Strategy Research Project

The Cyber Domain: Defining it and Norming Users' Behavior

by

Lieutenant Colonel Joshua Keisler
United States Marine Corps

Under the Direction of:
Colonel Timothy Frantz

United States Army War College
Class of 2016

The views expressed herein are those of the author(s) and do not necessarily reflect the official policy or position of the Department of the Army, Department of Defense, or the U.S. Government. The U.S. Army War College is accredited by the Commission on Higher Education of the Middle States Association of Colleges and Schools, an institutional accrediting agency recognized by the U.S. Secretary of Education and the Council for Higher Education Accreditation.

REPORT DOCUMENTATION PAGE	*Form Approved--OMB No. 0704-0188*

The public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing the burden, to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number. **PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.**

1. REPORT DATE *(DD-MM-YYYY)* 01-04-2016	**2. REPORT TYPE** STRATEGY RESEARCH PROJECT	**3. DATES COVERED** *(From - To)*

4. TITLE AND SUBTITLE The Cyber Domain: Defining it and Norming Users' Behavior	**5a. CONTRACT NUMBER** **5b. GRANT NUMBER** **5c. PROGRAM ELEMENT NUMBER**
6. AUTHOR(S) Lieutenant Colonel Joshua Keisler United States Marine Corps	**5d. PROJECT NUMBER** **5e. TASK NUMBER** **5f. WORK UNIT NUMBER**
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Colonel Timothy Frantz	**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.

Please consider submitting to DTIC for worldwide availability? **YES:** ☒ **or NO:** ☐ **(student check one)**

Project Adviser recommends DTIC submission? **YES:** ☒ **or NO:** ☐ **(PA check one)**

13. SUPPLEMENTARY NOTES

Word Count: 6,249

14. ABSTRACT

The cyber revolution is changing the characteristics of warfare. The land, sea, and air domains each have their own theorists who have attempted to provide the principals of warfare. Cyber does not have its own defining grand theorist, but perhaps it does not need one. Sun Tzu outlined an enduring framework for tactics. Kautilya provided a theory on statecraft. Clausewitz, Jomini, Mahan, Douhet and countless other theorists have provided characteristics of warfare that cross domain boundaries. Cyber does not need its own theorist. Existing theory sufficiently provides principals of warfare within the cyber domain. More so than theory, the cyber domain needs definition and behavioral norms. In order to maintain freedom within cyberspace, while also securing public, commercial, and governmental access, a framework for governance is needed. The U.S. should take an active role in leading the international community in developing a set of cyber norms.

15. SUBJECT TERMS

Behavioral Norms, Cyber Attack, Cyber Definitions, Cyber Theory

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT UU	**b. ABSTRACT** UU	**c. THIS PAGE** UU	UU	30	**19b. TELEPHONE NUMBER** *(w/ area code)*

The Cyber Domain: Defining it and Norming Users' Behavior

(6,249 words)

Abstract

The cyber revolution is changing the characteristics of warfare. The land, sea, and air domains each have their own theorists who have attempted to provide the principals of warfare. Cyber does not have its own defining grand theorist, but perhaps it does not need one. Sun Tzu outlined an enduring framework for tactics. Kautilya provided a theory on statecraft. Clausewitz, Jomini, Mahan, Douhet and countless other theorists have provided characteristics of warfare that cross domain boundaries. Cyber does not need its own theorist. Existing theory sufficiently provides principals of warfare within the cyber domain. More so than theory, the cyber domain needs definition and behavioral norms. In order to maintain freedom within cyberspace, while also securing public, commercial, and governmental access, a framework for governance is needed. The U.S. should take an active role in leading the international community in developing a set of cyber norms.

The Cyber Domain: Defining it and Norming Users' Behavior

In the 1960s, the Department of Defense (DoD) funded the Advanced Research Projects Agency Network (ARPANET), to launch a revolution in technology unlike any other. ARPANET development became the proving ground for cyber theory, which provided a foundation for the Internet. Since its debut in 1989, the internet has revolutionized commerce, communication, military activities, and governance.[1] As the cyber revolution continues to influence the international order, a set of globally accepted behavioral norms is needed to provide rules of the road for cyberspace. Strategic cyber warfare is thus a contest for access, control, use, and manipulation of the opponent's data, along with protection and confident use of one's own data.[2] Cyber warfare presents a complicated challenge, unlike land, sea, and air warfare, in that cyber is not solely a physical domain. Cyber is both physical and virtual. Offensive cyber operations are conducted by a wide range of actors and often covertly. Unlike the physical domains, anonymity is commonplace within cyber operations, making attribution an arduous task. Existing theory regarding land, sea, and air warfare apply across multiple domains. Although strategies may parallel between traditional domains and cyber, behavioral norms do not. This paper will begin with an analysis of classic theory, provide definitions to use as a baseline for understanding cyber, describe applicability of existing theory to the cyber domain, and demonstrate the need for international behavioral norms to protect the free and open nature of cyberspace.

While no fewer than six UN bodies and multiple regional and national fora have sought to build a consensus on Internet behavioral protocols, there has been little progress thus far. The nation has largely chosen not to contribute to this international effort. Instead, the U.S. has independently continued to develop both defensive and offensive capabilities.[3] U.S. leaders must not continue this go-it-alone approach to cyber activities. We can no longer entrust the ongoing stability of this system to the expertise of the private sector. An international cyber code is needed. It should provide agreed upon behavioral norms. Annegret Bendiek, Deputy Head of Research in the German Institute and Security Affairs, has called for a German / U.S. led Liberal Coalition for internet governance.[4] Bendiek proposes that the bilateral group should form a multinational coalition for liberal states that would arrive at a consensus of appropriate behavior to assure the continued free and open use of the Internet. Presently, a group of scholars sponsored by NATO's Cooperative Cyber Defence Centre of Excellence in Tallinn, Estonia are meeting to create a set of cyberspace behavioral norms; these proposed norms will then be subjected to global scrutiny.[5]

Although the issue of cyber operations is a relative newcomer on the global stage, the historical likelihood of nations leveraging new tools and techniques to win wars is undisputable. For over 13,000 years, humans have violently clashed over issues of fear, honor, and interest.[6] Tactics, techniques, and procedures have changed; however, the nature of warfare remains constant today. In 1964, archeologist Fred Werndorf discovered a Nubian grave site (identified as site 117) near the present Sudanese town of Jebah Sahaba. Within the archeological find, 59 bodies and remnants of others were found to be bludgeoned, stabbed, or otherwise killed. Site 17 is widely accepted as the first conclusive proof of warfare between settlements of people.[7] It is unfortunately not the last.

Perhaps Rousseau's theory of man's true nature as a moral and noble being is true. Or perhaps Hobbes' counterargument that man is naturally wicked and violent is correct. Both theorists use the collective singular of “man.” But when two or more humans gather, competing interests change the characteristics of the game: fear, honor, and interest then impact human behavior, often precipitating violent conflict.

Cain brutally murdered his brother Abel with a rock. Since that biblical time, men have used all tools and techniques available to force their will upon others. Sticks and stones of land warfare gave way to spears and swords, which gave way to guns and artillery. The use of primitive boats, with limited functions and capability, have evolved into modern warships. Today, destroyers can deliver munitions to any corner of the world, submarines covertly lurk under the seven seas, and aircraft carriers are equivalent to floating airports. Aircraft too have transformed warfare, bringing another domain into the picture. Balloons, dirigibles, airplanes, and jets have taken the fight to the skies by waging air warfare. Exploration beyond our atmosphere has opened another physical arena for warfare. Fear, honor, and interest have continued to motivate offensive and defensive strategies to be executed by national space programs.

Land, sea, air, and space have all become domains of warfare. They now challenge combatants to operate in an incredibly complex environment. As complicated as it may be to wage offensive operations and defend these physical domains, the advent of cyber warfare, although it has not altered the nature or war, has changed the character of war. Each of the physical domains of warfare have attracted theorists who advise how war should be conducted within their area of interest, yet cyber has not yet attracted its celebrated theorist. Cyber may not need its own theorist.

The cyber domain is different. It is not purely a physical phenomenon like the land, sea, air, and space domains. The cyber domain transcends each of the physical domains. Although it is not omnipresent, it is present and intertwined within each of the land, sea, air, and space domains. Rather than a grand cyber theorist, cyber warfare lacks a universal set of behavioral norms to identify what is and is not acceptable within the domain – and what actions and reactions are warranted when (not if!) those norms are violated.

Theory

Sun Tsu's *Art of War* is the preeminent collection outlining the principles of warfare application. Clausewitz's *On War* describes the enduring phenomenon of war. He and Jomini are regarded as fathers of modern land warfare. Mahan and Corbett are celebrated for their theories on sea warfare. Douhet and Mitchell for theories of air warfare. Cyber does not yet have its dominant theorist. Perhaps it doesn't need one. Cyber is a domain that transcends land, sea, and air, so it cannot be so neatly categorized like the other purely physical domains. Cyber is different. It operates within the land, sea, and air domains, which do not operate, but merely exist. For these reasons, perhaps, cyber must simply be considered different. Acknowledging its transcendent nature, theorists consider its unique characteristics and its potential to influence operations in other domains. Cyber does not change the nature of war; it merely changes the character of warfare that can be conducted in this new domain. Perhaps we need no brilliant cyber theorist. But we do need a set of behavioral norms which will allow for reasonably peaceful exploitation of the domain, for specification of violations of the domain, and for appropriate punishments for inappropriate behavior within the domain.

Chinese General and military strategist, Sun Tzu, lived during the spring and autumn periods of ancient China. The name "Sun Tzu" translates as "Master Sun."

Some scholars contend that Sun Tzu and his associated works were actually compilations collected and written by several strategists. Even so, Master Sun's framework for tactics have shaped warfare for thousands of years. His book, *The Art of War* dates back to the 5th Century B.C. It is widely advocated as a "must read" by each of the U.S. armed services – as well as many fortune 500 companies. It is commonly regarded as the seminal work on military tactics and strategy.

Kautilya's *Arithasthra* was written between 317 – 293 B.C.; it is one of the greatest political works of the ancient world. His theory on statecraft guided India's King, Changragupta, who conquered the Nanda Kings, halted the advances of Alexander the Great's successors, and united most of the subcontinent of the Indian empire. Kautilya was a political realist. He believed every nation seeks to maximize power and self-interest. Although he claimed that moral principles or obligations have little or no influence on actions among nations, he nonetheless advocated new alliances – so long as it was understood the alliance would only remain intact while it was in the best interest of the allied states. Kautilya argued that a leader would betray one's own people if the leader did not assume his friends as well as his enemies would turn on him as soon as it was in their best interest and they had the power to do so.[8] The principles of both of these ancients are applicable and universally relevant throughout the cyber domain.

Since the early 19th century, Clausewitz's *On War* continues to be the classic book on warfare.[9] Its reputation and lasting value resides in the fact it is not so much a guide for the conduct land warfare; rather, it describes the phenomenon that is war. Martin Libicki, senior management scientist with the Rand Corporation aptly notes that, *On War*'s staying power comes from Clausewitz's profound analysis of the role and purpose of military force in the relations among states and his explanation of the relationship between the goals of war and its reality in battle.[10] But, his descriptions of the fog and friction of war on the land can easily be applied to the other domains of war. Furthermore, as with the works of Sun Tzu and Kautilya, Clausewitzian theory has applications beyond classic warfare. Strategic theory advanced in *On War* is taught widely; it applies to many competitive fields, such as business, sports, romance, or in any situation in which two or more parties oppose each other. While sensors and other tools within cyber have the potential to cut through the fog of war, technology and vulnerabilities may also induce friction.

Jomini wrote his deliberations of maneuver theory over 200 years ago, yet he is still recognized as the father of Modern Strategy. One hundred and sixty-five years before DARPANET, he recognized that all strategy is controlled by invariable scientific principles. His principles warrant offensive action of mass forces against weaker enemy forces at some decisive point to achieve a strategic military victory.[11] The same principles apply within the realm of cyber. Of course, methods of warfare and landscapes of battle have evolved since Jomini's time. Just as Jomini's principle of maneuver was valid for land war, it is also valid in the modern realm of cyber.

Jomini's brilliance is most evident within the simplicity of these principles. As Jomini openly admitted, "The principle of maneuvering the mass of an army so as to threaten the 'decisive points' in a theater of war and then to hurl all available forces against a fraction of the enemy force defending those points is very simple."[12] His principle of maneuver has served as guide for many celebrated military leaders. It has been battle tested time and time again; it has contributed to many military victories.

U.S. Joint Operations Publication 3-0 is based on Jomini's principle of maneuver defining maneuver: it advocates, "The employment of forces in the operational area through movement in combination with fires to achieve a position of advantage in respect to the enemy."[13] Although U.S. doctrine affirms the relevance of Jomini's principle, this doctrine uses the words; "forces" and "they" as if alluding to people. Analyzing applicability of Jomini's principle of maneuver within the cyber realm requires an open mind and the de-personalization of these words. The cyber arena is not assessed according to the number of its soldiers or by quantity of its tanks. Within the cyber realm, Jomini's principle would assert that the employment of forces could involve a virus, a denial-of-service attack, a Trojan horse, or some other hack massed against a specific vulnerability in an adversary's information system.[14]

Cyber Definitions

First, when discussing cyber and the cyber domain of warfare it is important to understand there is no clear and accepted definition of what exactly *cyberspace* is, which foreshadows the complexity and difficulty in creating acceptable behavioral norms. NATO's Cooperative Cyber Defence Centre of Excellence lists twenty-one unique definitions for cyberspace. Ironically, one of the twenty-one definitions is provided by the International Organization on Standardization.[15]

Academia commonly defines "Cyberspace" in the following manner:

> a) physical infrastructures and telecommunications devices that allow for the connection of technological and communication system networks, understood in the broadest sense (SCADA devices, smartphones/tablets, computers, servers, etc.);

> b) computer systems (see point a) and the related (sometimes embedded) software that guarantee the domain's basic operational functioning and connectivity;
>
> c) networks between computer systems;
>
> d) networks of networks that connect computer systems (the distinction between networks of networks is mainly organizational);
>
> e) the access nodes of users and intermediaries routing nodes;
>
> f) constituent data (or resident data).
>
> Often in common parlance, and sometimes in commercial language, networks of networks are called internet (with lowercase i), while networks between computers are called intranet. Internet (with a capital I, in journalistic language sometimes called the Net) can be considered a part of the system. A distinctive and constitutive feature of cyberspace is that no central entity exercises control over all the networks that make up this new domain.[16]

Along the same lines, but in an abridged form, the U.S. Government defines Cyberspace as "a global domain within the information environment consisting of interdependent networks of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers."[17] The difficulties in defining cyberspace and lack of consensus across the international community is a primary reason why cyber does not have its own theory like the other domains.

While speaking to an audience at Maryland's National Harbor in April, 2015, Admiral Michael Rogers, commander of U.S. Cyber Command based at Fort George G. Meade Maryland, disclosed that "Cyber is an operational domain, and military leaders are going to have to understand its importance and the opportunities and challenges of operating in the domain."[18] Cyber operations may be understood as those operations that involve "the employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace."[19] Cyber operations constitute a relatively new dimension of warfare. Cyber warfare can be thought of as internet-based conflict involving politically motivated attacks on information and information systems.[20] These definitions, while not universally accepted, are a logical starting point to begin discussing the need for international adoption of behavioral norms within the cyber domain.

In 2011, a group of international experts met in Tallinn, Estonia, to consider how extant international legal norms apply to the cyber domain. The product of their three-year effort is documented in *The Tallinn Manual*.[21] Participating scholars represented over twenty nation members of the North Atlantic Treaty Organization (NATO). However, neither the group nor the manual have been endorsed by either NATO or its member states. The *Tallinn Manual* is based largely on the concept of *jus ad bellum,* the international principles governing state use of force as an instrument of their national policy, and on the concept of *jus ad bello*, international law regulating the conduct of armed conflict.[22]

International Law

Part I of *The Tallinn Manual* qualifies that the object and purpose of the term "international cyber security law" is to capture those aspects of public international law that relate to the hostile use of cyberspace, but are not formally subject to the concept of *jus in bello*. The manual primarily focuses on the concept of *jus ad bellum*. However, it also incorporates such legal concepts as sovereignty, jurisdictions, and state insofar as they relate to applicability of *jus ad bellum* and *jus in bello*.[23]

It is commonly accepted that the general principles of international law apply to cyberspace. Acts of aggression by one state upon another state within the cyber domain are considered the same as aggressive acts within the land, sea, and air domains. A state's right to defend itself from cyber acts of aggression remains as valid as when a state's physical domain is attacked kinetically. Cyber aggression becomes a bit more complicated however, because not all cyberattacks produce a kinetic result. Nor are cyberattacks quickly and easily recognized or readily attributable. In "Wild Wild Web," Ablon and Libicki aptly observe, "A unique aspect of operating in cyberspace is that it is simultaneously nowhere specific yet everywhere."[24]

U.S. Law of War Manual provides examples of types of operations that would and would not be considered cyber operations. Cyber operations include those operations that use computers to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves.[25] Cyber operations would generally not include activities that merely use computers or cyberspace without a primary purpose of achieving objectives or effects in or through cyberspace.[26] Using these criteria, reconnaissance actions (e.g, mapping a network), seizure of supporting positions (e.g., securing access to key network systems or nodes), and pre-emplacement of capabilities or weapons (e.g, implanting cyber access tools or malicious code) could all be considered cyber operations. Likewise, bombarding a network hub or jamming wireless communications would be considered cyberattacks as long as they are kinetic acts occurring outside of cyberspace.[27] Law of War rules apply, regardless of the technology, as the rules are not bound by specific technologies. Cyber operations are akin to other forms of technology used across the land, sea, and air domains when these operations cause effects similar to those caused by traditional uses of force. This would be considered under *jus ad bellum*.[28] Examples of such effect are meltdowns of nuclear plants, dam openings that could flood populated areas, or disabled air traffic control facilities that cause crashes.[29]

Cyber Actors

International Law may apply similarly across each of the warfare domains. However, the fog of war thickens within the cyber domain when the actors' roles are considered. It is fairly simple to identify an enemy tank or infantry battalion as they maneuver deep within friendly territory. Submarines and stealth bombers are by design concealed and employed covertly. They are physical objects whose physical presence can be discerned. Tanks, submarines, and stealth bombers are all very expensive technology to employ. They are generally acquired and employed only by state actors within the military forces. But cyber assets are different. Nation states, hacktivists' organizations, commercial entities, and individuals may all pose a threat within the cyber arena. President Obama clearly asserted the importance of cybersecurity: "America's economic prosperity, national security, and our individual liberties depend on our commitment to securing cyberspace and maintaining an open, interoperable, secure, and reliable internet."[30]

Why it Matters

Achieving global cyber superiority or global cyber control by any organization is no longer technically possible. Instead, the practicable overarching strategic objective should be to dominate one or more of the elements of cyberspace of most importance to the organization at any given time.[31] The successful nation in the cyber domain is the one that can achieve and maintain strategic and tactical dominance in its critical elements of cyberspace when required – similar to Corbett's theory of maritime control.[32]

Strategic cyber warfare is thus a contest for access, control, use, and manipulation of the opponent's data, along with protection and confident use of one's own data.[33] Cyber warfare is more a matter of calculated mitigation and responsive resiliency than a matter of gaining control and maintaining supremacy. The only way to guarantee control or supremacy would be to completely isolate the system from external interfaces such as power, network connectivity, or human interaction. Despite the best of intentions and hardening of a piece of equipment or a system, if that system requires external power, cyber targeting of the power source provides an opportunity for the cyber aggressor to render the item or system useless. As modern societies become more and more dependent on the Internet and networking, the vulnerabilities increase that an adversary can exploit this dependence to disrupt the society. Light bulbs and refrigerators can now be controlled by smart phones, as are doors and locks. Likewise, public utilities such as water treatment facilities, electrical grids, and sanitation stations are all controlled through networks of networks.

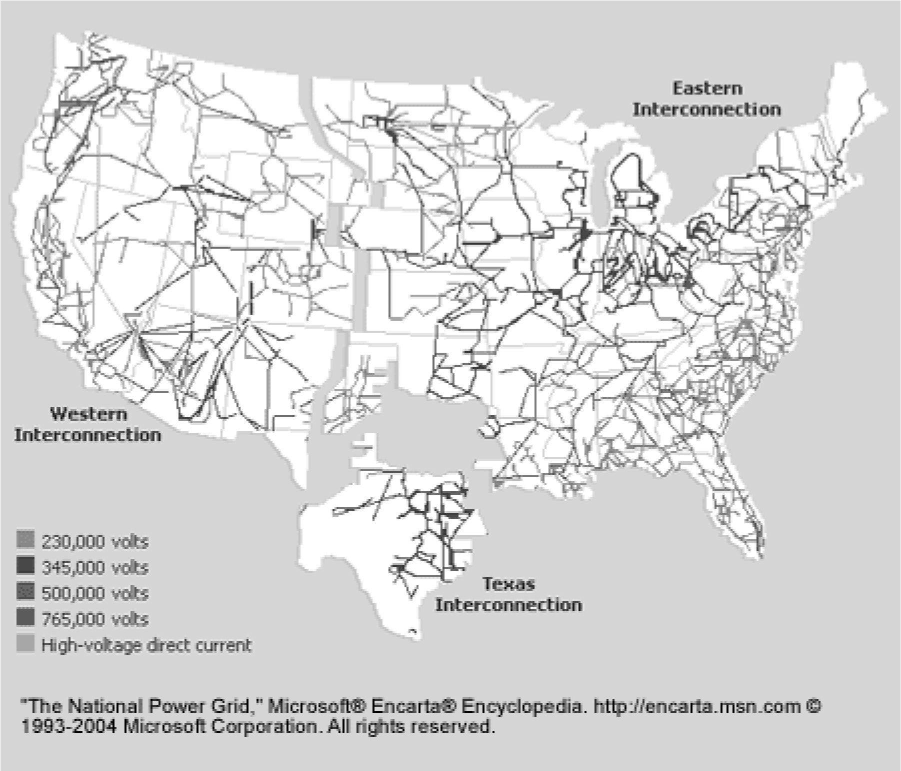
The cyber domain permeates nearly every part of modern existence. It lingers in the broadband networks beneath us and the wireless signals around us; the local networks in our schools, hospitals, and businesses; and the massive grids that power our nation. It serves the classified military and intelligence networks that keep us safe. It facilitates the World Wide Web that has made us more interconnected than at any other time in human history. We must secure our cyberspace to ensure that we can continue to maintain the nation's economy and protect our way of life.[34]

General Keith Alexander, Commander of USCYBERCOM in 2010, outlined three broad areas of cyber threats to the Unites States. First, the threat from hacker activity or exploitation enables cyber intruders to pilfer information from someone else's computer, to exploit financial information, or simply to remove money from an account. Besides putting personal information at risk, intellectual property and classified information are at risk from the same threats. Next, General Alexander cited multiple attacks on nation states in cyberspace, noting "a shift from exploitation to actually using the Internet as a weapons platform to get another country to bend to the will of another country."[35] Lastly, General Alexander forewarned, "the most destructive attacks are coming…those are things that can destroy equipment."[36]

In *American Foreign Policy: Past Present, and Future,* Peter Hastedt addresses cyber war in his "Small Wars" chapter.[37] Although it can be argued that the effects and reach of cyber warfare could be as impactful as any other type of warfare, Hastedt analyzes several specific examples of cyber operations. In 2010, the U.S. (allegedly, as the U.S. never admitted involvement) went on the offensive. Along with Israel, it launched the STUXNET virus attack on Iran's nuclear weapon program. In this case, the U.S. massed its cyber force against Iran's at a decisive point and energetically engaged it at the proper time. Each of Jomini's principles of war were applied: offensive, maneuver, mass decisive points, economy of force, and surprise. Although Hastedt specifically states the U.S. and Israel massed and employed STUXNET offensively against Iran, neither the U.S. nor Israel has ever officially acknowledged their involvement.[38] Within the Cyber realm, adversaries often hide in the shadows and leverage surprise and anonymity.

In November of 2014, National Security Agency (NSA) Director Michael Rogers testified, "Chinese cyber hackers can shut down the power grid in the United States and essentially end life as we know it in America."[39] In attempt to break down the threat in plain English, John McAfee (founder of software security giant McAffee) spoke about the fragility of the electrical grid. McAffee cited, "In the 2013 Infrastructure Report Card, prepared by the American Society of Civil Engineers, our power grid received a near failing grade of D.[40]

Most of the U.S. grid was built prior to the conception of the cyber revolution. The U.S. electrical grid is not one single grid. It is comprised of three smaller grids called interconnects. One grid primarily supports the states east of the Rocky Mountain range, one supports the states west of the Rockies, and smaller interconnect supports Texas. The grids each operate with independent automated controls. In the realm of cyber, Automated controls are prime targets for attack. Under normal operations, the grids support their region, providing power independently. When one grid becomes overloaded, the system is designed to allow support from one of the other grids in order to compensate for the shortfall. This happened during peaked usage periods like during heat waves in the summer months. By design, having three interconnected grids allows the national grid system the ability to provide surge capacity during times of need. The U.S American Recovery Act of 2009 provided the Department of Energy $4.5 Billion to modernize and increase the reliability of the grid.[41]



"The National Power Grid," Microsoft® Encarta® Encyclopedia. http://encarta.msn.com © 1993-2004 Microsoft Corporation. All rights reserved.

Figure 1. National Power Grid[42]

The system is vulnerable to cyberattack. As McAffee assessed, "Purposefully incorrect allocations, strategically sequenced and modulated, would overload subsets of the grid, causing instability and eventual meltdown."[43] McAfee warned, "Weaponized software, strategically inserted into the grid's control centers, would turn our grid into a pile of burned out rubble when activated."[44] The thought may seem farfetched to some. To the Ukrainian government and its people, it sounds frighteningly similar to their winter of 2015. In December 2015, hackers brought down the Ukrainian power grid for a day and half.[45] They did so with a crude piece of weaponized software called "Black Energy."[46] Although the event only lasted a day and a half, Ukrainian winters are harsh and this attack left many without power for heat and other electrically powered life support. The U.S. power grid is susceptible to similar attack. What makes the threat worse is the fact that the Black Energy software used during the attack on

Ukraine's grid pales in comparison to the type of weaponized software the Chinese and Russians possess. Former NSA Chief, General Michael Hayden, called the Ukrainian hack a "sign of darkening skies for America." A cyber war is clearly on the horizon.[47]

The U.S. Energy Department is aware of the threat. Since 2010, the U.S. has invested over $100 Million to enhance resiliency and protect the nation's grid system from cyber vulnerabilities.[48] Protecting the grid requires a not only a whole of government approach, it requires a national commitment. The public and private partners including the Department of Defense, the Department of Homeland Security, the National Institute of Standards and Technology, the intelligence community, private industry and energy-sector stakeholders all have to be involved in order to protect the national grid system from cyber threats.[49]

Darwin's theory of evolution contends that inherent dynamic forces allow only the fittest species or organizations to prosper in a competitive organization or situation.[50] Warfare, similar to any other complex organism or system, mutates and develops in its effort to survive. Combatants grappling in rudimentary hand-to-hand combat evolved to hurl rocks and spears. Advancements in metalwork and chemistry brought swords, rifles, and cannons to the battlefield. As technology has advanced, the face of warfare has evolved. Cyber warfare is the most recent evolution of warfare. Regardless of the technology or battle space, the underlying principles of war remain unchanged.

Behavioral Norms and International Law

Although there is no universally accepted precise definition of cyberspace, there is a need for consensus among the international community regarding acceptable behaviors in the cyber realm. Without acceptable behavioral norms, anything and everything becomes possible and arguably become acceptable. If everything is acceptable, it is logical to infer that cyberspace exists and will continue to exist in a state of anarchy. This is an unacceptable situation given the importance of securing a domain that permeates almost every facet of our modern lives. As the world becomes more advanced and complex, reliance on cyber becomes increasingly important.

Just as in physical / kinetic warfare conducted within the other domains (land, sea, air, & space), international agreements and treaties create limits which are formulated to prevent cruel and unthinkable actions from taking place between nation states. Unfortunately, international law does not have the capability or capacity to prevent cruelty and unthinkable actions at the hands of non-state and rogue actors. Terrorists and other extremists operate outside of the rules. Independent actors will continue to operate independently. By creating a set of cyber space behavioral norms within the international community, our leaders may subject cyberspace to reasonable governance. Then, a union of state actors can act as the regulating force to deter, interdict, and defeat unacceptable acts of aggression.

The term “warfare” has become malleable; it now is applied to many threats to U.S. interests, such as ‘The War on Drugs’ and ‘The War on Terror’. In this same likeness, the US faces a War on Cyber, which cannot be considered analogous to land, sea, or air domains. Cyber is simply different. Cyber aggression threatens not just our military assets; it threatens the nation’s infrastructure, economy, and citizens alike. In the land domain, when one army threatens another, its presence can be seen, heard, and felt. Sea warfare is much the same although submarines operate underwater with as much stealth as possible to mask and protect them. Naval operations are also conducted within the physical realm. Air warfare is the same. Its battles occur in the sky

- fought between aircraft, missiles, and other physical means. Drones are currently widely employed; as they can be operated for extended periods without putting their operators at risk. Although operators sit in control centers from many miles away, drones none the less operate in the physical domain and they are primarily levied against opposition forces. Cyber is different.

There are no “Rules of Engagement” or conventions (like the Geneva Convention) to set sets ground rules for cyber militants. Cyber is like the wild west, outside the reach of law. Cyber was created to operate in an ungoverned space, outside the span of control of any government. The internet is a place for collaboration and sharing, neither of which thrive under regulation by a government body. The premise of a governing body assumes that regulation and monitoring will occur. As long as the internet is intended to be an open space, governance remains a reach too far. What the cyber domain needs is international norms, formulated and agreed upon on the global scale - perhaps within the UN, which is the largest representative body of states. The Tallinn Convention is a good start for this endeavor; however, it is currently endorsed only by the members of the North Atlantic Treaty Organization (NATO).

What Lies Ahead?

In September 2015, Chinese President Xi Jinping and U.S. President Barack Obama shook hands following reaching agreement to restrict offensive cyber operations between the two states.[51] They agreed to refrain from conducting or supporting cyber theft of business secrets. This was a good start, but it also shines a spotlight on the lack of sufficient behavioral norms within the cyber domain. President Obama admitted the agreement was “a work in progress.”[52] One of the areas the President had hoped to tackle during the meetings was a promise not to conduct first strike attacks against the other nation’s critical infrastructure – the power grid, water system, and other national infrastructure should be off limits. “While such an agreement would represent an important first start, it also highlights long-standing shortfalls in U.S. preparedness and response capabilities in cyberspace beginning with a lack of well understood doctrine for cybersecurity.”[53] President Obama’s goals for the meetings were not fully realized; however, he and Premier Xi agreed “the countries would abide by ‘norms of behavior’ in cyberspace.”[54] Reporting on the discussions, Gerstein acknowledged, “Today, no such official doctrine guides international, or for that matter, U.S. cybersecurity policy. No comprehensive framework exists for thinking about cyberspace issues, managing concerns or even responding to crisis. There are no set limitations on potentially destabilizing behavior.”[55]

Agreements between nations are important, but only so far as the agreements are held. Kautilya aptly warned that agreements and alliances will dissolve as soon as one of the states sees an opportunity to improve their position by breaking the agreement. Kautilya was a realist and although his theories were developed long ago, they’ve withstood the tests of time and remain true today. Director of National Intelligence, James Clapper advised the U.S. should take a page from President Reagan’s position regarding nuclear disarmament - “trust but verify” when it comes to curbing Chinese cyberattacks.[56] Almost as soon as Xi departed the U.S., reports of Chinese hacks against U.S. businesses surfaced. Dimitri Alperovitch (cofounder and Chief Technology Officer of CrowdStrike) revealed numerous attacks targeting U.S. tech and pharmaceutical companies.[57] The Chinese attacks reinforced Kautilya’s perspective regarding the usefulness of treaties and alliances. Bilateral agreements are too limited and fragile to tame cyberspace. International norms must come from the international community and states that violate the international framework have to be held accountable. Nuclear Arms and other Weapons of Mass Destruction (WMD) are governed in this manner.[58] The Australia Group for chemical and biological weapons, the Missile Technology Control Regime and the Wassenaar Arrangements demonstrate the influence of multinational treaties addressing complex and dangerous challenges.[59]

As with other wicked or otherwise complicated problems, coalitions of the willing may provide a suitable response to challenges of cyberspace behavior. A follow-on project for the international group of experts after they published the *Tallinn Manual* in 2014 was a second gathering in The Hague. The second meeting sought to shift the scope of the original manual from an academic manual to drafting an international legal framework that could be applied to malevolent cyber operations.[60] The group began work on the Tallinn Manual 2.0 in February 2016. The product of their meeting is highly anticipated across the international community.

To be clear, cyber defense is not solely a governmental responsibility. Just as the cyber domain now permeates nearly every facet of modern life, cyber defense has an all-encompassing security responsibility. Cyber defense starts with the individual, who must safeguard their personal information and protect end-user devices. Cyber defense is a private sector responsibility; as network service providers and technology companies must accept responsibility to provide safe infrastructure for continued worldwide connectivity. Cyber defense must as well continue to be a whole-of-government effort. Every government agency has a role to play; this is not solely a problem for the Departments of Homeland Security and Defense. To defend the nation, DoD must build partnerships with other agencies of government to prepare to conduct combined cyber operations to deter and if necessary defeat aggression in cyberspace.[61]

The White House is backing its commitment to cyber defense with policy and money. In February 2016, President Obama released his administration's final budget proposal. In a statement highlighting key aspects of the plan, cyber security garnered specific attention: "We have to adapt to this national threat."[62] The President called upon Americans to "do their part to safeguard private and personal accounts"[63] President Obama's Cybersecurity National Action Plan (CNAP) also established a Commission on Enhancing National Cybersecurity. It allocated $3.1 billion to the Information Technology Modernization Fund. It created a new Federal Chief Information Security Officer, and committed investment of over $19 billion for cybersecurity – a 35% increase from previous budgets.[64] The White House has demonstrated cyber security is national concern that warrants focus and resources.

According to conservative estimates, thousands of cyberattacks against our defense systems are launched daily.[65] Since 2006, there have been over 204 significant cyber incidents against government agencies and defense high tech companies, along with economic crimes resulting in losses of more than a million dollars.[66] Most of these attacks can be attributed individual or hacker organizations intent on exploiting cyberspace's easy access to economic exploits. However, true attribution is difficult to pinpoint. Similarly, the actual intent of the attack is difficult to recognize. What is crystal clear is the reality of these attacks effects. In May 2015, the Internal Revenue Service (IRS) was hacked by suspected Russian hackers; resulting losses exceeded $50 million.[67] The month prior, unknown sources disclosed real-time non-public details of the

President's schedule that were hacked via the State Department network. In 2014, a five-year cyber espionage campaign attributed to Russian sources identified preparations for a zero-day attack against NATO, the EU, and the Ukrainian government.[68] Annual estimates indicate that more than $1 trillion is lost as a result of cyberattacks.[69]

Conclusion

Theory is useful to understand the dynamics of the nature and characteristics of operations within the domain; however, the nature of warfare does not change across the land, sea, air, or cyber domains. Cyber operations create seemingly unique challenges, given the newness and openness of cyberspace. Cyber warfare has a low cost of entry, allows actors the cover of anonymity, and extends global and near immediate reach to those who leverage it. The Council on Foreign Relations summarized concerns in global internet governance.

> With over 40 percent of the world's population now online, the Internet has revolutionized the way the world communicates. But with fast evolving technology, a proliferation of actors with access to the Internet, and an absence of international consensus on what should be permissible, the gap between existing world arrangements and the challenges posed by the Internet is in fact widening.[70]

In the past, the U.S. has abstained from participating in international bodies to set cyber governance. To date, the U.S. has developed bilateral agreements with numerous nations and internally focused its efforts on offensive and defensive capabilities.[71] The United Nations Convention on the Law of the Sea (UNCLOS) was written with the purpose of providing international rights and responsibilities pertaining to the world's seas. The U.S. was an active participant in the process. Although the U.S. chose not to become a signatory member, UNCLOS provides a credible set of norms by which the international community may operate peacefully and freely. Technology is extending the cyber domain beyond the physical reach of the land, sea, and air domains.

> International law is not purely a constraint, it frees us and empowers us to do things we could never do without law's legitimacy. If we succeed in promoting a culture of compliance, we will reap the benefits. And if we earn a reputation of compliance, the actions we do take will earn enhanced legitimacy worldwide for their adherence to the rule of law.[72]

As cyber is both physical and virtual, norms are desperately needed to maintain the freedom of the domain. The U.S. cannot afford to pursue an isolationist approach to cyber issues. The U.S. must provide leadership in this endeavor.

Endnotes

[1] Robert K. Knake, *Internet Governance in an Age of Cyber Insecurity,* Council Special Report No. 56 (New York: Council on Foreign Relations, September 2010), http://www.cfr.org/internet -policy/internet-governance-age-cyber-insecurity/p22832 (accessed February 19, 2016).

[2] Martin R. Stytz and Sheila B. Banks, "Toward Attaining Cyber Dominance," *Strategic Studies Quarterly*, Spring 2014, 55.

[3] Ibid.

[4] Annegret Bendiek, "A Liberal Coalition for Internet Governance," April 18, 2014, http://www.cfr.org/councilof councils/global_memos/p32783 (accessed December 19, 2016).

[5] Ibid.

[6] Lawrence H. Keeley, *War Before Civilization: The Myth of the Peaceful Savage* (New York: Oxford University Press, 1996), 36-38.

[7] Ibid.

[8] Roger Boesche and Arthur G. Coons, "Kautilya's Arthasastra on War and Diplomacy in Ancient India," http://www.defencejournal.com/2003/mar/kautilya.htm, (accessed January 18, 2016).

[9] Martin C. Libicki, "Why Cyber War Will Not and Should Not Have Its Grand Strategist," *Strategic Studies Quarterly*, Spring 2014, 24.

[10] Ibid.

[11] Antoine-Henri Jomini, *Tratie' de grandes Operations militarires*, Vol 4., 2nd ed. (Paris: Magimel, 1811), 3I2.

[12] Ibid., 154.

[13] U.S. Joint Chiefs of Staff, *Joint Operations*, Joint Publication 3-0 (Washington, DC: U.S. Joint Chiefs of Staff, August 11, 2011), III-28.

[14] LtCol Joshua Keisler, *Does the Principle of Maneuver Need a Tech Refresh; Jomini's Relevance in a Cyber World*, TWS Student Paper (Carlisle Barracks, PA: U.S. Army War College, October 2, 2016), 3.

[15] NATO Cooperation Cyber Defence Centre of Excellence, "Cyber Definitions," https://ccdcoe.org/cyber-definitions.html (accessed February 20, 2016).

[16] Marco Mayer et al., "How Would You Define Cyber?" May 19, 2014, https://www.academia.edu/7096442/How_would_you_define_cyberspace (accessed January 18, 2016).

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

[18] Jim Garamone, "CYBERCOM Chief Discusses Importance of Cyber Operations," http://www.defense.gov/news-article-view/article/604453/cybercom-chief-discusses-importance-of-cyber-operations (accessed January 6, 2016).

[19] U.S. Joint Chiefs of Staff, *Joint Operations.*

[20] Margaret Rouse, "What is Cyberwarfare?" http://searchsecurity.techtarget.com/definition/cyberwarfare (accessed September 24, 2015).

[21] NATO Cooperation Cyber Defence Centre of Excellence, "Research," https://ccdcoe.org/research.html (accessed December 2, 2015).

[22] Ibid.

[23] Michael N. Schmitt ed., *The Tallinn Manual on the International Law Applicable to Cyber Warfare* (New York: Cambridge University Press, 2013), 1-9.

[24] Lillian Ablon and Martin C. Libicki, "Wild Wild Web; For Not, Cybercrime Has the Upper Hand in Its Duel with the Law," *Rand Review,* Summer 2014, http://www.rand.org/pubs/periodicals/rand-review/issues/2014/summer/wildweb.html (accessed December 2, 2015).

[25] U.S. Department of Defense, *Department of Defense Law of War Manual* (Washington, DC: U.S. Department of Defense, June 12, 2015), 995 – 996.

[26] Ibid.

[27] Ibid., 996.

[28] Ibid., 998.

[29] Harold Hongju Koh, “International Law in Cyberspace,” public speech, USCYBERCOM Inter-Agency Legal Conference, Ft Meade, MD, September 18, 2013, http://www.state.gov/s/l/releases/remarks/197924.htm (accessed April 8, 2016).

[30] The White House, “Foreign Policy: Cyber Security,” https://www.whitehouse.gov/issues/foreign-policy/cybersecurity (accessed February 19, 2016).

[31] Stytz and Banks, “Toward Attaining Cyber Dominance,” 55.

[32] Chris Buckley, “China PLA Officers Call Internet Key Battleground,” *Reuters,* June 3, 2011.

[33] Stytz and Banks, “Toward Attaining Cyber Dominance,” 56.

[34] The White House, “Foreign Policy: Cyber Security.”

[35] U.S. Congress, House of Representatives, Subcommittee on Armed Services, *U.S. Cyber Command: Organizing for Cyberspace Operations,* Testimony given by General Keith Alexander before the House Armed Services Subcommittee, September 23, 2010, https://www.stratcom.mil/speeches/2010/52/House_Armed_Services_Subcommittee_Cyberspace_Operations_Testimony/ (accessed September 24, 2015).

[36] Ibid.

[37] Glenn P. Hastedt, *American Foreign Policy: Past, Present, and Future*, 10th ed. (New York: Rownman & Littlefield, 2015), 357-358.

[38] Ibid.

[39] John McAfee, “We aren’t Talking Enough about Cyber,” *Business Insider,* January 17, 2016, http://www.businessinsider.com/john-mcafee-we-arent-talking-enough-about-cybersecurity-2016-1 (accessed January 18, 2016).

[40] Ibid.

[41] Erin R. Pierce, “Top 9 Things You Didn’t Know about Americas Power Grid,” November 20, 2014, http://energy.gov/articles/top-9-things-you-didnt-know-about-americas-power-grid (accessed January 18, 2016).

[42] Off Grid World, “What is the Electric Power Grid? [U.S. Grid Map],” September 29, 2013, http://www.offgridworld.com/what-is-the-electric-power-grid-u-s-grid-map/ (accessed January 18, 2016).

[43] McAfee, “We aren’t Talking Enough about Cyber.”

[44] Ibid.

[45] Ibid.

[46] Ibid.

[47] Ibid.

[48] Ibid.

[49] Ibid.

[50] Mariam-Webster, “Darwinism,” http://www.merriam-webster.com/dictionary/darwinism (accessed September 24, 2015).

[51] Dan M. Gerstein, “Define Acceptable Cyberspace Behavior,” *The Rand Blog*, blog entry posted September 27, 2015, http://www.rand.org/blog/2015/09/define-acceptable-cyberspace-behavior.html (accessed December 2, 2015).

[52] Ibid.

[53] Ibid.

[54] Ibid.

[55] Ibid.

[56] Andrea Shalal, “Top U.S. Spy Says He’s Skeptical about U.S. – China Cyber Agreement,” *Reuters,* September 30, 2015, http://www.reuters.com/article/us-usa-cybersecurity-idUSKCN0RT1Q820150930 (accessed March 13, 2016).

[57] Ibid.

[58] Ibid.

[59] Gerstein, “Define Acceptable Cyberspace Behavior.”

[60] NATO Cooperative Cyber Defence Centre of Excellence, “Over 50 States Consult Tallinn Manual 2.0,” February 2, 2016, https://ccdcoe.org/over-50-states-consult-tallinn-manual-20.html (accessed March 3, 2016).

[61] U.S. Department of Defense, *Department of Defense Strategy for Operating in Cyberspace* (Washington, DC: U.S. Department of Defense, April 23, 2015), http://www.cfr.org/cybersecurity/department-defense-strategy-operating-cyberspace/p25479 (accessed February 19, 2016).

[62] Michael Daniel, Tony Scott, and Ed Felton, “The President’s National Cybersecurity Plan: What You Need to Know,” blog entry posted February 9, 2016, https://www.whitehouse.gov/blog/2016/02/09/presidents-national-cybersecurity-plan-what-you-need-to-know (accessed February 19, 2016).

[63] Ibid.

[64] Ibid.

[65] Julian Hale, “NATO-backed Project Explores Legal Options to Respond to Cyberattacks,” January 23, 2014, http://www.defensenews.com/article/20140123/defreg04/301230033/nato-backed-project-explores-legal-options-to-respond -to-cyberattacks (accessed December 2, 2015).

[66] Center for Strategic and International Studies, "Significant Cyber Incidents since 2006," December 11, 2015, http://csis.org/files/publication/151211_Significant_Cyber_Events_List.pdf (accessed March 30, 2016).

[67] Ibid.

[68] Ibid.

[69] Robert K. Knake, "Internet Governance in an Age of Cyber Insecurity," http://www/cfr.org/internet -policy/internet-governance-age-cyber-insecurity/p22832 (accessed February 19, 2016).

[70] Council on Foreign Relations, "The Gaps in Global Internet Governance are Growing, According to New CFR Interactive," October 22, 2015, http://www.cfr.org/global-governance/gaps-global-internet-governance-growing-according-to-new-cfr-interactive (accessed February 19, 2016).

[71] Knake, "Internet Governance in an Age of Cyber Insecurity."

[72] Koh, "International Law in Cyberspace."