REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
22-03-2016	Master's of Military Studies	SEP 2015 - APR 2016

4. TITLE AND SUBTITLE
Proposed Cyber Force Development Strategy

5a. CONTRACT NUMBER
N/A

5b. GRANT NUMBER
N/A

5c. PROGRAM ELEMENT NUMBER
N/A

6. AUTHOR(S)
Gurley, Nicholas, E, Lieutenant Commander, USN

5d. PROJECT NUMBER
N/A

5e. TASK NUMBER
N/A

5f. WORK UNIT NUMBER
N/A

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
USMC Command and Staff College
Marine Corps University
2076 South Street
Quantico, VA 22134-5068

8. PERFORMING ORGANIZATION REPORT NUMBER
N/A

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSOR/MONITOR'S ACRONYM(S)
Flynn, Matthew

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

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

13. SUPPLEMENTARY NOTES

14. ABSTRACT
In order to improve the nation's cyber capabilities, this paper recommends a cyber force development strategy. This paper introduces the challenges of the cyber domain, presents updated definitions of critical cyber concepts, and shows that previous theories (especially maritime domain theories) are applicable to the cyber domain. The paper uses the Law of Armed Conflict to argue that the military is the right choice for the nation's cyber force. The paper proposes the development of a framework to man, train, and equip the nation's cyber force based on the success of the frame-work used by the Navy Nuclear Propulsion Program. Additionally, the paper shows that the military is the right choice to innovate in the face of high technology challenges.

15. SUBJECT TERMS
Cyber Operations, Cyber Domain, Cyber War, Cyber Warfare, Cyber Attack, Military Cyber Forces, Law of Armed Conflict applied to Cyber War, Cyber Power

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			USMC Command and Staff College
					19b. TELEPHONE NUMBER *(Include area code)*
Unclass	Unclass	Unclass	UU	53	(703) 784-3330 (Admin Office)

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

MASTER OF MILITARY STUDIES

TITLE:

PROPOSED CYBER FORCE DEVELOPMENT STRATEGY

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

AUTHOR:

LCDR NICHOLAS E. GURLEY, USN

AY 15-16

Mentor and Oral Defense Committee Member: Matthew Flynn
Approved: _____
Date: _____ 3/22/16

Oral Defense Committee Member: J.W. Gordon
Approved: _____
Date: 3/22/16

DISCLAIMER

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

Executive Summary

Title: Proposed Cyber Force Development Strategy

Author: Lieutenant Commander Nicholas E. Gurley, United States Navy

Thesis: In order to improve the nation's cyber capabilities, this paper recommends a cyber force development strategy.

Discussion: In late 2014, a team of active-duty cyber force personnel was soundly defeated during a cyber operations exercise. The defeat caused cyber theorists to ask several questions, including whether the military should step aside in favor of an all-civilian cyber force, whether it was possible for the military to develop the culture required to find and retain the talent required for an effective cyber force, and whether the military could even innovate in the cyber domain. This paper introduces the challenges of the cyber domain, presents updated definitions of critical cyber concepts, and shows that previous theories (especially maritime domain theories) are applicable to the cyber domain. The paper uses the Law of Armed Conflict to argue that the military is the right choice for the nation's cyber force. The paper proposes the development of a framework to man, train, and equip the nation's cyber force based on the success of the framework used by the Navy Nuclear Propulsion Program. Additionally, the paper shows that the military is the right choice to innovate in the face of high technology challenges, using the rapid development of nuclear-powered ballistic missile submarines as a case study.

Conclusion: This paper reaches the conclusion that the nation's cyber forces should be composed of military personnel and presents a development strategy to properly man, train, and equip the cyber forces of the future. Additionally, it explores the implications of the three options available to the nation at this critical time, arguing that the most efficient and effective way to improve the nation's cyber forces is to transfer responsibilities for cyber operations to one service as opposed to continuing the current joint development path or attempting to develop a separate Cyber Service.

Table of Contents

Preface

I selected this topic because I grew up with information technology. As a child, I participated in the explosive growth of the Internet as client programs such as America Online and Prodigy took over the bulletin board computer systems, private networks linking users in regional markets. As a young man, I built computer systems and networks, assisting in maintaining my school's information network as a computer technician. I learned how to program, and designed front-end user interfaces for website databases. The implications of these technologies occupied my thinking for most of my life. However, it was not until I attended the Marine Corps University that I learned how to engage in the academic debate surrounding these technologies. For this, I am grateful.

It is important that I state clearly that I am a Surface Warfare officer, with a nuclear propulsion sub-specialty, in the United States Navy. As such, I have a bias favoring the Navy's nuclear propulsion program (NNPP). The reason for the bias is my personal experience, which has been overwhelmingly positive. Not only did the NNPP teach me, as a liberal arts business administration major, the intricacies of the hard sciences required to safely operate a nuclear propulsion reactor, it also taught me how to learn. It taught me the importance of "technical leadership". It taught me how to train successfully. It taught me the importance of continuous improvement. More importantly, the NNPP taught me how to apply these skills to a variety of other projects that grew into passions. As a successful framework, the NNPP has more to offer the nation.

This paper would not be possible were it not for the guidance and assistance of Colonel Gary Brown, United States Air Force (Retired) and Matthew Flynn, Ph.D. Additionally, Commander Russell Evans, United States Navy, contributed significantly by providing an important and significant perspective shift. Last, and certainly not least, this project would not have been possible without the support and editing prowess of my wife, Anyika King-Gurley. Thank you.

On August 4, 2014, Andrew Tilghman published a story for Navy Times describing the defeat of active-duty United States (U.S.) Cyber Command (USCYBERCOM) personnel by an opposing team of reservists, who worked in the information technology field in their private sector jobs, during a cyber operations exercise. The article quoted an unnamed Capitol Hill staffer who observed the exercise as noting the USCYBERCOM forces were "pretty much obliterated" and "didn't even know how they'd been attacked."[1] The article brings to mind significant concerns. Is the U.S. military capable of succeeding in a cyber conflict, or is it a job for civilians? Is the culture of the U.S. military conducive to getting and retaining the talent necessary to create an effective fighting force in the cyber domain? Is the U.S. military innovative enough to compete in the cyber domain?

This paper proposes a cyber force development strategy in order to improve the nation's cyber capabilities. By implementing this proposal, the nation's cyber forces will better meet the nation's requirements. Importantly, the cyber force will also become more efficient in its use of resources while preparing for future cyber operations.

This paper is organized in eight sections. The first section introduces the challenging nature of the cyber domain. Critical definitions are established in the second section. The third section develops the concepts of cyber power, cyber warfare, and cyber forces. The fourth section examines the question of whether the nation's cyber forces should be a military or civilian force. The fifth section proposes a method to organize the nation's cyber forces. The sixth section answers the question as to whether the military has the capability to innovate in the cyber domain. The conclusion explores the implications of the proposed solution. Should the nation's cyber forces continue on their current path of jointness or should the nation seek a different solution?

The Challenging Nature of the Cyber Domain

In 1969, the U.S. Department of Defense (DOD) agency Defense Advanced Research Projects Agency (DARPA) developed a survivable computer network, called the Internet: a persistent information processing, retrieval, and storage system resistant to destruction. Initially, only military and academic institutions had access to this system, partially because these institutions had a near monopoly on high technology. By the 1980s, many private corporations were using networked computer systems. Businesses introduced personal computers for use in the home. By 1991, the British scientist Tim Berners-Lee developed the World Wide Web, making the Internet easily accessible by the public. Over the past twenty years, the Internet has grown rapidly. Based on an infographic published in July 2014, Google has indexed only 0.004% of the Internet, requiring 200 terabytes of data. The implication of this amount is staggering, considering recent estimates that suggest the index contains more than 5 billion webpages.[2]

Access to the Internet has also grown dramatically. In 1998, 42.1% of American households had a computer and 26.2% had Internet access in the home.[3] The early 2000s saw an explosion of growth due to less expensive computers and the rise of Internet-connected smart phones. By 2013, 83.8% of American households had computers, with 74.4% reporting Internet subscriptions.[4] As of November 2015, the proliferation of affordable devices and communication access points brought Internet access to 46.4% of the world, more than 3.3 billion individuals.[5] In other words, with nothing more than a smart phone, all of these individuals have access to the cyber domain, with the capability to conduct cyber operations against a computer network. In 1965, Gordon Moore, co-founder of Intel, a computer technology company, described an observation known as Moore's Law in which approximately every two years, the number of com-

ponents on an integrated circuit doubles, with a resultant increase in processing power.[6] The implication is that every two years, the capability of handheld computing devices will continue to improve significantly, improving the cyber operations capability available to each technology user. Much of this is proving true in cyberspace.

While clearly beneficial, the use of cyberspace is not without its problems. The first successful challenge to the free information sharing on the Internet was the Morris worm, originally intended to survey the size of the Internet in 1988. Due to an error in the program's code, it copied itself on a target computer multiple times, eventually rendering infected computers useless. Estimates place the economic impact at $98 million, mostly based on the cost in man-hours to undo the damage caused by the worm.[7] This worm illustrates how a low barrier to entry to the cyber domain resulted in a significant denial of service and brought down the early Internet. In this case, the low barrier to entry was as simple as access to a computer on the Internet. In today's modern world, that barrier is lower: any person with a smartphone has the capability to conduct cyber operations against an Internet-connected target. Additionally, the Morris worm shows that nefarious motives are not a requirement to cause problems. Human error while developing software on an Internet-connected computer is enough.

Hackers executing modern cyber operations are purposeful and coordinated. Some have economic objectives, others political or military. For example, in 2011, hackers conducted an attack against Epsilon, a marketing company for major U.S. companies. The attackers successfully exfiltrated client personal information for several major companies including major financial institutions.[8] In 2007, pro-Soviet hacker groups targeted the government of Estonia, using a Distributed Denial of Service (DDoS) to disrupt targeted networks for twenty-two days.[9] In 2004, the U.S. government discovered what it called the Titan Rain exfiltration, resulting in the

compromise and removal of sensitive military and industrial technology from infiltrated systems, which included Lockheed Martin, NASA, and the Redstone Arsenal.[10] More recently, discovered in 2015, hackers, thought to be backed by the People's Republic of China (PRC), compromised the U.S. government Office of Personnel Management (OPM) for more than a year, resulting in the exfiltration of 21.5 million personnel records, including sensitive security-clearance-related information for federal employees and military personnel.[11] Most recently, hackers have even successfully shown the ability to control flying airplanes and driving cars.[12]

However, the types of cyber actions most concerning to security planners are those that directly affect the physical domain. For example, in July 2010, unknown hackers infected Iran's Natanz nuclear facility with the Stuxnet virus, causing one-fifth of their nuclear centrifuges to destroy themselves through the corruption of computer-driven control systems. The entire time, the centrifuge diagnostic systems reported that they were functioning normally, even displaying previous values recorded from the plant's protection system.[13] The dangers related to this kind of cyber action, which may have risen to the level of an attack due to the physical level of destruction, warrants concern by policy makers, especially due to the proliferation of locally and remotely computer-controlled systems in power plants, hydroelectric dams, factories, and hospitals. In the case of the Stuxnet virus, if the attack had been successfully attributed to another state, Iran would likely have been within its rights to exercise self-defense.[14]

There are many additional challenges faced when operating in the cyber domain. Matthew Crosston, Director of the International Security and Intelligence Studies Program at Bellevue University, discusses several of these while arguing for a cyber mutually assured debilitation national strategy, including correctly identifying the attack's origin, identifying the attacker, determining if retaliation is the correct course of action, determining when the retaliation threshold

is crossed, and avoiding unnecessary escalation.[15] William Goodman, advisor on defense issues to Senator Patrick Leahy, analyzing cyber deterrence effectiveness, brings attention to additional concepts including the wide range of effects that caused by a single tool (scalability) and the instantaneous nature of a cyber attack (temporality).[16] Doctrine provides even more challenges, such as the concern that a friendly cyber action may damage current intelligence collections operations, requiring at a minimum coordination with national, and allied, intelligence collection agencies prior to conducting a retaliation.[17] As a result of these challenges, current cyber release authority is likely not easy to receive. As Crosston notes, "the international community's response to evidence of direct governmental involvement in a cyber attack against another state could very easily be to consider it an act of war."[18]

Reducing Cyber Confusion: Critical Definitions

It is important to identify clearly the terms used in this paper. Due to the complex nature of the cyber domain, and the energetic academic debate surrounding the topic, there are several confusing and competing definitions. This paper presents updated definitions for the terms cyber domain, cyber warfare, and cyber attack. The purpose of the definitions is to better align the concept of cyber warfare with physical warfare, making legal comparisons easier while reducing the confusion surrounding cyber operations. Additionally, these terms will assist in developing the mission of the nation's cyber forces.

The first definition is the cyber domain. Doctrine calls this domain cyberspace, and describes it as consisting of "many different and overlapping networks, as well as the nodes (any device or logical location with an internet protocol [IP] address or other analogous identifier) on those networks, and the system data that support them."[19] Colin S. Gray, strategic theorist, pre-

fers the definition forwarded by Daniel T. Kuehl, information operations professor at National Defense University: "Cyberspace is a global domain within the information environment whose distinctive and unique character is framed by the use of electronics and the electromagnetic spectrum to create, store, modify, exchange, and exploit information via interdependent and interconnected networks using information-communication technologies."[20] Kuehl's definition is preferred to the doctrinal definition because it includes human use of the electromagnetic spectrum to connect information technology networks wirelessly, which is a critical connector to consider when discussing the cyber domain. For example, this is how Navy warships share tactical data from organic sensors to create the Common Operating Picture used by carrier strike groups, fleet commanders, and combatant commanders to understand the maritime situation. Not including the electromagnetic spectrum in a definition of the cyber domain results in separating electronic warfare-type operations and cyber operations, which increases confusion and introduces deceptive conceptual barriers when developing cyber power theories. This paper uses Kuehl's definition. Additionally, it uses the terms cyber domain and cyberspace interchangeably for readability.

The second definition is cyber warfare. Richard A. Clarke, White House security advisor, defines it as "actions by a nation-state to penetrate another nation's computers or networks for the purposes of causing damage or disruption."[21] While Richard Stiennon, security industry analyst, does not define it directly, he uses it as "two adjacent networked countries [engaged] in network attacks concurrent with tanks rolling across their borders."[22] Both of these definitions are unsatisfying, especially as they lump in all types of cyber activities, for example cyber espionage, in the definition of cyber warfare. In fact, combining all types of cyber activities under the rubric of cyber warfare is a theme of several definitions, including Amit Sharma, of the Ministry

of Defense of India, and Jeffrey Carr, cyber intelligence expert, who both use a definition based in the theories of Sun Tzu, paraphrased as cyber warfare is winning a war without physical conflict.[23] In other words, many theorists use cyber warfare too broadly. Doctrine sidesteps this problem by deigning to define cyber warfare, instead defining each type of cyber action separately and linking them under the umbrella term of Cyberspace Operations.[24] The problem with this approach is that the term cyber warfare does not appear in the Cyberspace Operations manual at all. This paper prefers the definition offered by Scott Applegate, cyber security analyst: "Cyber warfare is the use of armed attacks in and through cyberspace as an extension of one nation-state's politics to impose its political will onto another nation-state."[25] The importance of this definition is its exclusion of cyber operations, such as cyber crime and cyber espionage, from cyber warfare. Obviously, this definition excludes cyber warfare against non-state actors, such as terrorist groups. This is no different from conventional warfare, which is the purview of nation states. The use of this definition does not preclude the use of cyber force against a non-state actor, but rather keeps the concept of cyber warfare in the same orbit as conventional warfare.

The third definition is cyber attack. The doctrinal definition of cyberspace attack is unsatisfying, focusing on "denial effects" and "manipulation that leads to denial", using effects-based terms such as deny, degrade, disrupt, destroy, and manipulate.[26] In this case, the doctrine ignores concepts from the Law of Armed Conflict (LOAC), such as use of force and armed attack, and results in overclassifying cyber actions as cyberspace attack. Applegate provides a definition of cyber force, as a cyber action resulting in "physical damage, death, or injury, or threatens the political independence or territorial integrity of a nation-state".[27] The *Tallinn Manual*, published in 2013, is the authoritative "non-binding document applying existing law to cyber warfare" developed by the North Atlantic Treaty Organization (NATO) Cooperative Cyber De-

fense Center of Excellence.[28] It makes a distinction between cyber force and cyber armed attack, arguing that for a use of cyber force to rise to the level of an cyber armed attack, it must meet additional requirements of "scale and effect", the levels of which are in debate.[29] However, once a cyber action rises to the level of a cyber armed attack, the *Tallinn Manual* panel agrees that it triggers the state's right to self-defense.[30] This paper prefers a blend of the two descriptions, therefore: cyber armed attack is a use of cyber force which causes the level of physical damage, death, or injury, or threatens the political independence or territorial integrity of a nation-state, in a manner for which the state would normally execute the right of self-defense if caused by a kinetic weapon system. This paper uses the terms cyber attack and cyber armed attack interchangeably.

With these terms clearly defined, it becomes apparent that cyber warfare is not a new type of warfare. This clarity significantly reduces the confusion currently associated with concept of cyber war. Additionally, it makes clear that cyber warfare is a subset category of possible activities in the cyber domain, completely separate from cyber espionage and cyber crime. Cyber warfare should not be used as an umbrella designation encapsulating these two terms. Finally, clearly identifying this terminology is important when developing the mission of the nation's cyber forces as made clear in the following section.

Developing a Mission: Cyber Power, Cyber Warfare, and Cyber Forces

The purpose of this section is to develop the mission of the nation's cyber forces, by discussing the concept of cyber power and the object of cyber warfare. Just as a nation uses a strategy (ends) to develop a conventional military service (means) with specific capabilities (ways),

developing the cyber force requires developing their mission first. Interestingly, despite the pervasive claim that operations in cyberspace constitute a new type of warfare, it is actually a simple matter to view cyberspace operations using the concepts of maritime operations, suggesting that cyberspace operations are not as exotic as they first appear.

To start, modern nations must understand cyber power as well as their traditional understanding of land and sea power. As Gray observed when discussing maritime strategy: "In major conflicts between maritime and continental powers, each side must pursue a mixed strategy embracing both land and sea elements."[31] In today's world, connected by cyberspace, it is easy to understand that future conflicts will require a strategy in which cyber elements feature prominently with conventional methods of waging war. When discussing nation-state strategy regarding cyberspace, theorists can view cyber power through the lens of sea power. In this analogy, the cyber domain and the sea domain are the same. Sir Julian Corbett, strategic naval theorist of much acclaim, observes the natural state of the maritime domain: "the normal position is not a commanded sea, but an uncommanded sea."[32] This is also true of the cyber domain. As long as an information network is connected to the cyber domain as a whole, it is exposed to the risk of intrusion. This is the same as any bay connected to the sea. Therefore, modifying the maxims of Corbett gives this truth: Command of cyberspace, therefore, means nothing but the control of cyber communications, whether for commercial or military purposes.

It is just as important to realize that cyber power alone will not win wars. This is no different than attempting to use sea power or air power to win wars alone. Jakub Grygiel, international relations expert, wrote, "A maritime power must have a strategic beachhead in the form of allies or actual forces that put pressure directly on the territory of the land power."[33] In other words, in order to win conflicts, nations using cyber power must use it alongside traditional

methods of waging war. Therefore, drawing again from the maritime analogy, the cyber power of a nation is its ability to use the cyber domain for military or commercial purposes and prevent adversaries from using them.[34] Just as Gray argues that sea power influences a conflict's outcome through the strategic leverage of denying an enemy's use of maritime lines of communication, cyber power influences outcomes of a conflict through the advantage of denying an adversary nation's use of cyber lines of communication.[35]

With an understanding of cyber power, it is possible to develop the object of cyber warfare. Again, using the analogy of warfare in the maritime domain, Corbett remarked "the object of naval warfare must always be directly or indirectly either to secure the command of the sea or to prevent the enemy from securing it."[36] Therefore, the overarching object of cyber warfare is to directly or indirectly secure the nation's cyber lines of communication and prevent adversaries from doing the same.

With a clear definition of cyber warfare, an understanding of a nation's cyber power, and identification of the object of cyber warfare, it is possible to develop the missions of the nation's cyber forces. This paper develops four missions. Developing and defining the missions of the nation's cyber forces is critical because they are what drive the development of future capabilities.

First, it is important to understand that Corbett did not want his theories applied to entire sea domain; he understood the fallacy of statements like "the sea is all one."[37] Based on the preceding discussions regarding the challenges of the cyber domain, it is clearly not possible to demand that our forces establish and maintain command of the entirety of cyberspace. It is not technically feasible, at least with today's technologies, and defeats the benefits of an information-sharing global commons. Instead, quoting Corbett, "If the object of command of the sea

is to control communications, it is obvious it may exist in various degrees. We may be able to control the whole of the common communications as the result either of great initial preponderance or of decisive victory. If we are not sufficiently strong to do this, we may still be able to control some of the communications; that is, our control may be general or local."[38] Therefore, by applying the tenets of maritime warfare to the tenets of cyber warfare, it becomes clear that the first mission of the nation's cyber force is to directly or indirectly secure cyber lines of communication in a defined operations area while preventing adversaries from doing the same. During a conflict, when cyber lines of communication are contested, this may require the use of cyber attacks.

Second, it makes sense that the responsibility for defending military networks would fall to the cyber force. The Department of Defense Information Networks (DODIN) construct defines which military networks require defense. As of 2011, the DODIN was comprised of more than 15,000 computer networks with more than seven million information technology devices.[39] This is the second mission for the cyber force.

Third, when previously discussing the challenges of the cyber domain, there were allusions to non-state hackers causing havoc in the cyber domain. However, the nation cannot expect military cyber forces to handle every network intrusion that occurs within U.S. borders. Additionally, a nation's military cyber force cannot legally investigate and prosecute every hacker. To this end, the government's current lead agency for cybersecurity is the Department of Homeland Security (DHS). Instead, it is more appropriate to identify critical infrastructure networks for military cyber forces to defend. DHS developed the Critical Infrastructure and Key Resources (CIKR) Support Annex, which outlines the current government process to identify critical infrastructure from all types of threat, such as terrorist attack, natural disasters, or cyber

threats. The method outlined assigns responsibility to various government departments to create a list of CIKR for specific sectors, such as "agriculture and food" or "defense industrial base."[40] Fourteen agencies develop CIKR lists for seventeen sectors.[41] Although this method may be effective, the number of agencies participating in this planning process reduces the efficiency. Defining CIKR via this process does not separate those critical infrastructures especially vulnerable to cyber attack via a universally accepted categorization. The use of fourteen different agencies results in fourteen different characterizations. Additionally, it is doubtful that the various agencies have the requisite cyber experience, capacity, and resources to identify successfully the most vulnerable critical infrastructure networks. To solve this problem, President Barack Obama issued an executive order to improve critical infrastructure cybersecurity, requiring the Secretary of Homeland Security to develop an objective standard in identifying critical infrastructure and consult with the sector-specific agencies to develop a list of critical infrastructure vulnerable to cyber threats.[42] This executive order clearly defined critical infrastructure in terms of cybersecurity and also centralized the identification of critical infrastructure networks. This executive order identified critical infrastructure as "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact" on national security.[43] The centralization of critical infrastructure network identification is likely to be both effective and efficient in identifying those most vulnerable to cyber attack. However, although it requires the consultative development of a cybersecurity framework, it stops short of assigning responsibility for the protection of vulnerable critical infrastructure networks. The current process, as defined by the CIKR Support Annex, identifies different primary agencies responsible for various Emergency Support Functions (ESF) in the case of a disaster or terrorist attack, but does not include provisions for a directed attack by an-

other nation. As there is no specific Cybersecurity ESF, the Communications ESF is the most appropriate category, which encapsulates functions such as Information Technology, Communications, and Emergency Services.[44] This category currently assigns the roles of coordination and preparedness to three different agencies.[45] The lack of a cybersecurity ESF reduces the effectiveness of the process when defending against cyber threats, and the use of multiple agencies reduces the efficiency in terms of response. A military cyber force would have the experience, capability, and resources to defend properly identified critical infrastructure networks successfully. This paper advocates assigning military cyber forces responsibility for the protection of specific critical infrastructure networks identified by this process. For example, it would be inappropriate for a military cyber force to defend the network of a large retailer, such as Wal-Mart, from a cyber attack. However, it may be appropriate for the cyber force to defend the New York Stock Exchange network due to the implications to national security if the stock exchange computer network was lost. It is certainly appropriate for the cyber force to defend a nuclear power plant's computer network due to the capacity for destruction if an adversary force compromised the computer network. There are significant benefits to using military forces to defend these critical infrastructure networks. In the case of an adversary nation's cyber attack, using military cyber forces ensures the appropriate experience, capability, authority, and resources are available immediately to mitigate the situation without the coordination required if the lead agency is non-military. Similarly, if these critical infrastructure networks become targets of non-state cyber operations, or state cyber operations not including armed attack, cyber forces could defend against the intrusion and then hand off responsibility for follow-on investigation and prosecution to appropriate authorities. It is a relatively simple matter to scale down operations. Just as in physical domains, Title 10 of the U.S. Code (U.S.C) defines lawful military activity. As de-

scribed by doctrine, the illegal activities of American citizens in cyberspace fall under the purview of law enforcement agencies per Title 18 of the U.S.C.[46] Similarly, cyber espionage falls under the purview of agencies assigned under the Office of the Director of National Intelligence per Title 50 of the U.S.C.[47] Therefore, the third mission of the cyber force is to defend critical infrastructure networks as defined by higher authority.

Finally, doctrine states that the Title 10 of the U.S.C. responsibilities of the armed forces, relating to the cyber domain, is to "man, train, and equip U.S. forces for military operations in cyberspace."[48] This task can be understood as "be prepared to conduct military operations in cyberspace." This is the fourth mission for the cyber forces.

Taken holistically, the missions derived for the military cyber force align closely with the current mission statement of USCYBERCOM, with the exception of protecting critical infrastructure networks.[49] Although USCYBERCOM's mission statement is encouraging, this paper advocates translating the military cyber force missions developed previously into clear tasks, which will result in resourcing the cyber force appropriately. Therefore, based on the missions developed previously, the tasks derived for the nation's cyber forces are to directly or indirectly secure cyber lines of communication in a defined operations area while preventing adversaries from doing the same, defend the DODIN, defend critical infrastructure networks as defined by higher authority, and be prepared to conduct military operations in cyberspace.

A Legal Argument for Military Cyber Forces

In the previous sections, this paper discussed the challenging nature of the cyber domain, developed critical definitions, and established the mission of the cyber forces. This section en-

deavors to answer the question of whether the nation's cyber forces should be composed of military personnel or civilians by proposing that a military cyber force is the best answer.

As opposed to discussing the merits of either group based on performance metrics, this paper will approach this challenge from the legal aspects of conflict. Already, current U.S. legislation excludes civilians from performing inherently governmental functions such as "protecting and advancing" U.S. interests through military or any other action, which would include cyber war.[50] However, as opposed to using U.S. domestic law, this paper will examine the use of civilians through the lens of the internationally recognized law of armed conflict (LOAC). The cyber force will be involved in future conflicts, for which there are already established conventions. Per the Department of Defense's Law of War Manual, "the [LOAC] exists to protect combatants, noncombatants, and civilians from unnecessary suffering."[51]

In order to reduce the "evils of war", the LOAC distinguishes between military forces and civilians.[52] However, the LOAC does not bar a specific category of person from participating in cyber operations.[53] During conflicts, a nation's armed forces have certain responsibilities, and by executing them, receive certain rights. Similarly, civilians have certain responsibilities, which when executed, grant them specific rights. Persons who fall between the boundaries established by the definitions of armed forces and civilians, such as "private persons engaging in hostilities", or those "persons engaging in spying, sabotage, and similar acts behind enemy lines" fall into the category of "unprivileged belligerents."[54] Unprivileged belligerents must face the disadvantages of both combatant and civilian statuses without their benefits. The *Tallinn Manual* concurs with these assessments.[55]

In order to participate in a conflict, an armed force must act based on a state's authority.[56] A commander with the appropriate authority must be responsible for the armed force.[57] The

armed forces must have a "fixed distinctive sign recognizable at a distance" which separates them from the civilian populace, generally through the wear of a military uniform.[58] Weapons must be carried openly.[59] Finally, the military force must enforce the LOAC when conducting their operations.[60] Members of the armed forces engaged in the conflict are subject to attack by an enemy combatant, but they are also subject to the benefits of the Geneva Conventions when wounded or taken prisoner. The *Tallinn Manual* agrees with these requirements, with a few caveats. One, a minority of the experts who developed the *Tallinn Manual* state that the "sole qualification of combatant status for members of the armed forces is status as members."[61] This would grant cyber forces at a remote geographic location the same rights and responsibilities of the military forces actually engaged in the conflict by virtue of their membership in the military. Two, private individuals may be invited to fight for the nation (for example, the government may enter into an agreement with a private company that has technical capabilities that the military lacks) and, as long as the group's behavior "makes clear for which party the group is fighting", they may be afforded combatant rights and responsibilities.[62] Three, individuals of a group that are participating in the conflict but are not a member of the parties of the conflict (for example, hacktivist groups during an armed conflict) are considered unprivileged belligerents.[63] Military armed forces are a nation's traditionally accepted warriors. Using sanctioned military forces in cyber warfare eases the legal requirements of conflict.

Furthermore, the LOAC protects civilians. They "must not be made the object of an attack" as long as they take no direct part in hostilities.[64] The *Tallinn Manual* agrees, using the example of a civilian group of "patriotic hackers": once they take participate in cyber hostilities, adversary forces may target them lawfully during the time of their participation in the conflict.[65] Additionally, while participating in the conflict, civilians do not receive protections exempting

them from the adversary state's domestic law; civilians who take part in hostilities may face a trial and punishment by the adversary state.[66] In other words, civilians retain significant protections as long as they do not participate in hostilities. Although the cyber domain creates a situation in which cyber forces are not required to geolocate with engaged armed forces, using civilian personnel to engage in hostilities creates legal hurdles and inconsistencies, increasing the risk of an adversary attack on civilian centers in their attempts to neutralize private individuals participating in cyber hostilities.

There is a provision for civilians to act as a "person authorized to accompany the armed forces."[67] While civilians acting as cyber warriors provide support to military operations through information technology, they would become subject to additional risks. Although they are not to be made the direct object of an attack, they must accept "increased risk of incidental harm" through their proximity to the armed forces, including accepting that a confused enemy may believe them to be combatants based on their location.[68] In this capacity, they are entitled to Prisoner of War protections if captured.[69] However, there is no "general license" to participate in hostilities.[70] In fact, commanders who authorize the use of personnel in this capacity run the risk of later war crime prosecution for crimes committed by such civilian personnel.[71] Although feasible, the real risk is that opposing forces would reclassify these cyber warriors as unprivileged belligerents.

While there is also the possibility of hiring third-party private individuals to conduct cyber warfare, this is equivalent to hiring a mercenary. The *Tallinn Manual* describes the conditions that would reclassify a private individual as a mercenary, causing them to become an unprivileged belligerent: "special recruitment", "direct participation in hostilities", "desire for private gain as a primary motivation", "neither a national of a party to the conflict nor a resident of

territory controlled by a party", "not a member of the armed forces to a party to the conflict", and "not sent by another state on official duty as a member of its armed forces."[72] In other words, if one nation hires a private corporation of computer experts in a country not party to the conflict, all of the employees participating in cyber operations may be reclassified as unprivileged belligerents, lose their civilian protections, and be lawfully targeted. It is easy to see that this would be a possible accidental scenario if the nation turned to a civilian-only cyber force.

In conclusion, although the LOAC does not prohibit a category of person from participating in armed conflict, the legal protections offered to those categories differ greatly. As the LOAC was designed to reduce the effect of war on the civilian population, using civilians in cyber warfare is counterproductive. Using civilians confuses the legal framework and increases the risk that civilians will be misclassified, resulting in the loss of their rights during armed conflicts. For a civilian cyber force located in a population center, it is even more dangerous. If they should become lawful targets, it increases the risk of attack on innocent civilians co-located nearby. In terms of conflict between nation states, an armed military force is the most familiar and accepted method to conduct conflict. As a global leader modeling the desired behavior of the rest of the world, and in the hope of reducing the suffering of civilians during conflict, the best option for the U.S. is to use a military cyber force with established authorities, legal rights, and responsibilities.

Organizing Cyber Forces: A Development Strategy

The focus of this section is the development of military cyber forces, charged with the nation's cyber defense and the requirement to prepare for offensive cyber operations. These cyber forces should organize along familiar military lines. In other words, there should be two primary

classifications of personnel including commissioned officers and enlisted personnel. Commissioned officers, as the leaders, hold the authorities required to command their forces in conflict, as required by the LOAC and agreed to by the *Tallinn Manual*.[73] Enlisted personnel, as cyber force operators and technicians, are the actual warfighters, engaging cyber systems as ordered. This section is not meant to develop conventional military network administrators, who enable what doctrine calls "ordinary business operations" including "non-warfighting capabilities."[74] They would be continue to be manned, trained, and equipped according to their service-specific career development paths. There is a significant difference in the desired culture and performance of cyber warriors, where traits such as creativity and initiative are highly valued, versus network administrators, where a trait such as procedural compliance is more desirable. Civilian personnel participate as well, in traditional capacities of government support and corporate contractors. Government support personnel provide critical administrative and non-combat services, while corporate contractors perform duties such as maintaining critical equipment and developing new capabilities. Throughout this section, this paper refrains from recommending a tactical or unit organization for the cyber forces. Previously, the paper developed a recommended set of cyber force missions; cyber planners can use those to design the organization appropriate to their service. Instead, this paper proposes a framework for developing the cyber forces.

As one of the missions, the cyber forces are required to be prepared to conduct cyber operations, which requires manning, training, and equipping. There is a lot of discussion revolving around the type of personnel who will make a good cyber warrior, and whether or not the current military culture is conducive to these individuals. Colonel Gregory Conti, Director of West Point's Cyber Security Research Center, writing with Colonel David Ramond, a West Point professor, posits that the "ideal cyber warrior will possess a high technical aptitude, be a creative

problem solver, and possess a hacker mindset that enjoys manipulating complex systems and pushing technology in ways unintended by its designers."[75] These are not the "biggest cavemen" leaders of the traditional kinetic military branches.[76] Writing with Colonel Jen Easterly, former commander of the Army Network Warfare Battalion, Conti declares, "building the most effective Cyber Command will require fundamentally changing military culture – specifically how we think about networks and how we manage the talent that we need to leverage these networks for warfighting effects."[77]

A culture very similar to the one that Conti desires for our nation's cyber warriors exists: the culture of the Navy's Nuclear Propulsion Program (NNPP). The biggest difference is the NNPP focus on procedural compliance to ensure nuclear propulsion reactor safety instead of out-right creativity in using systems outside of the desires of the designers. However, analyzing the structure of the NNPP provides an excellent framework for developing the nation's cyber forces.

When manning the NNPP, there are two paths for new candidates to use. The first is as a commissioned officer, selected from a commissioning source such as the Naval Academy, Naval Reserve Officer's Training Corps (NROTC), or Nuclear Propulsion Officer Candidate (NUPOC) program. All midshipmen, regardless of their program, are required to complete advanced physics and calculus courses regardless of their commissioning source to ensure that they are, at a minimum, eligible for the NNPP's selection process at the time of their commissioning. To be clear, if a midshipman does not complete these hard science courses, regardless of their final degree, they will not earn their unrestricted line commission in the U.S. Navy. Prior to their commissioning, if the midshipman has expressed interest in the NNPP (sometimes, when recruitment is low, the Navy recommends promising candidates based on their technical aptitude), their record is screened by Naval Reactors technical personnel. Midshipmen with acceptable records are

flown to the Navy Yard in Washington, DC to perform face-to-face technical interviews with at least two Naval Reactors engineers. Following completion of these hour-long interviews, which include solving math and physics problems, discussing engineering concepts, and other probing questions to determine technical aptitude and program compatibility, the midshipman receives an interview with the Director of Naval Reactors, the four-star admiral in charge of the entire program. From this interview process, selected midshipmen are obligated to the NNPP, and receive a promissory bonus.[78] If serving aboard nuclear submarines, the new candidate heads directly to Naval Nuclear Power Training Command (NNPTC) after graduation and commissioning. If serving aboard nuclear aircraft carriers, the new candidate heads to a conventionally powered surface combatant (such as a destroyer) for a little less than two years prior to reporting to NNPTC. This serves to give the new officer a chance to develop leadership skills, learn more about the organizational culture of their service, and develop professional warfighting skills, such as driving and fighting a warship, prior to learning nuclear power.

For new Sailors desiring to enlist in the NNPP, they must first earn one of the highest scores on the Armed Services Vocational Aptitude Battery (ASVAB) test. If a candidate does not meet the requirements to enter the program solely based on the ASVAB, they can attempt the supplemental Navy Advanced Programs Test (NAPT). A passing score, combined with the previous ASVAB score, allows them to enter the program. As of this writing, newly enlisted Sailors in the nuclear program receive an entry bonus.[79]

This recruiting construct can be adapted to the nation's cyber forces. Of course, in this time of fiscal austerity, the question to answer is why is such a complicated construct required? It is because careful screening of future cyber force leaders is required. On one hand, these leaders will have access to technology with the ability to cause significant damage due to a simple

user error (for example, what occurred with the Morris worm discussed earlier). On the other hand, that same access, when coupled with the desired creative spirit of cyber warriors, may result in unintended consequences. As an example, Conti writes, "One downside of the hacking ethos is the siren song of conducting unethical or illegal activities, particularly as one's skills advance."[80] Quality, not quantity, must be the manning directive for the nation's cyber force. Senior leaders must vet candidate commissioned officers through an interview process, one that preferably includes a technical demonstration process including practical validation of skills (for example, using a computer simulation to demonstrate hacking, programming, or other relevant skills) and determining aptitude to understand complex technical tasks. An interview with the cyber force ranking officer is reasonable, and should focus on the personal leadership traits desired for the cyber force, for example, integrity, initiative, creativity, morality, and loyalty. In other words, if the initial interviews validate technical skills, the final interview ensures the candidate has the desired leadership ability and is compatible with the program's culture. In 2014, the U.S. Navy's Fleet Cyber Command instituted the requirement for restricted line Cyber Warfare Engineer candidates to interview with the Commander, Fleet Cyber Command prior to their appointment.[81]

Although a good start, a more robust process would provide better dividends in improving the quality of the cyber force. Additionally, using a process of sending new cyber officers to the operational forces as trainee for two years would allow them to develop leadership skills while improving their familiarity with the conventional forces, and may serve to improve the conventional forces' understanding of cyber capabilities. Similarly, enlisted personnel must meet the highest appropriate bar to enter the program. Senior leaders must not assume that a person growing up around technology automatically has the aptitude to use it as required by the

cyber forces following recruitment. A bonus structure would provide an additional incentive for these candidates to join the military program instead of pursuing a cyber security job at a private firm. Additionally, bonuses can help incentivize remaining in the cyber force following an initial commitment. For example, current nuclear officer continuation pay bonuses are paid annually, and in addition to other retention bonuses.[82]

The next major task in developing cyber forces is examining the training pipeline. Conti writes that his cyber warriors will be highly educated, often with their own higher degrees and additional industry certifications, who will expect their leaders to be just as technically competent. He describes a culture in which individuals "make every effort to answer their own question before asking an expert."[83] Once again, the NNPP provides a successful framework to emulate.

Officers attend Nuclear Power School at NNPTC, which offers a graduate-level education during a six-month period. Subjects taught include the same subjects that enlisted students receive, but at a greater depth.[84] The instructors at NNPTC include senior enlisted personnel and limited duty officers commissioned explicitly to teach the subjects required. Following theoretical training, students transition to a Naval Prototype Training Unit (NPTU) where they receive additional theory and hands-on training at an operating reactor plant over the next six-month period. In order to graduate, students must qualify on the reactor plant, practicing operations during normal and possible casualty situations.[85] The entire process includes multiple comprehensive essay-style examinations and oral knowledge demonstrations with qualified operators and engineers. Once they report to their nuclear-powered ship, they must completely requalify, which takes approximately four months before they are fully qualified to operate the reactor plant. Officers receive an additional bonus upon completion of the training pipeline.[86]

Enlisted personnel attend initial recruit training, also known as boot camp, prior to attending initial in-rate instruction at NNPTC. Upon successful completion, students transition to Nuclear Power School and complete a six-month program of collegiate level courses in the technical concepts required to safely operate and maintain a nuclear reactor. Similar to the officers, they transfer to an NPTU to complete an additional six months of theoretical and hands-on training at an operational reactor. They must also qualify on the watch stations applicable to their specialty prior to reporting to their ship. Once they reach their ship, they must completely requalify as well.

The program is different from most programs in the military. Officers and enlisted personnel work together throughout the training program, often reporting to their first ships together. The relationship between the two, while strictly professional, is often closer than that of any other specialty (save the special operations forces) because of the deep respect earned by working together during the training and qualification process. Additionally, the program works diligently to imbue nuclear operators with the culture required to safely operate nuclear reactors, presented as the Nuclear Watchstanding Principles: Integrity, Formality, Ownership, Understanding, Teamwork, Anticipation, and Procedural Compliance. Finally, the continuing training aspect of the program is significant. Throughout their careers, nuclear-training operators, both officer and enlisted, while posted to a nuclear command, must complete a mandated amount of training and pass monthly examinations to ensure their level of knowledge is maintained at the level expected of a qualified operator. Failure to do so results in remediation, and if necessary, disqualification and the requirement to requalify. Similarly, poor performance on casualty control drills may require remediation for an individual or an entire watch team. In other words,

level of knowledge and satisfactory performance are critical to the success of the program. In order to remain successful in the program, officer and enlisted operators must constantly learn.

The technical complexities of the cyber domain require the same level of training. As Conti discussed, the enlisted personnel expect their leaders to be at least as educated as they are.[87] The NNPP process ensures that this occurs. In order to meet this requirement, the cyber forces must establish a complete training, qualification, and continuing education pipeline. The initial training pipeline must be as long as required to teach the advanced technical concepts necessary to compete as a cyber warrior successfully. It must filter out officers and enlisted personnel that fail to meet the established standards. Officers and enlisted personnel should attend the schools together, which should include both theoretical and hands-on experience. Similar to the NNPP, the cyber force training schools should recruit instructors from industry, commissioning them specifically to teach cyber topics. Upon successful completion of the training program, cyber warriors must requalify at their first operational command, demonstrating their level of knowledge and understanding of operational concepts prior to receiving authorization to operate cyber systems. Additionally, a successful by-product of the training program must be the internalization of the culture desired for the nation's cyber forces. Already, the DoD Cybersecurity Culture and Compliance Initiative drew directly from the NNPP to establish five "operational excellence principles" for the DoD Cyber Enterprise.[88] Military cyber forces should do the same. Although this paper deigns to dictate the cyber force principles, perhaps a starting point may be to focus on integrity, transparency, level of knowledge, questioning attitude, initiative, and morality. As the cyber domain is constantly changing, a continuing training program is in order. Importantly, these training programs should result in developing an appropriate level of knowledge for cyber warriors to complete industry certifications, such as the Certified Infor-

mation Systems Security Professional (CISSP) or Global Information Assurance Certification (GIAC) Certified Incident Handler (CIH).

The final task is equipping the cyber force. Instead of using a narrow definition of equipping and discussing acquisition strategies, this paper will offer the idea that equipping is about developing the culture used to design, select, equip, and use the final technologies required by the cyber force. The father of the Nuclear Navy, Admiral Hyman G. Rickover, developed the engineering principles required to safely equip, operate, and maintain the nuclear propulsion plants.[89] He created a center of excellence at Naval Reactors, which allowed him to mobilize expert engineers to help solve problems.[90] Even today, if necessary, a nuclear-trained officer can contact Naval Reactors and discuss a problematic component with an engineer who is familiar with the component's specifications, design, location on the ship, and recent problems throughout the fleet.[91] Naval Reactors also performs critical tasks as an inspection and continuous improvement agency, with the authority to perform quality assurance checks on any part of the NNPP. Naval Reactors representatives are expected to randomly attend training at every point in the training pipeline, observe significant operations or maintenance, perform audits of records, or observe day-to-day operations. The goal of Naval Reactors is to maintain the high standard of engineering excellence demanded by the NNPP. To do so, they retain the responsibility and authority to do what is necessary to correct identified deficiencies.

For the cyber forces, developing a cyber center of excellence is a critical task. Employing cyber security experts, computer scientists, system engineers, cyber law experts, cyber theorists, and cyber strategists would go a long way to developing a successful foundation for the cyber force. Partnerships with private industry and technology corporations are also required, especially when developing the initial technologies to fill current gaps in cyber capabilities. The

ability of cyber forces to reach back to an expert to get an answer rapidly, especially in cyber warfare where time is of the essence, is a critical capability that must be developed. Additionally, cyber experts must be able to perform quality assurance checks on any aspect of the cyber forces, and must have a feedback mechanism to correct identified deficiencies.

The purpose of this section was to propose a framework to develop the cyber forces. The framework pioneered by the NNPP is unique to the Navy, recognized for its ability to "successfully manage technical systems," and serves as an excellent starting point for developing the nation's cyber forces.[92] Using it will improve the capabilities of the cyber force.

Rapid Military Innovation: A Case Study

This paper opened with a sobering portrayal of a cyber warfare exercise, begging the question if it is possible for the nation to increase cyber capabilities rapidly. Using the development of nuclear-powered ballistic missile submarines at the start of the Nuclear Age, this paper will show that the military has the experience, resources, and ability to innovate high technology solutions to new challenges.

On August 6th, 1945, the U.S. military successfully detonated a nuclear bomb over the Japanese city of Hiroshima in an attempt to end the Pacific War during World War II. On August 9th, 1945, a second nuclear bomb was detonated over Nagasaki. By August 15th, 1945, Emperor Hirohito addressed his citizens by radio, announcing Japan's surrender to the Allied forces. World War II was over, ushering in the Nuclear Age. Initially, the U.S. held the monopoly on nuclear weapons. Unfortunately, by late August 1949, the Soviet Union successfully tested their own nuclear weapon. Both superpowers now had the ability to destroy the other, and at the same time, the rest of the world.

As noted by Dr. Stephen McFarland, historian, the "atomic bomb blinded most people to the classical rules of war and paralyzed their strategic thinking but presented a new type of war."[93] He notes that the most significant change was the increase in speed of warfare, in which nuclear conflict meant "the next war might be over in minutes."[94] The result was the concept that "offense was no longer just the best defense; it was the only defense."[95] Famously, the result was President Eisenhower's New Look strategy, which used the nuclear weapon as a means of deterrent. By threatening use of the nuclear weapon first, President Eisenhower wanted to prevent a war from even starting.[96] By the 1960s, this evolved into the strategy of mutually assured destruction (MAD). The basic concept of MAD was in the event of a first strike attack from an adversary, the defender would have the ability to launch a devastating counter-strike, resulting in the complete destruction of both the attacker and defender. The hope of MAD was that the cost of a first strike attack was too high, ensuring no superpower would use their nuclear weapons lightly.

In order to maintain their relevance in the national defense strategy, as well as their associated public funds, the three U.S. military departments sought to harness nuclear power. However, harnessing this energy source required developing solutions to complex technical challenges. Leaders who desired to use this power in their own services needed to operationalize the complex theories developed by physicists. Each of the military services embarked on their own development programs in an effort to take advantage of the new power source. The Navy developed the nuclear powered propulsion plant for submarines and surface vessels and submarine launched Polaris ballistic missiles.[97]

Frank Wicks, writing about the Nuclear Navy, describes how Admiral Rickover commenced development of a nuclear propulsion system for use onboard submarines in 1946. Ad-

miral Rickover identified military and civilian atomic experts and recruited them to his team. He identified the need for civilian industry support, establishing Electric Boat Company, Westinghouse, and General Electric as the primary contractors. At a time when the primary calculating tool was a slide rule, his team built two different prototype propulsion reactors and selected the safest option vice the most powerful.[98] As a result, the U.S. Navy launched and commissioned the *USS Nautilus* (SSN-571) in 1954.

Similarly, Floyd Kennedy, retired U.S. Naval Intelligence Officer, writes about the submarine-launched Polaris missile system developed by the Navy during the start of the Cold War. The National Security Council (NSC) required a sea-based nuclear intercontinental cruise ballistic missile (ICBM) in order to improve the nation's nuclear deterrence and increase survivability of the nuclear arsenal to preserve a second-strike capability. The Navy's Special Projects Office began a "crash program" to develop the system from scratch, drawing "the resources and the personnel necessary for this accomplishment … from all corners of the Navy's strategic research and development community."[99] The weapon system was tested from the USS *George Washington* (SSBN 598) in 1960, less than five years after commencing the program. Kennedy writes, "The Polaris program must rank with the space program of the National Aeronautics and Space Administration as one of history's most successful advanced-technology endeavors."[100]

As nuclear technology became central to world reality, the example of the development of the nation's nuclear-powered submarines carrying nuclear-tipped ballistic missiles shows how the military was able to act quickly and responsibly to harness complex nuclear technology. In fact, after more than 50 years, nuclear powered warships have steamed more than 151 million miles safely.[101] The military, as demonstrated by the Navy, deftly used their resources and organizational expertise to develop the required culture of excellence and the corporate and civilian

relationships required to harness nuclear technologies safely. The technical innovation and cultural development required to operate in the cyber domain successfully are similar to the requirements to develop nuclear reactors and ballistic weapons systems responsibly. This example shows that military forces have the capacity, experience, and resources required to improve the nation's cyber capabilities rapidly.

Conclusion

The purpose of this paper was to propose a cyber force development strategy in order to improve the nation's cyber capabilities. To do so, the paper introduced the challenges of the cyber domain, developed critical definitions, and then identified the missions the cyber force would perform by examining the concept of cyber power and objective of cyber warfare. The question of whether the nation's cyber force should be military or civilian was resolved in favor of a military cyber force. Using the NNPP's framework as a guide, the paper recommended a framework to meet future manning, training, and equipping requirements. Finally, using the case study of the development of nuclear-powered ballistic missile submarines, this paper showed that the military has the ability to develop highly technical programs rapidly and successfully.

As of this writing, the Department of Defense is using a joint construct for the armed forces to operate in the cyber domain, through the establishment of USCYBERCOM. As a sub-unified combatant commander under U.S. Strategic Command (USSTRATCOM), USCYBERCOM is the military organization tasked to operate and defend the DODIN, conduct full spectrum military cyberspace operations, and ensure freedom of action in cyberspace while denying adversary access to the same.[102] It is a joint structure, which means that each of the services provides support to it. According to Clarke, it is a sub-unified command because, although

"an integrated multiservice structure was agreed upon in principle", many did not want to "make the Space Command mistake again."[103] In other words, the military was initially unwilling establish a separate combatant command for cyber operations and devote significant resources based on the experience of establishing a separate combatant command for space operations, and disestablishing it due to a lack of need. Clarke argues that the government disbanded Space Command in 2002 after "it had become clear that neither the U.S. nor any other government had the money to do much in space."[104] Unlike space operations, cyber operations have become incredibly important. Due to the unenthusiastic establishment of USCYBERCOM, and subsequent attempts to expand its capabilities, there are organizational structure issues and inefficiencies in capability development.

First, the joint structure appears to have significant issues. A July 2011 Government Accountability Office (GAO) reported, "Cyber command and control is unclear and divided among DOD components."[105] More specifically, the authorities and responsibilities for cyberspace operations are divided "among combatant commands, military service, and defense agencies" as delineated by "several policy and guidance documents" which "sometimes conflict with each other and remain unclear because of overlapping responsibilities."[106] Additionally, officials interviewed for the GAO report "recognized that fully addressing the cyber capability gaps they have thus far identified may take years to complete."[107]

Additionally, all four services are attempting to develop the technologies and capabilities required to operate effectively in the cyber domain separately. Per Title 10 of the U.S.C., each service must man, train, and equip their own cyber forces. In other words, each service would be required to develop the framework, including the recruiting program, training pipeline, and center of excellence discussed previously. Forcing each service to solve these issues on their own

lacks efficiency and effectiveness in today's fiscally austere environment. This joint structure does not lend itself to military strengths, in particular unity of command that will pay training, education, resources allocation, and finally operations benefits.

Looking forward, there are three options for the cyber force as it matures. One, it can continue down its current path as a significant joint construct, similar to the U.S. Special Operations Command (USSOCOM). Two, the government can create a separate Cyber Service. Three, which this paper advocates, is to assign the responsibilities for cyber warfare to one service to improve command and control and reduce the resource requirements of a successful cyber force.

In terms of the first option, USSOCOM, as a separate Combatant Command supplied by all four services, is a successful joint construct. However, it was not an immediate success. Although President John F. Kennedy ordered special operations forces (SOF) as early as 1961, who performed admirably throughout Vietnam, they were not an immediate joint success.[108] In fact, the failure of SOF at Desert One, in 1980, revealed serious problems in interoperability.[109] After reform failures, Congress took action in 1986, resulting in activation of USSOCOM.[110] In other words, it took nearly thirty years to integrate USSOCOM successfully. However, strong legislation was required. As noted in a RAND Corporation report identifying similarities between SOF and the current state of the nation's cyber forces, the services "failed to answer the needs of the SOF community" regardless of the important capabilities that SOF brought to the nation's military.[111] This remains a significant concern, as the failure of services to answer the needs of the cyber community would likely manifest in poor promotion or command opportunities for cyber warriors, a lack of budget allocation for the specialized training they require, and the failure to develop and acquire the high technology required for cyber forces to operate. Unfortunately, a

joint construct, without strong legislation to provide protection, allows these problems to occur, as there is less ownership by the services, and an understandable reluctance to reallocate funds, originally earmarked for a core competency, to a joint force. Although leaders can draw lessons from the development of USSOCOM to improve the current joint construct, attempting to maintain the joint structure for the nation's cyber forces is beyond the scope of this paper.

The second option, the creation of a new, separate Cyber Service, is also not palatable. As discussed previously, the military services have the ability to develop the framework necessary to recruit, train, and retain the desired cyber warriors of the future. It has the ability to develop the culture that results in highly capable cyber forces. There is no reason to duplicate the other functions that a military service must maintain to develop a separate Cyber Service (for example, administrative, human resources, pay, housing, acquisition, security, recruit entry training, uniforms, regulations, and mortuary). It is doubtful that the government has any desire to reduce the budget allotments of the other services to duplicate secondary capabilities. The other problem is the amount of time required to create another service. Take, for example, the Air Force. It was not created in a vacuum. It incubated in the Army for nearly twenty years, while theorists and leaders determined how an independent air force would operate. Throughout World War II, it operated nearly independently from the Army as the Army Air Corps. This allowed the Air Force to visualize the final structure and develop the critical cost and force estimates needed to create independent force. In fact, the Air Force took steps to prepare for independence as early as March 1946 through reorganization while still the Air Army Corps.[112] Although President Truman signed the National Security Act of 1947, which actually granted the Air Force's independence, it still took six months before the new Secretary of the Air Force was sworn in. It was not until April 1948 that the President finally issued a "detailed statement of the

functions of the armed forces" to reduce the turf issues that were still being fought to "a few core issues."[113] The amount of confusion required to create a brand new Cyber Service cannot be understated, and the effect on the capabilities of the new Cyber Service as it attempts to work through the issues of a new service cannot be overestimated.

The third option provides the most benefit in improving the nation's cyber forces. Instead of a joint construct, and instead of a separate Cyber Service, this paper advocates for a single established service to assume the Title 10 responsibilities for cyber operations. As a result, instead of each service developing a formal cyber force capable of executing the missions discussed previously, each service should retain the information technology capabilities they have already developed to operate "ordinary business operations."[114] Effectively, these capabilities, and their supporting functions such as training, are already operating and maintaining basic computing functions such as email, web browsing, file sharing, and database application use. Each service would be responsible for basic security functions as well, such as patching computers and conducting network audits. In other words, few changes would be necessary for the other services to continue computer operations as normal, resulting in a significant cost savings for the government as cyber force capabilities are improved.

With Title 10 responsibility, the identified service would receive funding appropriate to man, train, and equip the cyber forces. The identified service would also be held accountable for these requirements. This is important, as it provides a clear understanding of who is responsible for ensuring the effectiveness of the cyber forces. Unlike a joint system, a single service entity makes clear who deserves praise for successes and blame for failures.

Although the previous service in charge of cyber warfare prior to the joint structure was the U.S. Air Force, this paper advocates for the transition of these responsibilities to the U.S.

Navy and Fleet Cyber Command. As discussed previously, the theoretical underpinnings of Corbett's maritime strategic thought apply easily to the cyber domain. The result of this implication is important, and is argued well by Robert Farley, of the Patterson School of Diplomacy at the University of Kentucky. He notes, as a result of their view of maritime strategic thought, the Navy "sees the potential for positive-sum interaction in cyberspace while also maintaining capabilities for offensive and defensive action" based on their understanding that "in peacetime a safe, regulated commons could provide positive-sum benefits for the community of nations, allowing free, mutually beneficial trade and transit."[115] This view of the cyber commons is a constructive, positive view and is worth pursuing. Additionally, as shown previously, the successful framework required to recruit, train, and equip cyber warriors, such as those desired by Conti, can be created using the example of the Navy's successful NNPP. As the Navy already has the appropriate personnel policies to maintain the NNPP, it will take significantly less effort to create the required framework required to man, train, and equip the nation's cyber forces. Finally, as shown by the nuclear-powered ballistic missile submarine case study, the Navy has successfully demonstrated the ability to develop a highly technical program with longevity and a history of safety to solve significant strategic problems.

Although the cyber domain is challenging, the military has the ability, resources, and expertise to develop the required capabilities to secure the nation's cyber lines of communications while preventing adversary use, protect defense computer networks, and ensure the safety of the nation's critical infrastructure networks. Transferring responsibilities enshrined in Title 10 of the U.S.C. for cyber warfare to the U.S. Navy will improve command and control, increase efficiency in the development of a career path, increase effectiveness of a cyber center of excellence, and

leverage institutional experience while developing a high technology solution to the challenges of operations in cyberspace.

Citations and Endnotes

[1] Andrew Tilghman, "In a supersecret cyberwar game, civilian-sector techies pummel active-duty cyberwarriors," *Army Times*, August 4, 2014.
[2] "WorldWideWebSize.com: Daily Estimated Size of the World Wide Web," Maurice de Kunder, accessed January 15, 2016, http://www.worldwidewebsize.com/
[3] U.S. Census Bureau, *Home Computers and Internet Use in the United States: August 2000* (Washington, DC: Government Printing Office, 2001): 1-2.
[4] Thom File and Camille Ryan, U.S. Census Bureau, *Computer and Internet Use in the United States: 2013* (Washington, DC: Government Printing Office, 2014): 2.
[5] "Internet World States: Usage and Population Statistics", Miniwatts Marketing Group, accessed January 15, 2016, http://www.internetworldstats.com/stats.htm
[6] Gordon Moore, "Cramming More Components onto Integrated Circuits," *Electronics* (April 19, 1965): 114-117.
[7] Larry Boettger. "The Morris Worm: How It Affected Computer Security and Lessons Learned by it" (Global Information Assurance Certification Paper, SANS Institute 2000.), https://www.giac.org/paper/gsec/405/morris-worm-affected-computer-security-lessons-learned/100954
[8] Darlene Storm, "Epsilon Breach: hack of the century?" *Computer World*, April 4, 2011, http://www.computerworld.com/article/2471044/cloud-computing/epsilon-breach--hack-of-the-century-.html
[9] Will Goodman, "Cyber Deterrence: Tougher in Theory than in Practice," *Strategic Studies Quarterly* (Fall 2010): 110-111.
[10] Nathan Thornburgh, Matthew Forney, Brian Bennett, Timothy J. Burger, and Elaine Shannon, "The Invasion of the Chinese Superspies (and the Man Who Tried to Stop Them)," *Time Magazine* Vol. 166 Issue 10: 34-39.

[11] James Eng, "OPM Hack: Government Finally Starts Notifying 21.5 Million Victims," *NBC News Website*, October 1, 2015, http://www.nbcnews.com/tech/security/opm-hack-government-finally-starts-notifying-21-5-million-victims-n437126
[12] See both Evan Perez, "FBI: Hacker claimed to have taken over flight's engine controls," *CNN Website*, May 18, 2015, http://www.cnn.com/2015/05/17/us/fbi-hacker-flight-computer-systems/ and Andy Greenberg, "Hackers Remotely Kill a Jeep on the Highway – With Me In It," *Wired Website*, July 21, 2015, http://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/
[13] Michael B. Kelley, "The Stuxnet Attack on Iran's Nuclear Plant Was 'Far More Dangerous' Than Previously Thought," *Business Insider,* November 20, 2013, http://www.businessinsider.com/stuxnet-was-far-more-dangerous-than-previous-thought-2013-11
[14] Michael N. Schmitt, ed., *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge: Cambridge University Press, 2013): 54.
[15] Matthew Crosston, "World Gone Cyber MAD: How 'Mutually Assured Debilitation' Is the Best Hope for Cyber Deterrence," *Strategic Studies Quarterly* (Spring 2011): 112.
[16] Goodman, "Cyber Deterrence," 116.
[17] U.S. Joint Chiefs of Staff, *Cyberspace Operations*, Joint Publication 3-12(R) (Washington, DC: U.S. Joint Chiefs of Staff, February 5, 2013): II-9.
[18] Crosston, "World Gone Cyber MAD," 106.
[19] U.S. Joint Chiefs of Staff, *Cyberspace Operations,* I-2.
[20] Colin S. Gray, *Making Strategic Sense of Cyber Power: Why the Sky is Not Falling* (Carlisle, PA: Strategic Studies Institute, 2013): 8-9.
[21] Richard A. Clarke and Robert K. Knake, *Cyber War: The Next Threat to National Security and What To Do About It* (New York, NY: Ecco, an imprint of HarperCollins Publishers, 2010): 6.
[22] Richard Stiennon, *Surviving Cyber War* (Lanham, MD: Government Institutes, an imprint of The Scarecrow Press, Inc, 2010): ix.
[23] See both Amit Sharma, "Cyber Wars: A Paradigm Shift from Means to Ends," in *The Virtual Battlefield: Perspectives on Cyber Warfare,* ed. Christian Czosseck and Kenneth Geers (Amsterdam: IOS Press, 2009): 6 and Jeffrey Carr, *Cyber Warfare* (Sebatopol, CA: O'Reilly Media, 2012): 2.
[24] U.S. Joint Chiefs of Staff, *Cyberspace Operations,* II-2 through II-5.
[25] Scott Applegate, "Cyber Conflict: Disruption and Exploitation in the Digital Age," in *Current and Emerging Trends in Cyber Operations: Policy, Strategy and Practice,* ed. Frederic Lemieux (New York, NY: Palgrave Macmillan, 2015): 26.
[26] U.S. Joint Chiefs of Staff, *Cyberspace Operations,* II-5.
[27] Applegate, "Cyber Conflict," 27.
[28] Schmitt, *Tallinn Manual*, 1.
[29] Schmitt, *Tallinn Manual,* 54-61.
[30] Schmitt, *Tallinn Manual*, 54.
[31] Colin S. Gray, *The Leverage of Sea Power* (New York, NY: The Free Press, 1992): ix.
[32] Julian Corbett, *Some Principles of Maritime Strategy* (Annapolis, MD: Naval Institute Press, 1988): 91.
[33] Jakub J. Grygiel, "The Dilemmas of U.S. Maritime Supremacy in the Early Cold War," *Journal of Strategic Studies* 28:2 (April 2005): 209.
[34] Modified from Gray's maxim, "Sea power is the ability to use the seas and oceans for military or commercial purposes and preclude an enemy from doing the same." from Gray, *The Leverage of Sea Power,* 4.
[35] Gray, *The Leverage of Sea Power,* 5.
[36] Corbett, *Some Principles of Maritime Strategy,* 91.
[37] Corbett, *Some Principles of Maritime Strategy,* 103.
[38] Corbett, *Some Principles of Maritime Strategy,* 103.
[39] U.S. Department of Defense, *Department of Defense Information Technology Enterprise Strategy and Roadmap*, (Washington, DC: Government Printing Office, 2011): 2.
[40] U.S. Department of Homeland Security, *Critical Infrastructure and Key Resources Support Annex* (Washington, DC: Government Printing Office, 2008): 31.
[41] U.S. Department of Homeland Security, *Critical Infrastructure,* 31.

[42] Executive Order 13636 of February 12, 2013, Improving Critical Infrastructure Cybersecurity, *Code of Federal Regulations,* title 3 (2014): 217-223, https://www.gpo.gov/fdsys/pkg/DCPD-201300091/pdf/DCPD-201300091.pdf.
[43] Executive Order 13636, *Code of Federal Regulations*, 217.
[44] U.S. Department of Homeland Security, *Critical Infrastructure*, 32.
[45] U.S. Department of Homeland Security, *Critical Infrastructure*, 32.
[46] U.S. Joint Chiefs of Staff, *Cyberspace Operations,* III-3.
[47] U.S. Joint Chiefs of Staff, *Cyberspace Operations,* III-3.
[48] U.S. Joint Chiefs of Staff, *Cyberspace Operations,* III-3.
[49] "U.S. Cyber Command Fact Sheet," U.S. Strategic Command Website, accessed January 15, 2016, https://www.stratcom.mil/factsheets/2/Cyber_Command/
[50] Federal Activities Inventory Reform Act of 1998, Pub. L. No. 105-270, 112 Stat. 2382 (1998).
[51] U.S. Office of General Counsel Department of Defense, *Department of Defense Law of War Manual* (Washington, DC: Government Printing Office, 2015): 15.
[52] U.S. Office of General Counsel Department of Defense, *Law of War Manual*, 101.
[53] Schmitt, *Tallinn Manual*, 95.
[54] U.S. Office of General Counsel Department of Defense, *Law of War Manual*, 102.
[55] Schmitt, *Tallinn Manual*, 95-105
[56] U.S. Office of General Counsel Department of Defense, *Law of War Manual*, 121.
[57] U.S. Office of General Counsel Department of Defense, *Law of War Manual*, 122-123.
[58] U.S. Office of General Counsel Department of Defense, *Law of War Manual*, 123.
[59] U.S. Office of General Counsel Department of Defense, *Law of War Manual*, 125.
[60] U.S. Office of General Counsel Department of Defense, *Law of War Manual*, 125.
[61] Schmitt, *Tallinn Manual*, 97.
[62] Schmitt, *Tallinn Manual*, 98.
[63] Schmitt, *Tallinn Manual*, 98.
[64] U.S. Office of General Counsel Department of Defense, *Law of War Manual*, 128.
[65] Schmitt, *Tallinn Manual*, 105.
[66] U.S. Office of General Counsel Department of Defense, *Law of War Manual*, 129.
[67] U.S. Office of General Counsel Department of Defense, *Law of War Manual*, 143.
[68] U.S. Office of General Counsel Department of Defense, *Law of War Manual*, 145.
[69] U.S. Office of General Counsel Department of Defense, *Law of War Manual*, 147.
[70] U.S. Office of General Counsel Department of Defense, *Law of War Manual*, 148.
[71] U.S. Office of General Counsel Department of Defense, *Law of War Manual*, 148.
[72] Schmitt, *Tallinn Manual*, 104.
[73] Schmitt, *Tallinn Manual*, 96-102.
[74] U.S. Joint Chiefs of Staff, *Cyberspace Operations,* II-6.
[75] Gregory Conti and David Raymond, "Leadership of Cyber Warriors: Enduring Principles and New Directions," *Small Wars Journal* (July 11, 2011): 3.
[76] Conti and Raymond, "Leadership of Cyber Warriors," 4.
[77] Gregory Conti and Jen Easterly, "Recruiting, Development, and Retention of Cyber Warriors Despite an Inhospitable Culture," *Small Wars Journal* (July 29, 2010), http://smallwarsjournal.com/jrnl/art/recruiting-development-and-retention-of-cyber-warriors-despite-an-inhospitable-culture
[78] U.S. Department of the Navy, *Nuclear Officer Incentive Pay Program,* Instruction 7220.11E, December 29, 2014, 19.
[79] "Navy SLRP and Enlistment Bonus Update (FEB 1, 2015)," Thomas Goering, *Navy CyberSpace Blog*, July 13, 2015, https://www.navycs.com/blogs/2015/02/04/feb-2015-slrp-and-eb-update
[80] Conti and Raymond, "Leadership of Cyber Warriors," 3-4.
[81] U.S. Department of the Navy, *Program Authorization: Restricted Line/Special Duty Officer (Cyber Warfare Engineer)*, Program Authorization 121, September 18, 2014: 2.
[82] U.S. Department of the Navy, *Nuclear Officer Incentive Pay Program,* 19.
[83] Conti and Raymond, "Leadership of Cyber Warriors," 4.

[84] U.S. Department of Energy and U.S. Department of the Navy, *The United States Naval Nuclear Propulsion Program* (Washington, DC: Government Printing Office, 2013): 23.
[85] U.S. Department of Energy and U.S. Department of the Navy, *Naval Nuclear Propulsion Program,* 23.
[86] U.S. Department of the Navy, *Nuclear Officer Incentive Pay Program,* 19.
[87] Conti and Raymond, "Leadership of Cyber Warriors," 4.
[88] Secretary of Defense and Chairman, Joint Chiefs of Staff, *Department of Defense Cybersecurity Culture and Compliance Initiative*. September 28, 2015.
http://www.defense.gov/Portals/1/Documents/pubs/OSD011517-15-RES-Final.pdf
[89] Francis Duncan, *Rickover: The Struggle for Excellence* (Annapolis, MD: Naval Institute Press, 2001): 308.
[90] Duncan, *Rickover,* 309.
[91] Duncan, *Rickover,* 309.
[92] Secretary of Defense, *Cybersecurity Culture,* 2.
[93] Stephen L. McFarland, "The Air Force in the Cold War, 1945-60: Birth of a New Defense Paradigm," *Air & Space Power Journal* 10:3 (1996): 6.
[94] McFarland, "The Air Force in the Cold War," 6.
[95] McFarland, "The Air Force in the Cold War," 7.
[96] McFarland, "The Air Force in the Cold War," 11.
[97] McFarland, "The Air Force in the Cold War," 10-13.
[98] Frank Wicks, "Nuclear Power," *Mechanical Engineering* (January 2004): 31-36.
[99] Frank D. Kennedy Jr, "The Creation of the Cold War Navy, 1953-1962" in *In Peace and War: Interpretations of American Naval History*, ed. Kenneth J. Hagan and Michael T. McMaster (Santa Barbara, CA: Praeger Security International, 2008), 247-248.
[100] Kennedy, "The Creation of the Cold War Navy," 248.
[101] U.S. Department of Energy and U.S. Department of the Navy, *Naval Nuclear Propulsion Program,* 1.
[102] U.S. Strategic Command, *U.S. Cyber Command Fact Sheet.*
[103] Clarke and Knake. *Cyber War,* 36.
[104] Clarke and Knake. *Cyber War, 35.*
[105] U.S. Government Accountability Office, *Defense Department Cyber Efforts: DOD Faces Challenges In Its Cyber Activities* (GAO Publication No. 11-75) (Washington, DC: Government Printing Office, 2011): 34.
[106] U.S. Government Accountability Office, *Defense Department Cyber Efforts,* 34.
[107] U.S. Government Accountability Office, *Defense Department Cyber Efforts,* 41.
[108] Christopher Paul, Isaac R. Porche III, and Elliot Axelband, *The Other Quiet Professionals: Lessons for Future Cyber Forces from the Evolution of Special Forces*. (Santa Monica, VA: Rand Corporation, 2014): 5-6.
[109] Paul, et al, *The Other Quiet Professionals,* 7-8.
[110] Paul, et al, *The Other Quiet Professionals,* 12.
[111] Paul, et al, *The Other Quiet Professionals,* 39.
[112] Walter J. Boyne, *Beyond the Wild Blue* (New York, NY: St. Martin's Press, 1997): 29.
[113] Boyne, *Beyond the Wild Blue,* 37.
[114] U.S. Joint Chiefs of Staff, *Cyberspace Operations,* II-6.
[115] Robert M. Farley, *Grounded: The Case for Abolishing the United States Air Force* (Lexington, KY: University Press of Kentucky, 2014): 39.

Literature Review

The primary sources were selected based on their importance to the topic being addressed. As this paper is proposing the development of a military cyber force, many of the primary sources are joint military doctrine, government documents from the executive and legislative branches, and national security strategists.

In the section titled, "The Challenging Nature of the Cyber Domain," the references were used to demonstrate the size of the Internet, spread of Internet access, examples of recent cyber crime and espionage, and difficulties operating in the cyber domain. The website used demon-

strate the size of the Internet updates the size of the Internet on a daily basis. In terms of demonstrating the spread of the Internet access, U.S. Census Bureau data over a period of 15 years was used show the growth. It was augmented with a marketing report showing similar growth data for the world. The selection of references demonstrating recent cyber crime and espionage were magazine articles covering the specific instances, while the reference describing the Morris Worm used a certification paper, selected for its conciseness. To demonstrate the difficulties operating in the cyber domain, the primary reference was doctrinal, supported by additional academic research papers.

The section titled "Reducing Cyber Confusion" used references to define terms such as cyber domain, cyber warfare, and cyber attack. The first definition used doctrine to introduce the term, but selected Kuehl's definition, endorsed by Gray, because of its inclusion of the human use of the electromagnetic spectrum. The second term was defined using Applegate's definition as it clearly separates cyber warfare from cyber crime and cyber espionage, although doctrine was reviewed. Doctrine does not currently define cyber warfare. Additional examples of this definition were provided by scholarly articles and recent popular publications. The third term was defined by blending Applegate's definition with one from the *Tallinn Manual*, which is considered the authoritative document applying international law, including the law of armed conflict, to cyber warfare.

The section titled "Developing a Mission" used references to develop concepts such as cyber power, the object of cyber warfare, and the mission of cyber forces. To develop the idea of cyber power and the object of cyber warfare, this paper turned to the acclaimed Sir Julian Corbett, whose seminal work defined the strategic use of naval forces. Viewing cyber power through a Corbettian lens significantly reduces the confusion currently associated with the topic.

Supporting references included works by Gray and Grygiel. When discussing the mission of protecting critical infrastructure, the primary source was an executive order dedicated to improving critical infrastructure cybersecurity, supported by the Department of Homeland Security's Critical Infrastructure and Key Resources Support Annex. Finally, when discussing the requirement to man, train, and equip the cyber forces, doctrine and United States Code were used.

The section titled "A Legal Argument for Military Cyber Forces" used international law, such as the Law of Armed Conflict and Geneva Convention, supported by the *Tallinn Manual* and U.S. domestic law, to state the case for a military cyber force.

The section titled "Organizing Cyber Forces" used doctrine and publications by the U.S. Department of Energy and U.S. Department of the Navy, supported by the *Department of Defense Cybersecurity Culture and Compliance Initiative*, Duncan's biography *Rickover*, and articles authored Colonel Gregory Conti to demonstrate that the Navy Nuclear Propulsion Program offers a successful framework upon which to base future cyber force development.

The section titled "Rapid Military Innovation" used a scholarly article by McFarland to describe the challenges brought by the emergence of nuclear power. To describe the rapid and successful development of the nuclear-powered submarine, this paper used an article by Frank Wicks published in *Mechanical Engineering*. To describe the equally rapid and successful development of submarine-launched ICBMs, this paper used a scholarly article by Floyd Kennedy.

The conclusion used Clarke and Knake's popular *Cyber War* to describe the disestablishment of U.S. Space Command as a separate unified command. To identify issues with the current U.S. Cyber Command joint structure, this paper turned to the Government Accountability Office and their report, *Defense Department Cyber Efforts: DOD Faces Challenges In Its Cyber Activities*. To describe the delayed success of U.S. Special Operations Command, this paper

turned to the Rand Corporation report *The Other Quiet Professionals: Lessons for Future Cyber Forces from the Evolution of Special Forces.* In discussing the separation of the U.S. Air Force from the U.S. Army, this paper used Boyne's popular book, *Beyond the Wild Blue*. Finally, in discussing the difference between the lens the U.S. Air Force views operations in the cyber domain when compared to the way the U.S. Navy views similar operations due to their maritime past, this paper uses the views of Farley's popular book, *Grounded: The Case for Abolishing the United States Air Force.* His argument is based on the difference in views presented by the early air power theorists (Douhet) versus the early sea power theorists (Mahan and Corbett).

Overall, the sources reveal a good mix of primary material and key reading material related to the topic. The mix also reveals the absence of the implication of this paper – that the Navy is best suited to dictate military action in cyberspace. Expert cyber theorists have yet to make this point. Yet, the analysis here, bolstered by an analysis of maritime power theory, raises this key point. Moreover, what may be considered western-centric, for example, the *Tallinn Manual*, underscores the point that treating the cyber domain as a global commons is central to better understanding the challenges of operating in cyberspace. This idea, long established in operations in the maritime domain, best signals that naval thought and theories may better clarify the confusion currently associated with mitigating the challenges in cyberspace. Reducing the push for jointness in the cyber domain will better focus efforts to understand and improve the nation's capabilities in cyberspace.

Bibliography

Applegate, Scott. "Cyber Conflict: Disruption and Exploitation in the Digital Age." In *Current and Emerging Trends in Cyber Operations: Policy, Strategy and Practice*, edited by Frederic Lemieux. New York, NY: Palgrave Macmillan, 2015.

Boettger, Larry. "The Morris Worm: How It Affected Computer Security and Lessons Learned by it." Global Information Assurance Certification Paper, SANS Institute 2000, https://www.giac.org/paper/gsec/405/morris-worm-affected-computer-security-lessons-learned/100954

Boyne, Walter J. *Beyond the Wild Blue.* New York, NY: St. Martin's Press, 1997.

Carr, Jeffrey. *Cyber Warfare.* Sebatopol, CA: O'Reilly Media, 2012.

Clarke, Richard A. and Robert K. Knake. *Cyber War: The Next Threat to National Security and What To Do About It.* New York, NY: Ecco, an imprint of HarperCollins Publishers,

2010.

Conti, Gregory and Jen Easterly. "Recruiting, Development, and Retention of Cyber Warriors Despite an Inhospitable Culture." *Small Wars Journal* (July 29, 2010), http://smallwarsjournal.com/jrnl/art/recruiting-development-and-retention-of-cyber-warriors-despite-an-inhospitable-culture

Conti, Gregory and David Raymond. "Leadership of Cyber Warriors: Enduring Principles and New Directions." *Small Wars Journal* (July 11, 2011).

Corbett, Julian. *Some Principles of Maritime Strategy*. Annapolis, MD: Naval Institute Press, 1988.

Crosston, Matthew. "World Gone Cyber MAD: How 'Mutually Assured Debilitation' Is the Best Hope for Cyber Deterrence." *Strategic Studies Quarterly* (Spring 2011).

Duncan, Francis. *Rickover: The Struggle for Excellence*. Annapolis, MD: Naval Institute Press, 2001.

Eng, James. "OPM Hack: Government Finally Starts Notifying 21.5 Million Victims." *NBC News Website*, October 1, 2015, http://www.nbcnews.com/tech/security/opm-hack-government-finally-starts-notifying-21-5-million-victims-n437126

Executive Order 13636 of February 12, 2013, Improving Critical Infrastructure Cybersecurity. *Code of Federal Regulations*, title 3 (2014): 217-223. https://www.gpo.gov/fdsys/pkg/DCPD-201300091/pdf/DCPD-201300091.pdf.

Farley, Robert M. *Grounded: The Case for Abolishing the United States Air Force*. Lexington, KY: University Press of Kentucky, 2014.

File, Thom and Camille Ryan, U.S. Census Bureau. *Computer and Internet Use in the United States: 2013*. Washington, DC: Government Printing Office, 2014.

Goodman, Will. "Cyber Deterrence: Tougher in Theory than in Practice." *Strategic Studies Quarterly* (Fall 2010).

Gray, Colin S. *Making Strategic Sense of Cyber Power: Why the Sky is Not Falling*. Carlisle, PA: Strategic Studies Institute, 2013.

Gray, Colin S. *The Leverage of Sea Power*. New York, NY: The Free Press, 1992.

Greenberg, Andy. "Hackers Remotely Kill a Jeep on the Highway – With Me In It." *Wired Website*, July 21, 2015, http://www.wired.com/2015/07/hackers-remotely-kill-jeep-high way/

Grygiel, Jakub J. "The Dilemmas of U.S. Maritime Supremacy in the Early Cold War." *Journal*

of Strategic Studies 28:2 (April 2005).

"Internet World States: Usage and Population Statistics", Miniwatts Marketing Group, accessed January 15, 2016, http://www.internetworldstats.com/stats.htm

Kelley, Michael B. "The Stuxnet Attack on Iran's Nuclear Plant Was 'Far More Dangerous' Than Previously Thought." *Business Insider*, November 20, 2013, http://www.businessinsider.com/stuxnet-was-far-more-dangerous-than-previous-thought-2013-11

Kennedy Jr, Frank D. "The Creation of the Cold War Navy, 1953-1962." In *In Peace and War: Interpretations of American Naval History*, edited by Kenneth J. Hagan and Michael T. McMaster. Santa Barbara, CA: Praeger Security International, 2008.

McFarland, Stephen L. "The Air Force in the Cold War, 1945-60: Birth of a New Defense Paradigm." *Air & Space Power Journal* 10:3 (1996).

Wicks, Frank. "Nuclear Power." *Mechanical Engineering* (January 2004).

Moore, Gordon. "Cramming More Components onto Integrated Circuits." *Electronics* (April 19, 1965).

"Navy SLRP and Enlistment Bonus Update (FEB 1, 2015)," Thomas Goering, *Navy CyberSpace Blog*, July 13, 2015, https://www.navycs.com/blogs/2015/02/04/feb-2015-slrp-and-eb-update

Paul, Christopher, Isaac R. Porche III, and Elliot Axelband. *The Other Quiet Professionals: Lessons for Future Cyber Forces from the Evolution of Special Forces.* (Santa Monica, VA: Rand Corporation, 2014).

Perez, Evan. "FBI: Hacker claimed to have taken over flight's engine controls." *CNN Website*, May 18, 2015, http://www.cnn.com/2015/05/17/us/fbi-hacker-flight-computer-systems/

Schmitt, Michael N., ed., *Tallinn Manual on the International Law Applicable to Cyber Warfare.* Cambridge: Cambridge University Press, 2013.

Secretary of Defense and Chairman, Joint Chiefs of Staff. *Department of Defense Cybersecurity Culture and Compliance Initiative*. September 28, 2015. http://www.defense.gov/Portals/1/Documents/pubs/OSD011517-15-RES-Final.pdf

Sharma, Amit. "Cyber Wars: A Paradigm Shift from Means to Ends." In *The Virtual Battlefield: Perspectives on Cyber Warfare,* edited by Christian Czosseck and Kenneth Geers. Amsterdam: IOS Press, 2009.

Stiennon, Richard. *Surviving Cyber War*. Lanham, MD: Government Institutes, an imprint of The Scarecrow Press, Inc, 2010.

Storm, Darlene. "Epsilon Breach: hack of the century?" *Computer World*, April 4, 2011, http://www.computerworld.com/article/2471044/cloud-computing/epsilon-breach--hack-of-the-century-.html

Thornburgh, Nathan, Matthew Forney, Brian Bennett, Timothy J. Burger, and Elaine Shannon. "The Invasion of the Chinese Superspies (and the Man Who Tried to Stop Them)." *Time Magazine* Vol. 166 Issue 10.

Tilghman, Andrew. "In a supersecret cyberwar game, civilian-sector techies pummel active-duty cyberwarriors." *Army Times*, August 4, 2014.

U.S. Census Bureau. *Home Computers and Internet Use in the United States: August 2000*. Washington, DC: Government Printing Office, 2001.

U.S. Congress. Federal Activities Inventory Reform Act of 1998. Public Law No. 105-270. 105th Congress, 112 *Statutes at Large* 2382 (1998).

U.S. Department of Defense. *Department of Defense Information Technology Enterprise Strategy and Roadmap*. Washington, DC: Government Printing Office, 2011.

U.S. Department of Energy and U.S. Department of the Navy. *The United States Naval Nuclear Propulsion Program.* Washington, DC: Government Printing Office, 2013.

U.S. Department of Homeland Security. *Critical Infrastructure and Key Resources Support Annex.* Washington, DC: Government Printing Office, 2008.

U.S. Department of the Navy. *Nuclear Officer Incentive Pay Program.* Instruction 7220.11E. December 29, 2014.

U.S. Department of the Navy. *Program Authorization: Restricted Line/Special Duty Officer (Cyber Warfare Engineer).* Program Authorization 121. September 18, 2014.

U.S. Government Accountability Office. *Defense Department Cyber Efforts: DOD Faces Challenges In Its Cyber Activities.* GAO Publication No. 11-75. Washington, DC: Government Printing Office, 2011.

U.S. Joint Chiefs of Staff. *Cyberspace Operations*. Joint Publication 3-12(R). Washington, DC: U.S. Joint Chiefs of Staff, February 5, 2013.

U.S. Office of General Counsel Department of Defense. *Department of Defense Law of War Manual.* Washington, DC: Government Printing Office, 2015.

U.S. Strategic Command. *U.S. Cyber Command Fact Sheet*, accessed January 15, 2016. https://www.stratcom.mil/factsheets/2/Cyber_Command/

“WorldWideWebSize.com: Daily Estimated Size of the World Wide Web,” Maurice de Kunder, accessed January 15, 2016, http://www.worldwidewebsize.com/