue that "in the Gray Zone, where lethal and non-lethal requirements ebb and flow, there is no clear delineation of which focus takes priority, whether the enemy or the people. Comprehension of sensitive and powerful relationships in play is paramount when designing campaigns with a high probability of enhancing policy and national interest."[23] With such a wide problem set, the following will narrow the focus and identify an unconventional method to bolstering the resources and capacity of the USG to increase cyber security initiatives. Drawing from the causal mechanisms founded in the case study section, I intend to determine the utility of a militia derived from volunteer hacktivists who possesses the pre-existing skill sets necessary to augment ongoing national cyber security efforts.

"Militia" is a provocative word today. Nations have, however, mobilized and contracted private actors to assist in national security throughout history. From the issuance of letters of marque to privateers on the high seas, to the utilization of private security firms in recent decades, the state has often chosen to partner with private sector entities, rather than to produce all capabilities "in house" (within the uniformed services).[24] Recent research by Gavra, however, suggests that the militia concept may be revived, not to produce more combat power, but to rather garner other skills from the

[21] United States Special Operations Command, "The Gray Zone" (white paper, September 9, 2015).

[22] John Arquilla, "From Blitzkrieg to Bitskrieg: The Military Encounter with Computers," *Communications of ACM* 54, no. 10 (October 2011): 58.

[23] Sean R. Coffman, Jeffrey Givens, Robert Shumaker, "Perception Is Reality: Special Operations Forces in the Gray Zone" (master's thesis, Naval Postgraduate School, 2016), 18.

[24] On privateers see Janice E. Thomson. *Mercenaries, Pirates, And Sovereigns*. (Princeton: Princeton University Press, 1996). On private security firms see P.W. Singer. Corporate Warriors: The Rise of the Privatized Military Industry. Second edition. (Ithaca: Cornell University Press, 2007)

society that may be difficult for military services to recruit for or train for.[25] Cyber hacking skills are a perfect example that justifies exploration here.

How does the SOF community play a role here? SOF operators are selected and trained to engage and persuade communities that may be reticent to work in alignment with U.S. interests.[26] Though the community engagement for which they train is usually a tribe in the mountains of Afghanistan, it could conceivably be a hacker community often at odds with U.S. government rules and policy. Effectively paired with SOF, volunteer hacktivists could utilize their pre-existing skill sets to defend and respond to transgressions in the cyber realm. Similar to how Russia demonstrated its ability to prepare every aspect of the battlefield, to include cyber, during its siege of Ukraine, a volunteer hacker militia could complement ongoing USG efforts in Phase Zero operations, preparation of the battlefield, and improving transition efficiency during offensive operations. To maximize the potential utility of volunteer hacktivists, the hacker militia would be integrated early and often with SOF elements.

Hacktivists possessing specific skill sets could identify and improve the vulnerabilities in SOF's commercially procured warfighting technology, but their utility would be fully realized when they comprehend the SOF mission. With a knowledge and understanding of how SOF operates, volunteer hacktivists can then predict and preemptively resolve future vulnerabilities in warfighting technology before those issues would have otherwise been realized. Adversaries such as China and Russia are actively meshing governmental, military, and civilian cyber programs into a comprehensive strategy. Failing to leverage the existing national human capital could limit the capabilities and resources of ongoing USG cybersecurity initiatives.

[25] Daniel V. Gavra, "Militias: Exploring Alternative Force Structures for National Defense" (master's thesis, Naval Post Graduate School, June 2014), 70.

[26] Jessica Glicken Turnley. Cross-Cultural Competence and Small Groups: Why SOF Are The Way They Are. (Tampa: Joint Special Operations University Report 11-1, 2011)

D. METHODOLOGY

The methodology of this thesis uses primarily qualitative methods. More specifically, I employ "*Heuristic* case studies [to] inductively identify new variables, hypotheses, causal mechanisms, and causal paths."[27] The two case studies explore the colonial rebels of the American Revolution and the Polish Territorial Defense Forces (TDF). The basis for selecting these two militias is that many of the threats targeting present day Poland represent the hybrid challenges aimed at the USG by its adversaries. In response, Poland has invested in a model that its country has relied upon for generations, one that is representative of the colonial militia forces of the American Revolutionary War. Spanning over 200 years and occurring on opposite ends of the globe, the two studies will be used to identify generalizable factors that "uncover causal mechanisms" relevant to the phenomenon of militia recruitment.[28] In each case, the pre-existing human capital of the citizenry has, albeit by different methods, mobilized to augment national security efforts. The contributions of these volunteer militias have greatly increased the overall capacity of their respective conventional or unconventional entities.

In an increasingly interconnected world, operational and strategic gaps are being exposed by state sponsored cyberattacks. While these attacks do not resemble those experienced on the fields of Lexington and Concord or the edges of Poland's sovereign state, I seek to explore whether an unconventional mobilization of the citizenry, might be utilized to augment the resources and capacity of SOCOM and CYBERCOM.

---

[27] Alexander L. George and Andrew Bennett, *Case Studies and Theory Development in the Social Sciences* (Cambridge, MA: MIT Press, 2005), 75.

[28] Ibid.

THIS PAGE INTENTIONALLY LEFT BLANK

II. THE NEW HIGH GROUND: HOW CHINA AND RUSSIA LEVERAGE THE CYBER DOMAIN TO PROMOTE THEIR NATIONAL AGENDAS

The utility of the emerging cyber domain has been fully realized by nation-states and non-state actors alike. "The Department of Defense invented the Internet, and the possibility of using it in warfare was not overlooked even in its early days."[29] Beginning in 1994, the Department of Defense created the Joint Security Commission to address the vulnerabilities posed by networked technology. The commission discovered three main points.

> Information systems technology…is evolving at a faster rate than information systems security technology. The security of information systems and networks [is] the major security challenge of this decade and possibly the next century and…there is insufficient awareness of the grave risks we face in this arena. The report also noted that the increased dependence in the private sector on information systems made the nation as a whole, not just the Pentagon, more vulnerable.[30]

In response to the commission's report, the Clinton administration initiated the Presidential Commission on Critical Infrastructure Protection, which developed the National Plan for Information Systems Protection. However, as Richard A. Clarke and Robert K. Knake mentioned in their book *Cyber War: The Next Threat to National Security and What to Do about it*, the government lacked the willingness "to regulate the industries that ran the vulnerable critical infrastructure."[31]

Following the devastating Oklahoma City bombings, the Clinton administration tasked Air Force General Marsh with establishing a committee to evaluate the vulnerability of the country's critical infrastructure. What became known as the Marsh Committee consisted of leaders in industry, education, and the various government agencies. The results of the numerous Marsh Committee meetings held around the

---

[29] Richard A. Clarke and Robert K. Knake, *Cyber War: The Next Threat to National Security and What to Do about it* (New York: Ecco, 2010), 34.

[30] Ibid., 104.

[31] Ibid., 109.

country found that "the chief challenge [was] the role of the private sector, which owned most of what counted as critical infrastructure," as Clarke and Knake summarized it.[32]

Following cyberattacks such as Solar Sunrise in 1999, and Moonlight Maze, which hacked data systems and unclassified government computers for years, to a DDoS attack in 2000 that targeted online commerce sites, the incoming Bush Administration was in a unique position to fully comprehend threats generating from cyberspace. As such, the Bush administration implemented the Comprehensive National Cybersecurity Initiative and National Security Presidential Decision 54. As noteworthy as these efforts were, their attempts at establishing an "information warfare deterrence strategy and declaratory doctrine," as well as securing the financial and economic sector, were futile. In the end, these actions did little more than improve network security for internal government networks.[33]

Realizing the world is more interconnected politically, economically, and militarily, than ever before, President Obama encouraged many new cybersecurity initiatives. According to a 2015 report to Congress by the U.S.-China Economic and Security Review Commission, "As the largest and most web-dependent economy in the world, the United States is also the largest target for cyber espionage of commercial intellectual property."[34] With the many complexities the cyber domain presents, specifically attribution following an attack, improved relationships between the United States, the People's Republic of China (PRC), and Russia offer the possibility to create an environment that facilitates improved accountability for individual actors operating maliciously in the cyber domain.

So far, collaboration efforts with world powers such as the PRC and Russia have been compromised due to a vast array of malicious acts and disputes over the handling of the cyber domain. Initiating a solution will require a common lexicon and an

[32] Ibid., 107.

[33] Ibid., 114–115.

[34] U.S.-China Economic and Security Review Commission, *2015 Annual Report to Congress of the U.S.-China Economic and Security Review Commission* (Washington, DC: U.S. Government Publishing Office, November 2015), 192.

understanding of the foundations of the national agendas of these powers. As Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz write in *Cyberpower and National Security*, "Without close study of these and the approaches of nation-states to cyber issues, it would be akin to playing a game of basketball in which your focus was solely on your team's offensive and defensive philosophy while disregarding your opponent's skill set and strategy."[35] Cyber assets are being used to advance specific national interests that must be understood in order to be countered.

There are similarities and differences between the PRC's and Russia's cyber strategies. While both utilize the cyber arena to advance their own national agendas, there are considerable differences in each country's strategy and tactics.[36] However, before discussing these distinctions, it is imperative to recognize how the context of the words *cyber*, *network*, and *information* varies between the PRC, Russia, and the United States.

A. TERMINOLOGY MAKES A DIFFERENCE

Examining how the United States, the PRC, and Russia differentiate the meaning of the words *cyber*, *network*, and *information* is an essential first step to improving communications between the rival nations. Furthermore, such efforts could prevent potentially catastrophic misunderstandings during public addresses and declarations made by heads of state.

As Amy Chang writes in *Warring State: China's Cybersecurity Strategy*, at the most basic level, the "term 'cyber' is rarely used [in China or Russia] and not fully congruent with how the term is understood in the U.S. policy community."[37] To underline this point, Mikk Raud, researcher from the NATO Cooperative Cyber Defence Centre of Excellence, states "the Chinese term closest to what would translate as *cyberspace* merely entails the necessary components of a connected device and actions

---

[35] Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz, *Cyberpower and National Security* (Washington, DC: National Defense University Press, 2009), 487.

[36] Kenneth Geers, ed., *Cyber War in Perspective: Russian Aggression against Ukraine* (Tallinn, Estonia: NATO Cooperative Cyber Defense Centre of Excellence, 2015), 8.

[37] Amy Chang, *Warring State: China's Cybersecurity Strategy* (Washington, DC: Center for a New American Security, December 2014), 10.

related to it. For the Chinese, cyberspace is thus only a subset of information space—the landscape for the largest scale communication to the world's population."[38] The inability to properly navigate policy discussions and public discourse with the appropriate lexicon has the potential to compound the already complicated process of resolving cybersecurity issues in the international arena.

In a statement for the record to the Senate Select Committee in 2014, James Clapper, Director of the National Intelligence Agency, stated, "Russia and China continue to hold views substantially divergent from the United States on the meaning and intent of international cyber security. These divergences center mostly on the nature of state sovereignty in the global information environment states' rights to control dissemination of content online, which have long forestalled major agreements."[39] Differences aside, going forward, I will be using the National Academy of Sciences definition of cyberattack as "the use of deliberative actions to alter, disrupt, deceive, degrade, or destroy adversary computer systems or networks or the information and/or programs resident in or transiting these systems or networks."[40] Using this term, China and Russia's strategic agendas will be explained.

B. CHINA'S STRATEGIC AGENDA

The United States and China have discussed cybersecurity, however, they currently lack the proper level of dialogue to mitigate confrontation in cyberspace. To encourage healthier discourse, it is necessary to improve our understanding of China's strategic agenda and identify the governmental entities responsible for its foundations.

---

[38] Mikk Raud, *China and Cyber: Attitudes, Strategies, Organisation* (Tallinn, Estonia: NATO Cooperative Cyber Defence Centre of Excellence, 2016), 9.

[39] James R. Clapper, *Worldwide Threat Assessment of the U.S. Intelligence Community* (statement for the record, Tysons Corner, VA, January 29, 2014), 1.

[40] Jeffrey Kwong, "State Use of Nationalist Cyber Attacks as Credible Signals in Crisis Bargaining," in *China and Cybersecurity: Political, Economic, and Strategic Dimensions* (report from IGCC workshop on China and cybersecurity, UC San Diego, April 2012), 31.

China's cybersecurity strategy can be categorized into political, economic, and military subcategories.[41] Amy Chang, research associate at the Center for a New American Security, unpacks China's national strategic agenda:

> China's foreign policy behavior, including its cyber activity, is driven primarily by the domestic political imperative to protect the longevity of the Chinese Communist Party (CCP). Ensuring domestic stability, territorial integrity, modernization, and economic growth, while simultaneously preparing for the possibility of militarized cyber conflict in the future, are all objectives that directly or indirectly support the continuation of CCP rule. China espouses laws, norms, standards, and agreements in bi- and multilateral fora that allow for sufficient flexibility of interpretation to serve domestic needs and interests.[42]

The above summary highlights how integral the cyber domain is to promoting the CCP's national agenda. And to operationalize their initiatives, the CCP created the Third and Fourth Departments. In his article "Assessing the Chinese Cyber Threat," Larry Wortzel identifies an uncertain relationship between "China's military intelligence collection and cyber reconnaissance infrastructure, [which] supports a coordinated effort to combine civilian and military cyber programs and improve both offensive and defensive capabilities."[43] Furthermore, he highlights that the "PLA General Staff Department (GSD) Third Department and Fourth Department are organized and structured to systematically penetrate communications and computer systems, extract information, and exploit the information."[44]

The American Foreign Policy Council's e-journal, *Defense Dossier*, illuminates how "China's cyber strategy extends beyond the PLA and into the civil and commercial spheres. Several U.S.-China Economic and Security Commission reports have expressed concerns about some of China's largest telecommunications firms, [who] benefit from a network of state research institutes as well as government funding in programs that have

---

[41] Jimmy Goodrich, "Chinese Civilian Cybersecurity: Stakeholders, Strategies, and Policy," in *China and Cybersecurity: Political, Economic, and Strategic Dimensions* (report from IGCC workshop on China and cybersecurity, UC San Diego, April 2012), 5.

[42] Chang, *Warring State*, 7.

[43] Larry M. Wortzel, "Assessing the Chinese Cyber Threat," *Defense Dossier* 4 (August 2012), 2.

[44] Ibid.

affiliation or sponsorship of the PLA."[45] According to a 2015 report to Congress by the U.S.-China Economic and Security Review Commission, "China causes increasing harm to the U.S. economy and security through two deliberate policies targeting the United States: coordinated, government-backed theft of information from a variety of U.S.-based commercial enterprises and widespread restrictions on content, standards, and commercial opportunities for U.S. businesses."[46] These discoveries "reveal two overarching trends in China's thinking: consolidating political leadership over cyber issues, and framing the internet as part of China's national strategy."[47]

The PRC has skillfully meshed government and private industry, with civilian counterparts, to collectively promote the national agenda of the state. Given the foundations of the PRC's national agenda, the creation of the Integrated Network Electronic Warfare (INEW) should have been anticipated. The INEW reveals "a formal IW strategy…that consolidates the offensive mission for both Computer Network Attack (CNA) and Electronic Warfare (EW)."[48] Until a proper defensive strategy is confirmed by the U.S., the 2015 Annual Report to Congress on U.S.-China Economic and Security Review Commission maintains that

> hackers working for the Chinese government—or with the government's support and encouragement—[will continue to infiltrate] the computer networks of U.S. agencies, contractors, and companies, and [steal] their trade secrets, including patented material, manufacturing processes, and other proprietary information. The Chinese government has provided that purloined information to Chinese companies, including state-owned enterprises, in a major application of cyber espionage.[49]

The book *Unrestricted Warfare*, written by two former colonels in the People's Liberation Army, Qiao Lang and Wang Xiangsui, specifically identifies a multitude of

---

[45] Ibid., 3.

[46] U.S.-China Economic and Security Review Commission, *2015 Annual Report to Congress.*

[47] James A. Lewis and Simon Hansen, "China's Emerging Cyberpower: Elite Discourse and Political Aspirations" (special report, Australian Strategic Policy Institute, International Cyber Policy Centre, Canberra, Australian Capital Territory, November 2014). https://www.aspi.org.au/publications/chinas-cyberpower-international-and-domestic-priorities/SR74_China_cyberpower.pdf.

[48] Deepak Sharma, "Integrated Network Electronic Warfare: China's New Concept of Information Warfare," *Journal of Defense Studies* 4, no. 2 (2010): 37. www.idsa.in/system/files/jds_4_2_dsharma.pdf.

[49] U.S.-China Economic and Security Review Commission, *2015 Annual Report to Congress*, 192.

ways in which unconventional warfare can be employed against an enemy to prepare the battlefield and then capitalize on discovered weaknesses when the opportunity presents itself. The book's introduction notes, "The doctrine of total war outlined in *Unrestricted Warfare* clearly demonstrates that the People's Republic of China is preparing to confront the United States and our allies by conducting 'asymmetrical' or multidimensional attacks on almost every aspect of our social, economic, and political life."[50] The means by which the PRC hopes to achieve the basic tenets of its agenda draws similarities with Russia's infamous Gerasimov Doctrine, which I will explain in the following section. Both strategies describe how a "new form of warfare, which borrows from the ancient wisdom of Sun Tzu and his doctrines of surprise and deception, also employs civilian technology as military weapons 'without morality' and with 'no limits' in order to break the will of democratic societies."[51] China's emerging cyber strategy, which effectively blurs the lines between government, military and civilian cyber programs, presents a complex gray zone challenge for the national security apparatus.

C. RUSSIA'S STRATEGIC AGENDA

Realizing the utility of the cyber domain, Russia developed the Information Security Doctrine in 2000. Timothy Thomas, author of "Nation-State Cyber Strategies," says the doctrine "presented the purposes, objectives, principles, and basic directions of Russia's information security policy."[52] According to David J. Smith's article "How Russia Harnesses Cyberwarfare," Russia's strategic aims include a "much broader approach to information operations than do most western countries."[53] These sorts of tactics have escalated tensions throughout Europe and the West. Russia's approach to achieving its agenda highlights the interwoven relationships of the government with the

---

[50] Qiao Liang and Wang Xiangsui, *Unrestricted Warfare: China's Master Plan to Destroy America* (Panama City: Pan American Publishing, 2002), x.

[51] Ibid.

[52] Timothy Thomas, "Nation-State Cyber Strategies: Examples from China and Russia," in *Cyberpower and National Security*, eds. Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz (Washington, DC: Center for Technology and National Security Policy, National Defense University, 2009), 481.

[53] David J. Smith, "How Russia Harnesses Cyberwarfare," *Defense Dossier* 4 (August 2012): 7.

private industry and contracted forces.[54] As Azhar Unwala and Shaheen Ghori write in an article for *Military Cyber Affairs*,

> In official and unofficial doctrine, Russia typically refers to a holistic concept of "information warfare," which encompasses cyber espionage, cyberattacks, and strategic communications. Russia's official view of cyber power stems from its "Information Security Doctrine," dated September 9, 2000. This document affirms a long-standing policy of state influence over the media, arguing that the government must ensure pro-Russian messaging regardless of whether media sources are state-controlled or private.[55]

Kenneth Geers's book *Cyber War in Perspective: Russian Aggression against Ukraine* provides insight into Russia's strategic culture and how cyber warfare in particular is being leveraged to promote their national agenda. "Russian cyber activities, especially those associated with the recent conflict in Ukraine and the annexation of Crimea, probably offers the best example of the employment of cyberattacks to shape the overall political course of a dispute."[56] The main issue of these disputes is the perceived aggression of the North Atlantic Treaty Organization (NATO) against the sovereignty of Russia.

NATO, a collective of sovereign nations determined to "contribute to the security of the North Atlantic area," infringes on Russian hegemony of the region.[57] Recognizing the strengths and weaknesses of the NATO alliance and how the balky Western decision-making process relies so heavily on information before action, Russia successfully manipulated the strategy and relationship of NATO instead of participating in conventional direct engagement. By reducing the "death and destruction associated with any *fait accompli* to an absolute minimum," Russia exploited these gaps and limited NATO's ability to respond with conventional escalation.[58]

---

[54] Ibid.

[55] Azhar Unwala and Shaheen Ghori, "Brandishing the Cybered Bear: Information War and the Russia-Ukraine Conflict," *Military Cyber Affairs* 1, no. 1 (2015): article 7.

[56] Geers, *Cyber War in Perspective*, 30.

[57] NATO, "What Is Nato?", accessed on December 01, 2016. www.nato.int/nato-welcome/index.html.

[58] Geers, *Cyber War in Perspective.*

James J. Wirtz's article "Cyber War and Strategic Culture: The Russian Integration of Cyber Power into Grand Strategy" further unpacks Russia's tactics:

> Russia opted to pick a course of action not to defeat NATO, but to defeat NATO's *strategy*. By presenting the Western alliance with a *fait accompli* through actions that produce minimal death and destruction, Russia attempted to shift the onus of escalation onto NATO, thereby inflicting a strategic defeat on the Alliance at the outset of hostilities or even in the event of non-democratic changes to the status quo.[59]

While Ukraine is not a member of NATO, Russian exploitations against a sovereign country, echoed throughout the region. Further application of Russia's efforts in this space are well documented. As reported in a *New York Times* article, James R. Clapper, director of national intelligence, "warned Senate officials this year that Russia was escalating its espionage campaigns against the United States," using cyber espionage groups such as APT29 and APT28 whose targets are also targets of the Russian state.[60] Unlike hacktivist groups such as Anonymous and New World Hackers, "APT28's targeting of … the Caucasus (especially Georgian government), Eastern European governments and militaries, and specific security organizations"[61] validate suspicions of Russian state sponsorship.

Russia's masterful exploitation of the cyber and information arena raises many questions about its future conquests. Russia's actions should encourage member countries of NATO to accelerate the timeline for finding consensus on the obscurities that remain in NATO's current doctrine and laws. Many of Russia's tactics and procedures were revealed during its exploits in Estonia and Georgia, and they must be studied and compared to the Military Doctrine of the Russian Federation from February 5, 2010. Unwala and Ghori write, "This doctrinal update codified reforms to transition Russia's

---

[59] James J. Wirtz, "Cyber War and Strategic Culture: The Russian Integration of Cyber Power into Grand Strategy," in *Cyber War in Perspective: Russian Aggression against Ukraine*, ed. Kenneth Geers (Tallinn, Estonia: NATO Cooperative Cyber Defense Centre of Excellence, 2015), 34.

[60] Nicole Perlroth, "Hackers Trawl User Data in Hopes a Small Target Will Lead to a Big One," *New York Times*, September 23, 2016. http://www.nytimes.com/2016/09/24/technology/hackers-trawl-user-data-in-hopes-a-small-target-will-lead-to-a-big-one.html?_r=0; Geers, *Cyber War in Perspective*, 69.

[61] *APT28*: *A Window into Russia's Cyber Espionage Operations?* Accessed December 14, 2016. https://www.fireye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-apt28.pdf, 6.

mass-mobilization, Soviet-era military to a modern, highly mobile force. One of these reforms was the development of 'forces and resources for information warfare.'"[62]

Russian chief of general staff Valery Gerasimov was deemed the appropriate leader for this overhaul. General Gerasimov articulated his plan in a 2013 publication that has become widely known as the Gerasimov Doctrine.[63] Unwala and Ghori explain,

> Gerasimov recognizes that future conflicts must include an information element, which can asymmetrically lower an adversary's combat potential in addition to creating a "permanently operating front through the entire territory of an enemy state"…Modern warfare should also rely on covert action, special operations forces, and private contractors until the final stages of a conflict when success is guaranteed.[64]

If NATO hopes to correctly predict Russia's next move, its actions in Georgia, Estonia, and Crimea have exposed many tactics and procedures (TTP) that must be exploited. Furthermore, to engage this hybrid threat, it would behoove the U.S. government to leverage cyber entities and improve cyber policy so that an effective, timely, and appropriate response can be achieved.

D. LESSONS LEARNED

While conducting cyber operations, the PRC and Russia have exposed many capabilities and weaknesses in their quest to achieve the coveted seat at the cyber domain's highest ground. Throughout the research collection, I have found that both countries take aim specifically at the United States in the form of cyber espionage. Intellectual property theft in particular has a substantial return on investment and bolsters much-needed economic initiatives in each country. Admiral Mike McConnell, former national security advisor under the Clinton administration and director of national intelligence during the Bush administration, Michael Chertoff, former secretary of homeland security, and William Lynn, former deputy secretary of defense, stated in the

---

[62] Unwala and Ghori, "Brandishing the Cybered Bear."

[63] Mark Galeotti, "The 'Gerasimov Doctrine' and Russian Non-Linear War," *In Moscow's Shadows*, July 6, 2014. https://inmoscowsshadows.wordpress.com/2014/07/06/the-gerasimov-doctrine-and-russian-non-linear-war/.

[64] Unwalla and Ghori, "Brandishing the Cybered Bear."

Wall Street Journal in 2012 that "it is more efficient for the Chinese to steal innovations and intellectual property than to incur the cost and time of creating their own."[65] Had the conversation in the opinion piece been about Russia, the verdict would remain the same, according to David Smith's article "How Russia Harnesses Cyberwarfare."[66]

Amy Chang writes, "Evidence of China's intrusive cyber activity against U.S. national security infrastructure and industry is abundant. …China has exfiltrated critical information from foreign businesses, governments and militaries."[67] Case in point, the 2015 intrusion into the Office of Personnel Management, where "U.S. government databases holding personnel records and security-clearance files exposed sensitive information about at least 22.1 million people, including not only federal employees and contractors but their families and friends."[68] According to FBI director James Comey, the price tag of such actions by China against the United States alone is estimated to be billions.[69] Robert Miller, Daniel T. Kuehl, and Irving Lachow write in an article for *Joint Force Quarterly*, "The United States needs to consider the implications of information and infrastructure operations and decide explicitly what it wishes to do about them. To not decide potentially allows others to decide for us."[70]

Improved dialogue between the United States, the PRC, and Russia has the potential to facilitate understanding that creates discourse, which in turns fosters a chance for deterrence, specifically tailored deterrence. Kramer, Starr, and Wentz explain tailored deterrence as a concept that "suggests that important alliances (such as NATO) must develop a holistic philosophy that understands the goals, culture, and risk calculus of

---

[65] Mike McConnell, Michael Chertoff, and William Lynn, "China's Cyber Thievery Is National Policy—and Must Be Challenged," *Wall Street Journal*, January 27, 2012. http://www.wsj.com/articles/SB10001424052970203718504577178832338032176.

[66] Smith, "How Russia Harnesses Cyberwarfare."

[67] Chang, *Warring State*, 9.

[68] Ellen Nakashima, "Hacks of OPM Databases Compromised 22.1 Million People, Federal Authorities Say," *Washington Post*, July 9, 2015. https://www.washingtonpost.com/news/federal-eye/wp/2015/07/09/hack-of-security-clearance-system-affected-21-5-million-people-federal-authorities-say/?utm_term=.21b99f519a06.

[69] Chang, *Warring State*, 21.

[70] Robert Miller, Daniel T. Kuehl, and Irving Lachow, "Cyber War: Issues in Attack and Defense," *Joint Force Quarterly*, no. 61 (2nd quarter 2011): 23.

each of the potential adversaries, develops and plans for capabilities to deter these adversaries, and devises a strategy to communicate these concepts to the potential adversaries."[71] Without such a comprehensive plan, malicious cyberattacks that lack attribution could lead to escalatory attacks by states and non-state actors. Whether or not this form of tailored deterrence is fostered by all parties, secondary or tertiary effects of initiatives to facilitate a holistic, whole-of-government approach with the PRC and Russia could improve overall accountability of rogue actors through enriched information sharing and communication.

E. CONCLUSION

Russia's transgressions in the Baltic states and China's purported hack into the Office of Personnel Management are but two of many examples of how nation-states are applying cyberwarfare strategy to promote their own national agendas. Admiral McConnell stated that China is "the world's most active and persistent practitioner of cyber espionage today, [but] it is Russia's actions in the Baltics that specifically have me fascinated."[72] Geers writes that the manner in which Russia was able to "masterfully [exploit] the information gleaned from its worldwide computer network exploitation campaigns to inform its conduct, purposely distort public opinion, and maintain its dominant position in Ukraine" is momentous and speaks volume for the overall utility of present-day cyber operations.[73]

The lack of timely and effective responses by the USG and NATO demonstrates the complexities of cyber gray zone challenges. The responses that did eventually materialize, underscored Washington's ambivalence towards the situation.[74] The characteristics of the cyber domain appear to be as asymmetric as can be, and because of this the United States must acknowledge her shortfalls and learn from the techniques, tactics, and procedures demonstrated by Russia and the PRC.

---

[71] Kramer, Starr, and Wentz, *Cyberpower and National Security*.

[72] U.S.-China Economic and Security Review Commission, *2015 Annual Report to Congress*, 193; Wortzel, "Assessing the Chinese Cyber Threat."

[73] Geers, *Cyber War in Perspective*, 68.

[74] Unwala and Ghori, "Brandishing the Cybered Bear."

Miller, Kuehl, and Lachow suggest, further conversations should focus less "on dominating or controlling the cyber sphere, [which is reasonably] unhelpful, since the real touchstone of success is *effective use* rather than *physical control*. The former is possible, and the latter is probably not—which, of course, is exactly the way that the Air Force and Navy describe air and maritime superiority."[75] Contemplating cyberspace ownership as if it were strictly territory will not facilitate a solution to the current problem. Fortunately, SOCOM entertains an alternative view of the battlefield.

The 2014 Special Operations Joint Publication 3-05 states that "Special operations considers the totality of the cognitive, informational, physical, cultural, and social aspects of the operational environment to influence relevant populations, enhance stability, prevent conflict, and when necessary, fight and defeat adversaries. SOF capabilities complement CF capabilities."[76] The aforementioned doctrine of special operations is unlike any other in the services. As such, SOCOM appears to be the government entity best equipped with the knowledge and capacity necessary to achieve operational and strategic success in the gray zone. Paired with cyber warriors from CYBERCOM and leveraging the pre-existing skill sets of American hacktivists, the alliance may generate the appropriate resources and capacity necessary to respond and defend against future cyber threats.

---

[75] Miller, Kuehl, and Lachow, "Cyber War," 20.

[76] Joint Chiefs of Staff, *Joint Publication 3-05, Special Operations* (Arlington, Virginia: Pentagon, July 16, 2014), II–1.

THIS PAGE INTENTIONALLY LEFT BLANK

III. MILITIAS: UPDATING AN OLD IDEA

America's efforts to counter INEW and the Gerasimov Doctrine are summarized in the "Department of Defense Cyber Strategy" from April 2015 which outlined its four strategic goals—"Build and maintain ready forces and capabilities," "Defend the DOD information network," "Be prepared to defend the U.S. homeland and U.S. vital interests," and "Build and maintain robust international alliances to deter shared threats and increase international security and stability."[77] While the U.S. clearly recognizes the necessity of a comprehensive cyber strategy, critics identify issues with the current strategy and the organizational construct of the entities tasked with responding and defending cyberattacks.

Dr. Robert Miller and Dr. Daniel Kuehl, professors in the Information Resources Management College at the National Defense University, propose a possible solution. They introduce a more comprehensive term to U.S. policymakers: *information and infrastructure operations* (I^2O).[78] Collaborating with Lachow, they write, "The purpose of an I^2O would be to disrupt, confuse, demoralize, distract, and ultimately diminish the capability of the other side. These are not weapons of mass destruction, although they could have destructive secondary effects; they are more paralytic in nature—and are thus *weapons of both mass and precision disruption*."[79] In essence, the term describes what each side is currently doing or preparing to do as critical infrastructures such as the Internet become more interdependent and hypothetically more resilient. The ability to identify and then strike against and weaken a nation's critical infrastructure may have greater utility than investing in a singular, historically dominant weapons system.[80]

Russia has demonstrated to the world that it possesses a comprehensive assortment of tools and tactics to subvert perceived state security and global alliances

---

[77] Department of Defense, *The Department of Defense Cyber Strategy* (Arlington County, Virginia: Pentagon, April 2015).

[78] Miller, Kuehl, and Lachow, "Cyber War," 19.

[79] Miller, Kuehl, and Lachow, "Cyber War."

[80] Sam Biddle, "How to Destroy the Internet," Gizmodo, May 23, 2012, http://gizmodo.com/5912383/how-to-destroy-the-internet.

such as NATO. One specific tool is the Russian employment of private contractors to further complicate the gray zone challenge. Similarly in China, the "increase in Chinese civilian and military research on network security over the years reinforces [the state's] leadership prioritization of formulating and funding research into network security technologies and strategies."[81]

Fortunately, leveraging American human capital fits the American experience as well. American colonial rebel forces and Poland's Territorial Defense Forces (TDF) are separated by a 200-year period. Nevertheless, useful parallels can be drawn between their dispositions and organizational structures. Surging the ranks when threatened and operating autonomously or on the periphery of major conventional operations, the militia's utility in "defending the community it represents" continues to be realized today.[82]

A. AMERICAN COLONIAL REBELS

American colonial rebel forces incorporated a revolutionary strategy to achieve victory over British forces during the American Revolutionary War. In his book *The American Way of War*, Russell F. Weigley discusses how the strategy of hybrid warfare, pioneered by Nathanael Greene, "violated the principles of concentration" and allowed for the independent use of regular and irregular forces against a far superior enemy to leverage that enemy's strengths against it.[83] This strategy was fundamentally different than those that had been used before and most certainly than the one employed by General George Washington, who preferred a much more "conventional mode of war."[84]

Born out of necessity, the independent irregular forces would leverage their strengths against the larger and far superior conventional British force. The utility of conventional and irregular forces waging guerilla warfare and harassment operations against British general Burgoyne and his force of 10,000 men caused significant impacts

---

[81] Chang, *Warring State*, 20.

[82] Gavra, "Militias: Exploring Alternative Force Structures."

[83] Russell F. Weigley, *The American Way of War* (Bloomington: Indiana University Press, 1973), 29.

[84] Ibid., 20.

to supply lines that degraded a force which was initially far superior in size and strength to the colonial rebel forces.

The concept of hybrid warfare was progressive because in previous battles, irregular militia forces never enjoyed full autonomy from their conventional counterparts. Utilizing strategic positioning, independent irregular forces would later exploit General Cornwallis's strengths and use them against him. Cornwallis's temperament toward militia forces and his aggressive thirst for direct confrontations with a standing army caused him to blindly pursue American colonial rebel forces. As such, Cornwallis would often overextend his larger and far superior force. This meant the larger, less mobile conventional British force, hamstrung by its long lines of communications, became more vulnerable and susceptible to attack from the smaller, more agile colonial rebel forces.

Military theorist Carl Von Clausewitz hypothesized that strength is composed of a combination of force and will.[85] Much focus is spent on the aspect of force, but will, is equally important. Another military theorist, Mao Tse-Tung, also emphasized the human aspects of success on the battlefield.

> Weapons are an important factor in war, but not the decisive factor; it is people, not things, that are decisive. The contest of strength is not only a contest of military and economic power, but also a contest of human power and morale. Military and economic power is necessarily wielded by people.[86]

Unified under the guidance to avoid direct engagements with the far larger British forces and to wage a "no-holds-barred campaign of harassment against his outposts and supplies," as Weigley puts it, conventional and irregular forces descended upon the British forces.[87] Their efforts effectively "[wore] away the resolution of the British by gradual, persistent action against the periphery of their armies."[88]

---

[85] John Sheehan, "Masters of War" (lecture, Naval Postgraduate School, Monterey, CA, July 7, 2016).

[86] Tse-Tung, Mao, *Selected Military Writings of Mao Tse-Tung* (Peking: Foreign Language Press, 1967), 217.

[87] Weigley, *American Way of War*, 23.

[88] Ibid., 15.

Initially, Continental Army leadership was met with the difficulty of recruiting Southern colonials to join the revolutionary cause. However, a massive British failure in the Southern campaign soon galvanized the population. Not fully understanding their point of victory and not realizing they had attained their political objective in Charleston, General Cornwallis and the British forces proceeded to push further west, away from their port city strongholds. General Cornwallis's encroachment into the west had two major effects. One, infringing upon the lands of a Southern population that was once apathetic to the rebel cause fostered what Mao called a "mobilization of the people,"[89] with widespread anti-British sentiment that swelled the ranks of local militias.[90] Two, the British overextended their reach attempting to crack down on rebel sympathizers and generate direct engagements with colonial rebels. The multiple attempts at expanding beyond the safeguards of their encampments and safe harbors exposed vulnerabilities and flaws in British supply chains, mobility, and their ability to adapt to the rebels' fluid tactics.

The British forces, limited in their ability to maneuver outside of their large encampments and port cities, lost their historic conventional strength, the navy—a strength they had utilized to overwhelm scores of previous enemies. The true strength of the British armed forces and the reason they had been able to maintain their global hegemony was their navy. Without question, the British Navy was the best the world had ever seen. However, "the Americans were so poverty-stricken militarily that they could not be made much poorer," so the practicality of blockades was a fruitless endeavor.[91] Without a colonial rebel navy to fight against and because the British did not possess a naval force large enough to prohibit shipments to America from sympathetic countries, the British Navy's strength was all but negated. The strength that the British had enjoyed for many years could not discourage the colonial rebel forces, who were capable of living off the resource-rich landscape and were strengthened by generous allied support.

---

[89] Mao, *Selected Military Writings of Mao Tse-Tung,* 215.

[90] Weigley, *American Way of War,* 27–29.

[91] Ibid., 22.

The usefulness of this historical case study is twofold. The utility of the militias is relatively easily understood in this historical orientation. However, erasing the labels of the protagonist and antagonist from this historical reference could explain the current situation of the USG. The situation represents a conventionally minded America struggling in Iraq and Afghanistan against a seemingly faceless and amorphous collective group of irregular forces like al-Qaeda or ISIS. Likewise, modern-day state-sponsored hackers operating in the shadows appear to represent the colonial rebel forces and America's lethargic modification of its historically successful conventional tactics and strategies represent the British predicament. Failing to adapt historically successful organizational structures, strategies, and tactics to contemporary gray zone challenges will limit the capacity of the USG to handle threats from cyber space.

Examining the case study of the colonial rebels is meant to identify the force multiplying capacity and utility of a mobilized population when conventional forces are limited by their resources. In Poland, military forces and volunteers are mobilizing to repel the recent hybrid threats from Russia. Poland's Territorial Defense Forces play an integral role in complementing its nation's standing army in its effort to counter Russian hybrid threats.

B. POLAND'S TERRITORIAL DEFENSE FORCES

Poland has enjoyed a long tradition of using its whole society against adversaries. Beginning late in the 18th century and for a subsequent 123 years, Poland was without its sovereignty.[92] In the face of overwhelming aggression by larger nation states such as USSR, its population mobilized under the banner of resistance movements. Utilizing their pre-existing knowledge of the local terrain and conducting reconnaissance operations against the enemy, the resistance proved to be a tremendous resource in recapturing Polish sovereignty. A senior GROM officer acknowledged that "the defining characteristic of the Polish people is to resist; resistance is our national heritage."[93] This tradition is now being revived in the face of Russian aggression.

---

92 *Warsaw Rising* (multimedia site), accessed December 1, 2016. http://www.warsawrising.eu/?chapter=1.

93 Empirical data from CENETIX exercise, 2016.

During World War II, "most elements of resistance to the German regime organized under the banner of the Home Army (Armia Krajowa). …The Home Army became one of the largest and most effective underground movements of World War II. Commanding broad popular support, it functioned both as a guerrilla force, conducting a vigorous campaign of sabotage and intelligence gathering, and as a means of social defense against the invaders."[94] Ensuing violence and instability in the years following World War II, looked to destabilize the state. However, in 1999, Poland joined NATO and affirmed its independence.[95] Familiar with the benefits of the resistance and recognizing its utility in the face of hybrid threats from Russia, the Territorial Defense Forces role in the Ministry of National Defense has recently been re-evaluated. The results allocate increased funding of TDF equipment and training in order to better support their internal TDF and external Polish armed units.[96]

Polish Defense Minister Antoni Macierewicz stated that the TDF developments are aimed at renovating the training regimen of the Polish "civilian volunteers to form a National Guard-style paramilitary force aimed at preparing for a 'hybrid war' with Russia."[97] The TDF force, which is aspiring to reach 53,000 by 2019, will be trained by both active and retired members of the Poland's GROM, 1st Special Regiment. The percentage of GROM special forces personnel currently within the ranks of the TDF is approximately 10%.[98] This significant percentage of special forces representation in the TDF, speaks volumes for its utility in the overcoming Poland's gray zone challenges.

---

[94] InfoPoland, "Poland – The Historical Setting," SUNY Buffalo, accessed on December 1, 2016. http://info-poland.buffalo.edu/classroom/longhist5.html.

[95] Jane Perlez, "Expanding Alliance: The Overview; Poland, Hungary and the Czechs Join NATO," *New York Times*, March 13, 1999. http://www.nytimes.com/1999/03/13/world/expanding-alliance-the-overview-poland-hungary-and-the-czechs-join-nato.html.

[96] Empirical data from CENETIX exercise, 2016.

[97] GlobalSecurity.org, "Territorial Defense Forces: Obrony Terytorialnej," accessed on December 1, 2016. http://www.globalsecurity.org/military/world/europe/pl-army-ot.htm.

[98] Empirical evidence observed at CENETIX exercise, May 2016.

Defense Minister Macierwicz stated, "These units are the cheapest way to increase the strength of the armed forces and the defense capabilities of the country."[99] Once operationally capable, each of Poland's 16 regions, beginning on the Eastern front, will receive a brigade size element of volunteers, with the exception of the region surrounding the capital city of Warsaw, which will receive two brigades.[100]

While in support of a May 2016 Naval Postgraduate School's Center for Network Innovation and Experimentation (CENETIX) exercise conducted in Poland, I had the distinct pleasure of working with members of Poland's special forces units and their TDF. I participated in the CENETIX exercise in predominantly a technical support function, as the goal of the project was to verify the practicality of various communications platforms in austere locations. Working predominantly with the Jednostka Wojskowa, who are more commonly known as GROM, Poland's elite special forces operators, I observed how the TDF's unique capabilities were leveraged to benefit the overall operation. Though I will sidestep mentioning specific tactics, training, and procedures (TTPs) to keep this paper unclassified, the TDF effectively prepared and secured the battlefield in a manner which could only be done by individuals who were distinctly familiar with their particular area of operations.

Following the completion of the week-long training exercise, a senior officer from the MOD Bureau of the Territorial Army, conducted his debrief with the TDF. In that meeting was Kami C. Kami is a professional security researcher for a Polish technology company who also represents the regional TDF element as their executive officer. The two men explained to me the disposition of the civilian volunteers; similar to the hackers who volunteered to assist in the Hack the Pentagon program, the force represented all age groups, from high school teenagers to retired teachers who felt a calling to serve their country. Recent transgressions by Russian and rebel forces along the Polish border were the predominant motivating factor for TDF members to have joined the ranks.[101]

---

[99] "Poland to Build Territorial Defense Force by 2019," DW, November 14, 2016. http://www.dw.com/en/poland-to-build-territorial-defense-force-by-2019/a-36386036.

[100] GlobalSecurity.org, "Territorial Defense Forces: Obrony Terytorialnej."

[101] Empirical evidence observed at CENETIX exercise, May 2016.

Kami explained how their TDF leadership had received training from the GROM and an Illinois National Guard unit, which he said was "extremely beneficial in the realm of logistics and organization of a military unit," skills that improved his effectiveness as a leader on the ground.[102] Witnessing the impression senior GROM forces had on the young TDF members was especially memorable.

A senior GROM officer described how the partnership between the GROM and TDF typically worked for major operations. Similar to Nathaniel Greene's forces in the American Revolution, the TDF operated on the periphery of the front lines. The particular exercise I participated in concluded with a direct-action mission on a vehicle of interest (VOI). The TDF effectively prepared and secured the battlefield surrounding the VOI clandestinely, using only a footprint big enough to accomplish the mission but remain undetected as they maintained blocking positions. While some TDF members teased the senior GROM officer that "the TDF had done all the leg work for the training exercise and that the GROM did nothing but jump in and landed on the 'X' to do the fun stuff," the roles of both forces is clearly understood and respected.[103] Colonel Remigiusz Żuchowski, from the Bureau of the Territorial Defense Implementation, further clarifies the TDF's role alongside the main fighting forces of Poland. He classifies, "their role in the security system as the fifth branch of the Polish Armed Forces [next to the Army, Navy, Air Force and Special Forces]."[104]

In an environment such as Poland, where hybrid threats take the form of regular, irregular, cyber, and information, Polish conventional forces, the GROM, and TDF have responded with a unified plan of action that will hopefully secure their boundaries in the face of recent Russian belligerence. The empirical evidence collected in Poland has led me to believe there is a correlation between the utility of the 1st Special Regiment's influence on TDF operations in Poland and the the effects of a similar enterprise between SOCOM and a hacker militia.

---

[102] Ibid.

[103] Ibid.

[104] "The First Polish Conference on the Territorial Defence Forces," Defense Blog, November 24, 2016. http://defence-blog.com/news/the-first-polish-conference-on-the-territorial-defence-forces.html.

C. CONCLUSION

In the American Revolution, British blunders in the predominantly Loyalist South mistreated the citizenry and created a fantastic recruiting opportunity for local militia leaders, whose ranks began to swell with support. Similarly, in 2016, Poland perceived Russian aggression to be imminent. Under threat of hybrid attacks "the idea of resurrecting Poland's territorial defense units [which had been abandoned in 2008] gained traction following Russia's annexation of Crimea and its support for rebels fighting in eastern Ukraine."[105] And in America, in the face of increased cyberattacks, the trend continues. Hacktivists have mobilized to pursue individual initiatives to safeguard vulnerabilities in networks and software, and the Department of Defense announced it had reached its recruitment milestones and achieved initial operating capability of all 133 Cyber Mission Force Teams operating under CYBERCOM.[106]

As such, the timing appears palatable to introduce the idea of a vetted hacker militia to serve in concert with and at the service of the national security apparatus. Witnessing firsthand the benefit of integrating unlikely partners in operational scenarios in Poland with the TDF and GROM, I was encouraged to research the utility of an initiative that would utilize militia forces in a manner that opts for laptops over Kalashnikovs. Observing the progressive relationship between the TDF and GROM, I began to investigate how SOCOM could benefit from a hacker militia.

The mastery of specific computer-based skills and the holistic understanding of working in cyberspace sets qualified hacktivists apart from today's standing armies.[107] These pre-existing skills are extremely difficult to teach, and amid the current crisis, they could be leveraged to complement the national security apparatus's strategy for combatting cyber threats. In his article "Analysis from the Edge: Information Paralysis

---

[105] "Poland Plans Paramilitary Force of 35,000 to Counter Russia," BBC News, June 3, 2016. http://www.bbc.com/news/world-europe-36442848.

[106] U.S. Cyber Command News Release, "All Cyber Mission Force Teams Achieve Initial Operating Capability," Department of Defense, October 24, 2016. http://www.defense.gov/News/Article/Article/984663/all-cyber-mission-force-teams-achieve-initial-operating-capability.

[107] Nicholas R. Dubaz, "Analysis from the Edge: Information Paralysis and Decision Making in Complexity," *CTX Journal* 6, no. 2 (2016): 4.

and Decision Making in Complexity," Nicholas R. Dubaz likens the volunteer groups from the hacker community to "edge organizations…because they operate at the 'edge' of a theoretical command-and-control space that is diametrically opposite to traditional military organizations."[108] Dubaz says they are "uniquely situated to develop understanding, with their unconstrained ability to engage all actors in a system and achieve information superiority."[109] Unfortunately, the organizational construct and bureaucratic processes within the U.S. government and national security apparatus lack such agility.

SOCOM's white paper "The Gray Zone" further underscores the issue; "We struggle when dealing with challenges not fitting neatly into our traditional models. No organization in the U.S. government has primacy for gray zone challenges, so it is unsurprising our responses lack both unity of effort and unity of command."[110] Challenging that assertion, Special Operations Joint Publication 3-05 states, "SOF are selected, trained, and equipped to conduct all forms of IW."[111] Incorporating a vetted hacker militia under the leadership of SOCOM for offensive and defensive operations, may facilitate reciprocal benefits.

A discussion with Dr. Herb Lin, senior research scholar for cyber policy and security at Stanford University, highlighted the parallels between the battlefields in which special operations forces and hackers operate. Both battlefields represent asymmetric environments where conventional, unconventional, cyber, information, and other threats thrive. "Like special operators," notes *National Defense* magazine, "they will be asked to operate across all phases of the campaign. But they will be most valuable at the beginning, when they can shape the strategic environment and dissuade and deter kinetic operations from occurring."[112] Operational and strategic gaps exist that SOF,

---

[108] Ibid., 3.

[109] Ibid., 4.

[110] United States Special Operations Command, "The Gray Zone."

[111] Joint Chiefs of Staff, *Joint Publication 3-05.*

[112] Ibid.

CYBERCOM, and the hacktivist community can work to overcome to improve the overall capacity of all entities.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. MEET THE HACKERS: THE POTENTIAL FOR ENGAGING THE CURRENT CYBER COMMUNITY

> The term "hacker" was initially used for skilled computer enthusiasts that could 'hack' their way through technical problems. Today, hackers pose one of the principal threats against our information infrastructure by exploiting vulnerabilities in code and circumventing security measures. Hacking uses a wide variety of techniques with differing intentions and objectives. And in order for security professionals to protect against this threat, we must assess the security of our networks from the perspective of the hacker.
>
> —Chris Peake, 2003[113]

The volume and severity of cyberattacks by state and non-state actors against the U.S. government, her critical infrastructure, and her financial sectors continue to rise at an alarming rate.[114] Tasking the U.S. military with combatting this new threat may not be the appropriate near- or long-term solution. Consider the genesis of CYBERCOM, which is tasked with the planning, coordination, integration, synchronization, and coordination of offensive and defensive cyber operations, and how it was established on June 23, 2009, decades after the first documented cyberattacks against the United States.[115]

Tapping the military for the solution to cyber threats would be a form of inertial innovation. As James Callard and Peter Faber wrote in their article "An Emerging Synthesis for a New Way of War," "*Inertial innovation* tends to align itself too closely to the lessons learned from the past. It builds on past successes, and either minimizes or ignores the counter-innovations being developed by real or potential adversaries."[116] In short, the accomplishments the military has accrued in the past 15 years of conflict, though commendable, do not necessarily translate into service members having the

---

[113] Chris Peake, "Red Teaming: The Art of Ethical Hacking," Information Security Reading Room, SANS Institute, July 16, 2003.

[114] Department of Homeland Security, *ICS-CERT Monitor*.

[115] U.S. Strategic Command, "U.S. Cyber Command," September 29, 2016. https://www.stratcom.mil/factsheets/2/Cyber_Command/.

[116] James Callard and Peter Faber, "An Emerging Synthesis for a New Way of War," *Georgetown Journal of International Affairs* 3, no.1 (2002), 62.

capacity to confront this new enemy at the current moment in time. CYBERCOM and the combined cyber capabilities of the USG are insufficient for the challenges of cyber offense and defense.

Even if the government were to build a parallel structure with the expertise necessary to try to handle the current threats of cyber warfare, these experts, hamstrung by the limits of bureaucracy and lengthy acquisitions processes, would continuously be playing catchup in their attempt to keep pace with developing threats in the cyber realm. The massive role played by private corporations such as Booz Allen, Science Applications International Corporation, and the scores of other contractors who run and staff USG computer and cyber operations cannot be overstated. However, "Because we are situated precisely at the transition between the industrial and information ages, the ability of organizations to adapt is critical. …How much of a threat or a challenge a particular modernizing military or terrorist group represents depends in large part on its capacity to assimilate new technologies and leverage new capabilities."[117]

Appreciating how the government's bureaucratic protocols inhibit its ability to rapidly respond to expanding cyber threats and the private sector's concerns with increased governmental regulations, the U.S. government instead could utilize the pre-existing skill sets of its citizenry and forge a hacker militia to complement ongoing cybersecurity initiatives. Leaders from the hacker community such as Beau Woods maintain that volunteers have already mobilized against cyber threats and want to extend their knowledge and expertise. Unfortunately, the hacker community lacks the rapport the national security apparatus and private sector currently enjoy. However, positive outcomes from the Hack the Pentagon event in April of 2016 could provide a template for a hacker militia as a complimentary option to ongoing efforts by the government.

In an historic initiative, in line with the administration's Cyber National Action Plan of 2016, the Department of Defense invited "vetted hackers to test the department's cybersecurity under a unique pilot program. The 'Hack the Pentagon' initiative is the first

[117] Goldman and Blanken, "The Economic Foundations of Military Power," 2–12.

cyber bug bounty program in the history of the federal government."[118] The positive results from the program support the hypothesis that unconventional methods, may effectively complement the national security apparatus's ongoing cybersecurity initiatives.

The following will examine popular hacktivist groups such as Anonymous, New World Hackers, Telecomix, and The Cavalry. Objectives and targets of the various groups vary widely, from public safety initiatives to utilizing DDoS attacks to shut down governments who censor social media and the freedom of information.[119] This blurred line of legal and illegal activities that hackers appear to tread so brazenly has contributed to the greater public's negative opinion of the hacker community. This perception stifles necessary dialogue with the hacktivist community that has the potential to be a force multiplier for good. This latent utility could significantly strengthen ongoing national security efforts in the cyber realm.

A. ANONYMOUS, THE NEW WORLD HACKERS, AND TELECOMIX

Arguably the most well-known hacktivist organization of the day, Anonymous, is a "decentralized group of international activist hackers [that] has been linked to numerous high-profile incidents over the years, including internet attacks on governments, major corporations, financial institutions and religious groups."[120] Anonymous does not have a specific leader, and its membership is comprised of individuals from around the globe. Significant cyberattacks for which they have received public admiration include #OpEgypt. This specific hack supported the "Arab Spring uprising specifically in Tunisia and Egypt, to keep access to the Internet open for organizers on the ground."[121] For their

[118] Department of Defense, "Hack the Pentagon" (Press Release No. NR-070-16), accessed July 5, 2016.

[119] W3bsecurity, "Who Is Anonymous and What Is Their Mission?", accessed on October 15, 2016. http://www.w3bsecurity.com/who-is-anonymous-and-what-is-their-mission/.

[120] Geneva Sands, "What to Know about the Worldwide Hacker Group 'Anonymous,'" ABC News, March 19, 2016. http://abcnews.go.com/US/worldwide-hacker-group-anonymous/story?id=37761302.

[121] Ibid.

efforts, *Time* Magazine honored the hacktivist organization with a spot on their Most Influential People: 2012 list.[122]

Anonymous has inspired the creation of other hacktivist groups such as the New World Hackers and Telecomix. New World Hackers consists of a group of 12 hackers who previously took part in Anonymous's #OpParis, the campaign meant to identify and silence ISIS members working on Twitter after the November 13, 2015, Paris massacres. New World Hackers tactics include a DDoS weapon called "the 'BangStresser' tool [which disabled] all of the BBC's websites for a period of several hours in December 2015."[123] This same tactic has since been used to successfully disrupt websites associated with terrorist groups, Presidential campaign webpages, and government websites.

Telecomix is a hacktivist organization with no affiliation to Anonymous, whose members consider themselves "citizens of the Internet" and are a loose-knit group of globally distributed hackers.[124] A *Forbes* article states Telecomix "was created at a Gothenburg conference in 2009 to oppose the European Union's so-called Telecoms Package, industry-influenced laws that would have cut Internet access for anyone repeatedly downloading copyrighted files."[125] While their mission began with the promotion of free speech online, following the Blue Coat discovery, which revealed American technology had been assisting the Syrian government in spying on its people, "it now aims to also expose those who fight against that ideal, including any Western tech firm aiding the wrong side."[126]

From these summations of various hacker groups, it appears all hackers operate under the same supposition as Captain Barbosa, skipper of the *Black Pearl*, who describes the Pirate Code, i.e. the law, "as more what you'd call 'guidelines' than actual

---

[122] Barton Gellman, "The World's 100 Most Influential People: 2012: Anonymous," *TIME*, April 18, 2012. http://content.time.com/time/specials/packages/article/0,28804,2111975_2111976_2112122,00.html.

[123] W3bsecurity, "Who Is Anonymous?"

[124] Andy Greenberg, "Meet Telecomix, the Hackers Bent on Exposing Those Who Censor and Surveil the Internet," *Forbes*, December 26, 2011. http://www.forbes.com/sites/andygreenberg/2011/12/26/meet-telecomix-the-hackers-bent-on-exposing-those-who-censor-and-surveil-the-internet/#cba57231b308.

[125] Ibid.

[126] Ibid.

rules."[127] To further clarify, the interpretation of the law and lawful activities, vary by group and their specific agenda. Unfortunately, the rise in cyberattacks continues to stoke the flames of public aversion towards the hacker community as a whole. However, during my meeting with Beau Woods, deputy director of the Cyber Statecraft Initiative at the Atlantic Council and co-founder of The Cavalry, his position on cybersecurity researchers and hacktivists converted my outlook to a more encouraging estimation of the hacker community at large.

B. I AM THE CAVALRY

The Cavalry identifies itself as a security research organization that operates within the confines of the law.[128] Their mission statement declares that "The Cavalry is a grassroots organization that is focused on issues where computer security intersects public safety and human life. The areas of focus for The Cavalry are medical devices, automobiles, home electronics and public infrastructure."[129] Mr. Woods believes that "our dependence on technology is growing at a rate faster than our ability to safeguard ourselves."[130]

The Cavalry's initiatives include:

- To selectively improve visibility and awareness of these issues while preserving trust.
- To inform decision makers in public policy, manufacturing, oversight, and customer organizations so they take smart risks.
- To collaborate among all stakeholders, deal with concerns, and find a common way forward where everyone wins.
- To catalyze, amplify, and demonstrate public good done by security research of consequence.

---

[127] Gore Verbinski, *Pirates of the Caribbean: The Curse of the Black Pearl* (movie), 2003.

[128] Beau Woods, in interview with the author, September 6, 2016.

[129] "The Cavalry," accessed July 5, 2016. https://www.iamthecavalry.org/.

[130] I am The Cavalry, https://www.iamthecavalry.org/author/bwoods/.

- To promote systems thinking that examines interdependencies and externalities, not just pieces of the whole.[131]

Introducing the above initiatives at hacktivist events such as DEFCON and BSides, Mr. Woods and fellow hackers from The Cavalry have received much support from members within the hacker community. Mr. Woods likens hacktivist values of citizenship and the advancement of individual freedoms to Rousseau's social contract,[132] where "we have a shared ownership and responsibility of these risks with other stakeholders, and want to be proactive. The way forward is collaboration and leadership."[133]

The Cavalry's efforts, foundation, and mission statement appear transparent, legal, and ethical. Their efforts to promote public safety and human life by way of increased understanding and discussion of computer security appear ethically acceptable. A recent experiment by two hacktivists demonstrates the fact cyber researchers are mobilizing on their own to identify vulnerabilities in software and networks, the results of which, appear to be a valuable resource for the country's national security efforts.

According to an article in the *Washington Post*, in July 2015, "security researchers Charlie Miller and Chris Valasek demonstrated that they could hijack a vehicle over the Internet, without any dealership-installed device to ease access. By hacking into a 2014 Jeep Cherokee, the researchers were able to turn the steering wheel, briefly disable the brakes, and shut down the engine."[134] Following the manual ignition of the Jeep Cherokee, conducted by inserting and turning the actual jeep key, the two security researchers "found the vehicle's Internet address and, while sitting in [their] office and typing on a MacBook Pro, hacked in through the Uconnect dashboard information and entertainment system."

---

[131] I am The Cavalry, "Overview of The Cavalry." https://www.iamthecavalry.org/about/overview/.

[132] Beau Woods, in interview with the author.

[133] https://www.iamthecavalry.org/author/bwoods/

[134] Craig Timberg, "Hacks on the Highway," *Washington Post*, July 22, 2015. http://www.washingtonpost.com/sf/business/2015/07/22/hacks-on-the-highway/.

According to the developers of the Controller Area Network (CAN), a CAN bus "is a serial communications protocol which efficiently supports distributed real-time control with a very high level of security. Its domain of application ranges from high-speed networks to low-cost multiplex wiring. In automotive electronics, engine control units, sensors, anti-skid systems, etc. are connected using CAN with bitrates up to 1 Mbit/s. At the same time, it is cost effective to build into vehicle body electronics, e.g., lamp clusters, electric windows etc., to replace the wiring harness otherwise required."[135]

It was this exploitation of the CAN bus that caused "Charlie Miller and Chris Valasek [to grab] headlines last year by showing how they could kill a Jeep Cherokee's engine while it was traveling down a highway. The news prompted an embarrassing recall of 1.4 million Jeeps and other vehicles by parent company Fiat Chrysler."[136] Fortunately, because legislative amendments had been passed to mitigate the legal constraints pertaining to the act of "circumventing access-control measures"[137] in vehicles, Miller and Valasek could safely exploit these vulnerabilities for research and then present their findings to the Auto Alliance. Because communication platforms were accessible in the company, appropriate updates were made and patches created, thwarting future remote hacks of the system.

In a subsequent appraisal of the Auto Alliance's ability to patch the vulnerability, Miller and Valasek attempted to remote hack the Jeep while attending DEFCON 2016. The two security researchers were unable to find a way to do it. Fiat Chrysler argued that it was no longer possible, thanks to the changes they had made after Miller and Valasek's July 2015 hack.[138]

While hacks by Anonymous and New World Hackers grip the nation's attention, grassroots hacktivists like Beau Woods, Charlie Miller, and Chris Valasek are devoting their time and energy to overshadowing the negative opinion of those who hack for evil

---

[135] BOSCH, *CAN Specification: Version 2.0* (Stuttgart, Germany: 1991). http://www.bosch-semiconductors.de/media/ubk_semiconductors/pdf_1/canliteratur/can2spec.pdf, 5.

[136] Timberg, "Hacks on the Highway."

[137] Digital Media Law Project, "Circumventing Copyright Controls," accessed on October 15, 2016. http://www.dmlp.org/legal-guide/circumventing-copyright-controls.

[138] Timberg, "Hacks on the Highway."

purposes. Through engagement, more of these patriotic hacktivists could be cultivated and empowered to bring their pre-existing skill sets to bear to bolster the resources and capacity of the national security apparatus in this "era of digital warfare."[139]

As the number of devices and people connected to the Internet of Things continues to grow at a rapid rate, leaders in the government, private industry, and civilian population have opted for unconventional collaborative methods to battle the emerging cyber threat. Leaders in government, the military, and private industry are recognizing the impacts of cyber intrusions "are more long term than immediate,"[140] and the following initiatives demonstrate proactive efforts being made to counter these threats.

C. BUG BOUNTY

> No organization is so powerful that it does not need outside help identifying security issues, and this includes the Pentagon. Top companies rely on these bug bounty programs to improve their security, like Google, Facebook, Microsoft, Uber, Github, Twitter, Yahoo, and hundreds more. To be the most powerful, you must be open about your vulnerabilities, seek the help of others, and take corrective action quickly.[141]

As described in a *FederalTimes* article, bug bounties operate under "a concept that is relatively simple: An organization incentivizes outside researchers—or white-hat hackers—to test the security of its networks and applications and report what they find so that the organization can address the vulnerabilities."[142] The cost effectiveness and quick turnaround time provide leaders in the private technology industry with a method of identifying vulnerabilities within systems and software.

---

[139] David Rohde, "Digitizing the CIA: John Brennan's Attempt to Lead America's Spies into the Age of Cyberwar," Reuters Investigates, November 2, 2016. http://www.reuters.com/investigates/special-report/usa-cia-brennan/.

[140] McConnell, Chertoff, and Lynn, "China's Cyber Thievery Is National Policy."

[141] Mårten Mickos, "What Was It Like to Hack the Pentagon?", HackerOne, June 17, 2016. https://hackerone.com/blog/hack-the-pentagon-results.

[142] Tom Ruff, "6 Must-Haves for Fed Bug Bounty Programs," *FederalTimes*, October 4, 2016. http://www.federaltimes.com/articles/20-agencies-can-streamline-software-for-savings-says-gao.

The article goes on to say, "The Defense Digital Service (DDS), the Department of Defense's arm of the White House's U.S. Digital Service" decided to "follow in the footsteps of leading technology brands who crowdsource vulnerability discovery and disclosure while ensuring uptime and security."[143] *WIRED* magazine demonstrates the growing utility of crowdsourcing in private industry with the following explanation: "Technological advances in everything from product design software to digital video cameras are breaking down the cost barriers that once separated amateurs from professionals. Hobbyists, part-timers, and dabblers suddenly have a market for their efforts. …The labor isn't always free, but it costs a lot less than paying traditional employees. It's not outsourcing; its crowdsourcing."[144] Nevertheless, as efficient as crowdsourcing appears to be, its ability to provide a long-term solution to identifying and preventing cyber vulnerabilities remains to be seen.

D. HACK THE PENTAGON PROGRAM

According to Clarke and Knake, members of the hacker community meet at various times and locations throughout the country to participate in sponsored hackathons.[145] Describing a hacktivist conference he attended in Las Vegas, Clarke stated that he witnessed "a gathering of 'white hat' or 'ethical' hackers, people who are or work for chief of information officers (CIOs) or chief information security officers (CISOs) at banks, pharmaceutical firms, universities, government agencies, almost every imaginable kind of large (and many medium-sized) company."[146] Individuals or teams would then attempt to expose vulnerabilities in the current software of the day. In order to benefit from these individuals' capacities in the cyber realm, Clarke proposed giving the hackers a means to communicate observed vulnerabilities in a system to the software

[143] Ibid.

[144] Jeff Howe, "The Rise of Crowdsourcing," *WIRED*, June 1, 2006. https://www.wired.com/2006/06/crowds/.

[145] Clarke and Knake, *Cyber War*, 130–133.

[146] Ibid., 128.

company and the government.[147] This progressive foresight was finally realized in April of 2016.

Then Secretary of defense Ash Carter stated that "the Defense Department is investing aggressively in innovation, including in people, practices, and technologies, [and that] the 'Hack the Pentagon' program combined all those elements to 'considerable success'":[148]

> The pilot program was conducted against publicly available websites [defense.gov, dodlive.mil, dvidshub.net, myafn.net, and dimoc.mil], according to Chris Lynch, the director of the Defense Digital Service, the DoD agency that led the program. Mission-critical systems were not involved, he pointed out. He said they were looking for vulnerabilities that would allow someone to gain access to a system through a current user or allow a hacker to maliciously gain access to other networks or other systems.[149]

The DDS director's specific consideration to focus on public websites is consistent with recent threat reporting that identifies how "[hackers] trawl user data in hopes a small target will lead to a big one," according to the *New York Times.*[150]

"The participants in the bug bounty [were] required to register and submit to a background check prior to any involvement with the pilot program. Once vetted, these hackers" participated in a crowdsourcing event that spanned the globe.[151] "The power of a bug bounty program lies in the large number of highly skilled hackers looking at your code. Hackers' reports poured in from 44 states. California was the most active state, with U.S. expat participants based as far away as Japan, Germany, and England."[152]

---

147 Ibid., 129.

148 Lisa Ferdinando, "Carter Announces 'Hack the Pentagon' Program Results," Department of Defense, June 17, 2016, http://www.defense.gov/News/Article/Article/802828/carter-announces-hack-the-pentagon-program-results.

149 Ibid.

150 Perlroth, "Hackers Trawl User Data."

151 Press Operations, "Statement by Pentagon Press Secretary Peter Cook on DOD's 'Hack the Pentagon' Cybersecurity Initiative," Department of Defense, March 2, 2016. http://www.defense.gov/News/News-Releases/News-Release-View/Article/684106/statement-by-pentagon-press-secretary-peter-cook-on-dods-hack-the-pentagon-cybe.

152 Mickos, "What Was It Like?"

According to *FederalTimes*, "the Hack the Pentagon program ran from April 18 through May 12, during which time 252 vetted hackers submitted at least one vulnerability report each, for a total of 1,189 reports. As the hacker reports were submitted, DDS and DMA worked to qualify and remediate each vulnerability in real time with support from HackerOne."[153] HackerOne is a private organization that conducts vulnerability testing for companies. HackerOne CEO noted that "within 13 minutes of launching the first U.S. government commercial bug bounty program, we had our first submission. Just six hours later, that number grew to nearly 200."[154] Notably, the age range of active hackers who reported a vulnerability that warranted a bounty was between 14 and 53, which highlights the broad demographic of those participating and significantly contributing to this crowdsourcing event.[155] The cost effectiveness of this sort of program cannot be overstated. "The total contract value for Hack the Pentagon reports that qualified for the bounty, including the paid-out bounties, was approximately $150,000. In Secretary of Defense Ash Carter's estimation, DoD would have spent more than $1 million uncovering the same vulnerabilities if it had undergone its typical process of hiring an outside firm to conduct a security audit and vulnerability assessment."[156]

With 138 vulnerabilities patched within a month of concluding the program, the Hack the Pentagon program was indeed a major step forward in the Pentagon's efforts to collaborate with hacktivisits.[157] While I acknowledge an extensive system of vetting must be created in order to evaluate future members of the hacker militia, I caution those who are tasked to create such a formula to consider that even the most vetted individuals possess the capacity to breach security protocols. Look no further than the likes of Edward Snowden and former secretary of state and presidential candidate Hillary Clinton to illustrate that point. Accepting the risk of inviting outsiders to collaborate in an

---

[153] Ruff, "6 Must-Haves for Fed Bug Bounty Programs."

[154] Mickos, "What Was It Like?"

[155] Ibid.

[156] Ruff, "6 Must-Haves for Fed Bug Bounty Programs."

[157] Aaron Boyd, "'Hack the Pentagon' Sparks Era of Government Bug Bounties," C4ISRNET, June 20, 2016. http://www.c4isrnet.com/story/military-tech/cyber/2016/06/20/hack-pentagon-sparks-era-government-bug-bounties/86149110/.

unconventional method proved to be a profitable investment for the Pentagon. Unconventional problem-solving initiatives such as the Hack the Pentagon program demonstrated to the U.S. government and others, the force multiplying capacity of vetted hacktivists.

V. RECOMMENDATION/CONCLUSION

A. SUMMARY OF FINDINGS

Realizing how adversaries such as Russia and China utilize cyberwarfare strategy to promote their national agendas is a fundamental first step in recognizing the threats in cyber space. The second critical step is determining proactive initiatives that have the potential to secure American "effective use" in the sphere of cyber space.[158] A Tripwire report on cyberattacks from January 2016 notes, "According to [a 2015 Department of Homeland Security] end-of-year report by the Industrial Control Systems Cybersecurity Emergency Response Team (ICS-CERT), investigators responded to 295 reported incidents involving critical infrastructure in the U.S., compared to 245 in the previous year."[159] With criminal and critical infrastructure cyberattacks thus on the rise, a bold question should be asked: have the number of threats in cyberspace outpaced the resources at the disposal of the national security apparatus? If that is the case, could the integration of unconventional collaborative methods augment the existing resources and capabilities of SOCOM and CYBERCOM in order to preclude future attacks?

As the world becomes more interconnected, private sector vulnerabilities represent a liability towards our national security. Threats to the private or civilian sector from state or non-state actors, presents an exemplary gray zone challenge for the U.S. government. As the efficacy of hacktivists is realized, the utility of these individuals and similarly contracted organizations becomes increasingly obvious. Yet what now is a cost-effective method of conducting penetration testing on systems and software may not always be so. With the IRS launching a bug bounty program like Hack the Pentagon, and with the U.S. Army announcing its intent to "[follow] the Pentagon's lead,"[160] it appears

---

158 Miller, Kuehl, and Lachow, "Cyber War," 20.

159 Maritza Santillan, "ICS-CERT 2015 Report: Critical Infrastructure Sector Sees Spike in Cyber Attacks," *State of Security*, January 20, 2016. https://www.tripwire.com/state-of-security/latest-security-news/insufficiently-architected-networks-to-blame-for-uptick-in-critical-infrastructure-incidents-says-ics-cert/.

160 Aaron Boyd, "IRS Launches First Civilian Agency Bug Bounty Program," *FederalTimes*, November 15, 2016. http://www.federaltimes.com/articles/irs-launches-first-civilian-agency-bug-bounty-program.

time for the U.S. government to leverage its population's existing human capital for national security reasons.

While tech giants Google and Amazon boast the benefits of crowdsourcing on their security webpages, it is not the time to designate an unsubstantiated silver bullet when a 2015 congressional report states that "the United States is ill prepared to defend itself from cyber espionage when its adversary is determined, centrally coordinated, and technically sophisticated, as is the Chinese Communist Party (CCP) and government."[161] Nor is it the time when Russia is subsidizing state-sponsored hackers to promote its national agenda. The same report says that "American companies are being forced to fight a battle against adversaries possessing nation-state capabilities, which is not a fair fight,"[162] "the status quo is no longer acceptable,"[163] and the American people deserve better. Leon Fuerth's article "Cyberpower from the Presidential Perspective" maintains "It will be necessary to have a policy and management system dedicated to cyberpower, but it must also be fully integrated into all other systems that exist for the purpose of sustaining power of the United States and the well being of its citizens."[164] While open source crowdsourcing initiatives should still be leveraged, it would be unwise to rely entirely on this method to respond and defend against cyber threats.

According to The Cavalry's Beau Woods, continuous engagement with the hacker community has the possibility of creating a foundation that cultivates the empowerment of would-be patriotic and ethical hacktivists. Mr. Woods believes that hackers are motivated by "the six Ps; Protector, Puzzler, Profit, Prestige, Politics, and Patriotism."[165] The last of the Ps was specifically underscored in an article written by HackerOne CEO Martin Mickos at the conclusion of the Hack the Pentagon program. Mr. Mickos noted

---

[161] U.S.-China Economic and Security Review Commission, *2015 Annual Report to Congress*, 192.

[162] Ibid., 193.

[163] White House, *Cyberspace Policy Review*, WhiteHouse.gov, May 8, 2009. https://whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf.

[164] Leon Fuerth, "Cyberpower from the Presidential Perspective," in *Cyberpower and National Security*, eds. Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz (Washington, DC: Center for Technology and National Security Policy, National Defense University, 2009), 562.

[165] Beau Woods, in interview with the author.

that "we regularly hear that hackers are driven by the intellectual challenge, rewards, resume building, and improving their skills. This pilot, in particular, highlighted a motivation that is often overlooked: altruism. Time after time, participants shared their desire to contribute to their country's security. The patriotic upswell took even us at HackerOne by surprise, and played a central role in the program's success."[166] Mr. Woods and Mr. Mickos's summations substantiate the militia's critical skill of maintaining the pulse of their community and surging its ranks when threatened by an adversary.

B. APPLICABILITY IN SOCOM: OFFENSE AND DEFENSE

> There is nothing conventional about cyberspace operations, and there is nothing conventional about a cyberwarrior.
>
> — Mårten Mickos, 2016[167]

Increased funding and training from the 1st Special Regiment, GROM, has validated the efforts of Poland's TDF. With similar initiatives in America, vetted hacker militias could improve SOCOM's preparedness of strategic and operational endeavors. While tethered to SOCOM, the hacker militia would keep a pulse on ongoing initiatives and conduct proper risk assessments and training while maintaining enough autonomy so as not to slow the pace of their work. "In order to be agile at the speed of the Net, a big traditional force structure organization is not going to work in cyber or cyberwarrior organizations," said Josh Hartman, former congressional staffer and Defense Department executive. Regarding its relationship with CYBERCOM's cyberspace operations support, Special Operations Publication 3-05 maintains that "Elements provided to SOF units may require additional training or equipment to effectively and safely facilitate cyberspace support during special operations."[168] Retaining hacker militia units under SOCOM

---

[166] Mickos, "What Was It Like?"

[167] Stew Magnuson, "Do Cyberwarriors Belong at Special Operations Command?", *National Defense*, August 2011. http://www.nationaldefensemagazine.org/archive/2011/August/Pages/DoCyberwarriorsBelongatSpecialOperationsCommand.aspx.

[168] Ibid.

could alleviate such time consuming endeavors and improve SOCOM's efficiency in the emerging battle space of the cyber realm.

A RAND publication entitled "The Other Quiet Professionals," stated, "Both SOF and cyber forces are, at their operating core, small teams of highly skilled specialists, and both communities value skilled personnel above all else. Irregular warfare and SOF doctrine lagged operational activities, and the same is true of the cyber force."[169] Through collaboration, SOCOM could take a leadership role in shaping the future of CYBERCOM and the volunteer hacktivist militia. Learning from past mistakes, SOCOM could begin by encouraging initial discourse about cyber threat response and prevention. This sort of convergence would increase the overall efficiency of all parties involved.

Max Strasser's article "Why Ukraine Hasn't Sparked a Big Cyberwar, So Far" explains how the Russian Federation "subcontracts much of its cyberwarfare to nonstate actors."[170] The aforementioned analysis of APT 28 and China's Third and Fourth Departments, lends credence to this statement, and although many major defense contracting firms actively support ongoing national security initiatives of the USG, a hacker militia supports what these contracted companies cannot; a national message of resilience and an adaptive organizational model that could be effectively paired with SOCOM both offensively and defensively. A message of resilience towards cyber threats does not currently exist in our country. A volunteer hacktivist militia supports the message that our country's citizenry is mobilizing to the influx of cyber threats against individuals and critical infrastructure. While I acknowledge there are likely numerous efforts being made behind the scenes, the ability to promote a message of resiliency to the citizens of the United States by the citizens of the United States, has the potential to foster a stronger, more resilient country.

SOCOM's white paper "The Gray Zone" states "centralized government is becoming more expensive and less effective, while the tools available to non-state actors

---

[169] Christopher Paul, Isaac R. Porche III, Elliot Axelband, *The Other Quiet Professionals: Lessons for Future Cyber Forces from the Evolution of Special Forces* (Santa Monica, CA: RAND Corporation, 2014), http://www.rand.org/content/dam/rand/pubs/research_reports/RR700/RR780/RAND_RR780.pdf.

[170] Max Strasser, "Why Ukraine Hasn't Sparked a Big Cyberwar, So Far," *Newsweek*, March 18, 2014. http://europe.newsweek.com/why-ukraine-hasnt-sparked-big-cyberwar-so-far-232175?rm=eu.

are trending the opposite way."[171] Harnessing the skills of our country's talented volunteer hacktivists will complement ongoing national security efforts by bringing all instruments of national power to bear against our enemies. The utility of a hacker militia that augments ongoing SOCOM and CYBERCOM resources and capabilities cannot be overstated. Involvement in Phase Zero preparation of the environment by way of special reconnaissance and improving transition time between multiple targets, similar to current battle space handover procedures, would expedite the national security apparatus' ability to prosecute cyber threats. However, where the hacker militia would realize its true potential was in its convergence with SOCOM. Fully understanding SOCOM's mission and intent is a unique sort of knowledge that the hacker militia could leverage in order to predict future offensive and defensive needs and requirements of SOCOM operators, thereby increasing overall efficiency of their mission.

An article entitled "An Emerging Synthesis for a New Way of War," by James Callard and Peter Faber, underscores the importance of "examining and evaluating an opponent's possible innovations and countermeasures."[172] The aforementioned analysis of Unrestricted Warfare demonstrates the unconventional mindset leaders within the PLA are aggressively exploring. James A. Lewis Simon Hansen's article "China's Emerging Cyberpower: Elite Discourse and Political Aspirations" highlights China's "concern about social volatility is evident in China's discourse on cyberpower."[173] The perceived power cyberspace has to promote China's international standing, has a reciprocal effect domestically, where Chinese leaders recognize the potential cyber space has to cause instability from within its population.

Recognizing these vulnerabilities, the USG should maintain the capacity to exploit those weaknesses when necessary. General Votel's article "Unconventional Warfare in the Gray Zone" referenced methods such as sabotage and subversion that had been effectively utilized by members of historical resistance efforts. These very approaches could be leveraged by a volunteer hacktivist militia against foreign enemies

[171] United States Special Operations Command, "The Gray Zone."

[172] Callard and Faber, "Emerging Synthesis of War," 61.

[173] Lewis and Hansen, "China's Emerging Cyberpower," 9.

who threaten national resources via hybrid warfare in cyber space. General Votel specifically highlights,

> Subversive activities such as mass protests, work slowdowns or stoppages, boycotts, infiltration of government offices, and the formation of front groups. These activities are primarily aimed at undermining the military, economic, psychological, or political strength or morale of the government or occupation authority. …Sabotage can be a means of physically damaging the government's military or industrial production facilities, economic resources, or other targets.[174]

The utility of an integrated hacker militia cannot be overstated. Under the banner of SOCOM, mission specific hacktivist militias would have the unique appreciation and understanding of the direction the SOF community was headed, which would allow the hacktivists to preemptively converge their assets and knowledge with ongoing USG efforts. Callard and Faber's article states, "A better means used alone will not prevail over multiple means used together."[175]

Programs such as Hack the Pentagon, HackerOne, and I am the Cavalry represent opportunities for the national security apparatus to increase its scope in both resources and capacity to defend appropriately to cyberattacks. Safeguarding SOCOM's commercially procured communications equipment is paramount. Special Operations Joint Publication 3-05 states, "SOF communications systems must leverage national cyberspace capabilities, systems and services to the maximum extent possible."[176] This passage in Joint Publication 3-05 references CYBERCOM as the supporting element. However, resources and capabilities are limited with their 133 Cyber Mission Force units. Vetted hacktivists in the form of a hacker militia possess the latent force multiplier capacity that, if coordinated properly under the direction of SOCOM, could augment ongoing efforts by the national security apparatus to defend against cyber threats.

Dr. Dorothy Denning, distinguished professor at the Naval Postgraduate School, recommended the investigation of practices related to a militia could theoretically

---

[174] Votel et al, "Unconventional Warfare in the Gray Zone," 104.

[175] Callard and Faber, "Emerging Synthesis of War," 63.

[176] Joint Chiefs of Staff, *Joint Publication 3-05*, IV–14.

conduct penetration testing on government systems and software, networks that require the highest security.[177]

In this context, "Red teaming is a process designed to detect network and system vulnerabilities and test security by taking an attacker-like approach to system/network/data access. This process is also called 'ethical hacking' since its ultimate purpose is to enhance security."[178] In order to maximize its effectiveness in penetration testing,

> it must be carried out with the utmost confidentiality [where the] customer sets the scope of the project to specify the area of information to be assessed. Before the Red Team can proceed, several legal considerations must be addressed. The team must have explicit and direct permission to perform the test from the customer. This should also include a waiver of repercussions in the event a disaster should occur in the process of testing.[179]

Enlisting the assistance of hacktivists who possess the mission specific skill sets necessary to augment the aforementioned defensive and offensive activities has the potential to bolster ongoing USG cyber security initiatives. Serving under the coordination and leadership of SOCOM should satisfy the tenets of the Cybersecurity National Action Plan's (CNAP) "long-term strategy to enhance cybersecurity awareness and protections, protect privacy, maintain public safety as well as economic and national security, and empower Americans to take better control of their digital security."[180] Combined with ongoing cybersecurity initiatives, the resources and capabilities provided by volunteer hacktivists will bridge existing strategic and operational gaps between SOCOM and CYBERCOM, thus improving U.S. national security and resiliency.

The findings of this research validate the prospect of creating a hacker militia. Creating such an organization on an experimental basis would demonstrate the potential

---

[177] Peake, "Red Teaming: The Art of Ethical Hacking."

[178] Ibid.

[179] Ibid.

[180] Office of the Press Secretary, "FACT SHEET: Cybersecurity National Action Plan," White House, February 9, 2016. https://www.whitehouse.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan.

of these volunteer hacktivists. Aligning their pre-existing skill sets with the SOCOM community will require an appropriate vetting process, one that has the potential to deter some prospective volunteers. Nevertheless, as history has demonstrated with the colonial rebels of the United States and the Territorial Defense Forces of Poland, when the country is threatened, the population will mobilize. The USG must leverage its existing human capital to increase the overall cyber capacity of its national security entities.

LIST OF REFERENCES

Arquilla, John. “From Blitzkrieg to Bitskrieg: The Military Encounter with Computers,” *Communications of ACM* 54, no. 10 (October 2011): 58–65.

———. “The End of War as We Knew It?,” *Third World Quarterly* 28, no. 2 (2007): 369–386.

Arquilla, John, and David Ronfeldt. *Swarming and the Future of Conflict*. Santa Monica, CA: RAND Corporation, 2000.

Axberg, Stefan, and Jan Foghelin. *Perspective on Military Technology.* Sweden: Royal Swedish Academy of War Sciences, 2006.

Barragan, Bianca. “The Worst Day and Time to Drive on Every Los Angeles Freeway.” Curbed LA, August 27, 2015. http://la.curbed.com/2015/8/27/9926230/worst-freeways-traffic-los-angeles.

BBC News. “Poland Plans Paramilitary Force of 35,000 to Counter Russia.” June 3, 2016. http://www.bbc.com/news/world-europe-36442848.

Berman, Ilan, and Rich Harrison, eds. *Defense Dossier* 4 (August 2012).

Biddle, Sam. “How to Destroy the Internet.” Gizmodo, May 23, 2012. http://gizmodo.com/5912383/how-to-destroy-the-internet.

Biddle, Tami. *Strategy and Grand Strategy: What Students and Practitioners Need to Know*. Carlisle, Pennsylvania: Monograph, United States Army War College Press, 2015.

Bishop, Matt, and Emily Goldman. “The Strategy and Tactics of Information Warfare.” *Contemporary Security Policy* 24, no. 1 (2003).

Blanken, Leo J., and Jason J Lepore. “Slowing Down to Keep the Lead in Military Technology.” *Defence and Peace Economics* 22, no. 3 (2011): 317, doi: 10.1080/10242694.2010.491675.

Blinken, Antony J. “The Hunt for Weapons of Mass Destruction: Leveraging New Technology.” Innovation Forum workshop, Stanford University, 2016.

Bort, Julie. “Google Paid $50,000 to Hackers Who Found Some Really Bad Holes on Cloud,” *Business Insider*, December 31, 2014.

BOSCH. *CAN Specification: Version 2.0.* Stuttgart, Germany: 1991. http://www.bosch-semiconductors.de/media/ubk_semiconductors/pdf_1/canliteratur/can2spec.pdf.

Boyd, Aaron. "'Hack the Pentagon' Sparks Era of Government Bug Bounties." C4ISRNET, June 20, 2016, http://www.c4isrnet.com/story/military-tech/cyber/2016/06/20/hack-pentagon-sparks-era-government-bug-bounties/86149110/.

———. "IRS Launches First Civilian Agency Bug Bounty Program." *FederalTimes*, November 15, 2016, http://www.federaltimes.com/articles/irs-launches-first-civilian-agency-bug-bounty-program.

Butler, Matt. "Rapid Delivery of Cyber Capabilities: Evaluation of the Requirement for a Rapid Cyber Acquisition Process." Graduate research project, Air Force Institute of Technology, 2012.

Callard, James, and Peter Faber. "An Emerging Synthesis for a New Way of War." *Georgetown Journal of International Affairs* 3, no. 1 (2002).

Chang, Amy. *Warring State: China's Cybersecurity Strategy*. Washington, DC: Center for a New American Security, December 2014.

Christensen, Clayton M. *The Innovator's Dilemma.* New York: Harper Collins, 2003.

Christensen, Clayton M., and Michale E. Raynor. *The Innovator's Solution.* Boston: Harvard Business School Press, 2003.

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

Clapper, James R. *Worldwide Threat Assessment of the U.S. Intelligence Community*. Statement for the record, Tysons Corner, VA, January 29, 2014.

Coffman, Sean R., Givens, Jeffrey, Shumaker, Robert. "Perception Is Reality: Special Operations Forces in the Gray Zone." Master's thesis, Naval Postgraduate School, 2016.

Davis, Zachary, Frank Gaç, and Michael Nacht, with Joey L. Ching. "Strategic Latency and Warning: Private Sector Perspectives on Current Intelligence Challenges in Science and Technology." Report of the expert advisory panel workshop, Lawrence Livermore National Laboratory, Livermore, CA, January 8, 2016.

Davis, Zachary, Michael Nacht, and Ronald Lehman, eds. *Strategic Latency and World Power: How Technology Is Changing Our Concepts of Security*. Livermore, CA: Lawrence Livermore National Laboratory, 2014.

Defence Blog. "The First Polish Conference on the Territorial Defence Forces." November 24, 2016, http://defence-blog.com/news/the-first-polish-conference-on-the-territorial-defence-forces.html.

Defense Innovation Marketplace. “Defense Innovation Initiative.” Accessed September 8, 2016, http://www.defenseinnovationmarketplace.mil/DII_Defense_Innovation_Initiative.html.

Department of Defense. “Hack the Pentagon,” Press Release No. NR-070-16, accessed July 5, 2016.

———. *The Department of Defense Cyber Strategy*. Arlington, Virginia: Pentagon, April 2015.

Department of Homeland Security. “Incident Response Activity.” *ICS-CERT Monitor* (May/June 2015). https://ics-cert.us-cert.gov/sites/default/files/Monitors/ICS-CERT_Monitor_May-Jun2015.pdf

Digital Media Law Project. “Circumventing Copyright Controls.” Accessed October 15, 2016, http://www.dmlp.org/legal-guide/circumventing-copyright-controls.

Dubaz, Nicholas R. “Analysis from the Edge: Information Paralysis and Decision Making in Complexity.” *CTX Journal* 6, no. 2 (2016).

DW. “Poland to Build Territorial Defense Force by 2019,” November 14, 2016, http://www.dw.com/en/poland-to-build-territorial-defense-force-by-2019/a-36386036.

Earle, Edward Mead, “Adam Smith, Alexander Hamilton, and Friedrich List: The Economic Foundations of Military Power” in Peter Paret, ed., *Makers of Modern Strategy: From Machiavelli to the Nuclear Age* (Princeton: Princeton University Press, 1986).

Edwards, Haley Sweetland, and Matt Vella. “A Shocking Internet Attack Shows America’s Vulnerability.” *TIME*, October 27, 2016, http://time.com/4547329/a-shocking-internet-attack-shows-americas-vulnerability/.

Entous, Adam, Ellen Nakashima, and Greg Miller. “Secret CIA Assessment Says Russia Was Trying to Help Trump Win White House.” *Washington Post*, December 9, 2016, https://www.washingtonpost.com/world/national-security/obama-orders-review-of-russian-hacking-during-presidential-campaign/2016/12/09/31d6b300-be2a-11e6-94ac-3d324840106c_story.html?utm_term=.323e1594995f .

Everton, Sean F. *Disrupting Dark Networks.* New York: Cambridge University Press, 2012.

Ferdinando, Lisa. “Carter Announces ‘Hack the Pentagon’ Program Results.” Department of Defense, June 17, 2016, http://www.defense.gov/News/Article/Article/802828/carter-announces-hack-the-pentagon-program-results.

Fire Eye. *APT28*: *A Window into Russia's Cyber Espionage Operations?* Accessed December 14, 2016. https://www.fireye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-apt28.pdf.

Fischer, David Hacket. *Washington's Crossing.* Oxford: Oxford University Press, 2004.

Fuerth, Leon. "Cyberpower from the Presidential Perspective." In *Cyberpower and National Security*, edited by Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz, 557–562. Washington, DC: Center for Technology and National Security Policy, National Defense University, 2009.

Galeotti, Mark. "The 'Gerasimov Doctrine' and Russian Non-Linear War." *In Moscow's Shadows,* July 6, 2014, https://inmoscowsshadows.wordpress.com/2014/07/06/the-gerasimov-doctrine-and-russian-non-linear-war/.

Gavra, Daniel V. "Militias: Exploring Alternative Force Structures for National Defense." Master's thesis, Naval Post Graduate School, June 2014.

Geers, Kenneth, ed. *Cyber War in Perspective*: *Russian Aggression against Ukraine*. Tallinn, Estonia: NATO Cooperative Cyber Defense Centre of Excellence, 2015.

Gellman, Barton. "The World's 100 Most Influential People: 2012: Anonymous." *TIME,* April 18, 2012, http://content.time.com/time/specials/packages/article/0,28804,2111975_2111976_2112122,00.html.

George, Alexander L., and Andrew Bennett. *Case Studies and Theory Development in the Social Sciences.* Cambridge, MA: MIT Press, 2005.

GlobalSecurity.org. "Territorial Defense Forces: Obrony Terytorialnej." Accessed December 1, 2016, http://www.globalsecurity.org/military/world/europe/pl-army-ot.htm.

Goldman, Emily O., and Leo J. Blanken. "The Economic Foundations of Military Power." Working paper, University of California-Davis, 2016.

Goodrich, Jimmy. "Chinese Civilian Cybersecurity: Stakeholders, Strategies, and Policy." In *China and Cybersecurity: Political, Economic, and Strategic Dimensions*, 5–7. Report from IGCC workshop on China and cybersecurity, UC San Diego, April 2012.

Greenberg, Andy. "Meet Telecomix, the Hackers Bent on Exposing Those Who Censor and Surveil the Internet." *Forbes,* December 26, 2011. http://www.forbes.com/sites/andygreenberg/2011/12/26/meet-telecomix-the-hackers-bent-on-exposing-those-who-censor-and-surveil-the-internet/#cba57231b308.

Howe, Jeff. “The Rise of Crowdsourcing.” *WIRED*, June 1, 2006, https://www.wired.com/2006/06/crowds/.

I am the Cavalry. “Overview of The Cavalry,” accessed July 5, 2016. https://www.iamthecavalry.org/about/overview/.

InfoPoland. “Poland – The Historical Setting.” SUNY Buffalo. Accessed December 1, 2016. http://info-poland.buffalo.edu/classroom/longhist5.html.

Internet Crime Complaint Center. *2015 Internet Crime Report.* Federal Bureau of Investigation, 2015.

Joint Chiefs of Staff. *Joint Publication 3-05, Special Operations*. Arlington, Virginia: Pentagon, July 16, 2014.

Knorr, Klaus. *The Power of Nations.* New York: Basic Books, 1975.

Kramer, Franklin D., Stuart H. Starr, and Larry K. Wentz. *Cyberpower and National Security*. Washington, DC: National Defense University Press, 2009.

Krekel, Bryan, Patton Adams, and George Bakos. *Occupying the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage.* Northrop Grumman, March 2012.

Kwong, Jeffrey. “State Use of Nationalist Cyber Attacks as Credible Signals in Crisis Bargaining.” In *China and Cybersecurity: Political, Economic, and Strategic Dimensions*, 30–33. Report from IGCC workshop on China and cybersecurity, UC San Diego, April 2012, 31.

Lee, Doowan. “Resistance Dynamics and Social Movement Theory.” Working paper, Naval Postgraduate School, 2015.

Lewis, James A., and Simon Hansen. “China’s Emerging Cyberpower: Elite Discourse and Political Aspirations.” Special report, Australian Strategic Policy Institute, International Cyber Policy Centre, Canberra, Australian Capital Territory, November 2014. https://www.aspi.org.au/publications/chinas-cyberpower-international-and-domestic-priorities/SR74_China_cyberpower.pdf.

Liang, Qiao, and Wang Xiangsui. *Unrestricted Warfare: China’s Master Plan to Destroy America.* Panama City: Pan American Publishing, 2002.

Lothringer, Derek W., Matthew S. McGraw, Matthew D. Rautio, and Leif Thaxton. “Counterproliferation, Disruptive Innovation, and the Need to Improve Collaboration.” Master’s thesis, Naval Postgraduate School, 2015.

Magnuson, Stew. “Do Cyberwarriors Belong at Special Operations Command?” *National Defense*, August 2011, http://www.nationaldefensemagazine.org/archive/2011/August/Pages/DoCyberwarriorsBelongatSpecialOperationsCommand.aspx.

McAdam, Doug. *Political Process and the Development of Black Insurgency, 1930–1970*. Chicago: University of Chicago Press, 1982.

McConnell, Mike, Michael Chertoff, and William Lynn. “China's Cyber Thievery Is National Policy—and Must Be Challenged.” *Wall Street Journal*, January 27, 2012. http://www.wsj.com/articles/SB10001424052970203718504577178832338032176.

McRaven, William H. *Spec Ops: Case Studies in Special Operations Warfare – Theory and Practice*. New York: Presidio, 2011.

Mickos, Mårten. “What Was It Like to Hack the Pentagon?” HackerOne, June 17, 2016. https://hackerone.com/blog/hack-the-pentagon-results.

Miller, Robert, Daniel T. Kuehl, and Irving Lachow. “Cyber War: Issues in Attack and Defense.” *Joint Force Quarterly*, no. 61 (2nd quarter 2011).

Miller, Zeke J. “U.S. Sanctions North Korea over Sony Hack.” *TIME*, January 2, 2015. http://time.com/3652479/sony-hack-north-korea-the-interview-obama-sanctions/.

MooresLaw.org. “Moore’s Law.” Accessed March 15, 2016. http://www.mooreslaw.org/.

Morgan, Jacob. “A Simple Explanation of ‘the Internet of Things.’” *Forbes*, May 13, 2014. http://www.forbes.com/sites/jacobmorgan/2014/05/13/simple-explanation-internet-things-that-anyone-can-understand/#158dadb86828.

Nakashima, Ellen. “Hacks of OPM Databases Compromised 22.1 Million People, Federal Authorities Say.” *Washington Post*, July 9, 2015. https://www.washingtonpost.com/news/federal-eye/wp/2015/07/09/hack-of-security-clearance-system-affected-21-5-million-people-federal-authorities-say/?utm_term=.21b99f519a06.

Narizny, Kevin. *The Political Economy of Grand Strategy*. Ithaca, NY: Cornell University Press, 2007.

NATO. “What Is Nato?” Accessed December 1, 2016. www.nato.int/nato-welcome/index.html.

Office of Public Affairs. “U.S. Charges Five Chinese Military Hackers for Cyber Espionage against U.S. Corporations and a Labor Organization for Commercial Advantage.” Department of Justice, May 19, 2014. https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor.

Office of the Press Secretary. “FACT SHEET: Cybersecurity National Action Plan.” White House, February 9, 2016, https://www.whitehouse.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan.

Paret, Peter, ed. *Makers of Modern Strategy: From Machiavelli to the Nuclear Age.* Princeton: Princeton University Press, 1986.

Paul, Christopher, Isaac R. Porche III, and Elliot Axelband. *The Other Quiet Professionals: Lessons for Future Cyber Forces from the Evolution of Special Forces.* Santa Monica, CA: RAND Corporation, 2014. http://www.rand.org/content/dam/rand/pubs/research_reports/RR700/RR780/RAND_RR780.pdf.

Peake, Chris. “Red Teaming: The Art of Ethical Hacking.” Information Security Reading Room, SANS Institute, July 16, 2003.

Perlez, Jane. “Expanding Alliance: The Overview; Poland, Hungary and the Czechs Join NATO.” *New York Times,* March 13, 1999. http://www.nytimes.com/1999/03/13/world/expanding-alliance-the-overview-poland-hungary-and-the-czechs-join-nato.html.

Perlroth, Nicole. “Hackers Trawl User Data in Hopes a Small Target Will Lead to a Big One.” *New York Times,* September 23, 2016. http://www.nytimes.com/2016/09/24/technology/hackers-trawl-user-data-in-hopes-a-small-target-will-lead-to-a-big-one.html?_r=0.

Press Operations. “Statement by Pentagon Press Secretary Peter Cook on DOD’s ‘Hack the Pentagon’ Cybersecurity Initiative.” Department of Defense, March 2, 2016. http://www.defense.gov/News/News-Releases/News-Release-View/Article/684106/statement-by-pentagon-press-secretary-peter-cook-on-dods-hack-the-pentagon-cybe.

Rainie, Lee, Janna Anderson, and Jennifer Connolly. “Cyber Attacks Likely to Increase.” Pew Research Center, October 29, 2014. http://www.pewinternet.org/2014/10/29/cyber-attacks-likely-to-increase/.

Raud, Mikk. *China and Cyber: Attitudes, Strategies, Organisation.* Tallinn, Estonia: NATO Cooperative Cyber Defence Centre of Excellence, 2016.

Rohde, David. “Digitizing the CIA: John Brennan’s Attempt to Lead America’s Spies into the Age of Cyberwar.” Reuters Investigates, November 2, 2016. http://www.reuters.com/investigates/special-report/usa-cia-brennan/.

Ruff, Tom. “6 Must-Haves for Fed Bug Bounty Programs.” *FederalTimes*, October 4, 2016. http://www.federaltimes.com/articles/20-agencies-can-streamline-software-for-savings-says-gao.

Sands, Geneva. “What to Know about the Worldwide Hacker Group ‘Anonymous.’” ABC News, March 19, 2016. http://abcnews.go.com/US/worldwide-hacker-group-anonymous/story?id=37761302.

Santillan, Maritza. “ICS-CERT 2015 Report: Critical Infrastructure Sector Sees Spike in Cyber Attacks.” *State of Security*, January 20, 2016. https://www.tripwire.com/state-of-security/latest-security-news/insufficiently-architected-networks-to-blame-for-uptick-in-critical-infrastructure-incidents-says-ics-cert/.

Sharma, Deepak. “Integrated Network Electronic Warfare: China’s New Concept of Information Warfare.” *Journal of Defense Studies* 4, no. 2 (2010): 37. www.idsa.in/system/files/jds_4_2_dsharma.pdf.

Sheehan, John. “Masters of War.” Lecture, Naval Postgraduate School, Monterey, CA, July 7, 2016.

Singer, P.W. Corporate Warriors: The Rise of the Privatized Military Industry. Second edition. Ithaca, NY: Cornell University Press, 2007.

Soc.mil. “SOF Truths.” Accessed February 7, 2016. http://www.soc.mil/USASOCHQ/SOFTruths.html.

Smith, David J. “How Russia Harnesses Cyberwarfare.” *Defense Dossier* 4 (August 2012): 7.

Strasser, Max. “Why Ukraine Hasn’t Sparked a Big Cyberwar, So Far.” *Newsweek*, March 18, 2014. http://europe.newsweek.com/why-ukraine-hasnt-sparked-big-cyberwar-so-far-232175?rm=eu.

Sulmeyer, Michael, and Peter Roady. “Simplifying Cybersecurity.” *Hill*, February 26, 2016.

Terry C. Pierce. *Warfighting and Disruptive Technologies: Disguising Innovation.* London: Frank Cass, 2004.

Thomas, Timothy. “Nation-State Cyber Strategies: Examples from China and Russia.” In *Cyberpower and National Security*, edited by Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz. Washington, DC: Center for Technology and National Security Policy, National Defense University, 2009.

Thomson, Janice E. *Mercenaries, Pirates, And Sovereigns*. Princeton: Princeton University Press, 1996.

Timberg, Craig. “Hacks on the Highway.” *Washington Post*, July 22, 2015. http://www.washingtonpost.com/sf/business/2015/07/22/hacks-on-the-highway/.

Tse-Tung, Mao. *Selected Military Writings of Mao Tse-Tung.* Peking: Foreign Language Press, 1967.

U.S. Cyber Command News Release. “All Cyber Mission Force Teams Achieve Initial Operating Capability.” Department of Defense, October 24, 2016. http://www.defense.gov/News/Article/Article/984663/all-cyber-mission-force-teams-achieve-initial-operating-capability.

U.S.-China Economic and Security Review Commission. *2015 Annual Report to Congress of the U.S.-China Economic and Security Review Commission.* Washington, DC: U.S. Government Publishing Office, November 2015.

U.S. Special Operations Command. “The Gray Zone.” White paper, September 9, 2015.Unwala, Azhar, and Shaheen Ghori. “Brandishing the Cybered Bear: Information War and the Russia-Ukraine Conflict.” *Military Cyber Affairs* 1, no. 1 (2015): article 7.

U.S. Strategic Command. “U.S. Cyber Command,” accessed July 5, 2016. https://www.stratcom.mil/factsheets/2/Cyber_Command/.

Votel, Joseph L., Charles T. Cleveland, Charles T. Connett, and Will Irwin. “Unconventional Warfare in the Gray Zone.” *Joint Force Quarterly* 80 (1st quarter 2016).

Warsaw Rising. Multimedia site. Accessed December 1, 2016. http://www.warsawrising.eu/?chapter=1.

W3bsecurity. “Who Is Anonymous and What Is Their Mission?” Accessed on October 15, 2016. http://www.w3bsecurity.com/who-is-anonymous-and-what-is-their-mission/.

Weick, Karl E., and Kathleen M. Sutcliffe. *Managing the Unexpected: Assuring High Performance in an Age of Complexity.* San Francisco: Jossey-Bass, 2001.

Weigley, Russell F. *The American Way of War.* Bloomington: Indiana University Press, 1973.

White House. *Cyberspace Policy Review*. WhiteHouse.gov, May 8, 2009. https://whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf.

Wirtz, James J. “Cyber War and Strategic Culture: The Russian Integration of Cyber Power into Grand Strategy.” In *Cyber War in Perspective: Russian Aggression against Ukraine*, edited by Kenneth Geers, 29–36. Tallinn, Estonia: NATO Cooperative Cyber Defense Centre of Excellence, 2015.

Wortzel, Larry M. “Assessing the Chinese Cyber Threat.” *Defense Dossier* 4 (August 2012).

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California