REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
20-04-2018	Master's Thesis	Aug 2017 - Apr 2018

4. TITLE AND SUBTITLE
Cyber Deterrence:
The Wrong Question for the Wrong Problem

5a. CONTRACT NUMBER
N/A

5b. GRANT NUMBER
N/A

5c. PROGRAM ELEMENT NUMBER
N/A

6. AUTHOR(S)
CHARLES A. DEHOAG, GS-14, DOD

5d. PROJECT NUMBER
N/A

5e. TASK NUMBER
N/A

5f. WORK UNIT NUMBER
N/A

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Joint Advanced Warfighting School
Joint Forces Staff College
7800 Hampton Blvd
Norfolk, VA 23511

8. PERFORMING ORGANIZATION REPORT NUMBER
N/A

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
Joint Forces Staff College
7800 Hampton Blvd
Norfolk, VA 23511

10. SPONSOR/MONITOR'S ACRONYM(S)
JFSC

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

12. DISTRIBUTION/AVAILABILITY STATEMENT
N/A
Approved for public release, distribution is unlimited.

13. SUPPLEMENTARY NOTES
N/A

14. ABSTRACT

The United States has struggled with a comprehensive approach to theory, policy, and strategy in the cyber domain for more than twenty years. This has led to general misunderstanding of some of the nuances of the domain, leaving a theory of deterrence that incorporates activities in cyberspace elusive. Unfortunately, the adversaries and competitors of the United States, the so-called 4+1, appear to be ahead on grasping the intricacies of the domain and the implications for its use in modern warfare. Russia, in particular, has already fought the first armed conflict that incorporated an effective cyber-attack aspect during the 2008 invasion of Georgia. While a number of scholars and thinkers continue to seek a theory of specific deterrence in the cyber domain, this is the wrong way to approach the problem and the wrong idea upon which to expend time, effort, and resources. A comprehensive theory of deterrence that incorporates the cyber domain is needed, rather than a specific theory of deterrence in cyberspace, disconnected from the other domains. A unified theory of deterrence that includes cyber aspects should be agnostic of domain when it comes to the traditional deterrence modes of denial or punishment.

15. SUBJECT TERMS
Cyberspace, Cyber Deterrence, Deterrence, Cyber Operations, Hybrid Warfare, Cyber Security, Cyber Authorities, Cyber Legalities

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Charles A. DeHoag
Unclassified	Unclassified	Unclassified	SAR	47	19b. TELEPHONE NUMBER *(Include area code)* 571-294-7290

NATIONAL DEFENSE UNIVERSITY
JOINT FORCES STAFF COLLEGE

JOINT ADVANCED WARFIGHTING SCHOOL

CYBER DETERRENCE: THE WRONG QUESTION FOR THE WRONG PROBLEM

by

Charles A. DeHoag
U.S. Department of Defense Civilian

CYBER DETERRENCE: THE WRONG QUESTION FOR THE WRONG PROBLEM

by

Charles A. DeHoag

Civilian, U.S. Department of Defense

A paper submitted to the Faculty of the Joint Advanced Warfighting School in partial satisfaction of the requirements of a Master of Science Degree in Joint Campaign Planning and Strategy. The contents of this paper reflect my own personal views and are not necessarily endorsed by the Joint Forces Staff College or the Department of Defense.

This paper is entirely my own work except as documented in footnotes. (or appropriate statement per the Academic Integrity Policy)

Signature: _____

Thesis Advisor: Signature: _____

Robert M. Antis, Ph.D.
Professor, Joint Advanced Warfighting School

Approved by: Signature: _____

Miguel L. Peko, Captain, US Navy
Director, Joint Advanced Warfighting School

ABSTRACT

The United States has struggled with a comprehensive approach to theory, policy, and strategy in the cyber domain for more than twenty years. This has led to general misunderstanding of some of the nuances of the domain, leaving a theory of deterrence that incorporates activities in cyberspace elusive. Unfortunately, the adversaries and competitors of the United States, the so-called 4+1, appear to be ahead on grasping the intricacies of the domain and the implications for its use in modern warfare. Russia, in particular, has already fought the first armed conflict that incorporated an effective cyber-attack aspect during the 2008 invasion of Georgia.

While a number of scholars and thinkers continue to seek a theory of specific deterrence in the cyber domain, this is the wrong way to approach the problem and the wrong idea upon which to expend time, effort, and resources. A comprehensive theory of deterrence that incorporates the cyber domain is needed, rather than a specific theory of deterrence in cyberspace, disconnected from the other domains. A unified theory of deterrence that includes cyber aspects should be agnostic of domain when it comes to the traditional deterrence modes of denial or punishment.

TABLE OF CONTENTS

CHAPTER 1: INTRODUCTION

"The worst of all conditions in which a belligerent can find himself is to be utterly defenseless."[1]

National security leaders, professionals, and scholars should be coming to the realization that in terms of conflict and contest within the cyber domain, the United States of America is arguably in the Clausewitzian "worst of all conditions." For nearly two decades the United States has struggled to formulate a cyber strategy that is cohesive, effective, coherent, and adaptable. One point of failure has been the inability to concentrate the mission, funding, authorities, and responsibility for executing a comprehensive cyber strategy into an accountable agency or office that can actually implement such an endeavor.[2] Portions of this task have fallen to various entities spread across the government spanning services, agencies, offices, and directorates. Despite the citation of cybersecurity as a prominent factor in the both the 2015 and 2017 United States National Security Strategies and the creation of a position on the National Security Staff for an Executive Branch Cybersecurity Coordinator, a fully realized national cyber strategy remains elusive.[3]

A leading reason that effective national cyber strategy has yet to materialize is that the United States Government (USG) has yet to clearly differentiate between activities of sovereign actors in the cyber domain and the activities of cyber criminals.[4] Properly classifying a malign cyber activity is critical for ensuring the correct instruments are engaged to counter it, and to

---

[1] Karl Clausewitz, *On War (Complete Edition)*, Edited by Michael Howard & Peter Paret, (Princeton: Princeton University Press, 1976), 77.

[2] Laurie A. Mulford, *Let Slip the Dogs of (Cyber) War: Progressing Towards a Warfighting U.S. CYBER COMMAND,* Master's Thesis, (National Defense University, 2013).

[3] There is a general paucity of specific direction on a national cyber strategy across the corpus of executive level guidance, including but not limited to *National Security Strategy 2015*, *National Security Strategy 2017,* and *The Comprehensive National Cyber Security Initiative.* Interestingly, there is disagreement even among these meager offerings.

[4] Will Goodman, "Cyber Deterrence Tougher in Theory than in Practice?" *Strategic Studies Quarterly*, (2010): 112.

ensure that any such countering activity is within the bounds of applicable customs, laws and regulations. Although it may at first seem appropriate to simply not differentiate between criminal activity and sovereign activity in the cyber domain, it is important for a liberal democracy to not mix military and police functions without significant reflection, regulation, and oversight.[5] The military defends the nation from enemies of the state. The police protect and serve the people. When the military becomes both, the enemies of the state tend to become the people.[6]

Classifications and definitions have implications for a variety of challenges and problems when it comes to activity in cyberspace. Chief among them, and the focus for this work, are the implications for deterrence in the cyber domain as it relates to the activities of commonly recognized Westphalian states. Without clearly agreed upon classifications by the interagency and international partners and allies, formulation of policy and the strategies to implement policy will continue to be problematic, inefficient, and ineffective. Thankfully, the message appears to be finally gaining some degree of resonance at the highest levels of the USG.

The Senate Armed Service Committee Engages

Beginning in earnest in 2014, Senate Armed Services Committee (SASC) Chair John McCain (R-AZ) has repeatedly asked both Obama and Trump administration senior military leaders for a cyber deterrence strategy.[7] While the SASC may not fully understand the intricacies

[5] One of the nuances of highly proficient cyber activity is the blurring of the lines between criminal and sovereign military actions. The author recognizes this, and recognizes that the intersection of capacity, capability, and authorities can create quandaries as to how to respond to "gray" cyber activity. Nevertheless, in a liberal democracy, it is imperative that meaningful reflection occurs before utilizing the military to solve even quasi-law enforcement problems.

[6] Quoted from an episode of the re-imagined American science fiction / political drama "Battlestar Galactica". In Season 1, Episode 3, which first aired 01 November 2004. A focus of the episode was on the separation of police and military powers, authorities, and appropriateness of use.

[7] Space Foundation, "Senate Armed Services Committee Interested in Cyber Deterrence Strategy," February 28, 2014, https://www.spacefoundation.org/news/senate-armed-services-committee-interested-cyber-deterrence-strategy (accessed January 01, 2018).

of the cyber domain (as evidenced by questions such as to whether we can simply turn the internet off in discrete areas), its members and the Chairman do recognize that cyberattacks have tangible, potentially strategic effects and that America appears to be vulnerable.[8]

Unfortunately, no specific policy for what the USG wants to accomplish or deter within the cyber domain presently exists upon which to build a strategy, leading to the less-than-optimal outcome of policy created by way of strategy, rather than the preferred reverse. Speaking before the SASC, Admiral Michael Rogers, dual hatted as the Director of the National Security Agency (NSA) and the commander of U.S. Cyber Command (USCYBERCOM) as of this writing, attempted to bridge this policy/strategy gap by laying out a capabilities-based approach to cyber, targeted against the 4+1, and recognizing "gray zone" activity that would put US interests at risk but below the traditional threshold for war.[9] In essence, Admiral Rogers diplomatically informed the SASC that the Department of Defense (DoD) is operating in the dark when it comes to policy, so any strategy presented for cyber activities, cyber security, or cyber deterrence are essentially straw men.

Executive Order and National Defense Authorization Act of 2017

Whether this message got through or some other factor or combinations of factors came to bear is neither clear nor particularly relevant, but in May of 2017, the USG produced an executive level document from which a policy can be gleaned: The Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure (henceforth

[8] Interpreted by the author from various exchanges among the members of the Senate Committee on Armed Services and Admiral Michael S. Rogers, Commander, U.S. Cyber Command, during ADM Rogers' testimony before the Committee on 09 MAY 2017.

[9] The 4+1 is a reference to Russia, China, North Korea, Iran as the "4" and violent extremist organizations (VEOs) as the +1. The VEOs are lumped conveniently, if perhaps inelegantly, together.

referred to as the EO Cybersecurity).[10] The policy exhibits some flaws which will be discussed as a part of a later analysis, but securing a policy at least enables the authoring of useful and relevant strategies.

This also allows the Department of Defense to finally proffer a cyber deterrence strategy, first required of it in the National Defense Authorization Act of 2017. Complications abound here as well. Cyber is rapidly evolving. There are few common ground rules for cyber, no common lexicon, and no theory of cyber warfare. While the 4+1 adversaries are organizing force structures to exploit the asymmetric advantages that cyber offers them in terms of a confrontation with the United States, America's approach is haphazard, disjointed, and lacks a unity of effort and vision. This is perhaps ironic given that the United States has been the progenitor of many of the most impressive technological achievements of the modern age, but it is also a reflection of the exceptionalism that helps define America's strategic culture.

Ends: Standalone Cyber Deterrence is a Dangerous Myth

Cyberspace may prove to be a great equalizer. Each of the 4+1 adversaries have already manifested the advantages of mastery, or even simple proficiency, within the cyber domain. Russia's cyberattack on Estonia and Georgia, and China's hacking of the USG's Office of Personnel Management are just some of the definitive case studies that highlight the threat presented by losing competitive advantage in cyberspace. It is clear from these examples, and well recognized by American military and political leaders, that the security of the United States

[10] United States Government Publication, *Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure,* https://www.whitehouse.gov/presidential-

can be jeopardized in cyberspace.[11] Addressing this threat is thus vital to the most critical of the national interests, the defense of the homeland. A credible cyber deterrence strategy is a must.

Unfortunately, what a cyber deterrent looks like and how to implement a deterrent is a great source of consternation in the United States, but in fact it should not be. Looking for a cyber deterrent is asking the wrong question about the wrong problem. Just as the country does not need an air deterrent or a land deterrent or a sea deterrent, it also does not need a domain-specific deterrent peculiar to cyberspace. *The need is for a committed, credible, articulated, unified, and fully integrated multi-domain approach to deterrence that includes the cyber domain as an equal domain to the natural, traditional domains and recognizes modern changes in the character of war. A foundation of this multi-domain deterrence should include a provision that hostile cyber activity can be considered an attack upon, or direct threat to, the United States homeland, and could generate a response in any domain or by means of any instrument of national power. A malign cyber activity need not be answered only in cyberspace.*

Ways and Means: Roadmap for the Discussion

Chapter One sets the tone for the continuation of the discussion. The United States appears woefully behind when it comes to understanding the intricacies of the cyber domain, and this folly could lead to disaster. Senior decision and policy makers often ask not-quite right questions when it comes to cyber security policy, which in turn can be interpreted as these same policy makers possessing an incomplete comprehension of the nature of the problem. The concepts of cyber security and cyber deterrence are conflated and/or blurred, even in executive branch policy issuances, further muddying the picture.

[11] Department of Homeland Security, *Cybersecurity Overview*, https://www.dhs.gov/cybersecurity-overview (accessed November 22, 2017).

Chapter 2 explains why the confusion must end. The designated 4+1 adversaries of the United States all demonstrate asymmetric capabilities within cyberspace for which the US has no immediate response. Chapter 2 will show that the 4+1 have seized the initiative and are setting conditions deleterious to US and US ally/partner activities around the world. Russia, in particular, has demonstrated a capability to synchronize multi-domain activities, to include the incorporation of cyber, to achieve strategic effects. Russia's cyber activities in Estonia and Georgia will be reviewed by way of case study, with the conclusion that Estonia was essentially a test bed for the hybrid warfare approach Russia conducted later in Georgia.

Chapter Three provides a review of the May 2017 Executive Order on Cyber from the Trump administration. The analysis will provide additional evidence that the USG must evolve its understanding of cyber and cultivate a richer understanding of the domain and the complex web of implications for deterring malign activity within the domain. The chapter will present a discussion of deterrence theory in general, attempt to draw connections from deterrence theory as it exists to the Executive Order's command to deter in cyberspace, and perhaps elucidate some additional vectors of approach to the problem.

In the final chapter, a synthesis of the policy, ideas, and thoughts presented throughout chapters 1 through 3 will lead to an explanation of why cyber deterrence must not be divorced from a more comprehensive, unified theory of deterrence. A theory of multi-domain deterrence will be presented and explored. Nestled within the overarching theory will be a number of threads that can lead to additional vectors of discourse. While these threads will be mentioned, in some cases they will not be explored due to the confines of the scope of this work. The intention is to spur additional discussion and drive scholarship in the field.

CHAPTER 2: THREATS TO US NATIONAL SECURITY

"To introduce into the philosophy of war a principle of moderation would be an absurdity."[1]

Risk: Our 4+1 Adversaries Have Seized the Initiative

Cyber-attacks are not simply inconveniences that keep people from viewing their favorite social media site or email application. The scope of the cyber threat against the United States is both broad and deep, and the complexity of the threat often seems to evolve at a pace beyond America's ability to grasp. Both state and non-state actors routinely probe DoD computer networks for weaknesses, access, and vulnerabilities. Russia, China, Iran, North Korea, ISIL, and a litany of other violent extremist organizations continue to become increasingly more capable opponents in the cyber domain, and there is no indication that their threat is decreasing.[2]

Unfortunately, there is no paucity of examples for this increasing threat. Likely emanating at the direction of the Russian government, cyberattacks in 2007 brought Estonia back into the dark ages without a single shot fired. A year later, in 2008, Russian cyber actors crippled Georgia by means of a massive distributed denial of service attack, similar in appearance to the Estonia attack but showing signs of refinement. Estonia was likely a dress rehearsal for the invasion of Georgia. Unlike the cyber-attack of Estonia, ground and air strikes began shortly after the cyber-attack against Georgia and the Russians made a military gamble to take back a portion of the former Soviet Union via a very effective hybrid warfare effort.[3] As recently as December 2016, Russia again demonstrated their cyber-attack capabilities by bringing down

---

[1] Karl Clausewitz, *On War (Complete Edition)*, Edited by Michael Howard & Peter Paret, (Princeton: Princeton University Press, 1976), 76.

[2] Richard A. Clarke and Robert K. Knake, *Cyber War: The Next Threat to National Security and What to Do About It* (New York: Harper Collins, 2010), 65-72.

[3] Eurasianet.org, Michael Lambert, *Tracing the Roots of Russia's Hybrid Warfare Tactics,* http://www.eurasianet.org/node/85521 (accessed December 12, 2017).

Ukraine's power grid and inflicting damage to the control systems for the nation's entire electrical grid. "The hackers appear to have been testing the most evolved specimen of grid-sabotaging malware ever observed in the wild." [4]

Russia, of course, is not alone in its malign activity in the cyber domain. There are credible instances of Iranian cyber actors penetrating the defense of a hydroelectric dam in New York State, and who later made various, albeit ineffectual, forays into banking systems across the nation in an attempt to disrupt the US economy. Offended by the portrayal of North Korean leader Kim Jong Un in the movie *The Interview,* North Korea lashed out and successfully breached Sony Studios, the distributor of the film, exposing not only weaknesses in the security apparatus of a major US business, but also the private emails and communications of various studio executives and celebrities. The effects resonated throughout both traditional and social media for some time. ISIL, as well as other violent extremist organizations, continue to use the cyber domain to incite attacks, recruit, transmit disinformation and confusion, and sew discord.[5]

Certainly, DoD maintains a capable, comprehensive cyber security posture, but as can be seen by the wide array of targets discussed above, cyber security is not the unique purview of DoD. Within the United States alone, there are implications for law enforcement, homeland security, business, and industry. American partners and allies are affected as well. Given the degree to which the world has embraced globalization, a ripple in the financial markets in Europe, caused by a malign cyber act, can have repercussions across the entire global economic market. The United States cannot afford to ignore the problem, to delay the formulation of

---

[4] WIRED, Andy Greenberg, *'Crash Override': The Malware that Took Down a Power Grid,* https://www.wired.com/story/crash-override-malware/ (accessed January 1, 2018).

[5] This entire paragraph is a summary taken from: Robert Mandel, *Optimizing Deterrence: A Comprehensive Strategy for Preventing Foreign Cyberattack* (Washington D.C.: Georgetown University Press, 2017).

solutions, or to kick the problem down the road. It also cannot afford for its 4+1 adversaries to obtain, sustain, and improve overmatches in cyber capability lest the US forfeit relevance on the world stage and cease to wield the ability to maintain and shepherd the world order to its benefit and the mutual benefit of its allies and partners.

The 2017 National Security Strategy refers to both China and Russia as revisionist powers.[6] There is an argument to be had, outside the limitations of this work, as to whether this is true. Both Russia and China appear to have successfully mastered the nuance of the current world order through hybrid models of warfare that incorporate cyber as part of a unified warfighting effort, control of the flow and flavor of information, and through savvy exploitation of international legal structures by means of what some call "lawfare".[7] In other words, they seem to have mastered the current world order to the point of being able to manipulate the rules. Activities in the cyber domain are cornerstones to their success in these endeavors, and the United States is lagging behind, not in the sophistication of the technology, but in the sophistication of the understanding of the domain and its utilization.

The United States cannot afford a crisis of relevancy when it comes to advanced technology. Such a condition would be sadly ironic, given the incredible contributions to technology and innovation that the US has made over the course of its history. The United States is the birthplace of flight, the winner of the space race, the harbinger of the nuclear age, and the homeland of personal computing. The United States should not stand befuddled by a new technology, nor by emergent, nuanced, and novel uses of it. It should be leading. The price of falling behind is too high.

---

[6] United States Government Publication, *National Security Strategy 2017.*

[7] Orde S. Kittrie, *Lawfare: Law as a Weapon of War* (New York: Oxford University Press, 2016), 41.

Russia Effortlessly Paralyzes Estonia, a NATO Ally

In early 2007, Estonia was completely overwhelmed by a massive Russian cyber-attack, unprecedented in scale and efficacy. This event has since been dubbed the world's first cyber war. This was the first time the world had seen a politically motivated, sustained cyberattack on a nation's entire electronic infrastructure.[8] Despite being a member of both NATO and the European Union, Estonia was entirely unable to deter aggression in the cyber-domain, and paid a heavy price for its vulnerability.

Although no precise linkage was ever openly announced showing the connections between the attack and the Putin administration, cyber experts agree that this was the work of the Russian government.[9] The historical fault lines between ethnic Russians and their Estonian countryman remained from the annexation of the Baltic States by the Soviet Union in 1940, and the subsequent immigration of hundreds of thousands of ethnic Russians into the region. Estonia believed at the time that the influx of Russians was an attempt by Stalin to inundate his new possessions with loyal followers, a move the people of Estonian largely resented. Unlike its Baltic neighbors of Lithuania and Latvia, Estonia refused to grant immediate citizenship to these Russian immigrants, instead forcing them to go through a lengthy naturalization process. This set the stage for deep seeded ethnic animosity, a powder keg awaiting a spark.

In early 2007, years of tension between ethnic Russians and the rest of the population of Estonia boiled over into heated debates, riots, and general civil disobedience following a sharp increase in bellicose Russian rhetoric towards the European Union, of which Estonia is a

---

[8] The European Institute, Kertu Ruus, *Cyber War I: Estonia Attacked From Rusia,* http://www.europeaninstitute.org/index.php/component/content/article?id=67:cyber-war-i-estonia-attacked-from-russia (accessed November 09, 2017).

[9] WIRED, Joshua Davis, *Hackers Take Down the Most Wired Country in Europe,* https://www.wired.com/2007/08/ff-estonia/ (accessed October 20, 2017).

member, regarding natural gas supplies. Pro-Russian activists, as well as counter protestors, began to gather regularly at a well-known and symbolic landmark, the *Bronze Soldier*. The statue, erected in 1947 following the Soviet liberation of Estonia from Nazi Germany, was seen by pro-Russians as a symbol of the strength and kinship of the Estonian relationship with Russia, and with a sense of gratitude for freeing Estonia from Nazi control. Pro-Estonians, on the other hand, viewed the statue as a symbol of Soviet, now Russian, oppression and menace, and had previously lobbied for demolishing the *Bronze Soldier* as an offense to Estonian national pride and identity.[10]

In the pre-dawn hours of 27 April 2007, the government of Estonia sought what they no doubt believed to be a moderate solution, and removed the *Bronze Soldier* from its prominent location in Tonismagi Park, placing it in the more remote and less accessible Tallinn Military Cemetery. This triggered violent riots, looting, bloodshed, and murder – mostly on the part of ethnic Russians – and led the government of Estonia to respond with water cannons, tear gas, and other aggressive counter measures. Tallinn had descended into chaos.[11]

President Vladimir Putin of the Russian Federation, always a deft hand at the utilization of coercion, propaganda, and political warfare, seized the opportunity firmly. Both he and his foreign minister, Sergei Lavrov, immediately took to the air and framed the situation as an example of Estonian ultra-nationalism, claiming that Estonia had forgotten the sacrifices of Russian soldiers in the battle with Nazi fascism during World War II. They created an environment where the ethnic Russian minority, although woefully misbehaving, was justified in its rage.

---

[10] Robert Mandel, *Optimizing Cyber deterrence* (Washington D.C.: Georgetown University Press, 2017), 76.

[11] Ibid., 78.

As Putin stirred the pot and ethnic Russians hurled Molotov cocktails at government riot police, the Estonian Minster of Defense Jaak Aaviksoo attempted to log in to the Prime Minister's website, but found that he was unable to do so. What the Minister of Defense discovered was that at 2200 on 26 April 2007, a massive distributed denial of service campaign had begun against Estonia's critical infrastructure, which had remained "...relatively unnoticed for the first twenty-four hours."[12] However, by 27 April, a massive attack had paralyzed the nation. Every ministry was offline, as were banks, media outlets, universities, and the prominent political parties. All electronic communication stopped, and Estonia was crippled. Eventually, around the middle of May 2007, Estonia mounted a defense, in coordination with international partners, that successfully ended the attack by locating key nodes from which the attack emanated and blocking those nodes' access to the internet.

With access to systems returning and the cyber infrastructure of Estonia returning to normal, the Estonian government immediately blamed Russia for the attack, pointing to Putin's inflammatory comments just before the attack and the general discontent of the ethnic Russian population as evidence. Estonian investigators traced at least one node of attack back to a member of the Russian government, but Russia vigorously denied any wrong doing, and claimed to know nothing about those responsible for the attack. Since a massive distributed denial of service attack like the one that crippled Estonia linked literally millions of computers from across the world and co-opted them into service for the attack, tracing to an origin point and connecting that to culpability was problematic. Computers in other parts of Europe, Asia, and even the United States had been brought to bear for the attack, so laying blame on those fronts was pointless. United States and NATO investigators were also unable to trace the attack back to an

[12] Jason Richards, "Denial-of-Service: The Estonian Cyberwar and its Implications for U.S. National Security." International Affairs Review (2009): 66.

agreed upon single source, one that the Alliance could hold directly accountable for the attack.[13] A great deal of suspicion and circumstance pointed to Russia, but without a smoking gun in hand, no official assignment of responsibility was possible.[14]

Because this was the first time an entire nation had been brought to its knees through only the cyber domain, the United States, NATO, and the EU took a deep look at the implications of the attack.[15] Estonia was the perfect cyber target in many respects. It is one of the most wired countries in the world, having embraced technology in order to modernize itself and make itself more relevant in first world markets. Tallinn houses the electronic infrastructure for the e-government model upon which Estonian government is founded. The government of Estonia managed all services through the internet, providing a speed and efficiency that is unheard of in many nations of the world. However, this reliance on technology was also its Achilles heel. Although a marvel of technological achievement and socio-political integration, the e-government system had insufficient defenses and no credible deterrent to attack. Estonia was exquisitely, perfectly vulnerable.[16]

In the aftermath of the cyber-attack, Estonia went through a gamut of responses ranging from knee-jerk in the beginning to more nuanced, elegant solutions as time progressed. Immediately following the attack, Estonia essentially disconnected from the rest of the internet so as to assess its damage and mitigate weaknesses where possible. Although the average

---

[13] It is important to note that investigators may have also been reticent to announce culpability if the cyber forensic tools or procedures used were either classified or one-shot opportunities.

[14] Mandel, 77.

[15] The European Institute, Kertu Ruus, *Cyber War I: Estonia Attacked From Rusia,* http://www.europeaninstitute.org/index.php/component/content/article?id=67:cyber-war-i-estonia-attacked-from-russia (accessed November 09, 2017); Richards, "Denial-of-Service: The Estonian Cyberwar and its Implications for U.S. National Security," 72; Mandel, *Optimizing Cyber deterrence* (Washington D.C.: Georgetown University Press, 2017), 77; WIRED, Joshua Davis, *Hackers Take Down the Most Wired Country in Europe,* https://www.wired.com/2007/08/ff-estonia/ (accessed October 20, 2017).

[16] Mandel, 77.

Estonian could still be a part of the e-government in terms of access to email, banking, and the ability to interact with civic institutions, this move cut off Estonians abroad completely from the bedrock of their digital citizenship. It was only a few weeks before the Estonian government realized this was not an optimal solution and rejoined the internet, perhaps a little more timidly than before.

The Estonian situation spurred the NATO alliance to action as well. It moved relatively quickly to establish a unified Policy on Cyber Defense. NATO also stood up a Cyber Defense Management Authority that set the ground work for the current state of affairs for NATO's position that cyber defense is a part of the collective defense responsibilities of the members of the alliance.[17] That stated, NATO did not make it clear as to whether or not a cyber-attack triggers an Article 5 response, nor did it recommend what how that response might look. Article 5 is flexible, and provides a much broader selection of response options than is generally recognized. It is not an automatic tripwire to go to war.[18]

If one accepts that Russia, as a state actor, was the attacker in this instance, it is reasonable to assert that the cyber-attack on Estonia was a essentially dress rehearsal for a similar attack in Georgia. The savvy with which Putin interlaces political, cultural, and physical domains with more aggressive activities in the cyber domain are striking, and point to a form of hybrid conflict. The cyber-attack did not just take down military and government targets, as the attack also crippled banking, education, and media targets as well. Russia completely nullified the Estonian critical infrastructure, both military and civilian, without a single conventional shot fired. It should be inconceivable that a NATO ally could be subdued in such a way with little to

[17] North Atlantic Treaty Organization, *NATO*. JAN 01, 2017, https://www.nato.int/cps/en/natohq/topics_78170.htm (accessed October 15, 2017).

[18] The Economist explains, *How NATO's Article 5 Works*, https://www.economist.com/blogs/economist-explains/2015/03/economist-explains-6 (accessed October 12, 2017).

no repercussion. Estonia in 2007 is a chilling, cautionary tale for cyber policy, and a clarion call for an effective cyber deterrent.

Russia Conducts Hybrid Warfare Against Georgia

Russia likely took great interest in the lack of cogent response from either the United States or NATO as Estonia flailed under a crippling cyber-attack. Although ultimately international partners came together to ease the attack, assist in the mitigation of the effects, and to help Estonia re-establish cyber normalcy, it was very clear that the NATO alliance did not know how to effectively respond.[19] There was argument over attribution for the attack, argument over whether a cyber-attack could even be considered attack, argument over whether such an event was a trigger for Article 5 response, and a general relief that nothing more serious had occurred. In the final analysis, no lives were lost as a direct result of malign cyber activity in Estonia, but cyber activity had spurred destruction and murder in the form of violent mobs and ethnically fueled protests in the streets. More to the point, Russia now had clear evidence that it could act with impunity in the cyber domain and have little to fear in terms of effective, deterring retaliation from either the United States or NATO.

A year later, in 2008, the situation in the country of Georgia was reaching critical mass. For years, tensions had been building between the majority Western leaning portions of the country and the two Russia-leaning regions of South Ossetia and Abkhazia. The government of the former Soviet Republic began a flirtation with NATO in 1992 when it joined the North

[19] In the years following, NATO made several moves to establish a better understanding of what the complexion of a comprehensive alliance response to various levels of cyberattack would look like. An online article at The National Interest.org by Russ Read entitled "Would NATO Go to War Over a Cyberattack" is a good resource for an overview of these activities. http://nationalinterest.org/blog/the-buzz/would-nato-could-go-war-over-cyber-attack-20948 (accessed January 1, 2018).

Atlantic Cooperation Council and in 1994 when Georgia joined the Partnership for Peace.[20] Momentum for alignment with and even membership in NATO picked up after the 2003 Rose Revolution, a pro-Democracy, pro-West movement that saw the ouster of the last vestige of Soviet power in Georgia, President Eduard Shevardnadze. Much of Georgia rejoiced, but the people of South Ossetia were concerned. Most South Ossetians felt a closer kinship to Russia than to their Georgian countrymen.

The leader of the Rose Revolution, Mikhail Saakashvili, was formally elected President of Georgia in 2004, and immediately set upon a policy path of instituting and strengthening Democratic reforms. One of his administration's articulated goals was to improve the relationship with the Russian leaning provinces through the growth and strengthening of democratic governance.[21] Neither the people of South Ossetia nor the government of Russia were particularly enamored with this endeavor.

In 2006, as Georgia applied its full effort into political reforms, the Saakashvili administration expelled four Russian military officers, accusing them of espionage and fomenting discontent within South Ossetia.[22] The Russian government took this opportunity to intensify its pressure on the region and immediately instituted a wide ranging economic embargo on Georgia. Russia proceeded to cut communication lines and transportation routes from Russia into Georgia, further crippling the Georgian economy.[23] Russia had very effectively set the theater to its advantage.

---

[20] The history of Georgia's relationship with NATO is laid out by the Georgian Ministry of Foreign Affairs at https://web.archive.org/web/20080827220629/http://www.mfa.gov.ge/index.php?sec_id=89&lang_id=ENG (accessed November 09, 2017).

[21] Mandel, 83.

[22] Civil Georgia, *4 Russian Officers Arrested, Charged with Espionage*, http://www.civil.ge/eng/article.php?id=13658 (accessed December 18, 2017).

[23] Randall Newnham, *"Georgia on my Mind? Russian sanctions and the end of the 'Rose Revolution',"* Journal of Eurasian Studies (2015): 161-170.

Georgian and South Ossetian troops skirmished off and on throughout 2007, but in July of 2008 the two forces engaged in an artillery duel, escalating the situation significantly and giving Russia the excuse it needed to take more provocative action. Russia began an exceptionally large-scale military exercise near its border with Georgia, under the pretense of moving forces into proximity with a potential border conflict. Georgia was well within the Russian sphere of influence, and few could argue the reasonability of Russia moving forces into a position to stabilize a conflict on its own border.

In the early part of August 2008, the Georgians and South Ossetians were again at one another's throats, claiming various breaches of the cease fire and security agreements that had ended the shelling from the month prior. Russian troops were still in the region, having drawn out the conclusion of its "exercises" significantly. On 08 August, 2008, as the world watched the opening of the Olympic Games and attention was effectively diverted, Russia advanced armor and other forces in South Ossetia, claiming that Georgian aggression had exacerbated the situation in both South Ossetia and Abkhazia to the point that Russia could no longer sit idly by.[24] Claiming to be conducting a peace keeping operation, Russia began a comprehensive, multi-domain invasion of Georgia with the end goal being the liberation and recognition of the Russian leaning provinces.

What had gone largely unnoticed in the buildup to armed conflict was that Russian based cyber actors were preparing the battlefield as early as July of 2008.[25] Russian based hackers probed the electronic infrastructure of the Georgian government and began testing defenses and

---

[24] Russia Today, *Putin blames Georgia for raising tensions in Abkhazia* https://web.archive.org/web/20080421185341/http://www.russiatoday.ru/news/news/23724 (accessed December 18, 2017). Russia Today cannot be considered an impartial news source given its ties to the Russian government, but the article supports author's explanation of Putin's claims regarding the unfolding situation in the break-away Georgian republics at the time.

[25] New York Times, John Markoff, *Before the Gunfire, Cyberattacks* http://www.nytimes.com/2008/08/13/technology/13cyber.html (accessed January 01, 2018).

detection capabilities. Russian hackers attacked via a distributed denial of service campaign the President of Georgia's website and some associated government sites. This was very similar to the beginning of the Estonia cyber-attack from 2007. The hackers discovered no effective cyber defense or security in place, and were able to bring down every website they attacked with ease.[26] Just before the Russian physical invasion of Georgia on August 8th, cyber-attacks struck Georgia en masse, bringing down the majority of the critical electronic infrastructure, to include government web-based services, the majority of the communications network, and various civilian networks supporting national banking, political parties, industry, and universities.[27] This sowed chaos within the Georgian government and allowed Russian forces to effectively seize the initiative.

Russia achieved control of the land, sea, and air domains quickly. Russian armored units secured ground at a break neck pace. Russian troops delivered by warships secured strategically important positions along the Black Sea coastline. Air strikes were pinpoint and devastating, going after Georgian air defense capabilities, critical infrastructure, and command and control elements. It was essentially a text book conventional operation, with one exceptionally critical difference – it was the first time in recorded military history that the world had seen a coordinated cyber-attack that provided decisive supporting effects for major combat operations emanating from the physical domains. Russia's hybrid, multi-domain warfare model was entirely successful.

The invasion of Georgia cost approximately one thousand lives, and displaced another one hundred and seventy-five thousand or so. For those who had consistently argued that cyber-

---

[26] Mandel, *Optimizing Cyber deterrence* (Washington D.C.: Georgetown University Press, 2017), 84.

[27] Markoff, *Before the Gunfire, Cyberattacks* http://www.nytimes.com/2008/08/13/technology/13cyber.html (accessed January 01, 2018).

attacks did not result in deaths, and therefore questioned as to whether or not cyber-attack should even be considered an "attack", there was new food for thought. Computers had not killed anyone directly, certainly, but computers had made the very efficient killing of humans a battlefield reality.

The United States, NATO, and the western democracies encountered lessons in Estonia but failed to grasp them. The lessons in Georgia were starker. Georgia, like Estonia, found itself essentially alone against a much more powerful, capable, and aggressive predator. There was no effective deterrent to Russia's activities, and Russia took full advantage.[28] This case study presents a more thorough failure in deterrence than just in the cyber domain, but for the first time cyber played a major role in a conflict that had lethal effects.[29] Russia knew from Estonia that cyber would not trigger a military response (or really any credible response at all). Without the cyber component, Russia would have lost a key tool in preparing the operating environment with "fires" below the threshold for conflict, and the follow on Blitzkrieg style attack could have been blunted. Had Russia not been confident that its cyber operations would degrade Georgian responses to its activities, Russia might not have invaded. In such case, an effective deterrent that touches on the cyber domain could have prevented the invasion.

After action reviews from Georgia and various international partners and scholars, including the United States, found that former Soviet republics, including Georgia, are very reliant on Russian internet pipelines, with generally poor access to other on ramps to the information superhighway.[30] This is likely by Russian design, as it facilitates Russian cyber and hybrid warfare modalities. Membership and partnership with nations or organizations that can

---

[28] Ketevan Tsikhelashvili and Natasha Ubilva, *Case Study of the Conflict in South Ossetia* (Boston: Martinus Nijhoff Publishers, 2008).

[29] Mandel, *Optimizing Cyber deterrence* (Washington D.C.: Georgetown University Press, 2017), 85.

[30] Ibid.

provide internet connectivity as a way to break reliance on Russian provided services would be a good start on enhancing the cyber-security of nations within the Russian sphere of influence. These partnerships, if fully and completely realized and acknowledged, can also begin to build a de facto deterrent to Russian aggression, placing greater and greater potential cost on risky, aggressive Russian activities. Moving against a member of an alliance or partnership should ensure that the other members of the partnership respond in a collective defense posture, using whatever means are available, appropriate, and proportionate.

The move against Georgia (and Estonia) also exposed a general lack of internationally accepted and practiced restraining norms within the cyber domain. Without internationally accepted binding agreements or meaningful norms, cyber-attackers have free rein to impose their predations as they please.[31] Russia is effectively setting the cyber norms in its own favor by taking action without consequence and essentially inuring the globe to its vision of cyber dominance. The United States, its allies, and partners must challenge this norming effort as contrary to prosperity and the accepted world order. Enshrining the notion that cyber aggression is not an accepted norm in international relations will also have a deterrent effect to its use.[32]

The United States must act now on these issues. Georgia was an evolutionary leap over the malign cyber activity in Estonia. The US does not want to have to cope with whatever the evolutionary leap from Georgia may look like.

---

[31] Ibid., 86.

[32] For the purposes of this paper, Author asserts that attribution of agency in a cyber activity is possible far more often than it is not, based on a wide corpus of academic work. For a survey of attribution scholarship, see *Attributing Cyber Attacks* article in *The Journal of Strategic Studies,* and its excellent bibliography.

CHAPTER 3: THE PRESIDENT ORDERS DOD TO DETER CYBER AGGRESSION

"Any complex activity, if it is to be carried on with any degree of virtuosity, calls for appropriate gifts of intellect and temperament." [1]

A New Executive Order on Cyber

As previously discussed, on 11 May 2017, President Donald Trump issued the Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure.[2] This EO Cybersecurity is the first substantive update to cyber policy at the executive level since 2013, and reflects an urgency that has been previously lacking from the discourse. EO Cybersecurity delineates responsibilities and expected lines of effort among DoD, the Department of Homeland Security, the Department of Justice, the Office of the Director of National Intelligence (ODNI), the Department of State, and various other executive branch entities. The intent is to address serious concerns for cybersecurity in the realms of Federal networks and critical infrastructure. Perhaps most interesting, the EO Cybersecurity places accountability for the cybersecurity mission on the heads of the various agencies.[3]

Overall, EO Cybersecurity got some very important issues right, but could stand to improve on others.[4] Experts universally agree that the information technology infrastructure (IT) for the Federal Government is in desperate need of modernization, and the EO Cybersecurity

---

[1] Karl Clausewitz, *On War (Complete Edition)*, Edited by Michael Howard & Peter Paret, (Princeton: Princeton University Press, 1976), 100.

[2] United States Government Publication, *Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure.*

[3] Previously, the responsibility for the cybersecurity mission resided with various agency IT departments. In this configuration, there was little risk to the agency heads, because a cybersecurity failure could be blamed down the chain of command and solved with a firing or replacement of IT personnel. No true responsibility was previously evident at the executive level.

[4] Don Maclean, *Cybersecurity executive order: What works and what's missing* https://federalnewsradio.com/commentary/2017/07/cybersecurity-executive-order-what-works-and-whats-missing/ (accessed December 30, 2017).

clearly identifies and prioritizes this need. EO Cybersecurity also notes that modernization is not a single event, and is in fact a continuum of evolution that never ends. Advances and efficiencies in technology continue to march forward. The Federal IT infrastructure faces a crisis of modernity, which has become a crisis of efficacy and relevancy. The EO Cybersecurity also forces agencies to better account (or to account for at all) the budgetary constraints that impact improvements and modernization, and to look for ways to mitigate cost through shared services and other efficiencies. The days of agencies operating in an IT vacuum are numbered, and this is entirely well and good.

Prima facia, pinning accountability for cybersecurity on agency heads sounds like an excellent idea. Properly implemented, it is. However, the EO Cybersecurity lacks clear metrics for failure, beyond an obvious catastrophic breech such as occurred at the Internal Revenue Service or the Office of Personnel Management. It is also not clear if there is a spectrum of discipline or punitive actions that would be taken should failure occur, what the adjudication and appeals process would be, etc. Also of note, agencies are allowed to assess their own risks and vulnerabilities. This task most often falls to contract personnel who are doing business with the agency. This setup may create an atmosphere of impropriety where the contracting firm feels obligated to paint a rosier picture than might otherwise be warranted, based on a desire to maintain a business relationship.

Not unexpectedly given the complexion of the Trump administration, much of the EO Cybersecurity's concepts appear to originate from the perspective of a civilian Chief Executive Officer. Accountability of and by senior managers is key to business success. Budgetary awareness, efficiencies, and synergies are highlighted. Deterrence, however, is from the realm of international relations, and has no obvious equivalent factor in the business realm. The

administration is clear on managing money and risk through accountability, but deterrence theory does not seem to fully resonate.

Enhancing cybersecurity can fold into a deterrent by denial, of course, but specific mention of deterrence in the cyber domain proper is lacking within the EO Cybersecurity. This is not necessarily a weakness, as at least it identifies a need to address the issue specifically. Section 3, paragraph (b) of EO Cybersecurity is entitled Deterrence and Protection. The entirety of a cyber deterrence policy is constrained to a single paragraph, shared (and arguably conflated with) protection. It states in whole:

> "(b) Deterrence and Protection. Within 90 days of the date of this order, the Secretary of State, the Secretary of the Treasury, the Secretary of Defense, the Attorney General, the Secretary of Commerce, the Secretary of Homeland Security, and the United States Trade Representative, in coordination with the Director of National Intelligence, shall jointly submit a report to the President, through the Assistant to the President for National Security Affairs and the Assistant to the President for Homeland Security and Counterterrorism, on the Nation's strategic options for deterring adversaries and better protecting the American people from cyber threats."[5]

This paragraph is the only mention of deterrence or deterring in the entire document, but it is more helpful in this instance to view the vagueness here as an opportunity to design and define unconstrained solutions rather than as a hindrance due to lack of guidance. As previously discussed, a single domain approach to cyber deterrence is the wrong approach, but what elements of existing deterrence theory should fold into a comprehensive unified theory of deterrence, appropriate to the modern era, that includes the cyber domain?

[5] United States Government Publication, *Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure,* https://www.whitehouse.gov/presidential-actions/presidential-executive-order-strengthening-cybersecurity-federal-networks-critical-infrastructure/ (accessed December 30, 2017).

Theories of Deterrence as Building Blocks to Unified Theory

As with any field of international relations, deterrence has its supporters and detractors. Theories of and approaches to deterrence seek to bring a level of simplicity to inherently hostile relationships between potential adversaries, most notably demonstrated as a desire to control the release of nuclear weapons. Cowing an enemy, or intimidating it into submission, are not complicated concepts to absorb. Presently, the United States DoD defines deterrence as "prevention from action by fear of the consequences. Deterrence is a state of mind brought about by the existence of a credible threat of unacceptable counteraction."[6] Most theorists go on to break down deterrence into two approaches: deterrence by punishment is the threat of retaliation if an adversary takes an action; and deterrence by denial is the threat of successfully defeating an adversary's action.[7]

Deterrence tends to dominate all other American theories of international relations, likely a byproduct of America becoming the first and later one of the preeminent nuclear powers of the world. When a state can initiate Armageddon, it naturally follows that theorists would study exactly what that means for relations with the global neighbors, especially if they too can spark a global nuclear oblivion.

General theories of deterrence have formed in so-called waves, but the essential premise throughout is that deterrence is characterized by either denial or punishment, and that the deterring actor must be credible, capable, and committed.[8] The various waves are bounded in

---

[6] Quoted from the Department of Defense Dictionary, updated February 2018.

[7] Jeffery W. Knopf, "Three Items in One: Deterrence as Concept, Research Program, and Political Issue", in *Complex Deterrence: Strategy in the Global Age,* ed. T.V. Paul, Patrick M. Morgan, and James J. Wirtz (Chicago: University of Chicago Press), 38.

[8] Deterrence theory enjoys an expansive corpus of scholarship. Author utilized Lawrence Freedman's 2004 *Deterrence* to reference the so-called waves and the broad strokes of the theories, but the author also recognizes specific contributions to Deterrence Theory by such scholars as Bernard Brodie, Thomas Schelling, Alexander George and Richard Smoke, among many, many others excellent thinkers, strategists, and philosophers.

time by rough borders, coinciding with changes in technology, culture, globalization, and experience. The First Wave came in the 1940s and 1950s, very soon after the development and employment of the atomic bomb and is best exhibited as a doctrine of massive retaliation, which was championed by Secretary of State John Dulles and adopted by President Dwight Eisenhower. The First Wave maintained that a massive nuclear counter strike was the answer to any conventional or nuclear aggression on the part of the Soviet Union. In addition to being exceedingly inflexible (would a single Soviet aircraft penetrating US airspace be grounds for massive retaliation?), its apparent net effect was to create a security dilemma with the Soviet Union. The massive retaliation doctrine was met by Soviet desire to create a first strike capability that would render the massive retaliation moot. Massive retaliation doctrine likely had some impact on the Soviet decision to place nuclear weapon in Cuba, where the flight times of the nuclear weapons were short and they could conceivably target bombers belonging to the Strategic Air Command before takeoff, thus blunting the massive retaliation. This pushed deterrence theory into the next wave.

Second Wave deterrence came about in the 1960s, and was marked by the influences of game theory, rational deterrence theory, and concepts like Mutually Assured Destruction (MAD). The notion of rational actors making risk analysis likely resonated with members of Kennedy's administration like Secretary of Defense McNamara and his staff of wunderkind from the world of civilian business and industry. By assuming rationality on the part of an adversary and allowing for more flexible responses than total war, Second Wave approaches expanded rather than limited the tools in Kennedy's tool kit and allowed for deterrence options that were more responsive to changes in foreign policy. Critics were concerned that rational actor and game theory models were excellent math, but did not accurately reflect the complexity of the

human factor in international affairs. Nevertheless, this was the approach that carried through a preponderance of the Cold War, which notably did not include any employment of nuclear weapons nor a general nuclear war.

By the 1970s and throughout the 1980s, however, the critics of rational actor theory of deterrence were gaining significant traction. These critics became the Third Wave, and they sought to do away with the largely untested, intuition based arguments of the Second Wave and instead apply greater rigor resulting in empirical proofs of concepts. Behavioral science was also brought to bear, asserting that humans were not capable of making the kinds of cost/benefit analysis that rational actor theorists believed, and that formed the core foundations of the Second Wave of deterrence. This was especially true within an existential crisis, such as nuclear exchange. Resulting scholarship pushed the theory of deterrence towards balancing military capabilities against interests and resolve, seeking to correlate these factors with outcomes to bargaining and negotiation. In other words, to provide even more flexibility on the engagement and foreign policy front without losing the deterrent effect.

Beginning in the 1990s and including current scholarship, a Fourth Wave of Deterrence Theory has emerged. Theories and approaches on how to apply deterrence to smaller powers and conflicts with asymmetric opponents came to the forefront. Immediately following the fall of the Soviet Union and the end of the Cold War, the world found itself in essentially a unipolar environment. Scholars examined whether the idea of deterrence was even relevant in the absence of the Soviet Union, and deterrence diminished in importance for military thinkers to some degree, although it never disappeared completely. The diminishment resulted in policies during the Clinton administration, as an example, that concentrated on compellence and intervention, with varying degrees of success. The concept of tailored deterrence emerged from this wave,

wherein actors are specifically deterred by correctly analyzing the actor's motivations and thought processes and tailoring a deterrent that fits precisely the need at hand.

The preceding broad overview demonstrates that deterrence theory essentially reflects, and is informed by, the prevailing concurrent theories on international relations and war. The influence of politics of the times is always at play. In order to chart a course forward on an effective approach to deterrence that includes the cyber domain, a general understanding of the evolution of deterrence theory is necessary. Grasping a history of deterrence frames discussions on evolving theories of war that include the cyber domain and on deterrence theories within that same context. Old and new approaches are colliding and coalescing, leading to the emergence of new vantages and approaches. What will be the contours of the wave of deterrence that include cyber space?

CHAPTER 4: CONCLUSION – TOWARDS A UNIFED THEORY OF DETERRENCE TO INCLUDE THE CYBER DOMAIN

"Genius consists in a harmonious combination of elements, in which one or the other ability may predominate, but none may be in conflict with the rest."[1]

A Theory of Cyber Warfare

The frontier of cyberspace is the new battleground of the 21st century. It is not the sole one, of course, but whomever achieves an understanding of cyberspace will have a profound strategic advantage over their adversaries and competitors. Success in cyberspace will increasingly impact success in any of the other domains. Cyberspace permeates land, sea, air, and space. It binds them together, and can produce effects throughout them all. The problem for the United States is that it speaks cyber ineloquently, and comprehends the environment incompletely. America is playing checkers while its adversaries are playing chess, and yet the potential of the game board is limitless and not yet understood in an enlightened way by anyone. What is evident, though, is that humans have instinctually appreciated a new way to conduct warfare.

Humans, much as Clausewitzian war, are defined by reason, passion, and chance. The eternal struggle among these abstractions has led to incredible advances in technologies, and the opportunity to realize a better peace and better existence for all mankind through the benevolent and ethical employment of same. The nuclear age, sparked by the Manhattan Project, came with the potential for limitless, cheap, environmentally friendly energy coupled with an opportunity for America to break away from reliance on overseas, often confrontational suppliers of fossil

[1] Karl Clausewitz, *On War (Complete Edition)*, Edited by Michael Howard & Peter Paret, (Princeton: Princeton University Press, 1976), 100.

fuels. The nuclear age offered a chance at true prosperity. Unfortunately, the ultimate human expression of the nuclear age stayed with the atomic bomb, a weapon so terrible that it impelled the focus of Deterrence Theory so as to avoid the destruction of the entire human civilization.

Thomas Hobbes would no doubt be unsurprised that humans would squander the bountiful opportunity of the nuclear age on creation of a weapon so terrible that it defines entire geopolitical landscapes and underwrites the power and legitimacy-by-force of any nation that wields it. North Korea is an excellent example. North Korea does not want to have nuclear weapons in order to project ultimate power on an adversary anywhere around the world. North Korea seeks instead to have the inherent influence engendered by the nuclear capability. A nuclear armed and capable North Korea carries the so-called "big stick". It can then choose to walk at whatever intensity it desires. This status essentially adds a North Korea chair to the table of influential world powers, gives North Korea a voice on a world stage in a manner impossible without nuclear arms, and challenges US perception of its ability to strategically deter in the nuclear realm vis a vis proliferation.

The problem for Kim Jong Un, however, is that in the final analysis, utilizing a nuclear weapon would make his life, and the life of his regime, nasty, brutish, and short. The single most likely response to a nuclear first strike by North Korea would be an overwhelming counter attack from another nuclear power, likely the United States and its allies. Such a counter attack runs the risk of provoking a general nuclear war, which could have world-devastating implications. Enlightened, constructivist-leaning tailored deterrence would quickly revert to realist massive retaliation.

Kim Jong Un, although operating within a sphere of bounded rationality, likely recognizes that while the nuclear weapon buys him entrée to the international big show, the use

of the weapon would be fatal for the regime. Survival of the dynasty, and certain elements of the regime, are at the core of any domestic and foreign policy for North Korea – the Kims must survive, and they must rule, as essentially a divine mandate. It is virtually certain that Kim Jong Un has learned the lessons presented by the case studies of Estonia and South Ossetia, not to mention his own country's breech of Sony Pictures: neither the United States nor NATO will effectively respond to a cyberattack, even when it is followed by lethal, multi-domain conflict. What Kim Jong Un desires most is a capability that goes hand in hand with the menacing but practically unusable nuclear weapon, a capability that is strategic in scope and effect but that can be employed without risking a massive counter strike that endangers the continuation of his rule. A capability that aligns nicely against a weakness of his primary opponent, the United States of America.

Technology provides exactly what North Korea, and any of the 4+1 adversaries, need in order to take advantage of this gap in American credibility, capability, and commitment by way of the internet. Originally intended as an information super highway allowing for near instantaneous communication worldwide among scientists, academics, and scholars, the internet promised to link the entire world together in ways never before dreamt.[2] Knowledge could be gained, analyzed, and disseminated at incredible speeds. Societies could be linked to one another in new and novel ways, and humans could be drawn together. As complexity, sophistication, and globalization evolved the early internet, humans again were on the cusp of something truly amazing, something which could spur peace and prosperity in amazing new ways - cyberspace.

The attack terminology mentioned above is not simply relegated to cruel posts on social media or anonymous phishing emails. Cyberattack, as discussed in the case studies, can have

[2] Janet Abbate, *Inventing the Internet,* (Cambridge: Massachusetts Institute of Technology), 7-43.

multi-domain effects. A cyber actor can attack critical infrastructure and kill the power to a grid or system, effectively blinding military early warning or subjecting the civilian population to misery and peril. A cyber actor can devastate computer networks, deny service to entire sectors of the economy, and essentially sow confusion and chaos. It can generate fog and friction on command. Vital information can be stolen without putting a single human asset at risk, information which could have grave implications for national security of the victim.

Viewing all of cyberspace as only a new domain for battle is an oversimplification, just as the seas are not in place simply for maritime engagements. But humans have far less agency deciding the nature of the sea, or any of the other natural domains, than they do the nature of cyberspace. Cyberspace is a construct of human origin, and could be subject to human governance in ways that are impossible in the other domains – land, sea, air, and space. Cyberspace may even be something of a truer reflection of human nature, given humans have the potential to form and dominate the realm with approaching omnipotence and have largely chosen to use it to project conflict rather than utilize the space as a widely, nearly universal, forum for discourse. However, this is a digression for another work.

The U.S. military identification of cyberspace as a domain within which fighting can take place has placed it at the same heady strategic level as the employment of nuclear weapons, an unreasonably high perch.[3] American military thinking towards cyberspace is somewhat constrained, however, by a number of shortfalls. Neither the American military, nor its close allies nor allied organizations, have an agreed upon interoperable standard lexicon.[4] No universally accepted vocabulary exists to describe cyberspace or to describe military activities

[3] The Department of Defense Cyber Strategy 2015.

[4] NATO Cooperative Cyber Defense Center of Excellence, "Resources: Cyber Definitions," https://ccdcoe.org/cyber-definitions.html (accessed December 8, 2017).

within it. Military thinkers currently apply terminology more apropos of other domains, such as *dominance, superiority, supremacy,* and *combat power overmatch*. The words used to describe or define something are important, and psychological implications of a vocabulary are quite clear. By using terms that only have true relevancy in other domains, military thinkers are prone to approaching the cyber domain as a great analogy to the other domains rather than recognizing the unique features that the domain presents and adjusting thinking accordingly. This has implications not just for what activity occurs in the cyber domain, but how to deter it.

Because of this thinking by analogy, U.S. cyber strategy is something of a mixed bag. Partially declassified via the Freedom of Information Act, cyber strategy shows a general mismatch of terms, akin to those previously described. The strategy points to retaining "freedom of action" for the American military and the denial of same to adversaries. The strategy points to the need for a capability to "seize the initiative". This kind of thinking begs the question – how does one maintain freedom of action and seize the initiative where the high rate of operational maneuver approaches the speed of light?[5] An attack can occur in literally the blink of an eye, with the few if any indications and warnings also taking place in a blink of an eye. Cyber thrusts, parries, and ripostes occur at speeds only artificial intelligence can truly monitor.

But humans do retain an advantage in cyberspace. Humans not only created cyberspace but can also exert agency over cyberspace in ways it cannot in the natural domains. This is an important nuance that the United States may have missed, much to the advantage of the 4+1 adversaries. The U.S. military acknowledges this human created domain of cyberspace as an equivalent domain to the others in terms of the potential for warfighting activities and effects, but this is an incomplete synthesis of the situation. While certainly a step in the right direction it

[5] Clarke and Knake, *Cyber War: The Next Threat to National Security and What to Do About It,* 45.

stops short of thoroughly grasping the battlespace, and thus, how to create effective deterrence for activities within it.

In some ways, cyberspace is actually not an equivalent domain – it is a supra-domain. Humans have a degree of influence over the essential nature of cyberspace in a way that is simply impossible with the other domains. With some hardware and some deft key strokes, an information technology professional can create entire universes, can define the existential fabric of the new creation, can bring applications and programs into virtual life and establish an ecosystem of immense and evolutionarily linked creations, entire system of systems, out of nothingness. The Air Force cannot, as an example, create more sky.

Cyberspace is not bounded by geopolitical borders in its current configuration, meaning that there are issues of sovereignty that cannot be easily solved. Searching for models in other domains, such as China's spurious claims to the South China Sea, India's occasional rumblings that the Indian Ocean is named so for a reason, and contested claims to stakes of land like Jerusalem are potential launching points for how to approach issues of virtual territory, but are incomplete and not entirely one for one equations. This approach remains fraught with the same inadequacies of analogy brought by the application of an ill-suited taxonomy. How does one claim territory in cyberspace? Can one occupy cyberspace? Should cyberspace be treated similarly to intended approach to the space domain, i.e. no weapons of mass destruction and the domain should only be used for peaceful purpose? What are the implications for deterrence among these philosophical points?

Given how the weaponization of space is proceeding at a brisk pace and an overall realist perspective of the preceding discussion, it is unlikely that cyberspace as a domain would be relegated to benevolent use, even though, ironically, the creation of cyberspace was for just so

lofty of goals. Each of the 4+1 adversaries has taken great leaps forward to weaponize cyberspace, and has demonstrated the ability to use cyber capabilities to have tactical, operational, and strategic effects. There is a perceptional nuance to be had here, one that could better inform U.S. policy, strategy, and operational design. It is this nuance that the United States' 4+1 competitors appear to have noted, and to have mastered, as demonstrated in the case studies. Russia has integrated its cyber and information warfare capabilities into its full range of military operations and therefore presents a multi-domain, hybrid warfare threat to the United States in ways American senior decision makers seem to not fully comprehend.

Part of the problem is educational in nature. During the 2011 revolution in Egypt that saw violent protests and a general uprising against Mubarak regime, Egypt briefly seemed to disappear from the internet.[6] This led some American political leaders to believe that it was possible to simply turn the internet off in a problem country. Cyber experts ultimately explained that Egypt only had five internet service providers, and that the government called each via landline and asked them to set the internet protocol handlers to send all traffic to null addresses. In other words, the internet was not off, but it was directing all traffic straight to the bin and was not functional. This response was akin to scuttling the ship to avoid capture – it is effective in the short term but is borderline Pyrrhic, does not preserve the capability, and does not actually stop the continuation of attack. Also, civilian sector cyber experts are fairly uniform in the opinion that internet simply cannot be turned off at this point. Even if broken in separate sections, the segments would function as smaller versions of their parent whole, and would even begin to make additional connections to backfill the missing connections from the divide.

---

[6] Charles Arthur, *Egypt cuts off internet access* https://www.theguardian.com/technology/2011/jan/28/egypt-cuts-off-internet-access (accessed December 19, 2017).

If there is a general misunderstanding of the cyberspace domain at the policy level, it is not a far leap to assess why the cyberspace domain is difficult at the strategic level. A good strategy acts as a bridge from policy to operations. The U.S. has seen the effects of strategy absent policy at various, usually painful points throughout its history, most notably in Vietnam. It would be unwise to adopt the same poor approach to cyberspace, but America's track record of seizing lessons presented by history is spotty. The American military has yet to produce an operational artist of Abram's caliber for the cyberspace domain, so it is possible there will be several cyber Westmorelands to muddle through first.[7] Time will tell.

While lacking a cyber Abrams, it should be noted that the Western world is without a cyber Jomini as well. There are no cogent theories being presented on the nature of war in the cyberspace domain, which could also inform theories of deterrence. As Clausewitz and Jomini defined the land, so did Mahan the sea and Douhet the skies. Whence comes a cyber Mahan? Mahan is an interesting choice here, as potentially the cyberspace domain could be visualized from many of the same vantages from which Mahan viewed the maritime domain. Mahan theorized that control is impossible, for both friendly and enemy forces and that maintain sea lines of communication were the primary indicator of success. Perhaps maintaining the sea (cyber) lines of communication and providing supporting fires to other domains would be enough to define command of the cyber.

Lacking a firm conceptualization of how to describe the domain, how to operate within it, or how to theorize as to the cyberspace's essential fabric and what it means to contest in the

[7] Author is referring to US Army General Creighton Abrams and General William Westmoreland, as related to their tenures as commanders of the Military Advising Command – Vietnam during the Vietnam Conflict. Some historians assert that Abrams demonstrated a better grasp of the Vietnam environment and that his operational art and approach to the Vietnam was more nuanced and effective than Westmoreland's, who often receives poor reviews in his handling of the conflict. See *Westmoreland: The General Who Lost Vietnam* by Lewis Sorely for additional details and discussion.

domain, American military thinkers are faced with ever more wicked problems in terms of theories of conflict and deterrence. Various schools of thought approach what causes conflict, but there are some commonalities to be parsed. Generally, conflict is more likely if there is a shared border, and if the political entities in question have been in conflict before. Thucydides' offering that fear, honor, and interest lead to conflict is still relevant, as is Hobbes' assertion that glory, diffidence, and competition are the roots of bellicosity.[8] The question for cyberspace, however, is whether to consider the domain as having no borders whatsoever, or conceptualizing that every country in cyberspace borders every other country in cyberspace. And then there are the "New Wars" theories of Mary Kaldor and her tribe, describing entirely borderless disputes and violence that are rooted in identity politics rather than political ideology or power.[9] There are distinct differences in the take away from both positions, and there are profound implications for the applicability of conflict and deterrence theory models.

So, what, if any, aspects of historical deterrence theory should be brought to bear in order to approach a solution vector for this wicked problem, and also of course to answer the directive within EO Cybersecurity to deter adversaries in cyberspace? Deterrence, like war, reflects the spirit of the age. Across the so-called waves of deterrence theory, one can find the impact of realism, of liberalism, and of constructivism in how the deterrence theories were viewed, implemented, and embraced. Philosophy and action were and shall remain intertwined.

---

[8] Donald Kagan, Thucydides: The Reinvention of History (New York: Penguin Group, 2010); Thomas Hobbes, Leviathan (Cambridge: Cambridge University Press, 1904).

[9] Mary Kaldor, *New and Old Wars* (Cambridge: Polity, 2012). Mary Kaldor is a leading "New Wars" theorist, and posits that the nature of war has changed to reflect violence as among varying combinations of state and non-state actors; in fighting in the name of identity politics instead of ideology; in attempts to achieve political, rather than physical control of populations through fear; and in conflict financed through predatory means as a continuation of violence. This has also been referred to as wars among the people by scholars such as General Rupert Smith in his work, Utility of Force.

What world view would best reflect the spirit of the current age, and the spirit of the relatively young administration of President Donald J. Trump? If the first year is an indication of how the administration will approach international relations and view the United States' place in the world, then there will be some fairly significant upheaval in the status quo of the world order, potential upheaval in the character and strength of the relationships among the US and its traditional partners and allies such as NATO, and potential upheaval in the relationships with traditional adversaries and competitors. This is not intended as a value judgment on the changes, but rather to point out that rapid, large scale changes in posture and demeanor on the world stage could have unpredictable effects on the degree to which the United States is perceived as capable, credible, and committed to its policies, agreements, and treaties. Those factors are the essential holy trinity when it comes to an effective deterrent in any domain, cyberspace most certainly among them.

Both Old War and New: Deterrence that Bridges the Generations

Deterrence in cyberspace is complex, difficult, and divisive because the cyber domain is itself complex, difficult, and divisive. In order to truly achieve the acme of excellence in cyberspace, one must understand that cyber warfare is actually an evolutionary bridge between Clausewitzian "Old Wars" and Kaldorian "New Wars", retaining aspects of both but combining in surprising, emergent ways as well.[10]

As seen in the invasion of Georgia, Russian hackers utilized the cyber domain to have Old War effects by generating fog and friction from the cyber domain in order to support major combat activities in the other domain concurrently. They also facilitated New War effects by promoting and supporting identity politics struggles by appealing to Russian leaning Georgians

[10] Clausewitz, *On War*; Kaldor, *New and Old Wars*.

who felt disaffected by their central government and the reforms it was implementing. Russia hybridized the tactics, techniques, and procedures (TTP) of both Old and New approaches to warfare, utilized the appropriate domain to enhance the effectiveness of those TTPs, and conducted a startling, unique, and entirely successful campaign to meet its political objectives without fundamentally shifting its position in the accepted norms of international engagement.

It is this mastery of both Old and New war, and control over the domain from which that mastery can be most effectively wielded, that the United States and NATO absolutely must deter. Deterrence of the Old war aspect is actually quite straightforward, but requires some resolve. Deterrence of the New War aspect is somewhat more problematic.

And Old Approach, and a New One

As an articulated and public policy of record, the United States should indicate that it considers any activity which violates its sovereignty, regardless of the domain from which that threat emanates, as an attack. America retains the inherent right to self-defense, and will respond as appropriate based on the context of the incident, perceived intention of the attacker, and the best judgment of the President of the United States as exercised by the power vested in the office by the Constitution, and by any means of any instrument of national power (Diplomatic, Informational, Military, or Economic) as deemed necessary and proper by same. Specifically, an attack emanating from the cyber domain need not only be countered in the cyber domain. Efforts to punish cyber-attacks by land, sea, air, and space vectors are viable, possible, and entirely appropriate. Simply put, cyber-attacks should be considered equal in threat to attacks from any other domain and should be responded to accordingly.

Also as a matter of public policy, the United States should indicate that it considers similar intrusions into the sovereignty of members of the NATO alliance as attacks, worthy of an

Article 5 response. Article 5 is sufficiently broad in scope as to allow for a spectrum of contextualized responses, and the United States should push the NATO alliance in the same philosophical direction. Cyber is a domain where even the smallest of the allied nations can have easy access and relatively cheap logistics – there are no troops or equipment or supplies to transport in order to get to the fight, so to speak.

Traditionally, deterrence by punishment requires a trigger – crossing a border, sailing into contested waters, or flying into someone's airspace, as examples. There are no physical borders in cyberspace, but one should not conceptualize punishment triggers in cyberspace in analogous terms. The United States should apply the definition of the U.S. Person, as found in 22 U.S. Code §6010, to all aspects of cyberspace (computers, servers, clouds, etc.) and consider any intrusion or attack on those aspects as attacks on protected U.S. Persons and as a trigger for deterrence by punishment.[11]

In terms of denial, the continual improvement of the cyber security for both the United States and NATO must continue. Hard targets are a deterrent in and of themselves. This must occur in concert with a reinvigorated collective defense posture that recognizes the cyber domain as an attack vector.

New Wars, as described by Mary Kaldor and the New Wars theorists, presents a paradigm shift in the nature of war in the modern era. Wars fought as ideas punctuated with violence. Westphalian states no longer have the monopoly on that violence, instead sharing it with the people or other non-state actors. This is a hyper dangerous, quickly shifting landscape that breaks many of the accepted rules and norms for how the world is supposed to work.

[11] 22 U.S. Code §6010: any individual who is granted U.S. permanent residence ("Green Card" holder); or. any individual who is granted status as a "protected person" under 8 U.S.C. 1324b(a)(3); any corporation/business/organization/group incorporated in the United States under U.S. law; any part of U.S. government.

Information warfare, denial and deception, and propaganda are not new, but cyberspace and cyberwarfare have allowed for a quantum leap forward in the scope, intensity, and reach of these tools. Savvy modern warriors such as Russia have hybridized the Old and the New Wars approaches, and an effective deterrent must address both.

Although Kaldor questions whether deterrence is even relevant or possible, the author asserts that deterrence is still a valid approach to counter Kaldorian New Wars. However, the deterrent is infinitely more complex than simple denial and punishment.[12] In fact, denial and punishment (short of genocide) tends to harden the very ideologies that the deterrent is seeking to constrain. New Wars deterrence instead involves engagement and information dominance. The United States cannot surge trust; it cannot only start meaningful engagement once conflict has begun. The best deterrent to ideological wars is persistent engagement throughout the world. The US must sustain and reinforce international norms that promote liberal democracy, equality, prosperity, and that are conducive and responsive to promoting American values.

Final Thoughts

There is no such beast called cyber deterrence. Cyber is simply another warfighting domain, and cyber should be included as another facet of a comprehensive and unified theory of deterrence that addresses denial, punishment, engagement, and information dominance. Malign activities in the cyber domain are subject to multi-domain responses, and should be triggers for mutual defense pacts or agreements, such as NATO Article 5. The United States must prove it is willing to respond appropriately, assuredly, and rapidly to cyber-attack, and to set international norms to its advantage and the advantage of its allies and partners when it comes to the

[12] Kaldor, *New Wars and Old Wars*

acceptable utilization of the cyber domain in not only the conduct of war, as reflected by the spirit of the age, but also in the conduct of peace and international engagement.

BIBLIOGRAPHY

Abbate, Janet. *Inventing the Internet.* Cambridge: Massachusetts Institute of Technology, 2009.

Arthur, Charles. *Egypt cuts off internet access.* January 28, 2011. https://www.theguardian.com/technology/2011/jan/28/egypt-cuts-off-internet-access (accessed December 19, 2017).

Bachmann, Sascha-Dominik, and Hakan Gunneriuson. "Hybrid Wars: 21st Century's New Threats to Global Peace and Security." *South African Journal of Military Studies*, 2015: 77-98.

Bisogni, Fabio, Simona Cavallini, and Sara di Tocchio. "Cybersecurity at European Level: The Role of Information Availability." *Communications & Strategies*, 2011: 105-124.

Brodie, Bernard. *The absolute weapon: Atomic power and the world order.* New York: Longman, 2006.

Civil Georgia. *4 Russian Officers Arrested, Charged with Espionage.* September 27, 2006. http://www.civil.ge/eng/article.php?id=13658 (accessed December 18, 2017).

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

Clausewitz, Karl. *On War (Complete Edition).* Edited by Michael Howard, & Peter Paret. Princeton: Princeton University Press, 1976.

Comb II, Peter C. "Traditional Military Activities in Cyberspace: The Scope of Conventional Military Authorities in the Unconventional Battlespace." *Harvard National Security Journal*, 2016: 526-576.

Cordes, Joseph. *An Overview of the Economics of Cybersecurity and Cybersecurity Policy.* GW-CSPRI-2011-6, Washington D.C.: George Washington University Cybersecurity and Policy Institute, 2011.

Davis, Joshua. *Hackers Take Down the Most Wired Country in Europe.* August 21, 2007. https://www.wired.com/2007/08/ff-estonia/ (accessed October 20, 2017).

Denning, Dorothy. "Rethinking Cyber Domain and Deterrence." *JFQ: Foint Force Quarterly*, 2Q 2015: 8-15.

Department of Homeland Security. *Cybersecurity Overview.* September 27, 2016. https://www.dhs.gov/cybersecurity-overview (accessed November 22, 2017).

Freedman, Lawrence. *Deterrence.* Cambridge: Polity, 2004.

Goodman, Will. "Cyber Deterrence Tougher in Theory than in Practice?" *Strategic Studies Quarterly*, 2010: 102-135.

Greenberg, Andy. *'Crash Override': The Malware That Took Down a Power Grid.* June 12, 2017. https://www.wired.com/story/crash-override-malware/ (accessed January 1, 2018).

Huth, Paul. "Deterrence and international conflict: Empirical findings and theoretical debates." *Annual Review of Political Science*, 1999: 25-48.

Iasiello, Emilio. "Is Cyber Deterrence and Illusory Course of Action?" *Journal of Strategic Security*, 2014: 52-67.

Jensen, Eric Talbot. "Cyber Deterrence." *Emory International Law Review*, 2012: 773-824.

Jervis, Robert. *Perception and misperception in international politics.* Princeton: Princeton University Press, 1976.

Jervis, Robert. "Rational deterrence: Theory and Evidence." *World Politics*, 1989: 289-324.

Kagan, Donald. *Thucydides: The Reinvention of History.* New York: Penguin Group, 2010.

Kaldor, Mary. *New and Old Wars.* Cambridge: Polity, 2012.

Kandelaki, Giorgi. "Georgia's Rose Revolution: A Participant's Perspective." *United States Institute for Peace.org.* July 2006. https://www.usip.org/sites/default/files/sr167.pdf (accessed December 18, 2017).

Kirschbaum, Joseph W. *DoD's Monitoring of Progress in Implementing Cyber Strategies Can be Strengthened.* GAO Report , Washington, D.C.: General Accounting Office, 2017.

Kittire, Orde S. *Lawfare: Law as a Weapon of War.* New York: Oxford University Press, 2016.

Knopf, Jeffery W. "Three Items in One: Deterrence as Concept, Research Program, and Political Issue." In *Complex Deterrence: Strategy in the Global Age*, by T V Paul, Patrick M. Morgan, & James J. Wirtz, 30-45. Chicago: University of Chicago Press, 2009.

Lambert, Michael. *Tracing the Roots of Russia's Hybrid Warfare Tactics.* October 11, 2017. http://www.eurasianet.org/node/85521 (accessed December 12, 2017).

Lucas, Nathan, and Kathleen McInnis. *The 2015 National Security Strategy: Authorities, Changes, Issues for Congress.* Information Paper, Washington D.C.: Congressional Research Service, 2016.

Maclean, Don. *Cybersecurity executive order: What works and what's missing.* July 12, 2017. https://federalnewsradio.com/commentary/2017/07/cybersecurity-executive-order-what-works-and-whats-missing/ (accessed December 30, 2017).

Magnuson, Stew. "Role, Responsibilities of Cyber Command Debated." *National Defense*, February 2017: 37-38.

Mandel, Robert. *Optimizing Cyberdeterrence.* Washington DC: Georgetown University Press, 2017.

Markoff, John. *Before the Gunfire, Cyberattcks.* August 12, 2008. http://www.nytimes.com/2008/08/13/technology/13cyber.html (accessed January 01, 2018).

McGhee, James. "Liberating Cyber Offense." *Strategic Studies Quarterly*, 2016: 46-63.

Mulford, Laurie A. *Let Slip the Dogs of (Cyber) War: Progressing Towards a Warfighting U.S. CYBER COMMAND.* Masters Thesis, Washington DC: National Defense University, 2013.

Murphy, Matt. *War in the Fifith Domain.* July 01, 2010. http://www.economist.com/node/16478792 (accessed January 01, 2018).

Newnham, Randall. "Georgia on my Mind? Russian sanctions and the end of the 'Rose Revolution'." *Jounral of Eurasian Studies*, 2015: 161-170.

North Atlantic Treaty Organization. *NATO.* JAN 01, 2017. https://www.nato.int/cps/en/natohq/topics_78170.htm (accessed October 15, 2017).

Peniston, Bradley. "Future US Navy Accident Investigations Will Look for Cyber Attacks." *Defense One.* September 14, 2017. http://www.defenseone.com/threats/2017/09/future-navy-accident-investigation-cyber-attacks/141014/?oref=d1-ios-app (accessed September 24, 2017).

Rhodes, Bill. *An Introduction to Military Ethics.* Santa Barbara: Praeger Security International, 2009.

Richards, Jason. "Denial-of-Service: The Estonian Cyberwar and its Implications for U.S. National Security." *International Affairs Review*, 2009: 65-72.

Rid, Thomas, and Ben Buchanan. "Attributing Cyber Attacks." *The Journal of Strategic Studies*, 2015: 4-37.

Rivera, Lieutenant Commander Matthew. *Deterrence in Cyberspace.* Masters Thesis, Washington, D.C.: National Defense University, 2012.

Rudolph, John B., Chomeau, Anne C. "Intelligence Collection and Analysis: Dilemmas and Decisions." In *Ethics and National Defense The Timeless Issues*, edited by James C. Gaston and Janis Bren Hietala, 113-132. Washington: National Defense University Press, 1993.

Russia Today. *Putin blames Georgia for raising tensions in Abkhazia.* April 21, 2008. https://web.archive.org/web/20080421185341/http://www.russiatoday.ru/news/news/23724 (accessed December 18, 2017).

Ruus, Kertu. *Cyber War I: Estonia Attacked From Rusia.* April 12, 2008. http://www.europeaninstitute.org/index.php/component/content/article?id=67:cyber-war-i-estonia-attacked-from-russia (accessed November 09, 2017).

Senate Committee on Armed Services. "Testimony of Admiral Michael Rogers, Director National Security Agency/Commander US CYBERCOM." *United States Senate Committee on Armed Services.* May 09, 2017. https://www.armed-services.senate.gov/hearings/17-05-09-united-states-cyber-command (accessed November 16, 2017).

Smith, Rupert. *The Utility of Force: The Art of War in the Modern World.* New York: Random House, 2007.

Sorley, Lewis. *Westmoreland: The General Who Lost Vietnam.* New York: Houghton Miffline Harcourt Publishing Company, 2011.

Space Foundation. *Senate Armed Services Committee Interested in Cyber Deterrence Strategy.* February 28, 2014. https://www.spacefoundation.org/news/senate-armed-services-committee-interested-cyber-deterrence-strategy (accessed January 01, 2018).

Stout, David. *The New York Times.* February 07, 2002. http://www.nytimes.com/2002/02/07/international/geneva-convention-to-be-applied-to-captured-taliban-fighters.html (accessed August 10, 2017).

The Economist explains. *How NATO's Article 5 Works.* May 09, 2015. https://www.economist.com/blogs/economist-explains/2015/03/economist-explains-6 (accessed October 12, 2017).

Tsikhelashvili, Ketevan, and Natasha Ubilva. *Case Study of the Conflict in South Ossetia.* Case Study, Boston: Martinus Nijhoff Publishers, 2008.

United States Department of Defense Publication. "Department of Defense Strategy for Operation in Cyberspace." *National Institute of Standards and Technology Information Technology Library.* July 2011. http://csrc.nist.gov/groups/SMA/ispab/documents/DOD-Strategy-for-Operating-in-Cyberspace.pdf (accessed August 22, 2017).

—. "The DoD Cyber Strategy 2015." *United States Department of Defense.* April 17, 2015. The DoD/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf (accessed September 09, 2017).

United States Government Publication. "Cyberspace Policy Review." *The Department of Homeland Security.* January 2009. https://www.dhs.gov/sites/default/files/publications/Cyberspace_Policy_Review_final_0.pdf (accessed September 09, 2017).

—. "Executive Order 13636: Improving Critical Infrastructure Cybersecurity." *United States Department of Homeland Security.* July 12, 2013. https://www.dhs.gov/sites/default/files/publications/dhs-eo13636-analytic-report-cybersecurity-incentives-study.pdf (accessed September 05, 2017).

—. "National Security Strategy 2015." *United States Army G8 Homepage.* February 06, 2015. http://www.g8.army.mil/pdf/National_Security_Strategy_6Feb2015.pdf (accessed September 07, 2017).

—. "National Security Strategy 2017." *Whitehouse.gov.* December 18, 2017. https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905-2.pdf (accessed January 1, 2018).

—. "Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure." *whitehouse.gov.* May 15, 2017. https://www.whitehouse.gov/presidential-actions/presidential-executive-order-strengthening-cybersecurity-federal-networks-critical-infrastructure/ (accessed December 30, 2017).

—. "The Comprehensive National Cybersecurity Initiative." *Federation of American Scientists.* May 2009. The /irp/eprint/cnci.pdf (accessed August 29, 2017).

—. "The National Strategy to Secure Cyberspace." *United States Computer Emergency Readiness Team.* February 2003. https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf (accessed September 01, 2017).

United States National Research Council. *Proceedings of a Workshop of Deterring Cyberattacks: Informing Strategies and Developing options for U.S. Policy.* Proceedings, Washington, D.C.: The National Academies Press, 2010.

VITA

Charles A. DeHoag

Mr. DeHoag is a former Sailor in the United States Navy and a veteran civilian employee of the U.S. Department of Defense. Prior to attending this senior service school / war college program, Mr. DeHoag was the Deputy of the Middle East and North Africa Division of the Defense Attaché Service (DAS). Mr. DeHoag's primary duties were providing advocacy, oversight, and guidance for DAS members in the Middle East and Africa Regional Center, located on Joint Base Anacostia-Bolling, as well as forward deployed members working out of embassies throughout U.S. Central Command, U.S. Africa Command, and U.S. Europe Commands' areas of responsibility.

Mr. DeHoag joined the department in 2003. His experience includes multiple deployments to both Iraq and Afghanistan in support of combat operations, a tour as the Deputy Defense Attaché in Sri Lanka, tours in several embassies throughout South and Southeast Asia, and as Branch Chief for Defense Attaché operations in Southeast Asia, and in the Levant, and North Africa.

Mr. DeHoag holds a Bachelor of Arts Degree in English Literature, a Master of Arts Degree in Crisis Management and Communication, and a Master of Science in Joint Campaign Planning and Strategy from the Joint Forces Staff College – National Defense University.