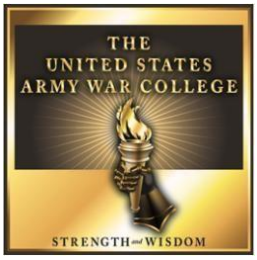
Strategy Research Project

The Role of Cyber as an Instrument of Power

by

Lieutenant Colonel Anne-Marie R. Wiersgalla
United States Army

Under the Direction of:
Dr. Marybeth P. Ulrich



United States Army War College
Class of 2018

REPORT DOCUMENTATION PAGE

Form Approved--OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From - To)*
01-04-2018	STRATEGY RESEARCH PROJECT	

4. TITLE AND SUBTITLE
The Role of Cyber as an Instrument of Power

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Lieutenant Colonel Anne-Marie R. Wiersgalla
United States Army

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Dr. Marybeth P. Ulrich

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
U.S. Army War College, 122 Forbes Avenue, Carlisle, PA 17013

10. SPONSOR/MONITOR'S ACRONYM(S)

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

12. DISTRIBUTION / AVAILABILITY STATEMENT
Distribution A: Approved for Public Release. Distribution is Unlimited.
I understand this document will be included in a research database and available to the public. Author: ☒

13. SUPPLEMENTARY NOTES
Word Count: 7063

14. ABSTRACT

Cyberspace is a hyper-integrated borderless domain upon which the United States relies on for everything from providing the basic elements of life to its citizens to ensuring free trade and global commerce. The United States should develop a comprehensive whole of government cyberspace policy not only to elevate cyber power to a recognized instrument of national power, but also to establish a national-level cyber organization to develop and apply a cogent, synchronized cyber strategy to take the lead in safeguarding the cyber commons. This comprehensive approach is necessary in order to align and synchronize government efforts and to secure American interests at home and abroad. In the 21st century national and international stability rely on a safe and secure cyber commons. The United States and other nations require freedom of navigation within the cyber domain in order to maintain stability and to project power to secure national interests and maintain national and international order.

15. SUBJECT TERMS
Cyber Policy, Cyber Organization, Cyber Commons, National Interest

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			**19b. TELEPHONE NUMBER** *(w/ area code)*
UU	UU	UU	UU	37	

The Role of Cyber as an Instrument of Power

(7063 words)

Abstract

Cyberspace is a hyper-integrated borderless domain upon which the United States relies on for everything from providing the basic elements of life to its citizens to ensuring free trade and global commerce. The United States should develop a comprehensive whole of government cyberspace policy not only to elevate cyber power to a recognized instrument of national power, but also to establish a national-level cyber organization to develop and apply a cogent, synchronized cyber strategy to take the lead in safeguarding the cyber commons. This comprehensive approach is necessary in order to align and synchronize government efforts and to secure American interests at home and abroad. In the 21st century national and international stability rely on a safe and secure cyber commons. The United States and other nations require freedom of navigation within the cyber domain in order to maintain stability and to project power to secure national interests and maintain national and international order.

The Role of Cyber as an Instrument of Power

An effective strategy is like a symphony performance resulting from the guiding hand of the maestro and the combined efforts of the musicians. The achievement of national interests requires an analogous combination of policy guidance and strategies to combine all the instruments of national power. This paper explores how a more coherent national cyber policy can contribute to the development of effective strategies to better achieve U.S. interests. This paper argues that in the dynamic 21st century environment, where cyberspace permeates nearly every aspect of human existence, the United States should establish a policy to leverage cyberspace in the attainment of national interests. Such a policy would recognize cyber as an instrument of national power, call for the establishment of a single cyber organization within the executive branch, and embrace a U.S. global leadership role for safeguarding the cyber commons.

This paper explores this idea in four parts. First, this paper examines the definitions of cyber, cyberspace, and cyber power, followed by a discussion of the role of cyber power as an instrument of national power. Second, it discusses why a single executive branch organization should lead and integrate cyber activities to attain national interests. Third, it outlines the U.S. role in safeguarding the cyber commons. It concludes with a brief discussion of the application of cyber power in achieving U.S. interests. The purpose of this examination is to generate further discussion and illuminate a more relevant conception of the application of cyber power and cyber strategy (see Figure 1).

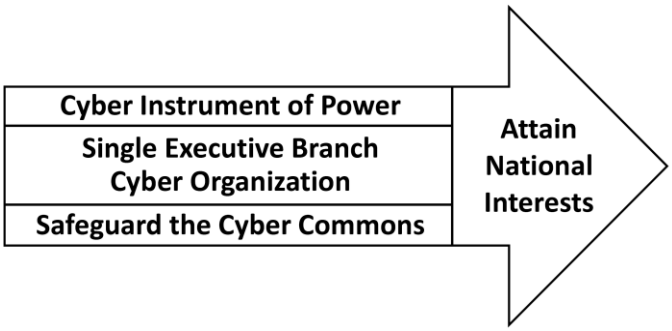


Figure 1. Cyber Lines of Effort

Cyber, Cyberspace, and Cyber Power

To frame the discussion, this paper first defines a few key terms: cyber, cyberspace, and cyber power. Defining these terms helps to develop an understanding of the nuances associated with cyber terminology. A common lexicon contributes to developing a clear conceptualization of cyber and assists with determining how differing conceptions shape the use of cyber at the individual, state, and international level.

What Is Cyber

In the modern age, we hear many words incorporating the terms cyber: cyberspace, cybersecurity, cyber-attack. Fans of "Doctor Who" are even familiar with "Cybermen." But what is cyber and how does the word cyber differ from its use as a modifier in the words listed above? This paper will focus first on defining the terms cyber, cyberspace, and cyber power. The Oxford and Cambridge English Dictionaries have similar but not identical definitions of the term cyber. Using both definitions with slight modifications, this paper defines cyber as all those things involving computers, information technology (IT), virtual reality, and its relating culture.[1] Cyber activities include the physical network, logical network, persona aspects, and cognitive dimension.

Cyberspace

There are many definitions of cyberspace within the international community. These definitions help frame how nations consider cyberspace and therefore has implications for the development of cyber policies and strategies.[2] To help understand the concept of cyberspace, we will look at several definitions from other nations and then discuss how the United States currently defines cyberspace. The United Kingdom defines cyberspace as encompassing "all forms of networked, digital activities; this includes the content of and actions conducted through digital networks."[3] The Canadian definition states that cyberspace is "the electronic world created by interconnected networks of information technology and the information on those networks."[4] *Canada's Cyber Security Strategy* goes on to say, "It is a global commons where more than 1.7 billion people are linked together to exchange ideas, services, and friendship."[5] Australia once preferred the term Internet instead of cyberspace.[6] But in 2016, *Australia's Cyber Security Strategy* transitioned to the term cyberspace.[7]

The United States views cyberspace in a context closely related to its western partners. The 2009 *U.S. Cyberspace Policy Review* identified cyberspace as the "globally-interconnected digital information and communications infrastructure [that] underpins almost every facet of modern society..."[8] Its common use refers to interactions between people, the exchange of information, and virtual environments.[9] The U.S. Department of Defense (DoD) definition of cyberspace draws from the definition in the *U.S. National Security Presidential Directive 54/Homeland Security Presidential Directive 23 (NSPD-54/HSPD23)*[10]. According to *Joint Publication (JP) 1-02, DOD Dictionary of Military and Associated Terms,* cyberspace is "a global domain within the information environment consisting of the interdependent network of

information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers."[11] Although all of these definitions are useful in trying to understand exactly what cyberspace it, each of them has limitations.

China and Russia do not use the term cyber, preferring the term "informationization."[12] This terminology difference indicates the variance in how China and Russia view the man-made artificial domain the west calls cyberspace and how it conceptualizes and employs it. This variance in terminology highlights their focus on "information" and the digital world as a medium to pursue an information advantage vice the more western view of the physical implications of cyberspace.[13] Russia even considers the threat of "information weapons" in some of its strategy documents.

Understanding these views leads us to the realization that cyberspace is more than a domain consisting of objects through which information flows. In the modern age, cyberspace is a pervasive environment that touches almost all aspects of human existence. Cyber activity is the interplay that occurs between the physical and logical components, the individual human being, and the cognitive sphere. It occurs predominantly in cyberspace but cyber activity can achieve effects outside cyberspace. It influences cognitive thought, how individuals and groups evolve, and how and where societies form. It is a digitalized "living organism" in which billions of people work and play.[14] It is also a source of identity, wealth, and power.

Cyber Power

Cyberspace influences all aspects of the environment: individual, societal, geo-political, and geo-economic, and cognitive. In ancient Greece, the politician Themistocles stated: "He who controls the sea controls everything."[15] In the cyber age,

it is arguable, that whoever controls cyberspace, can control the world. Therefore, cyber power is the ability to control cyberspace. In 2009 the U.S. National Defense University (NDU) defined cyber power as “the ability to use cyberspace to create advantages and influence events in the other operational environments and across the instruments of power.”[16] This definition, however, does not consider the implications of creating effects within cyberspace and how that might also garner power. Another definition is that cyber power is the process of converting information into strategic effect.[17] While cyber power does not have a common definition, both cyber power definitions emphasize how the use of cyber power can fulfill the ends of a strategy. It is not simply a medium for asserting power. In a digital world, where more than half of humanity is connected (and the percentage increases every day), the individual, group, or state that can control cyberspace possesses extraordinary power.[18] This power is built through physical and logical networks, perceptions, and intellect. Cyber power can attain national interests through influence, control, and manipulation or through physical, social, and mental destruction. Cyber power is the ability to control cyberspace; more specifically, it is the ability of a nation to secure and safeguard cyberspace, lend confidence to its citizens in the security of that space, and project power through that space.[19] It adds weight to a state’s diplomatic, economic, and military power.[20]

Cyber as an Instrument of National Power

The world has transitioned from the Information Age of the 1970s to the Cyber Age of the 21st century. Within cyberspace, actors may wage wars, destroy infrastructure, and convey messages to achieve an objective. Governments, businesses, transnational actors, and individuals all use cyberspace. It is more than just the medium for utilizing the information instrument of power. Indeed, cyberspace

transcends any one instrument of national power as seen in events such as Stuxnet, WannaCry, not Petya, intellectual property, and identity theft. For example, North Korea is relying increasingly on cyber power and views it as a low-cost and tailored instrument of national power. North Korea is using cyberspace to produce income alongside its desired political, information, economic, and financial outcomes.[21] This pervasive nature of cyberspace and its unique capabilities warrant consideration of cyber power's elevation and recognition as an instrument of national power.[22] A more comprehensive approach would adapt the U.S. instrument of power lexicon mnemonic diplomacy, information, military, and economic to include cyber power as an equal instrument of national power; DIMEC or DIME-FILC.[23] Such a designation would enable its more effective application in achieving national interests.[24]

National Power

According to Joshua Goldstein, "Power is often defined as the ability to get another actor to do what it would not otherwise have done, or not to do what it would have done."[25] Additionally, Karen Mingst offers: "It is the ability to control outcomes that would not have occurred naturally."[26] National power is the sum of all resources available in the pursuit of an outcome and is derived from various "national" elements such as geography, resources, and population as well as "social" elements to include economic, political, military, psychological, and informational. [27] Today both states and non-state actors wield power. However, power exists only in relation to how a state or non-state actor perceives such power. Power also depends on an actor's ability to use such power to influence another actor to bend to its will. The instruments of national power are a construct used to help conceptualize the resources a nation has available

to achieve policy objectives.[28] They assist policy-makers in developing strategies to achieve national interests within the international environment.

The United States, and in particular the U.S. government, generally subscribes to the idea that national power consists of four instruments: diplomacy, information, military, and economics, commonly referred to as DIME.[29] Contemporary U.S. national security policy thinking expanded the instruments of power to include Finance, Intelligence, and Law Enforcement, DIME-FIL.[30] It is the effective integration and employment of these instruments that determines the U.S. ability to achieve national strategic objectives and advance U.S. interests.[31] The military instrument of power can be applied across the land, air, sea, space, and cyberspace domains. These domains are environments through which the United States defends and projects military power.

Currently, cyber power is viewed as a subcomponent of military power, employed at the President's direction. Military power then integrates with other instruments of national power to advance and defend U.S. values, interests, and objectives. This leads to a myopic approach to the application of cyber power through a military lens, as opposed to a more panoptic approach integrating the diverse aspects of cyber power.

Cyber Power and the Instruments of National Power

Unlike land, sea, and air domains where power is applied through military force, the power diffusion and ease of access of achieving effects in the cyber domain extend it beyond a purely militarily application. State and non-state actors are using cyber power as "a low-cost tool of statecraft" to achieve virtual and physical effects that impact finance, commerce, politics, and society, and "to achieve strategic objectives.[32] The multitude of diverse effects contributes to cyber power's influence. Therefore, the magnitude of cyberspace's impact, and by extension cyber power, warrants additional

consideration when discussing national interests and the application of the instruments of national power. This section compares cyber power with the other instruments of national power and contends that cyber power is on par with the military, economic, and diplomatic instruments of national power.

Carl Priechenfried argued that the changing character of conflict warrants the modification of the instruments of power.[33] However, cyberspace is doing more than just changing the character of conflict, it is changing the character of human existence. 21st century communities with limited access to the basic elements of life, such as water, healthcare, and reliable electricity, possess cell phones with internet access. Today, activities in cyberspace produce implications across the geo-political spectrum. The Director of National Intelligence, Daniel R. Coats, testified before Congress that, "adversaries and malign actors will use all instruments of national power—including information and cyber means—to shape societies and markets, international rules and institutions, and international hotspots to their advantage."[34] Cyberspace affects how the United States and other actors conduct diplomacy, exchange information, employ military capabilities, and supports economic activities. These implications require consideration and synchronization when applying each of the instruments of power. (see figure 2).[35]

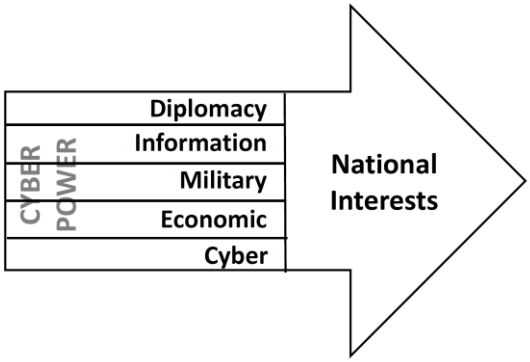


Figure 2. Cyber Is a Standalone Instrument of Power and Buttresses Each Instrument of Power

Cyber and Diplomacy

Diplomacy is "the formation and execution of foreign policy on all levels, the highest as well as the subordinate."[36] The U.S. House of Representatives passed *The Cyber Diplomacy Act of 2017*, which is currently under review by the Senate Committee on Foreign Relations. This Act demonstrates the criticality of cyber activities to the United States. Its designation of an "Office of Cyber Issues" within the Department of State (DOS), responsible for leading diplomatic cyberspace efforts highlights the significant role cyber plays in the international community.[37] This Act calls for a congressionally mandated and Senate-confirmed position as the head of the Department of State Office of Cyber Issues and highlights the prominence cyber activities play in world power politics.[38]

Cyber and the Military

Historically, the basis for a state's power resided in its military strength. Today, however, the interdependencies associated with cyberspace extend its effects beyond solely military applications. This is because the greatest threats in cyberspace span the spectrum of human activity. They are not solely from the military, but also emanate from intelligence services, criminals, and hackers. The threats target not only governments and the military, but business, industry, and individuals as well.[39] Governments should consider these evolving threats, opportunities, and risks when discussing cyber as an instrument of power in a whole of government discussion. The ability of states and non-state actors to hold non-military entities as a "cyber hostage" generates its own unique form of power that can have both physical and psychological effects.

Cyber and Economics.

While hardly mentioned in National Security Strategy (NSS) documents prior to 1987, economic security considerations have gained prominence.[40] This transition to include an economic dimension in U.S. National Security Strategy recognized the changed perceptions of national power over time. Increasing economic interdependence led to the importance of economics as an instrument of national power. Like American economic well-being, American cyber well-being is similarly important. In the modern world, cyberspace underpins the economy and economic well-being. This is particularly the case as individuals, non-state actors, and even some states are transitioning to economies that are reliant on cyberspace. Therefore, cyber power, like a strong domestic economy, can produce soft-power within international politics.

Cyber and Information

Of the four, information is the instrument of national power that has most recently come to the fore.[41] Its addition to the national security lexicon demonstrates how the instrument of power model changed with the advent of the Information Age. Its inclusion highlighted the reliance on technology in employing the nation's security strategy to achieve U.S. interests. While there is no universal definition of the information instrument of national power Drs. Dan Kuehl and Bob Nielson describe the information instrument as: "Use of information content and technology as strategic instruments to shape fundamental political, economic, military, and cultural forces on a long-term basis to affect the global behavior of governments, supra-governmental organizations, and societies to support national security."[42]

The DOD JP 1 discussion on the “informational” instrument of national power focuses predominantly on written and spoken messages, and images that communicate DOD intent.[43] However, neither definition reflects the current significance cyberspace plays in daily life or its criticality in the modern age to current human existence. Both definitions reflect a time when information technology was predominantly a medium for the transmission of messages. While the information instrument of power operates in cyberspace, cyber power is not synonymous with the information instrument of power.

The information instrument is ultimately about the conveyance of thoughts and ideas and the ability to influence a person or group of persons. Like Diplomacy, the information instrument may be a source of soft-power. According to political scientist Joseph S. Nye, soft power is the ability to achieve preferred outcomes through co-optive means such as persuasion and attraction.[44] Conversely, hard power uses coercion and payment to attain desired outcomes.[45] Cyber power can result in either soft power or hard power.

As soft power, cyber power extends beyond the information instrument of power and its use of words and ideas to convey messages. Cyber power influences not only what we think but encroaches into how we think and the way we associate our individual identities and social constructs. Cyberspace may even be changing the structure of the human brain.[46] This makes the potential application of cyber power even more significant. The reliance on digital devices and connections, both physical and virtual, is transforming society. Individuals are becoming dependent and even addicted to the digital world. Cyber power may also be wielded as hard power.

As hard power, cyber power manifests through the manipulation, denial, or destruction of physical devices or logical code creating an effect inside or outside the cyber domain.[47] One example of the application of cyber power as hard power would be undermining trust in financial markets. Contemporary financial markets require trust in the integrity of its networked systems. If an actor weakens that trust by casting doubt on the integrity of these systems, this could cause disruption in market operations. The result would be severe financial impacts leading to an economic crisis and public panic.

The Nature of Power in Cyberspace

Power is what people believe it is. The reputation for power, in other words, confers power on a nation-state regardless of whether that power is real or not.[48] The nature of power in cyberspace derives from its physical, virtual, and cognitive aspects.[49] Understanding this nature of cyber power is critical to understanding how to apply it. Cyberspace has sociological, cultural, economic, and political aspects. These profound attributes of the nature of cyber power show that cyber power is more than the application of offensive and defensive capabilities by the military. As the NDU definition states, cyber can be about influencing behavior, but this influence extends beyond the DIME instruments of power. It is also about affecting, both physically and virtually, an environment so pervasive that it crosses territorial boundaries and creates and maintains its own societies.

Cyber is a virtual world that extends beyond the borders of sovereign nation-states, where individuals and groups create their own unique social groups and identities. Cyberspace creates a world unto itself, where individuals live, virtual societies develop, and those who can control this virtual world yield power. Cyberspace is indeed

pervasive, and to apply cyber power requires an understanding of the nature of power within it.

Tim Jordan describes the nature of power in cyberspace as three intertwined levels: individual, social, and societal, each infused by a different type of power.[50] While his view is very constructivist in nature, his ideas on the nature of power in cyberspace assist in understanding the application of cyber power and its recognition as an instrument of national power.

Jordan notes, first, that cyberspace is an individual tool. When considered as such, cyber power appears as an individual possession, which then gives rise to issues such as cyber-politics, privacy, encryption, and censorship. Second, he identifies cyberspace as a social place, where communities exist. This is where cyber power manifests as a technopower; those who can control and manipulate cyberspace and its virtual world and technologies have greater freedom of action.

Regarding this form of cyber power, Jordan states that while cyberspace appears to be an empowering medium to the individual, in reality, it is technologically empowered elites that dominate it. Finally, it is possible to consider cyberspace in terms of a society or digital nation. At that point, cyber power appears to the individual as a means to a virtual life with similar commitments to groups and organizations as one would recognize in the physical world.[51]

The dynamic and pervasive nature of cyberspace and the existence of unique societies within this space, outside of the territorial boundaries of sovereign nations, is an additional justification for its consideration as a separate instrument of power. In the 21st century, he who wields power in cyberspace can very well control both the virtual

and physical worlds. The evolution of the European Union (EU) illustrates how power is contextual. This supranational regional organization developed through the convergence of political and economic influences. The EU now transcends nation-state territorial sovereignty and national psychology. Cyberspace is developing a supranational dimension, as virtual organizations and societies develop and transcend geographic boundaries. Violent extremist organizations are one example of such an entity. Cyberspace is no longer merely a medium for the utilization of the instruments of national power. It is a separate instrument which bears equal consideration when projecting national power to further U.S. interests.

The routine interaction of the instruments of national power is fundamental to U.S. activities in the strategic security environment. The United States Government's (USG) ability to achieve its national strategic objectives depends on employing the instruments of national power in effective combinations and in all possible situations from peace to war. The USG can use the cyber instrument of national power in differing approaches that vary in purpose, size, scale, scope, risk, and intensity. Most cyber activities occur below the threshold of armed conflict. Leaders must consider the employment of cyber power in a complex, interconnected, and global environment across a continuum, ranging from cooperation to competition, to armed conflict. Today the careful integration of cyber power with other instruments of national power is necessary to achieve U.S. objectives. A national-level, executive branch cyber organization can align USG efforts in this regard.

A National Level Cyber Organization

The National Security Council (NSC) plays a key role in the integration of all instruments of national power, facilitating presidential direction, cooperation, and unity

of effort. To accomplish this integration, the USG should establish a national level cyber organization. The organization will interact with the other departments and agencies as well as private industry to develop a mutual understanding of the capabilities, limitations, and consequences of cyber actions and to identify the ways in which cyber capabilities complement the application of the other instruments of national power. Furthermore, this organization would be responsible for the synchronization and integration of all aspects of cyber operations across the whole of government.

There is a case for a single organization responsible for synchronizing cyber operations, developing U.S. cyber strategy, and coordinating cyber efforts across the instruments of national power and with private industry. Currently, the responsibility for cyber operations is distributed across the U.S. government and private industry. With the threat of a cyber Katrina or a cyber Pearl Harbor rising in the wake of the growing capabilities of state and non-state actors, it appears that it is only a matter of time until a catastrophic event significantly affects the United States.[52]

The Current Government Organization

There is currently a myriad of government organizations responsible for conducting cyber activities. This arrangement poses both opportunities and challenges. The DoD, Department of Homeland Security (DHS), intelligence community (IC), Department of Justice (DOJ), and DOS are only some of the government organizations responsible for applying cyber power to achieve national interests. This diffusion of responsibility has the potential to cause friction when attempting to create a unified approach to cyber operations to deal with national security threats. The DoD is responsible for military aspects, such as conducting cyber-attacks. DHS is responsible for the domestic aspect, including protecting critical infrastructure. The Federal Bureau

of Investigation (FBI) is responsible for the law-enforcement aspect along with other federal and state government organizations, and the Department of State is responsible for cyber diplomacy. Both the Under Secretary of Defense for Policy and U.S. Cyber Command (USCYBERCOM) are responsible for aspects of DoD cyber operations. The National Cybersecurity & Communications Integration Center (NCCIC) is responsible for cyber within DHS, and the FBI has its own cyber-crimes division. The DOS had a cyber coordinator, but Secretary Tillerson's redesign eliminated the position. However, congressional legislation could reinstate this capability.[53]

Currently, there is no single entity at the national level responsible for coordinating and synchronizing cyber activities. In contrast, there is a national level terrorism task force, the National Joint Terrorism Task Force (NJTTF) is responsible for coordination of activities to combat terrorism, including oversight of the 104 FBI Joint Terrorism Task Forces around the country and for regionally coordinating local, state, and federal efforts to combat terrorism.[54] There is also an Office of the Director for National Intelligence (ODNI), which is responsible for leading and synchronizing national-level intelligence activities.[55] The White House appointed a Cybersecurity Coordinator beginning in 2009, responsible for the development and implementation of U.S. national and international cybersecurity strategy and policy.[56] However, this position has no prescribed authority over government agencies. With cyber's capacity to essentially shut down the United States, the lack of an authoritative unifying body outside the NSC is concerning. In the 21st century, cyber activities underpin how a nation conducts its daily business at home and abroad. Consequently, the United States

should establish a single national-level organization responsible for cyber activities and the application of cyber power.

A Single Cyber Organization

Cyberspace is vital to the national interest and requires the coordinated application of cyber activities by U.S. government departments and agencies. The United States currently treats cyberspace as a domain for its military instrument of power to use to achieve political objectives in times of conflict or crisis. The Department of Homeland Security focuses on cybersecurity efforts and protecting critical U.S. infrastructure. The intelligence community exploits cyberspace to collect foreign intelligence and the Department of Justice conducts law enforcement activities. These are all accomplished without concerted synchronization.

The events of 9/11 show the potential impact of having multiple organizations and agencies operating independently and without coordination within the national security environment.[57] A review of events leading up to the 9/11 attacks demonstrates the importance of having a single entity responsible for leading, integrating, and synchronizing operations. Consequently, the 9/11 Commission recommended the establishment of the ODNI to synchronize intelligence information and activities across the U.S. government. Similarly, a single authority, with the responsibility and authority for achieving unity of effort in cyber activities, would create efficiencies when dealing with multiple organizations that share responsibilities for cyber activities within the national security environment.

The Necessity of a Single Cyber Organization

While a single executive cyber office with directive authorities associated with it may not be a panacea, it is certainly a step in the right direction. Secretary of State

Tillerson's removal of the cyber coordinator position and the subsequent House Bill mandating the establishment of a DOS Cyber Issues Officer highlights the ramifications of the disconnects regarding cyber activities across the government.[58] A Center for Strategic and International Studies (CSIS) Cyber Policy Task Force report highlights the interdependencies amongst government agencies in attaining national cybersecurity objectives.[59] However, these interdependencies and U.S. interests related to cyberspace extend beyond cybersecurity. They also include diplomacy, economic, and military applications. Hence, the need exists not only for an executive level cybersecurity organization but also for a single national level cyber organization responsible for coordinating all cyber activities.

Securing the Cyber Commons

A theory or framework for understanding cyberspace as a new and unique aspect of the global commons can assist in shaping an approach to develop national level policy. This section discusses some history of the term commons and explores the consideration of cyberspace as a new form of commons.

The Global Commons

The geopolitical theorist Admiral Alfred Thayer Mahan originally identified the term *commons* in his seminal work *The Influence of Sea Power upon History 1660-1783*. Mahan stated, "The first and most obvious light in which the sea presents itself from the political and social point of view is that of a great highway; or better, perhaps, of a wide common, over which men may pass in all directions."[60] Mahan highlighted the benefits gained from these lines of communication and the power projection capabilities a state could secure by dominating seaborne commerce.

As Mahan advocated in 1890, the United States must look outward. Today the United States should recognize the lines of communication that define the 21st century. The security and stability of the United States depend on both access and protection within cyberspace. As a great power, the United States must lead the way in this endeavor. Barry R. Posen stated, "[C]ommand of the commons is the key enabler of the U.S. global power position. It allows the U.S. to exploit more fully other sources of power, including its own economic and military might as well as the economic and military might of its allies."[61]

The United States has long safeguarded American lives and trade abroad and protected access to the global commons. Military power has provided security and prosperity for the nation and has protected the free flow of ideas, commerce, and people around the world. The United States and the global community must have unimpeded and assured access to cyberspace. In this interdependent environment, loss of access would significantly affect the United States and its ability to provide critical resources domestically and globally. Michèle Flournoy, while serving as the Undersecretary of Defense for Policy, recognized the critical importance and increasing challenges associated with the cyberspace domain. She went as far as to state that, "[W]e also see in some cases the rising tensions in the global commons...and we have a strong economic interest and security interest in keeping those global commons open and free from threat."[62]

The Cyber Commons

A variety of practitioners, scholars, governments, and international organizations have recognized the cyber domain as part of the global commons. However, there is ambiguity, debate, and a lack of consensus regarding the inclusion and acceptance of

the cyber domain into the global commons lexicon. Scholarly articles published by such institutions as the Center for a New American Security (CNAS) include cyberspace as part of the global commons.[63] Even the North Atlantic Treaty Organization (NATO) in its *Assured Access to the Global Commons Final Report* identified the global commons as "the 'connective tissue' of the vibrant global economy" and recognized that the global commons comprised four domains: maritime, air, outer space, and cyberspace.[64] Both former U.S. Secretary of Defense Robert Gates and the former Under Secretary of Defense for Policy Michèle Flournoy have echoed this inclusion of cyberspace as part of the global commons.[65]

However, some academics such as Nye contest such a statement. Asserting instead that cyberspace is at best an "imperfect commons" or a "common pool resource."[66] For the purpose of this paper, the term commons refers more closely to the Mahanian view of a "great highway" or "a wide common, over which men may pass in all directions." In the 21st century, cyberspace presents itself politically, economically, and socially as that of a great highway or a common. This is the context in which this paper considers the cyber commons. Not as a common natural resource or common birthright, but as a common man-made space, a modern great highway on which diplomacy, military operations, economic activity, and society depend.

In order to protect U.S. interests at home and abroad, the United States must safeguard and assure access to the cyber commons. As an interlinked domain, cyberspace is critical to the prosperity and security of the United States and its allies. Like the other domains it is vulnerable, but these vulnerabilities are unique. Its ubiquitous nature, which integrates each of the other domains, and influences each of

the other instruments of national power, should give cyber power the status of a separate instrument of power. The ability to protect the cyberspace global commons is paramount to the progress, well-being, and stability of the United States and the international community.

The United States increasingly relies on the cyber commons for its daily activities to provide the basic elements of life to its citizenry such as food, water, and energy. In the 21st century, cyberspace has become the equivalent of the seas of yesteryear. Similar to the seas, it is a space critical to international commerce and communication.[67] Today, securing U.S. interests includes the ability to freely navigate through the cyber commons with the assurance that nefarious actors will not use this shared freedom to do harm to the United States and its citizens.

The U.S. Role in Safeguarding the Cyber Commons

Cyberspace is a complex system of systems that both private industry and governments own and operate inside and outside sovereign state territory. Regardless of ownership, in the 21st century nation-states and their citizenry require access and freedom of navigation in cyberspace for finance, commerce, and the basic elements of life. President Barack Obama proclaimed the digital infrastructure as a "strategic national asset" and stated that "protecting this infrastructure will be a national priority."[68] To assure access the United States must extend its influence beyond its territorial boundaries. As it secures the maritime domain through the projection of naval power and as it secures its interests and allies abroad through U.S. military presence in over 170 countries, so too it must secure cyberspace.[69] In fact, U.S. Defense Secretary Gates recognized the importance of safeguarding this 21st century "global commons"

and identified the responsibility for protecting the cyber commons as a DoD key task in a speech delivered at the Air War College in 2008.[70]

In the 21st century, the security of territory and geographic borders cannot be the United States' only national security concern. U.S. interests are critically dependent on the cyber commons. However, these commons are increasingly at risk and increasingly contested. The United States must not only improve its own security in this domain. It must also lead the international effort in safeguarding the cyber commons. Space and cyberspace domains have significantly less governance than the sea and air domains. Although the 1967 Outer Space Treaty governs the space domain and defines states' rights to access and use space for peaceful purposes, cyberspace lacks such formal governance.[71]

The construct of the cyberspace domain, in which data may reside and transit across multiple sovereign boundaries in an instant, presents challenges requiring concerted international effort to protect it. Cyberspace is the only commonly accessible domain in which the burden of responsibility to provide security falls primarily outside the government. Freedom of action and navigation in cyberspace are further complicated by several factors, including the particularly high level of private ownership of cyber assets. To assist in overcoming these issues requires institutionalized cooperation like that of the sea, air, and space domains.

A strong, defensible cyber infrastructure fosters economic growth, protects U.S. liberties, and advances U.S. national security.[72] However, a strong and defensible cyber infrastructure that does this goes beyond U.S. geographic boundaries. The United States, as mentioned in the 2017 NSS, recognizes the advantages of strong relations

with allies and partners, including within the cyber domain.[73] The United States, in cooperation with its allies and partners, must project power through cyberspace to secure the domain in the interest of protecting U.S. national interests as well as those of its partners and allies.

The Application of Cyber Power

President Obama's 2011 national level cyber strategy took a slightly different approach than President George W. Bush's 2003 strategy. The 2003 document focused on U.S. cybersecurity in the context of defending the homeland and its infrastructure while the 2011 strategy emphasized building international relationships.[74] Since 2003 DoD and DHS have published cyber strategies reflecting their respective areas of responsibility. However, these documents did not take a whole of government approach toward integrating the instruments of national power to secure and safeguard U.S. interests domestically and internationally.

In 2003 *The National Strategy to Secure Cyberspace* discussed international counter-intelligence cooperation in response to cyber-attacks, cyber-crime, and cooperation with industry partners.[75] However, the 2003 strategy lacked discussion on how the United States should leverage and implement cyber power to secure and defend its national interests at home and abroad. The *2011 International Strategy for Cyberspace* alluded to a U.S. leadership role for ensuring a "peaceful and reliable" cyberspace.[76] However, since its publication, the United States has only minimally applied this proposed leadership role.

Cyber Power Applied: Developing a Cyber Strategy

There is no universal definition of strategy. U.S. JP 1-02 defines strategy as a prudent idea or set of ideas for employing the instruments of national power in a

synchronized and integrated fashion to achieve theater and multinational objectives.[77] In an age where everything is or will soon be interconnected, the impact of cyber on strategy demands examination.

Timothy Thomas offers two definitions of cyber strategy. First, cyber strategy can be the application of cyber technology and associated competencies to gain or maintain a relative power advantage and control (both offensive and defensive) in a competitive environment. Second, cyber strategy can be the achievement of cyber advantage and control (both offensive and defensive), based on an analysis of the strategic environment or situational context, through the thoughtful integration of cyber devices and human cognition in accordance with policy and political goals.[78]

While the U.S. 2011 *International Strategy for Cyberspace* addressed the need for capacity building and partnerships, it also re-affirmed a strong military role in cyber activities and cyberspace security.[79] The strong military role annotated in this strategy includes military partnerships in cyberspace security and the protection of U.S. critical infrastructure. The reliance on the military in domestic and international cyberspace activities inhibits the broader development of a comprehensive cyber strategy and the integration of cyber power in a whole of government approach.

The 2015 U.S. NSS states, “Our influence is greatest when we combine all our strategic advantages.”[80] In the 21st century, the ability to apply cyber power is certainly a strategic advantage. The NSS goes on to say that, “[W]e will also leverage a strong and well-regulated economy to promote trade and investment while protecting the international financial system from abuse.”[81] These statements allude to the importance of wielding cyber power in the 21st century. A safe and secure cyberspace environment

underpins the economy, trade, and financial systems. Cyber influences and affects all of a nation's political and social aspects of power.

Applying Cyber Power within the Cyber Commons

Mark D. Young argues that, "The protection of vital U.S. interests in cyberspace requires adjustments to the applications of all aspects of U.S. power."[82] He goes on to state that the United States continues to limit itself based on its adherence to geographic boundaries. Even in the interconnected world of the 21st century geography, sovereignty and territorial boundaries still matter. However, it is important to make special consideration of cyberspace's capacity to transcend territorial limits. Adversaries, in the form of both sovereign nations and criminals, do not adhere to the same constraints of geographic territorial sovereignty in the borderless and ubiquitous cyberspace.

The 2011 *International Strategy for Cyberspace* states the United States will confront cyber challenges while preserving the core principles of fundamental freedom, privacy, and the free flow of information.[83] Power projection and the preservation of American core principles are not mutually exclusive. Creating a national-level organization responsible for simultaneous application through the inter-agency process is an effective way to safeguard cyberspace.

Way Ahead

The United States should consider the far-reaching domestic and international implications of cyber and consider how to integrate and synchronize cyber across the instruments of power. The best approach to address cyber at its proper level of importance in the global strategic dynamic is to elevate it to its rightful position as an instrument of national power. It is important not to subordinate cyber activities to the

military instrument of power but consider instead its ubiquitous influence. Cyberspace is more than a tool used for diplomatic, information, military, or economic purposes. Cyber activities inform and shapes the development and application of a nation's diplomacy, information, military, and economics. The U.S. Government should create an organization under the executive branch responsible for the development of the nation's overarching cyber strategy, integrate cyber power with the other instruments of national power, and coordinate executive branch organizations to successfully implement that strategy. Furthermore, the President should consider appointing the chief of this new organization as an NSC permanent member instead of having a cyber policy advisor and coordinator. This cyber director would be responsible for assessing and conveying the application and implications of cyber on domestic and international issues, integrating the cyber instrument of power within the inter-agency community, and carrying out cyber policy initiatives. Finally, the United States should take the international lead in safeguarding the cyber commons.

Conclusion

This paper has attempted to make clear the benefits to a broader U.S. conception of cyber power and its subsequent application. To prevail in the modern complex security environment, the United States requires comprehensive cyberspace policies, strategy, and capacity to ensure access, project power, and defend against emerging threats. Cyber power is more than deterrence and reaches beyond the DIME conception of instruments of power. Cyber responsibilities exceed the application and implications of cyber security and cyber defense. To properly apply cyber power and secure the cyber commons, the United States must elevate the status of cyber power from a subordinated instrument under the military instrument. The United States must

synchronize and hone all activities with a cyber mindset to successfully ensure its interests. This requires a national level, whole of government approach.

With the advent of cyberspace, a ubiquitous domain touching and encapsulating the lives of over half of humanity with growing influence every day, the United States must re-evaluate the current construct used to implement national policy and strategy in pursuit of national interests. Cyberspace is more than a domain that must be either defended or exploited to achieve a physical effect. To ensure the U.S. position in the international system and guarantee attainment of U.S. interests in the cyber age, a discussion of the role cyber plays in U.S. national strategy and in achieving national interests is necessary. Based on the magnitude of its influence, the United States should re-evaluate its current thoughts and methods toward cyber. This paper proposed a 3-pronged approach based on the premise that in the current age cyber influences all aspects of the environment: individual, societal, geo-political and geo-economic, even human cognition (e.g. what and how we think). Therefore, in the dynamic 21st century where cyber activity permeates nearly every aspect of human existence, the United States should establish an approach to better leverage cyber in the attainment of national interests. To do this the United States should recognize cyber as an instrument of national power, establish a single organization within the executive branch responsible for cyber, and take the international lead in safeguarding the cyber commons.

Endnotes

[1] The dictionary definitions of the word cyber are: “relating to or characteristic of the culture of computers, IT, and virtual reality,” *Oxford English Dictionary Online*, https://en.oxforddictionaries.com/definition/cyber (accessed February 17, 2018) and “involving,

using, or relating to computers, especially the internet," *Cambridge Dictionary Online*, https://dictionary.cambridge.org/us/dictionary/english/cyber (accessed February 17, 2018).

[2] David J. Betz & Tim Stevens, "Chapter One: Power and Cyberspace", *Cyberspace and the State: Toward a Strategy for Cyber-Power Online*, Adelphi Series 51, no. 424 (2011): 36, https://www.tandfonline.com/doi/full/10.1080/19445571.2011.636954, in Taylor & Francis Online (accessed December 26, 2017).

[3] Cabinet Office, *Cyber Security Strategy of the United Kingdom: Safety, Security and Resilience in Cyber Space* (Norwich: The Stationery Office, 2009), 7, http://webarchive.nationalarchives.gov.uk/+/http:/www.cabinetoffice.gov.uk/media/216620/css0906.pdf (accessed March 4, 2018).

[4] Public Safety Canada, *Canada's Cyber Security Strategy: For a Stronger and More Prosperous Canada* (Ottawa: Government of Canada Publications, 2010), 2, https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cbr-scrt-strtgy/cbr-scrt-strtgy-eng.pdf (accessed March 4, 2018).

[5] Ibid.

[6] Attorney-General's Department, *Cyber Security Strategy* (Canberra: Commonwealth of Australia, 2009) https://www.ag.gov.au/RightsAndProtections/CyberSecurity/Documents/AG%20Cyber%20Security%20Strategy%20-%20for%20website.pdf (accessed March 4, 2018).

[7] Commonwealth of Australia, Department of the Prime Minister and Cabinet, *Australia's Cyber Security Strategy: Enabling Innovation, Growth & Prosperity* (Canberra: Commonwealth of Australia, 2016) https://cybersecuritystrategy.pmc.gov.au/assets/img/PMC-Cyber-Strategy.pdf (accessed March 4, 2018).

[8] White House, *United States Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure* (Washington, DC: The White House, May 29, 2009), iii, https://www.dhs.gov/sites/default/files/publications/Cyberspace_Policy_Review_final_0.pdf (accessed January 7, 2018).

[9] Ibid, 1.

[10] The U.S. *National Security Presidential Directive 54/Homeland Security Presidential Directive 23* defines cyberspace as, "the interdependent network of information technology infrastructures, and includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers in critical industries." See George W. Bush, *National Security Presidential Directive 54/Homeland Security Presidential Directive 23 (NSPD-54/HSPD-23)* (Washington, DC: The White House, January 8, 2008), 3, https://fas.org/irp/offdocs/nspd/nspd-54.pdf (accessed November 26, 2017).

[11] U.S. Joint Chiefs of Staff, *DoD Dictionary of Military and Associated Terms*, Joint Publication 1-02 (Washington, DC: U.S. Joint Chiefs of Staff, August, 2017), 58, http://www.dtic.mil/doctrine/new_pubs/dictionary.pdf (accessed November 26, 2017).

[12] Timothy L. Thomas, "Nation-State Cyber Strategies: Examples from China and Russia," in *Cyberpower and National Security*, ed. Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz (Washington, DC: National Defense University (NDU) Press and Potomac Books, 2009), 465.

[13] Ibid.

[14] George Dyson, "A Universe of Self-Replicating Code," *Edge*, March 26, 2012, https://www.edge.org/conversation/george_dyson-a-universe-of-self-replicating-code (accessed February 18, 2018).

[15] *Australian Defence Magazine Online* (January 10, 2008): http://www.australiandefence.com.au/CE98DE40-F806-11DD-8DFE0050568C22C9 (accessed March 21, 2018).

[16] Dr. Stuart H. Starr, "Towards an Evolving Theory of Cyberpower," in *Cyberpower and National Security*, ed. Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz (Washington, DC: National Defense University (NDU) Press and Potomac Books, 2009), 5.

[17] John B. Sheldon, "The Rise of Cyberpower" in *Strategy in the Contemporary World*, 4th ed., eds. John Baylis, James J. Wirtz, and Colin S. Gray (Oxford, UK: Oxford University Press, 2013), 306.

[18] International Telecommunication Union, *ICT Facts and Figures 2016* (Geneva, Switzerland: International Telecommunications Union, June 2016), 1, (https://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2016.pdf (accessed February 19, 2018).

[19] Sheldon, "The Rise of Cyberpower," 306-311; Daniel T Kuehl, "From Cyberspace to Cyberpower: Defining the Problem," in *Cyberpower and National Security*, ed. Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz (Washington, DC: National Defense University (NDU) Press and Potomac Books, 2009), 37-40.

[20] Steven H. McPherson and Glenn Zimmerman, "Cyberspace Control," in *Securing Freedom in the Global Commons*, ed. Scott Jasper (Stanford, CA: Stanford University Press, 2010), 83-85.

[21] David E. Sanger, David D. Kirkpatrick, and Nicole Perlroth, "The World Once Laughed at North Korean Cyberpower. No More," *The New York Times Online* (October 15, 2017): https://www.nytimes.com/2017/10/15/world/asia/north-korea-hacking-cyber-sony.html (accessed March 4, 2018).

[22] The following sources describe the pervasiveness of the internet. John Smith, "Here's How Many Internet Users There Are," *Time.com,* May 26, 2015; http://time.com/money/3896219/internet-users-worldwide/ (accessed March 5, 2018); Mary Smith, "Digital in 2018: World's Internet Users Pass the 4 Billion Mark," *Wearesocial.com,* January 30, 2018; https://wearesocial.com/blog/2018/01/global-digital-report-2018 (accessed March 5, 2018); Twitter processes 7TB of data/day, Vinod Maan Akanksha, "A Review on Data Mining with Big Data," in *International Journal of Computer Science Trends and Technology (IJCST)* 5 no. 2 (Mar – Apr 2017): 316, http://www.ijcstjournal.org/volume-5/issue-2/IJCST-V5I2P60.pdf (accessed March 5, 2018); Facebook processes 600TB of data/day; Pamela Vagata, and Kevin Wilfong, "Scaling the Facebook Data Warehouse to 300PB," *Facebook.com,* April 10, 2014, https://code.facebook.com/posts/229861827208629/scaling-the-facebook-data-warehouse-to-300-pb/ (accessed March 5, 2018).

[23] DIME is Diplomacy, Information, Military, and Economics, FIL is Financial, Intelligence, and Law Enforcement; Timothy Thomas, "Creating Cyber Strategists: Escaping the 'DIME' Mnemonic," *Defense Studies Online* 14, no. 4 (August 28, 2014): 370-93, https://www-

tandfonline-com.usawc.idm.oclc.org/doi/abs/10.1080/14702436.2014.952522, in Taylor & Francis Online (accessed December 13, 2017).

[24] This CNAS report identified cyber as an instrument of national power. Elizabeth Rosenberg, et al., *The New Tools of Economic Warfare: Effects and Effectiveness of Contemporary U.S. Financial Sanctions* (Washington, DC: CNAS, April 2016), 20, https://s3.amazonaws.com/files.cnas.org/documents/CNASReport-EconomicWarfare-160408v02.pdf (accessed October 10, 2017).

[25] Joshua S. Goldstein, *International Relations*, 2nd ed., (New York: Harper Collins Publishers, Inc., 1986), 53; For more on power as influence, see Robert A. Dahl, *Modern Political Analysis*, 3rd ed. (Englewood Cliffs, NJ: Prentice Hall, 1976), 30-31.

[26] Karen A. Mingst, *Essentials of International Relations*, 3rd ed. (New York: W.W. Norton & Company, 2004), 108.

[27] David Jablonsky, "National Power," *Parameters* 27, no. 1 (Spring, 1997): 34-54, in ProQuest (accessed July 12, 2017).

[28] Robert H. Dorff, "A Primer in Strategy Development", in *The U.S. Army War College Guide to Strategy* (Carlisle Barracks, PA: Strategic Studies Institute, 2001), 12, https://ssi.armywarcollege.edu/pdffiles/PUB362.pdf (accessed November 26, 2017).

[29] Joint Publication 1, *Doctrine for the Armed Forces of the United States* further explains these instruments.; U.S. Joint Chiefs of Staff, *Doctrine for the Armed Forces of the United States*, Joint Publication 1 (Washington, DC: U.S. Joint Chiefs of Staff, March 25, 2013, Incorporating Change 1 12 July 2017), I-11 – I-14, http://www.dtic.mil/doctrine/new_pubs/jp1_ch1.pdf (accessed November 26, 2017).

[30] The White House, *National Strategy for Combating Terrorism* (Washington, DC: The White House, February 2003), 1, https://www.cia.gov/news-information/cia-the-war-on-terrorism/Counter_Terrorism_Strategy.pdf (accessed March 4, 2018).

[31] U.S. Joint Chiefs of Staff, *Doctrine for the Armed Forces of the United States*, I-11 – I-14.

[32] For more on how state and non-state actors are conducting operations in cyberspace below the threshold of war that impact individuals, societies, businesses, and governments, see Daniel R. Coats, *Statement for the Record Worldwide Threat Assessment of the U.S. Intelligence Community* (Washington, D.C., February 13, 2018), 5, https://www.dni.gov/files/documents/Newsroom/Testimonies/2018-ATA---Unclassified-SSCI.pdf (accessed March 6, 2018).

[33] Carl Priechenfried's, *Untying Our Hands: Reconsidering Cyber as a Separate Instrument of National Power*, Master's Thesis (Quantico, VA: Joint Forces Staff College, April 21, 2017), www.dtic.mil/dtic/tr/fulltext/u2/1032283.pdf (accessed January, 29 2018).

[34] Daniel R. Coats, *Statement for the Record Worldwide Threat Assessment of the U.S. Intelligence Community*, 4.

[35] See Figure 2 in David Jablonsky, "Why is Strategy Difficult?" in *The U.S. Army War College Guide to National Security Issues, Volume I: Theory of War and Strategy* (Carlisle Barracks, PA: Strategic Studies Institute, 2012), 9.

[36] Hans J. Morgenthau, *Politics Among Nations: The Struggle for Power and Peace*, 6th ed. (New York: McGraw-Hill Publishing Company, 1985), 158.

[37] Cyber Diplomacy Act of 2017, H.R.3776, 115th Congress, (January 18, 2018), https://www.congress.gov/115/bills/hr3776/BILLS-115hr3776rfs.pdf (accessed February 18, 2018).

[38] Cameron F. Kerry, "Cyber Diplomacy Act Gives Cyber the Importance It Needs at the State Department," *Brookings*, December 4, 2017, https://www.brookings.edu/blog/techtank/2017/12/04/cyber-diplomacy-act-gives-cyber-the-importance-it-needs-at-the-state-department/ (accessed February 18, 2018).

[39] Derek S. Reveron, *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World* (Washington, D.C.: Georgetown University Press, 2012), 3.

[40] Don M. Snider and John A. Nagl, "The National Security Strategy: Documenting Strategic Vision," in *The U.S. Army War College Guide to Strategy* (Carlisle Barracks, PA: Strategic Studies Institute, 2001), 131, http://www.au.af.mil/au/awc/awcgate/ssi/00354.pdf (accessed February 12, 2018).

[41] David Jablonsky, "National Power," in *The U.S. Army War College Guide to Strategy* (Carlisle Barracks, PA: Strategic Studies Institute, 2001), 90, http://www.au.af.mil/au/awc/awcgate/ssi/00354.pdf (accessed February 12, 2018).

[42] Dennis M. Murphy, Jeffrey L. Groh, David J. Smith and Cynthia E. Ayers, eds. *Information as Power: An Anthology of Selected United States Army War College Papers Volume One* (Carlisle Barracks, PA: U.S. Army War College, 2006), vii, http://www.au.af.mil/au/awc/awcgate/army-usawc/info_as_power.pdf (accessed February 19, 2018.

[43] U.S. Joint Chiefs of Staff, *Doctrine for the Armed Forces of the United States*, I-12.

[44] Joseph S. Nye Jr., *The Future of Power* (New York: Public Affairs, 2011), 16.

[45] Ibid.

[46] John Naughton, "The Internet: Is It Changing The Way We Think?," *The Guardian Online* (August 14, 2010): https://www.theguardian.com/technology/2010/aug/15/internet-brain-neuroscience-debate (accessed February 18, 2018).

[47] Nye, *The Future of Power*, 126.

[48] Jablonsky, "National Power," 89.

[49] As research in the integration of automation and biology evolve, the "cognitive domain" may potentially develop into its own domain.

[50] Tim Jordan, “Cyberpower: The Culture and Politics of Cyberspace”, https://www.isoc.org/inet99/proceedings/3i/3i_1.htm#s5 (accessed December 31, 2017).

[51] Ibid.

[52] “The potential for surprise in the cyber realm will increase in the next year and beyond as billions more digital devices are connected—with relatively little built-in security—and both nation states and malign actors become more emboldened and better equipped in the use of increasingly widespread cyber toolkits.,” Daniel R. Coats, *Statement for the Record Worldwide Threat Assessment of the U.S. Intelligence Community*, 5.

[53] Kerry, "Cyber Diplomacy Act Gives Cyber the Importance It Needs at the State Department."

[54] Federal Bureau of Investigation, U.S. Department of Justice, “Joint Terrorism Task Forces,” https://www.fbi.gov/investigate/terrorism/joint-terrorism-task-forces (accessed February 17, 2018).

[55] Office of the Director of National Intelligence, “Who We Are,” https://www.dni.gov/index.php/who-we-are (accessed February 11, 2018).

[56] Federal Business Council, Inc., “Rob Joyce, National Security Council, The White House, Special Assistant to the President, Cybersecurity Coordinator,” https://www.fbcinc.com/e/ias/speakerpopup.aspx?id=Q6UJ9A0135FR (accessed February 18, 2018).

[57] National Commission on Terrorist Attacks upon the United States, *The 9/11 Commission Report: Executive Summary* (Washington, DC: U.S. Government Printing Office, July 22, 2004), 20, http://govinfo.library.unt.edu/911/report/911Report_Exec.pdf (accessed February 12, 2018).

[58] Kerry, "Cyber Diplomacy Act Gives Cyber the Importance It Needs at the State Department."

[59] Center for Strategic and International Studies (CSIS) Cyber Policy Task Force Report *From Awareness to Action: A Cybersecurity Agenda for the 45th President* (Washington, DC: CSIS, January 2017), https://csis-prod.s3.amazonaws.com/s3fs-public/publication/160103_Lewis_CyberRecommendationsNextAdministration_Web.pdf (accessed March 5, 2018).

[60] A.T. Mahan, *The Influence of Sea Power upon History: 1660-1783* (Boston: Little, Brown, 1890), http://www.gutenberg.org/files/13529/13529-h/13529-h.htm (March 4, 2018).

[61] Barry R. Posen, “Command of the Commons: The Military Foundation of U.S. Hegemony,” *International Security Online* 28, no. 1 (2003): 5-46, https://www.belfercenter.org/sites/default/files/files/publication/posen_summer_2003.pdf (accessed February 28, 2018).

[62] Michèle Flournoy, "Rebalancing the Force: Major Issues for Quadrennial Defense Review 2010," *DISAM Journal of International Security Assistance Management Online* 31, no. 3 (November 2009): 95-101, in ProQuest (accessed March 5, 2018).

[63] Cyberspace is referred to as a global commons by U.S. policy makers and in a variety of published works including NATO publications, U.S. government documents, and academic writings.

[64] Maj. Gen. Mark Barrett, Dick Bedford, Elizabeth Skinner, and Eva Vergles, *Assured Access to the Global Commons*, (Norfolk, VA: North Atlantic Treaty Organization, April 2011), http://www.act.nato.int/globalcommons (accessed December 21, 2017).

[65] Michèle Flournoy, "Stability Operations: A Comprehensive Approach to the 21st Century," Comments at the Brookings Institution, Washington, DC, 27 March 2009, https://www.brookings.edu/wp-content/uploads/2012/04/20090327_stability.pdf (accessed March 3, 2018); Robert M. Gates, "Speech to the International Institute for Strategic Studies" Singapore, 31 May 2008, http://archive.defense.gov/Speeches/Speech.aspx?SpeechID=1253, (accessed March 3, 2018); Robert M. Gates, "Speech: International Institute for Strategic Studies," Singapore, 30 May 2009, https://www.iiss.org/en/events/shangri-la-dialogue/archive/shangri-la-dialogue-2009-99ea/first-plenary-session-5080/dr-robert-gates-6609, (accessed March 3, 2018).

[66] Nye, *The Future of Power*, 142-43.

[67] Scott Jasper and Scott Moreland, "Introduction: A Comprehensive Approach" in *Conflict and Cooperation in the Global Commons: A Comprehensive Approach for International Security* (Washington, D.C.: Georgetown University Press, 2012), 1.

[68] Barack Obama, "Remarks by the President on Security Our Nation's Cyber Infrastructure," public speech, The White House, Washington, DC, May 29, 2009, https://obamawhitehouse.archives.gov/the-press-office/remarks-president-securing-our-nations-cyber-infrastructure (accessed February 23, 2018).

[69] Defense Manpower Data Center, "Military and Civilian Personnel by Service/Agency by State/Country," *DOD Personnel, Workforce Reports & Publications,* https://www.dmdc.osd.mil/appj/dwp/dwp_reports.jsp (accessed February 23, 2018).

[70] Robert M. Gates, "Remarks to Air War College," lecture, U.S. Air War College, Maxwell-Gunter Air Force Base, Montgomery, AL, April 21, 2008, http://archive.defense.gov/Speeches/Speech.aspx?SpeechID=1231 (accessed February 18, 2018).

[71] Tara Murphy, "Security Challenges in the 21st Century Global Commons," *Yale Journal of International Affairs Online* (Spring/Summer 2010): 30-31, http://yalejournal.org/wp-content/uploads/2010/09/105205murphy.pdf (accessed December 26, 2017).

[72] Donald J. Trump., *National Security Strategy of the United States of America* (Washington, DC: The White House, December 18, 2017), 13, https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905-2.pdf (accessed December 20, 2017).

[73] Ibid, 2.

[74] George W. Bush, *The National Strategy to Secure Cyberspace*, (Washington, DC: The White House, February 2003), https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf (accessed December 17, 2017).

[75] Ibid.

[76] Barack Obama, *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World* (Washington, DC: The White House, May 2011), 11,

https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/internationalstrategy_cyberspace.pdf (accessed December 17, 2017).

[77] U.S. Joint Chiefs of Staff, *Doctrine for the Armed Forces of the United States*, I-7.

[78] Timothy Thomas, "Creating Cyber Strategists: Escaping the 'DIME' Mnemonic," 370-93.

[79] Obama, *International Strategy for Cyberspace;* The strategy states an inherent right to self-defense and that the U.S. would respond to hostile acts in cyberspace as it would any other threat to the United States, 10-14.

[80] Barack Obama, "Introduction," *National Security Strategy* (Washington, D.C.: The White House, February 2015), 4, https://obamawhitehouse.archives.gov/sites/default/files/docs/2015_national_security_strategy.pdf (accessed June 14, 2017).

[81] Ibid.

[82] Mark D. Young, "National Cyber Doctrine: The Missing Link in the Application of American Cyber Power," *Journal of National Security Law & Policy Online* 4, no. 1 (2010): 173, http://jnslp.com/wp-content/uploads/2010/08/12_Young.pdf (accessed September 19, 2017).

[83] Obama, *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World*, 10-14.