# REPORT DOCUMENTATION PAGE

*Form Approved*
*OMB No. 0704-0188*



| 1. REPORT DATE *(DD-MM-YYYY)* | 2. REPORT TYPE | 3. DATES COVERED *(From - To)* |
|---|---|---|
| 04-05-2020 | Master of Military Studies (MMS) thesis | AY 2019-2020 |

**4. TITLE AND SUBTITLE**
American Cyber Warfare: Defend the Private Sector

**5a. CONTRACT NUMBER**
N/A

**5b. GRANT NUMBER**
N/A

**5c. PROGRAM ELEMENT NUMBER**
N/A

**6. AUTHOR(S)**
Martinez, Michael J., Major, USA

**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)**
N/A

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

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

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

**13. SUPPLEMENTARY NOTES**

**14. ABSTRACT**

America and its citizens have consistently fallen victim to cyber-attacks, and the cost has been substantial. As people and technology continue to progress in the cyber domain, issues regarding national security and prosperity will continue to compound. There is an obvious need to reestablish and maintain supremacy in the cyber domain to protect citizens and American interests. The United States currently has organizations to defend the government as a whole and critical infrastructure. Still, the commercial industry and the civilian population are, for the most part, left to protect themselves against cyber threats. These government cyber organizations such as the Department of Defense, the National Security Agency, and the Department of Homeland Security fall under different authorities to which they can function, such as Title 10 and Title 50. These authorities limit what actions they can take in cyberspace and delay response time to active threats. It is also difficult to distinguish the source of a threat. What might be perceived as a substantial threat to one organization may not be to another. Having a higher authority to which all cyber organizations can go to for decisions will allow the United States to increase its cyber resiliency and defense. American competitors and advisories have different models of government that give them an advantage in cyberspace. Our democratic process prevents rapid change, resource allocation, and unity of effort, while dictatorships by nature can overcome all those challenges quickly. What dictatorships will not do is empower their citizens. The United States, on the other hand, can and should allow its citizens to participate in defending the homeland through education, experience, and opportunities. Cyber-security comes at a price. It is a balance between protection that confines and freedom of information that liberates.

**15. SUBJECT TERMS**
Cyber Warfare, Cyber Defense, Cyber Department, Cyber Force, Cyber Education

| 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 |
| Unclass | Unclass | Unclass | UU | | 19b. TELEPHONE NUMBER *(Include area code)*<br>(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: American Cyber Warfare: Defend the Private Sector**

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

**AUTHOR: Major Michael J. Martinez, United States Army**

AY 2019-20

---

Mentor and Oral Defense Committee Member: Dr. Matthew Flynn

Approved: Yes

Date: May 4, 2020

Oral Defense Committee Member: LtCol Christopher Curtin

Approved: Yes

Date: May 4, 2020

## Executive Summary

**Title:** American Cyber Warfare: Defend the Private Sector

**Author:** Major Michael J. Martinez, United States Army

**Thesis:** The United States cyber defense is a civic duty that must be coupled with the private sector and government to protect national power.

**Discussion:** America and its citizens have consistently fallen victim to cyber-attacks, and the cost has been substantial. As people and technology continue to progress in the cyber domain, issues regarding national security and prosperity will continue to compound. There is an obvious need to reestablish and maintain supremacy in the cyber domain to protect citizens and American interests. The United States currently has organizations to defend the government as a whole and critical infrastructure. Still, the commercial industry and the civilian population are, for the most part, left to protect themselves against cyber threats. These government cyber organizations such as the Department of Defense, the National Security Agency, and the Department of Homeland Security fall under different authorities to which they can function, such as Title 10 and Title 50. These authorities limit what actions they can take in cyberspace and delay response time to active threats. It is also difficult to distinguish the source of a threat. What might be perceived as a substantial threat to one organization may not be to another. Having a higher authority to which all cyber organizations can go to for decisions will allow the United States to increase its cyber resiliency and defense. American competitors and advisories have different models of government that give them an advantage in cyberspace. Our democratic process prevents rapid change, resource allocation, and unity of effort, while dictatorships by nature can overcome all those challenges quickly. What dictatorships will not do is empower their citizens. The United States, on the other hand, can and should allow its citizens to participate in defending the homeland through education, experience, and opportunities. Cyber-security comes at a price. It is a balance between protection that confines and freedom of information that liberates.

**Conclusion:** The Unites States was the first to pioneer the uncharted realm of cyberspace, but the flood gates have opened, and the cyber domain has become home to most of the world's population. There are threats within the realm of cyber that can shift where world power resides. The United States must properly defend its private sector with the strategies and actions to mitigate those threats. The Department of Cyber, a Cyber Force, and cyber citizens are the answer to properly defending the private sector to which American draws her strength.

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.

## *Table of Contents*

## *Introduction*

The World Population Review website reported that the United States population in 2019 was approximately 330 million.[1] There were close to 312 Americans online in 2019,[2] which means 94 percent of all U.S. personnel are vulnerable to cyber-attacks. Former Director of National Intelligence, Daniel R. Coats, reported that "China, Russia, Iran, and North Korea increasingly use cyber operations to threaten both minds and machines in an expanding number of ways—to steal information, to influence our citizens, or to disrupt critical infrastructure."[3] The impact of cyber-attacks is real. It leaves American people holding the bill for billions of dollars from damages caused.[4] The United States is continuously expanding the realm of the cyber as it moves toward an "Internet of Things," where anything with an on/off button can connect to the Internet.[5] The more devices on the domain, the more vulnerabilities will be exploited, and the more significant cyber-attacks will become. The 2018 U.S. National Cyber Strategy (NCS) stated that "Cyberspace is an inseparable component of America's financial, social, government, and political life."[6] The convenience of having everything electronically accessible via digital application outweighs the potential of a cyber-attack to the average individual, so the waves of Americans moving to online devices will continue to increase. The 2018 NCS further states that "cyberspace [is] an arena where the United States' overwhelming military, economic, and political power could be neutralized and where the United States and its allies and partners are vulnerable."[7] These facts naturally lead to concerns for the safety of every citizen and the stability of national power.

A few decades ago, cyber-attacks were not as sophisticated as today and produced an image of a teenager in a basement who is hacking into government systems. Today, there are armies of cyber warriors, equipment, and software that do that work. Although it is still possible

for one person to wreak havoc in cyberspace, most people can defend themselves from such threats with good cyber hygiene and commercial software. The challenge comes when a nation-state attacks an individual or a small business with capabilities far beyond what they can defend. The rapidly increasing cyber threat to the United States is overwhelming and requires greater coordination between the government and the private sector to combat it. With the creation of a Department of Cyber, a Cyber Force to help arm every cyber citizen to adequately defend those individuals and small businesses that are not currently vulnerable to a cyberattack. In cyberspace, the Department of Defense (DOD) protects itself, the Department of Homeland Security (DHS) guards U.S. infrastructure and government, but the American people are left to defend the rest on their own. The American people are the well that feeds the sources of national power. The United States must protect its citizens in cyberspace to protect national power.

### *Intended Audience*

The intended audience for this paper is the general public, national security professionals, and leaders who can implement the required changes. The audience will learn the challenges that lead to this point, what is currently being done by U.S. Cyber Command, and how the creation of a Cyber Force, Department of Cyber, and cyber citizens can protect American interests. The target audience of this paper should recognize that they have a vested interest in understanding the premise of this work. It is their lives and the lives of those near them that will be affected by its outcome. Cyber defense is a civic duty but must be coupled with the private sector and government to provide adequate security for the American people.

### *Definitions*

To understand the scope of this document, one must first understand the use of some basic terms and concepts that will appear throughout this work. The Military Joint Publication 3-12, Cyberspace Operations defines cyberspace as, "A global domain within the information environment consisting of the interdependent networks of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers."[8] Chip Morningstar and F. Randall Farmer state, "that a cyberspace is defined more by the interactions among the actors within it than by the technology with which it is implemented."[9] The interactions of actors and technology both play a role in cyberspace because official U.S. military doctrine says it is composed of layers:

> Three aspects or layers: a physical layer, a logical layer, and a cognitive or social layer…The physical layer of cyberspace consists of the information systems, servers, hardware, wires, cables, routers, and even the radio frequencies that make up the network architectures of the Internet and other interconnected and closed networks…The logical layer of cyberspace consists of the connections between nodes where nodes are essentially any device or service represented by an Internet Protocol (IP) address…The cognitive layer of cyberspace consists of the information and the human beings that interact with it.[10]

Each layer serves a different function and can sometimes confuse those who are not familiar with them because they attribute vulnerabilities or strengths collectively or directly to a layer interchangeably. For this discussion, the terms cyberspace and cyber are the same. The terms cyberspace and cyber will include definitions that cover everything from physical to the social interactions that happen within the domain unless otherwise specified.

Richard A. Clarke and Robert K. Knake define cyberwar in their book, *Cyber War*, as "actions by a nation-state to penetrate another nation's computers or networks for the purpose of causing damage or disruption."[11] In the book *Current and Emerging Trends in Cyber Operations*, Scott Applegate defines cyber warfare as "the use of armed attacks in or through

cyberspace as an extension of one nation-state's politics to impose its political will onto another nation-state."[12] For the sake of this paper, cyberwar will be about any unlawful or unethical actions in cyberspace by one entity toward another. Non-state and nation-state actors effortlessly intertwine in cyberspace. For example, Russia is notorious for advanced cyber-attacks performed by "patriotically minded private Russian hackers,"[13] but claim the actions are not of the state. Therefore, the latter definition is preferred.

### *Current U.S. Cyber Defense for the Private Sector*

An examination of cyber defense in the U.S. has revealed a critical shortfall that is costing the American people billions of dollars a year. Massive armies of cyber warriors belonging to nation-states are exploiting banks, businesses, and individual citizens.[14] Without a Cyber Force to defend the entire private sector, the United States will suffer due to economic travails and loss of public trust. A Cyber Force must become a separate branch of service, equal to the Army, Navy, Marine Corps, Air Force, and Space Force. Each service is capable of leading the fight in its domain while the other services play enabling or supporting roles. Some may claim that there is already a Cyber Command that fills that function. Although Cyber Command fulfills part of that role through offensive operations, it does not cover all the defense that the United States requires.

When it comes to protecting American citizens and interests in other domains, there is very little debate. If there are national interests in danger at sea, the nation sends the Navy. If the welfare of the nation is in danger on land, the country directs the Army to the conflict. If they are under threat in the air, the Air Force is involved, and if there is a crisis that needs an immediate multi-domain capability, the government sends the Marines. If a citizen is in danger in cyberspace, the nation may or may not respond but will most likely leave it up to the private

sector to figure it out and pay for it on their own. This behavior does not coincide with the values of the United States or fulfill the inherent responsibility of the government to protect the homeland and its national interests.

Lieutenant General Robert Elder, Director of the Air Force Cyberspace Operations Task Force, stated that "if we are defending in cyberspace, you're already too late. If you do not dominate in cyberspace, you cannot dominate in other domains. If you are a developed country [and you are attacked in cyberspace], your life comes to a screeching halt."[15] The idea that if you are "defending in cyberspace, you're already too late," supports the direction the United States has taken to make its strategy an offensive approach. Or, in the words of the 2018 Cyber Strategy, "defend forward to halt or degrade cyberspace operations targeting the Department."[16] The school of thought is the "best defense is a good offense." By keeping the opposition preoccupied with their systems and vulnerabilities, the United States would not have to worry about heavily fortifying itself. Besides, the United States' cyber capabilities can cause significant damage to any opposition. General Elder's statement gives a sense of unpreparedness for the future as he explained that the need to "dominate in cyberspace" was required to dominate in other domains. These points make sense, but a misguided strategy that puts the focus on offense and neglects to defend the private sector that is not directly being protected by the government creates a risk that requires mitigation. What good is it to dominate the offensive if the defense is compromised.

The government's offense for a defense approach ends up being reactionary and does not provide a suitable defense. For example, when North Korea's cyberattack on Sony in 2014 happened, Sony's internal data was stolen, such as employee personal information, emails, and unreleased films.[17] Not only was Sony's data taken, but their data was erased, and for a specific

time, their network inoperable.[18] The stolen data caused Sony to lose more than information. They violated the trust of their employees, they suffered the loss of an enormous amount of money, but the most considerable loss was their freedom of speech. The purpose of the cyberattack was to prevent Sony from releasing the movie *The Interview*, a film about "a pair of bumbling journalists who go to North Korea to interview Kim Jong Un and eventually assassinate him."[19] Many theaters yielded to the terrorist threats and chose not to play the film.[20] Sony also submitted to the intimidation and limited the release and roll-out of the movie.[21]

There was an expectation in the cyber community that if a nation-state attacked the private sector that the United States would respond on their behalf. Allegedly, the United States did retaliate after Sony was attacked by denying North Korea access to the Internet for a short duration, approximately ten hours with connectivity issues for several days after that.[22] The United States also place additional sanctions on North Korea, but North Korea claimed the attack had little effect on them.[23] Even if the counteraction had an equal or greater impact on North Korea than it had on Sony, it still left Sony at a loss. There was no compensation for the damage done to Sony. So, the idea that an offensive reaction to a cyberattack to the homeland is not practical. In cases like Sony's, where a nation-state attacks the American private sector, the responsibility should fall under the purview of the DOD, just as it would for an attack in any other domain.

Placing a higher priority on offense in cyber operations is flawed because while the U.S. is busy defending forward, the enemy is exploiting U.S. homes, businesses, and institutions of learning not directly covered by government cyber defense. One of the reasons the United States took on an offensive focused approach in cyberspace because it is easy to attack and hard to defend in cyberspace. Herman Kahn explained this principle in his book, *On Thermonuclear*

*war*. He wrote, "the aggressor has to find only one crucial weakness; the defender has to find all of them, and in advance,"[24] The ease of maintaining a strong cyber offense outweighs investing in a labor and resource-intensive defense. It was merely a more natural way to go in a resourced constrained environment. Jack Goldsmith elaborates this point in the book, *Current and Emerging Trends in Cyber Operations: Policy, Strategy, and Practice.* He wrote, "even if (as is often not the case) those trying to find and patch computer vulnerabilities outnumber those trying to find and exploit the vulnerabilities, the attacker often still has an advantage."[25] Since the attacker only has to find one vulnerability to exploit, offensive operations in cyberspace are easier than defense, where the defender must know every weakness to prevent the exploitation of that vulnerability.

Former National Security Agency (NSA) Director, Vice Admiral John Michael (Mike) McConnell, had another perspective on primarily being an offensive cyber force. He said that "all the offensive cyber capability the U.S. can muster won't matter if no one is defending the nation from a cyberattack."[26] McConnell also explained that a developed country's reliance on cyberspace could result in lives coming to "a screeching halt" from cyberattacks. The United States' critical infrastructure and the Internet of things have created a larger strike surface for enemies, competitors, and terrorists to attack. A massive strike surface and a U.S. dependency on cyberspace are one of the reasons its cyber strength is not as high as other developed countries and requires a more robust defense.

### *U.S. Cyber Defense Challenges*

Three factors measure cyberwar strength: offense, dependence, and defense.[27] America's high dependency and substandard private-sector protection make the United States cyberwar strength lower than it should be. China's automation for critical systems, on the other hand,

requires a significant degree of manual control.[28] Manual control means the systems cannot be accessed electronically and therefore are not vulnerable to cyberattacks. China scored high on defense for that reason and also "because it has plans and capability to disconnect the entire nation's networks from the rest of cyberspace."[29] China's network is like that of a business where there is an intranet that connects to the Internet.[30] The Chinse government provides network defense for the nation because they are an internet service provider.[31] China protects its country by monitoring what comes in and out of their network.[32] If necessary, China can isolate itself during a cyberwar by turning off the circuits that connect it to the rest of the world. [33] The United States does not have that same capability because internet service providers are privately owned and operated.[34] With a high cyber dependency and no national cyberspace protection for the private sector, the U.S. portion of the cyber domain may tempt hostile actors to attack America.[35] The ship has sailed on reducing cyber dependency since virtually everything that needs to be protected is somehow tied to a network of some sort. With that in mind, it leaves the two factors of which the only one is lacking, and that is American cyber defense. The way to improve cyberwar strength is to enhance security by establishing a Cyber Department, a Cyber Force, and arming every cyber citizen with knowledge, experience, and means to contribute towards a collective U.S. cyber defense.

A misguided defense strategy has not alleviated the ramifications of the lack of protection for the private sector. Former National Security Agency Director Ken Minihan expressed his concerns that Cyber Command and the cyber organizations within the sister services only defend the Department of Defense. Still, there is not an agency to protect corporate cyberspace, which makes America function online.[36] Corporate cyberspace is the high-end portion of the private sector that stimulates a large part of the American economy. Joint Publication 3-08 defines the

private sector as "an umbrella term that may be applied to any or all of the nonpublic or commercial, individuals and businesses, specified nonprofit organizations, most of academia and other scholastic institutions, and selected NGOs [Non-Government Organizations]."[37] Richard Clark highlighted the point that the United States private sector cyberspace is not protected by the government in his book *Cyber War*. He wrote that "Even if the U.S. military's own networks were secure and reliable, those of its contractors, who often rely upon the public internet, may not be."[38] Contractors who work in the private sector in support of the military are a massive liability if their systems are compromised. Secrets for operational support or future technologies could be stolen, deleted, or manipulated. The private sector must be protected to prevent the compromise of America's instruments of national power.

Two former National Security Agency Directors, Ken Minihan and John McConnell, recognized the need to protect the private sector and "believed that the mission [of defense], should be handled by the Department of Homeland Security (DHS)."[39] Minihan gave the DOD a verbal lashing when he said that, "though it is called the 'Defense' Department, if called on to defend the U.S. homeland from a cyberattack carried out by a foreign power, your half-trillion-dollar-a-year Defense Department would be useless."[40] His point highlights that the defense strategy was misguided, and therefore investments where not being made in the proper areas. Clark also wrote about a meeting he had with Secretary of Homeland Security, Janet Napolitano. He asked her in 2009, "if U.S. Cyber Command is protecting the dot-mil and you will one day protect dot-gov, who is protecting everything else, like the critical infrastructure, which is in the private sector?"[41] In fact, "the private sector owns or operates approximately 85 percent of the nation's critical infrastructure."[42] Napolitano advocated [that defense of those areas] "was not Homeland Security's job."[43] Richard stressed that protecting critical infrastructure like power

grids needed to be a high priority for the nation.[44] The U.S. government heeded his plea, and the responsibility for protecting critical infrastructure fell upon the DHS.

In November 2018, the DHS established "the Cybersecurity and Infrastructure Security Agency (CISA). CISA builds the national capacity to defend against cyberattacks and works with the federal government to provide cybersecurity tools, incident response services, and assessment capabilities to safeguard the '.gov' networks that support the essential operations of partner departments and agencies."[45] The DHS took on some of the responsibilities of homeland cyber defense, but not all. Primarily they took on the government networks at first and later 16 critical infrastructure sectors: Chemical, Commercial Facilities, Communications, Critical Manufacturing, Dams, Defense Industrial Base, Emergency Services, Energy, Financial Services, Food and Agriculture, Government Facilities, Healthcare, and Public Health, Information Technology, Nuclear Reactors, Transportation Systems, and Water and Wastewater Systems.[46] CISA posted that "DHS has partnered with the critical infrastructure community to establish a voluntary program to encourage the use of the Framework for Improving Critical Infrastructure Cybersecurity to strengthen critical infrastructure cybersecurity."[47] Since the United States government does not own all of the nation's infrastructure, cyber defense with critical infrastructure is a voluntary partnership. Although critical infrastructure is key to protecting the country, it still does not cover the entire private sector. The DHS is currently working to protect critical infrastructure by using a "collective approach to prevent, protect against, mitigate, respond to, investigate, and recover from cyber incidents."[48] CISA has mounted a defense, but the partnership does not cover the whole private sector. It is a decade later since identifying the problem of defending the private sector, and there is still not an agency responsible for their collective protection.

Along with the debate of who should take the responsibility of protecting the private sector is the conflict of authorities between Title 10 and Title 50. The term "Title 10 authority" is often used "as a catchall phrase to describe the legal authority for military operations," but, "the U.S. military's true operational authority stems from the U.S. Constitution and the President's Commander-in-Chief power."[49] Title 10 covers the organization of the military while the constitution and the president govern the application of that authority.[50] Title 10 authority appears in the day to day operations of the military, which is why they are accustomed to its application. On the other hand, Title 50 of the United States Code, also known as "refers to intelligence agencies, intelligence activities, and covert action."[51] The military can also act under Title 50 authority, but it is not inherent in its organization and therefore requires procedures to obtain that authority.[52] In contrast, other organizations such as the DHS and CIA have Title 50 authority inherent to their day to day operations, which authorizes intelligence activities.[53] Intelligence activities in cyberspace may obtain access to a source. From a DHS or CIA perspective, they may want to keep that source to exploit it for as long as possible. Whereas, from a military standpoint, the source may be viewed as a target that requires immediate elimination. Activities, whether based on intelligence or military action, must receive prior notification from the congressional committee to which it belongs.[54] Therefore, "the Title 10-Title 50 debate is really about oversight and accountability" by congress.[55] The Title 10-Title 50 debate comes into play in cyberspace when organizations that have Title 10 authority run into situations that transition to Title 50. For example, the National Security Agency (NSA) has a Title 10 authority, which allows them to penetrate networks to collect information. Still, they are restricted from warfighting because they do not hold Title 50 authority.[56] To deconflict these authorities, a higher governing body of a Cyber Department would be applicable. The Cyber

Department could establish the means to which the Cyber Force could transition seamlessly through authorities to effectively perform their duties of cyber defense for DOD, DHS, and the private sector. For the DOD to take its rightful place as a defender of all Americans, it must address the Title 10/ Title 50 hurdle.

It is the responsibility of the government to protect its citizens from harm. For example, if someone broke into a home and stole something, the expectation is that the police will investigate and that legal processes will ensure justice. When a nation-state attacks an individual or group, the United States could respond with military force. In the realm of cyber, if a nation-state steals information from a company, shuts down a website, or causes networks to crash, the government is not likely to respond. President Barack Obama demonstrated this behavior when he said, "so let me be very clear: my administration will not dictate security standards for private companies."[57] President Obama allowed the private sector to continue to defend their systems to prevent having to regulate them.[58] Imagine if during the Cold War, "the Pentagon told the U.S. Steel and General Motors to go buy their own Nike missiles to protect themselves? That's in effect what the Obama Administration [said]."[59] The private sector does not have the authority nor the means to defend itself against nation-states' military-grade cyber capabilities properly. Therefore, the responsibility should fall within the DOD on this issue, but specifically to Cyber Command. For Cyber Command to effectively own that responsibility, they must grow into a full Cyber Force with increased capabilities and budget that will enable them to fulfill that responsibility.

CYBERCOM's mission is "to direct, synchronize, and coordinate cyberspace planning and operations to defend and advance national interests in collaboration with domestic and international partners."[60] CYBERCOM understands that superiority in cyberspace requires unity

of effort from not only within the organization but equally with how it can leverage external organizations. This concept will not change when a Cyber Force is created and even more so since they will be covering a larger part of the cyber domain that includes the private sector. CYBERCOM is in the pursuit of five imperatives that will enable it to "retain the initiative in cyberspace."[61] Of the five imperatives, only the fifth speaks of the private sector and CYBERCOM is not talking about defending it, but rather leveraging it for "threat information sharing, operational planning, capability development, and joint exercises."[62] Cyber Command is not currently focused on defending the private sector, nor does it have the means to do so. A Cyber Command must grow into a full Cyber Force to take on the additional responsibility of protecting Americans that do not fall under the purview of the current government coverage. The Cyber Force does not have to end private enterprise in cyberspace, but partner with industry to cover gaps that require a layer of military defense. Adequate protection will require teamwork between the government and the civil sector to protect national instruments of power.

World powers recognize the potential to impact other nation's instruments of power and have invested heavily in their cyber capabilities because of it. Cyber Warfare, A Multidisciplinary Analysis, written by Richard Stiennon, shared that, "The rise of global connectivity and the impact of the Internet on commerce, communication, and social interaction, have made possible attacks that, even if not directed by states, served their purposes. The increased threat of cyber-attack has been a key driver for organizational change, investment, and the development of cyber capabilities by other states."[63] The United States will be remiss if they do not continue on the same path by the creation of a Cyber Force. Other states have allowed government oversight of the cyber industry to violate the longstanding U.S. belief in private industry.

The Government Accountability Office (GAO) conducted a study to investigate U.S. Strategic Command's claim that the DOD was in "the midst of a global cyberspace crisis." The study revealed that the "DOD has assigned authorities and responsibilities for implementing cyber operations among combatant commands and military services; however, the supporting relationships necessary to achieve command and control of cyber operations remain unclear."[64] The remedy to the DOD's lack of clarity is the establishment of the overarching leadership of a Cyber Force. The U.S. Strategic Command recognizes that the "DOD's cyber workforce is undersized and unprepared to meet the current threat, which is projected to increase significantly over time."[65] The Cyber Force would create unity of effort and produce a workforce that is more apt to defend the DOD and private sector.

### *Providing an Adequate Cyber Defense*

There are several ways that the Cyber Force can fulfill the responsibilities of protecting the private sector. It can manage the malware deep packet scanning, and circuit shut down at the ISPs, work in collaboration with the Cyber Department to resolve the Title 10/ Title 50 challenge, respond to nation-state attacks on the private sector, and unify the DOD cyber effort to achieve greater results.

A proposed model to assist a Cyber Force in protecting Americans in cyberspace is a layered defense, as partially covered by the Cyber Solarium Commission's six pillared recommendations, which are: "Reform the U.S. government's structure and organization for cyberspace. Strengthen norms and non-military tools, promote national resilience. Reshape the cyber ecosystem. Operationalize cybersecurity collaboration with the private sector. Preserve and employ the military instruments of national power."[66] The pillars support a defend forward concept for the military but do not emphasize the individual who resides at the core of a layered

defense. The institution in which the individual belongs to a network, the Internet Service Provider (ISP), is the next layer. DOD's Cyber Force covers the external layer. Each layer has its responsibilities in cyber defense. The individual layer will be covered later in this paper, where arming every citizen is mentioned**.** The parts to emphasize here are the ISP and Cyber Force layers.

The Cyber Force can tie into the major ISPs that hook up to the trunk lines which connect the United States to the rest of the world, similar to China's model mentioned earlier. The idea of tying into the ISPs to defend the private sector is not new, but there are some obstacles to this course of action. Richard Clark explained that deep packet inspections, a process that examines information at the data level, can identify and can combat malware produced to attack the private sector.[67] Deep packet inspection has to resolve the technical problem of slowing down internet traffic, and the policy problem of violation privacy before application,[68] but Clark proposed that there is the technology that allows traffic to flow so quickly that it causes no latency.[69] He also claimed that a "rigorous oversight by an active Privacy and Civil Liberties Protection Board," can ensure that privacy violations do not occur. Clark argues that the ISPs should run this equipment and process to prevent the idea that Big Brother is watching."[70] It stands to reasons that the responsibility of deep packet inspection falls on the Cyber Force. The Cyber Force can use the same equipment and processes to manage the protection of citizens in cyberspace. Deep packet inspection will allow the Cyber Force to serve as a defender of the private sector. The Cyber Force is ideal for this task because it can identify malware, and its source, then take offensive actions without hesitation. Some may argue that these methods seldom work and that the watchdog can be used to cover inappropriate actions of the government. The United States

has organizations such as the Government Accountability Office and media to maintain the transparency required to sustain operations while at the same time protecting citizen's privacy.

There may be some entities in the private sector who oppose the deep packet inspection of their data and would instead take a risk or attempt to mitigate that risk on their own. The packet inspection could be made optional for those who fall within that category. For those who do not have the means for defense or do not object to the inspection, they can choose to have their data routed through the Cyber Force's defenses. Ideally, the equipment required for deep packet inspection would be in the ISP to prevent the establishment of another link, but if not, it could be tied into the Cyber Force facilities and monitored from there. Also, the Cyber Force can turn off circuits to contain threats or repel them from entering or exiting the network. In a cyberwar, this would allow traffic that is external to the United States to be blocked while still allowing internal traffic to flow. The deep packet inspection and circuit control performed by the Cyber Force is the way the United States can protect their private sector from state actors who are out to harm or take advantage of Americans.

The challenge of balancing Title 10 and Title 50 is bound to be manifest when it comes to dealing with state actors and deep package inspection. The Cyber Force can eliminate the challenge of balancing Title 10 and Title 50 authorities between the DOD and DHS by the endowment of both within the Cyber Force. There are legal actions required to enable both authorities to reside within an organization, but that is not the biggest hurdle in the debate.[71] The main issue is that Title 10 wants to operate in the open, and Title 50 wants to operate unseen.[72] The Cyber Force commander can decide when to use which authority to resolve the issue at that level instead of leaving it to a higher power to decide. The Center for International Maritime Security stated that "operational authorities in cyberspace are hamstrung by concerns about

blending Title 10 military operations with Title 50 intelligence activities…but blending cyber operations with rapid, fused intelligence is vital, and go hand-in-hand— to separate them completely would be to take the leash that already exists around USCYBERCOM's neck and tie their hands with it as well."[73] The blending of the Title authorities into one organization would unleash a Cyber Force that is capable of obtaining information and acting on it. A proper reporting system for attacks will have to be maintained to facilitate rapid transitions between Title 10 and Title 50. In effect, the military will run the outer layer of the network. Some may view this as a complete militarization of cyberspace and the end of democracy. Still, just like the U.S. Navy enables freedom of movement in the sea domain, the Cyber Force will allow movement in cyberspace.

Posturing the Cyber Force to protect the private sector and to respond to attacks from nation-states will come from monitoring the network. For cyber-attacks that managed to get passed defenses, the Cyber Force can establish a reporting system to get involved immediately. When symptoms of an attack are made known by others in the network, they can report like the DHS. CISA already has processes in processes in place for reporting,[74] so when nation-states attack, the Cyber Force can intervene to protect the private sector. The collaborated effort between DHS's CISA and the Cyber force is another example of how to address the unity challenge that exists within the United States cyber community today.

One way the private sector feeds the instruments of power is through the individuals who work in those areas. Increasing cyber capabilities with a Cyber Force will require individuals with an aptitude for working on and in cyberspace. The United States waits too long to introduce fundamental cyber knowledge to young Americans. The U.S. Department of Education focuses on "secondary and postsecondary educational institutions to help meet the growing need for

cybersecurity professionals."[75] Postsecondary educational institutions allow students to gain a somewhat greater understanding, but programs are still "lack the resources to maintain state of the art programs."[76] Expertise in Cyber career fields is usually achieved at an institution of higher learning or through individual development. In contrast:

> North Korea selects elite students at the elementary-school level to be groomed as future hackers. These students are trained on programming and computer hardware in middle school and high school, after which they automatically enroll at the Command Automation University in Pyongyang, where their sole academic focus is to learn how to hack into enemy network systems. Currently, 700 students are reportedly enrolled. They conduct regular cyber warfare simulated exercises against each other, and some infiltrate Japan to learn the latest computer skills.[77]

Granted, the values of the United States will not support the exact educational model of North Korea, but some principles can be implemented. For example, starting cyber education in elementary school, providing advanced technical training in middle school and high school, and providing real-world experience in the higher learning environments, these steps can be taken. Trained personnel within the U.S. educational system could participate in cyber attacks by using a gaming interface in conjunction with botnets for Denial-of-Service attacks or other activities requiring the massing of systems. Empowering youth through cyber education and opportunities is just one way the cyber citizen can contribute to increasing American cyberwar strength.

Some may argue that there is no need for every child to learn about cyberspace because an understanding of how something works is not required to operate it. It is like turning on a light switch; one does not need to understand it to make it work. Although this argument sounds logical, the analogy is not entirely transferable. The design of a light switch protects the user from being exposed to the circuit within. The design of the Internet was not to protect the user from being exposed to the content within. Therefore, the protection must come through

education. If Americans understand how cyberspace works, they can better perform their duties in their layer of defense.

Every citizen must be armed with cyber education to create a shared understanding of cyber realities, develop future cyber professionals, and to aid in defense of American interest associated with networking. Although the Internet has been a prominent part of life for Americans for over twenty years, not everyone understands how it works or the threats associated with it. When cyber professionals attempt to educate the people they support, the information can be overwhelming. Most cyber professionals are technical experts, not teachers, so when it comes to explaining concepts or sharing information that will strengthen network capabilities and defenses, the message falls on deaf ears. Proper asset allocation is difficult to achieve when communication is not clear. If professionals in other career fields understand cyber concepts from an early age, they will be better prepared to manage and support cyber capabilities for their career fields. Education at an early age will be even more beneficial for those who decide to make cyber their profession. Like learning languages, sports, or music at an early age, learning about cyberspace will aid in the development of experts that will support and sustain cyber superiority for the United States. Lastly, Americans who not only operating in cyberspace but understanding how it works will be better prepared to defend it. Cyber educated Americans will create a collective strength that will protect them from the cyber abuse that has been so prevalent in the past. Every citizen must be armed with cyber education to fill cyber organizations such as the proposed Cyber Force and Department of Cyber. Filling the cyber ranks will enable the government to fulfill its role in defending the private sector.

The creation of a Cyber Department will provide a source to govern and unify all things relating to cyber properly. As Scott Applegate says, “The discussion concerning government

leadership in cyberspace is most often a debate over whether we should have the Department of Defense or the Department of Homeland Security in charge. The simple answer is neither."[78] Cyberspace is interwoven into almost every facet of life. That makes it difficult for any existing entity, such as the DOD or the DHS, to govern it. But there must be a governing body that can lead to all matters cyber and delegate to subordinate authorities based on requirements. A Cyber Department will be that governing body to lead cyber into the future. Creating the Cyber Department will naturally require more cyber professionals to enter the government workforce. It will be ideal if the department to fill its workforce with trained cyber professionals from the pool of cyber citizens who have been prepared from their youth for such a purpose since such a pool is currently limited. Cybercrime Magazine reports that a lack of cybersecurity talent will leave 3.5 million positions unfilled globally in 2021.[79] Leaders and cyber warriors will most likely come from existing organizations that already fall short on their cyber responsibilities due to the lack of resources available, primarily workforce. Although human resources are an issue, it should not stop the United States from forming the institutions required for success in the future. Once the organizations are instituted, the market will rise to fill the gaps. For the Cyber Department to govern all things cyber, it will need a special force to cover current security gaps regarding who protects Americans and their interests in cyberspace. The Cyber Force will fill that role as a branch equal to that of the other sister service. In the long term, cyber citizens will be the answer to sustaining cyber superiority for the United States.

## *Conclusion*

The cyber threat in America is real and must be addressed before a catastrophic event or suffer from a slow economic downfall that results in a significant reduction of national power. Cyberspace Solarium Commission warned that "the coronavirus pandemic has proven that we

have no time to waste," because "the cost of being unprepared is unacceptable [and in] the case of the electric grid, [it's] wholly unnecessary,"[80] The stay-at-home-orders issued by each state required many Americans to move work and education into the home. Moving work and learning into the house has pushed the private sector industry and education into the most vulnerable part of the U.S. cyberspace. The large strike surface eluded to earlier in this paper has arrived prior than anticipated. Although American vulnerability in cyberspace has increased, there has still not been a devastating cyber incident to gain the attention required for rapid change. When it comes to cyber defense, there has not been a Coronavirus pandemic, Pearl Harbor, or cyber 9/11 to trigger a large-scale adjustment to address the issues in cyberspace. Former White House cyber-security and cyber-terrorism advisor, Richard Clark warned that:

> Every major company in the United States has already been penetrated by China […] My greatest fear […] is that, rather than having a cyber-Pearl Harbor event, we will instead have this death of a thousand cuts. Where we lose our competitiveness by having all of our research and development stolen by the Chinese. And we never really see the single event that makes us do something about it. That it's always just below our pain threshold. That company after company in the United States spends millions, hundreds of millions, in some cases billions of dollars in R&D and the information goes free to China […] After a while you can't compete.[81]

The United States must act now and create the Department of Cyber that can lead the efforts of the coalition of cyber professionals comparable to that effort of the COVID19 team and prevent the economic "death of a thousand cuts." President Dwight D. Eisenhower believed, "that a strong economy, and not numbers of men under arms, was the true source of national security.[82] Cyberspace was not a part of President Eisenhower's world, and his observation was partially correct. National security does come from a strong economy, but "under arms" had a different meaning in his time. The moment information and information sources became weaponized, it introduced a new definition of the term. Now the expression includes cyber warriors and, as

proposed in this paper, cyber citizens. The slow, limited, or refusal to defend the private sector with a Cyber department, Cyber Force, cyber citizens will result in the economic decline that will remove the United States from being the world superpower that it is.

Some may contend that the U.S. defense budget is already unsustainable, and the addition of government agencies and initiatives are not a wise allocation of resources. Compared to the economic loss from malicious cyber activity, it is a small investment. The Council of Economic Advisers reported that the economic impact of cyber-attacks cost "between $57 billion and $109 billion in 2016."[83] To put that into context, that is 8.7 to 16.8 percent of the entire DOD budget for 2016.[84] A fraction of the economic loss per year will easily cover the cost of the solutions proposed in this paper. The DOD fiscal year 2021 proposed budget for the Space Domain, which includes the newly formed Space Force, Space Command, and Space Development Agency, is $15.98 billion.[85] For an equivalent investment, the Cyber Force, Department of Cyber, and cyber education, as outlined in this paper, could be achieved. The American people will pay for their cyber defense, whether they pay directly to the government and keep the money circulating in the U.S. economy, or pay it to their adversaries when it is taken from them. The logical choice is to fund cyber defense to strengthen the economic instrument of national power and prevent funding the enemy.

The discovery and evolution of cyberspace have created a contestable domain that has the potential to shift world power. More significant efforts need to be taken to defend the American people in cyberspace, specifically the private sector. Avoiding responsibility for protecting the private sector has gone on long enough. The idea that a potent offense is our plan to defend the private sector is not the standard and must be corrected. The Internet of things and infrastructure dependency on cyber has created a large strike face that requires an improved defense. Offense,

dependence, and defense are all aspects of cyberwar strength to which the United States is deficient in the first two. Although it is easier to conduct offensive operations in cyberspace, the American people are not going to reduce their dependency on the cyber domain. Therefore, neglect of the private sector defense must not be permitted to continue. The DHS and other government and non-government organizations contribute to cybersecurity. Still, there needs to be a Department of Cyber to synchronize efforts between these organizations for the proper defense of every American. The challenges of managing authorities should reside with the Cyber Force for a rapid response to attacks from nation-states or with the Cyber Department. The Cyber Force will exist to fulfill the United States' responsibilities for protecting the private sector. The establishment of a Cyber Force is the answer to protecting the private sector and achieving superiority in cyberspace. A Cyber Force will bring about an improved cyber defense for the United States that will complement its mighty offense. It is the responsibility of the nation to protect its citizens, and that includes cyberspace. For the United States to maintain its national power and remain competitive in cyberspace in the future, there must be a Cyber Department, Cyber Force, and cyber citizens to protect its people. Though the implementation of these three recommendations will increase the capabilities of the government, it will be the cyber citizen, the American people, that will continue to be the real source of American national power.

## ***Endnotes***

[1] World Population Review, "United States Population," accessed January 17, 2020, http://worldpopulationreview.com/countries/united-states-population/
[2] Statista, "United States: number of internet users 2000-2019," accessed January 17, 2020, https://www.statista.com/statistics/276445/number-of-internet-users-in-the-united-states/
[3] Daniel R. Coats, "Director of National Intelligence, Statement for the Record: Worldwide Threat Assessment of the US Intelligence Community," accessed January 29, 2020. https://www.intelligence.senate.gov/sites/default/files/documents/os-dcoats-012919.pdf

[4] White House, "The Cost of Malicious Cyber Activity to the U.S. Economy," accessed January 18, 2020, https://www.whitehouse.gov/wp-content/uploads/2018/03/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf

[5] Jacob Morgan, Forbes, "A Simple Explanation Of "The Internet Of Things," accessed January 17, 2020, https://www.forbes.com/sites/jacobmorgan/2014/05/13/simple-explanation-internet-things-that-anyone-can-understand/#2dbe9ccd1d09

[6] Jim Mattis, "Summary of the 2018 National Defense Strategy of The United States of America," 1. accessed November 20, 2018, https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf

[7] Jim Mattis, "Summary of the 2018 National Defense Strategy of The United States of America," 1. accessed November 20, 2018, https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf

[8] Joint Publication 3-12, "Cyberspace Operations", GL-4, accessed November 21, 2018, https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf

[9] Chip Morningstar and F. Randall Farmer, "Cyberspace: First Steps," ed. Michael Benedikt (Cambridge: MIT Press, 1991), 274. https://ia802900.us.archive.org/31/items/CyberspaceFirstSteps/Cyberspace%20First%20Steps%20%281991%29.pdf

[10] Frederic Lemieux, ed. *Current and Emerging Trends in Cyber Operations: Policy, Strategy and Practice*, (New York: Palgrave Macmillan, 2015) 22-23.

[11] Richard A. Clarke and Robert K. Knake, *Cyber War: The Next Threat to National Security and What to Do About It* (New York: HarperCollins Publishers, 2010), 6.

[12] Frederic Lemieux, ed. *Current and Emerging Trends in Cyber Operations: Policy, Strategy and Practice*, (New York: Palgrave Macmillan, 2015) 26.

[13] Andrew Higgins, New York Times, "Maybe Private Russian Hackers Meddled in Election, Putin Says," accessed January 22, 2020, https://www.nytimes.com/2017/06/01/world/europe/vladimir-putin-donald-trump-hacking.html

[14] Lee Mathews, Forbes, "North Korean Hackers Have Raked in $670 Million Via Cyberattacks," accessed January 22, 2020, https://www.forbes.com/sites/leemathews/2019/03/11/north-korean-hackers-have-raked-in-670-million-via-cyberattacks/#4d66e5597018

[15] Richard A. Clarke and Robert K. Knake, "Cyber War: The Next Threat to National Security and What to do About it," (HarperCollins, 2010), 36.

[16] Department of Defense, 2018 Cyber Strategy (Washington DC: Department of Defense 2018), 2, https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF

[17] Lori Grisham, USA Today, "Timeline: North Korea and the Sony Picture hack," accessed January 22, 2020. https://www.usatoday.com/story/news/nation-now/2014/12/18/sony-hack-timeline-interview-north-korea/20601645/

[18] Lori Grisham, USA Today, "Timeline: North Korea and the Sony Picture hack," accessed January 22, 2020. https://www.usatoday.com/story/news/nation-now/2014/12/18/sony-hack-timeline-interview-north-korea/20601645/

[19] Richard Stengel, Vanity Fair, "The Untold Story of the Sony Hack: How North Korea's Battle with Seth Rogen and George Clooney Foreshadowed Russian Election Meddling in 2016," accessed January 22, 2020, https://www.vanityfair.com/news/2019/10/the-untold-story-of-the-sony-hack
[20] Lori Grisham, USA Today, "Timeline: North Korea and the Sony Picture hack," accessed January 22, 2020. https://www.usatoday.com/story/news/nation-now/2014/12/18/sony-hack-timeline-interview-north-korea/20601645/
[21] Lori Grisham, USA Today, "Timeline: North Korea and the Sony Picture hack," accessed January 22, 2020. https://www.usatoday.com/story/news/nation-now/2014/12/18/sony-hack-timeline-interview-north-korea/20601645/
[22] Lori Grisham, USA Today, "Timeline: North Korea and the Sony Picture hack," accessed January 22, 2020. https://www.usatoday.com/story/news/nation-now/2014/12/18/sony-hack-timeline-interview-north-korea/20601645/
[23] Lori Grisham, USA Today, "Timeline: North Korea and the Sony Picture hack," accessed January 22, 2020. https://www.usatoday.com/story/news/nation-now/2014/12/18/sony-hack-timeline-interview-north-korea/20601645/
[24] Frederic Lemieux, ed. *Current and Emerging Trends in Cyber Operations: Policy, Strategy and Practice,* (New York: Palgrave Macmillan, 2015) 53.
[25] Frederic Lemieux, ed. *Current and Emerging Trends in Cyber Operations: Policy, Strategy and Practice,* (New York: Palgrave Macmillan, 2015) 53.
[26] John A. Adams, "Cyber Blackout: When the Lights Go Out—Nation at Risk," (FriesenPress, 2015), 50.
[27] Richard A. Clarke and Robert K. Knake, "Cyber War: The Next Threat to National Security and What to do About it," (HarperCollins, 2010), 148.
[28] Richard A. Clarke and Robert K. Knake, "Cyber War: The Next Threat to National Security and What to do About it," (HarperCollins, 2010), 147.
[29] Richard A. Clarke and Robert K. Knake, "Cyber War: The Next Threat to National Security and What to do About it," (HarperCollins, 2010), 148.
[30] Richard A. Clarke and Robert K. Knake, "Cyber War: The Next Threat to National Security and What to do About it," (HarperCollins, 2010), 146-147.
[31] Richard A. Clarke and Robert K. Knake, "Cyber War: The Next Threat to National Security and What to do About it," (HarperCollins, 2010), 146-147.
[32] Richard A. Clarke and Robert K. Knake, "Cyber War: The Next Threat to National Security and What to do About it," (HarperCollins, 2010), 146-147.
[33] Richard A. Clarke and Robert K. Knake, "Cyber War: The Next Threat to National Security and What to do About it," (HarperCollins, 2010), 146-147.
[34] Richard A. Clarke and Robert K. Knake, "Cyber War: The Next Threat to National Security and What to do About it," (HarperCollins, 2010), 148.
[35] Richard A. Clarke and Robert K. Knake, "Cyber War: The Next Threat to National Security and What to do About it," (HarperCollins, 2010), 149.
[36] Richard A. Clarke and Robert K. Knake, "Cyber War: The Next Threat to National Security and What to do About it," (HarperCollins, 2010), 43-44.
[37] Joint Publication 3-08, "Interorganizational Cooperation," accessed February 19, 2020, xiii, https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_08pa.pdf?ver=2018-02-08-091414-467

[38] Richard A. Clarke and Robert K. Knake, "Cyber War: The Next Threat to National Security and What to do About it," (HarperCollins, 2010), 227.
[39] Richard A. Clarke and Robert K. Knake, "Cyber War: The Next Threat to National Security and What to do About it," (HarperCollins, 2010), 43.
[40] Richard A. Clarke and Robert K. Knake, "Cyber War: The Next Threat to National Security and What to do About it," (HarperCollins, 2010), 44.
[41] Richard A. Clarke and Robert K. Knake, "Cyber War: The Next Threat to National Security and What to do About it," (HarperCollins, 2010), 120.
[42] Joint Publication 3-08, "Interorganizational Cooperation," accessed February 19, 2020, xv, https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_08pa.pdf?ver=2018-02-08-091414-467
[43] Richard A. Clarke and Robert K. Knake, "Cyber War: The Next Threat to National Security and What to do About it," (HarperCollins, 2010), 120.
[44] Richard A. Clarke and Robert K. Knake, "Cyber War: The Next Threat to National Security and What to do About it," (HarperCollins, 2010), 277.
[45] U.S. Department of Homeland Security, "Cybersecurity," accessed February 19, 2020, https://www.dhs.gov/topic/cybersecurity
[46] U.S. Department of Homeland Security, CISA, "Critical Infrastructure Sectors," accessed February 19, 2020. https://www.cisa.gov/critical-infrastructure-sectors
[47] U.S. Department of Homeland Security, CISA, "Protecting Critical Infrastructure," accessed February 19, 2020. https://www.cisa.gov/protecting-critical-infrastructure
[48] U.S. Department of Homeland Security, CISA, "Protecting Critical Infrastructure," accessed February 19, 2020. https://www.cisa.gov/protecting-critical-infrastructure
[49] American University, National Security Law Brief, "CIA or DOD: Clarifying the Legal Framework Applicable to the Drone Authority Debate," Accessed April 4, 2020. https://nationalsecuritylawbrief.com/2013/04/04/cia-or-dod-clarifying-the-legal-framework-applicable-to-the-drone-authority-debate-2
[50] American University, National Security Law Brief, "CIA or DOD: Clarifying the Legal Framework Applicable to the Drone Authority Debate," Accessed April 4, 2020. https://nationalsecuritylawbrief.com/2013/04/04/cia-or-dod-clarifying-the-legal-framework-applicable-to-the-drone-authority-debate-2
[51] Andru E. Wall, "Demystifying the Title 10-Title 50 Debate: Distingushing Miltiary Operations, Intelligence Activity & Covert Action," Harvard National Security Journal Vol. 3 (2011), 87, https://www.soc.mil/528th/PDFs/Title10Title50.pdf
[52] American University, National Security Law Brief, "CIA or DOD: Clarifying the Legal Framework Applicable to the Drone Authority Debate," Accessed April 4, 2020. https://nationalsecuritylawbrief.com/2013/04/04/cia-or-dod-clarifying-the-legal-framework-applicable-to-the-drone-authority-debate-2
[53] Michael E. DeVine, "Covert Action and Clandestine Activities of the Intelligence Community: Selected Definitions in Brief," Congressional Research Service, (June 2019). https://fas.org/sgp/crs/intel/R45175.pdf
[54] Michael E. DeVine, "Covert Action and Clandestine Activities of the Intelligence Community: Selected Definitions in Brief," Congressional Research Service, (June 2019). https://fas.org/sgp/crs/intel/R45175.pdf

[55] American University, National Security Law Brief, "CIA or DOD: Clarifying the Legal Framework Applicable to the Drone Authority Debate," Accessed April 4, 2020. https://nationalsecuritylawbrief.com/2013/04/04/cia-or-dod-clarifying-the-legal-framework-applicable-to-the-drone-authority-debate-2
[56] Richard A. Clarke and Robert K. Knake, "Cyber War: The Next Threat to National Security and What to do About it," (HarperCollins, 2010), 40.
[57] Richard A. Clarke and Robert K. Knake, "Cyber War: The Next Threat to National Security and What to do About it," (HarperCollins, 2010), 118.
[58] Richard A. Clarke and Robert K. Knake, "Cyber War: The Next Threat to National Security and What to do About it," (HarperCollins, 2010), 118.
[59] Richard A. Clarke and Robert K. Knake, "Cyber War: The Next Threat to National Security and What to do About it," (HarperCollins, 2010), 144.
[60] Command Vision for US Cyber Command, "Achieve and Maintain Cyberspace Superiority," accessed December 18, 2019. https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20April%202018.pdf?ver=2018-06-14-152556-010
[61] Command Vision for US Cyber Command, "Achieve and Maintain Cyberspace Superiority," accessed December 18, 2019. https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20April%202018.pdf?ver=2018-06-14-152556-010
[62] Command Vision for US Cyber Command, "Achieve and Maintain Cyberspace Superiority," accessed December 18, 2019. https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20April%202018.pdf?ver=2018-06-14-152556-010
[63] Cyber Warfare, A Multidisciplinary Analysis, ed. James A. Green (London and New York: Routledge, 2015), 7.
[64] United States Government Accountability Office, "Defense Department Cyber Efforts: DOD Faces Challenges In Its Cyber Activities," accessed December 19, 2019. https://www.gao.gov/assets/330/321818.pdf
[65] United States Government Accountability Office, "Defense Department Cyber Efforts: DOD Faces Challenges In Its Cyber Activities," accessed December 19, 2019. https://www.gao.gov/assets/330/321818.pdf
[66] Senator Angus King and Representative Mike Gallagher, Cyberspace Solarium Commision, "CSC Final Report," accessed April 10, 2020. https://drive.google.com/file/d/1ryMCIL_dZ30QyjFqFkkf10MxIXJGT4yv/view
[67] Richard A. Clarke and Robert K. Knake, "Cyber War: The Next Threat to National Security and What to do About it," (HarperCollins, 2010), 161.
[68] Richard A. Clarke and Robert K. Knake, "Cyber War: The Next Threat to National Security and What to do About it," (HarperCollins, 2010), 161.
[69] Richard A. Clarke and Robert K. Knake, "Cyber War: The Next Threat to National Security and What to do About it," (HarperCollins, 2010), 162.
[70] Richard A. Clarke and Robert K. Knake, "Cyber War: The Next Threat to National Security and What to do About it," (HarperCollins, 2010), 162.

[71] Andru E. Wall, "Demystifying the Title 10-Title 50 Debate: Distingushing Miltiary Operations, Intelligence Activity & Covert Action," Harvard National Security Journal Vol. 3 (2011), 88, https://www.soc.mil/528th/PDFs/Title10Title50.pdf
[72] Andru E. Wall, "Demystifying the Title 10-Title 50 Debate: Distingushing Miltiary Operations, Intelligence Activity & Covert Action," Harvard National Security Journal Vol. 3 (2011), 87, https://www.soc.mil/528th/PDFs/Title10Title50.pdf
[73] David Schroeder and Travis Howard, Center for International Maritime Security, "Why It Is Time For A U.S. Cyber Force," accessed December 20, 2019. http://cimsec.org/why-it-is-time-for-a-u-s-cyber-force/37390
[74] Department of Homeland Security, CISA, "Report an Incident," accessed March 4, 2020. https://www.us-cert.gov/forms/report?
[75] U.S. Department of Education, Office of Career, Technical, and Adult Eductions, "New Cybersecutiry Education Funding Opportunity," Accessed April 25, 2020. https://sites.ed.gov/octae/2016/05/12/new-cybersecurity-education-funding-opportunity/
[76] U.S. Department of Education, Pilot Program from Cybersecurity Education Technological Upgrades for Community Colleges, "Program Description," accessed April 25, 2020. https://www2.ed.gov/programs/ppcetucc/index.html
[77] Richard A. Clarke and Robert K. Knake, "Cyber War: The Next Threat to National Security and What to do About it," (HarperCollins, 2010), 28.
[78] Scott Applegate, *Current and Emerging Trends in Cyber Operations*, ed. Frederic Lemieux (Michigan: Palgrave Macmillan, 2015), 113.
[79] Steve Morgan, Cybercrime Magazine, "Cybersecurity Talent Crunch to Create 3.5 Million Unfilled Jobs Globally By 2021." Accessed April 15, 2020. https://cybersecurityventures.com/jobs/
[80] John Shkor, The Hill, "We weren't ready for a pandemic – imagine a crippling cyberattack," accessed April 4, 2020, https://thehill.com/opinion/cybersecurity/489660-we-werent-ready-for-a-pandemic-imagine-a-crippling-cyber-attack
[81] Frederic Lemieux, ed. *Current and Emerging Trends in Cyber Operations: Policy, Strategy and Practice*, (New York: Palgrave Macmillan, 2015), 88.
[82] Donald A. Carter, *The U.S. Army before Vietnam, 1953-1965* (Center of Military History, 2015), 20.
[83] Council of Economic Advisers, "The Cost of Malicious Cyber Activity to the U.S. Economy," accessed April 29, 2020, https://www.whitehouse.gov/wp-content/uploads/2018/03/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf
[84] Macrotrends, "U.S. Military Spending/Defense Budget 1960-2020," accessed April 29, 2020, https://www.macrotrends.net/countries/USA/united-states/military-spending-defense-budget
[85] U.S. Department of Defense, "DOD Releases Fiscal Year 2021 Budget Proposal," published February 10, 2020. https://www.defense.gov/Newsroom/Releases/Release/Article/2079489/dod-releases-fiscal-year-2021-budget-proposal/

## ***Bibliography***

American University, National Security Law Brief, "CIA or DOD: Clarifying the Legal Framework Applicable to the Drone Authority Debate," last modified August 27, 2016,

https://nationalsecuritylawbrief.com/2013/04/04/cia-or-dod-clarifying-the-legal-framework-applicable-to-the-drone-authority-debate-2

Andrew Higgins, "Maybe Private Russian Hackers Meddled in Election, Putin Says," New York Times, published June 1, 2017, https://www.nytimes.com/2017/06/01/world/europe/vladimir-putin-donald-trump-hacking.html

Chip Morningstar and F. Randall Farmer, "Cyberspace: First Steps," ed. Michael Benedikt (Cambridge: MIT Press, 1991), 274. https://ia802900.us.archive.org/31/items/CyberspaceFirstSteps/Cyberspace%20First%20Steps%20%281991%29.pdf

Command Vision for US Cyber Command, "Achieve and Maintain Cyberspace Superiority," published April 2018, https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20April%202018.pdf?ver=2018-06-14-152556-010

Council of Economic Advisers, "The Cost of Malicious Cyber Activity to the U.S. Economy," accessed April 29, 2020, https://www.whitehouse.gov/wp-content/uploads/2018/03/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf

Daniel R. Coats, "Director of National Intelligence, Statement for the Record: Worldwide Threat Assessment of the US Intelligence Community," published January 29, 2019. https://www.intelligence.senate.gov/sites/default/files/documents/os-dcoats-012919.pdf

David Schroeder and Travis Howard, Center for International Maritime Security, "Why It Is Time For A U.S. Cyber Force," published August 29, 2018. http://cimsec.org/why-it-is-time-for-a-u-s-cyber-force/37390

Department of Homeland Security, CISA, "Report an Incident," accessed March 4, 2020. https://www.us-cert.gov/forms/report

Donald A. Carter, *The U.S. Army before Vietnam, 1953-1965*, Center of Military History, 2015.

Frederic Lemieux, ed. *Current and Emerging Trends in Cyber Operations: Policy, Strategy and Practice*, (New York: Palgrave Macmillan, 2015) 22-113.

Jacob Morgan, Forbes, "A Simple Explanation Of "The Internet Of Things," published May 13, 2014, https://www.forbes.com/sites/jacobmorgan/2014/05/13/simple-explanation-internet-things-that-anyone-can-understand/#2dbe9ccd1d09

James A. Green, ed. Cyber Warfare, A Multidisciplinary Analysis, London and New York: Routledge, 2015.

Jim Mattis, "Summary of the 2018 National Defense Strategy of The United States of America," 1. accessed November 20, 2018, https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf

John A. Adams, "Cyber Blackout: When the Lights Go Out—Nation at Risk," FriesenPress, 2015.

John Shkor, The Hill, "We weren't ready for a pandemic – imagine a crippling cyberattack," published March 30, 2020, https://thehill.com/opinion/cybersecurity/489660-we-werent-ready-for-a-pandemic-imagine-a-crippling-cyber-attack

Joint Publication 3-08, "Interorganizational Cooperation," validated October 18, 2017, xiii-xv, https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_08pa.pdf?ver=2018-02-08-091414-467

Joint Publication 3-12, "Cyberspace Operations", GL-4, published June 8, 2018, https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf

Lee Mathews, Forbes, "North Korean Hackers Have Raked in $670 Million Via Cyberattacks," published March 11, 2019, https://www.forbes.com/sites/leemathews/2019/03/11/north-korean-hackers-have-raked-in-670-million-via-cyberattacks/#4d66e5597018

Lori Grisham, USA Today, "Timeline: North Korea and the Sony Picture hack," published December 18, 2014, https://www.usatoday.com/story/news/nation-now/2014/12/18/sony-hack-timeline-interview-north-korea/20601645/

Macrotrends, "U.S. Military Spending/Defense Budget 1960-2020," accessed April 29, 2020, https://www.macrotrends.net/countries/USA/united-states/military-spending-defense-budget

Michael E. DeVine, "Covert Action and Clandestine Activities of the Intelligence Community: Selected Definitions in Brief," Congressional Research Service, (June 2019). https://fas.org/sgp/crs/intel/R45175.pdf

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

Richard Stengel, Vanity Fair, "The Untold Story of the Sony Hack: How North Korea's Battle with Seth Rogen and George Clooney Foreshadowed Russian Election Meddling in 2016," published October 6, 2019, https://www.vanityfair.com/news/2019/10/the-untold-story-of-the-sony-hack

Senator Angus King and Representative Mike Gallagher, Cyberspace Solarium Commision, "CSC Final Report," published March 2020. https://drive.google.com/file/d/1ryMCIL_dZ30QyjFqFkkf10MxIXJGT4yv/view

Statista, “United States: number of internet users 2000-2019,” accessed January 17, 2020, https://www.statista.com/statistics/276445/number-of-internet-users-in-the-united-states/

Steve Morgan, Cybercrime Magazine, “Cybersecurity Talent Crunch to Create 3.5 Million Unfilled Jobs Globally By 2021.” published October 24, 2019. https://cybersecurityventures.com/jobs/

U.S. Department of Defense, *2018 Cyber Strategy*. Washington DC: Department of Defense, 2018. https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF

U.S. Department of Defense, “DOD Releases Fiscal Year 2021 Budget Proposal,” published February 10, 2020. https://www.defense.gov/Newsroom/Releases/Release/Article/2079489/dod-releases-fiscal-year-2021-budget-proposal/

U.S. Department of Education, Office of Career, Technical, and Adult Eductions, “New Cybersecutiry Education Funding Opportunity,” accessed April 25, 2020. https://sites.ed.gov/octae/2016/05/12/new-cybersecurity-education-funding-opportunity/

U.S. Department of Education, Pilot Program from Cybersecurity Education Technological Upgrades for Community Colleges, “Program Description,” accessed April 25, 2020. https://www2.ed.gov/programs/ppcetucc/index.html

U.S. Department of Homeland Security, CISA, “Critical Infrastructure Sectors,” accessed February 19, 2020. https://www.cisa.gov/critical-infrastructure-sectors

U.S. Department of Homeland Security, “Cybersecurity,” accessed February 19, 2020, https://www.dhs.gov/topic/cybersecurity

U.S. Government Accountability Office, *Defense Department Cyber Efforts: DOD Faces Challenges In Its Cyber Activities.* Washington DC: Government Accountiblity Office, July 2011. https://www.gao.gov/assets/330/321818.pdf

Wall, Andru E., “Demystifying the Title 10-Title 50 Debate: Distingushing Miltiary Operations, Intelligence Activity & Covert Action,” Harvard National Security Journal Vol. 3 (2011), https://www.soc.mil/528th/PDFs/Title10Title50.pdf

White House, “The Cost of Malicious Cyber Activity to the U.S. Economy,” published February 2018, https://www.whitehouse.gov/wp-content/uploads/2018/03/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf

World Population Review, “United States Population,” accessed January 17, 2020, http://worldpopulationreview.com/countries/united-states-population/