AIR WAR COLLEGE

AIR UNIVERSITY

A CYBER PEARL HARBOR?

by

Kevin R. Bray, Lt Col, USAF

A Research Report Submitted to the Faculty

In Partial Fulfillment of the Graduation Requirements

Advisor: Group Captain Shaun Harvey

3 February 2017

DISCLAIMER

The views expressed in this academic research paper are those of the author and do not reflect the official policy or position of the US government, the Department of Defense, or Air University.

Biography

Lieutenant Colonel Kevin Bray is assigned to the Air War College, Air University, Maxwell AFB, AL. He has been an air traffic controller since 1990 and is currently an airfield operations officer with operational test and evaluation, Air Staff, Office of the Secretary of Defense for Policy, and technical training experience. He has over 27-years of service in the United States Air Force.

Abstract

An alarmist school of thought that views cyber as a revolutionary innovation changing the nature of war is driving today's public narrative with claims that the United States is losing a "cyber war" or that a "cyber Pearl Harbor" is looming. Without critical analysis or debate and lacking a common lexicon for understanding the threats emanating from cyber, there is a danger for escalation to armed conflict or strategic investment in areas that do too little to mitigate the true threat faced by the United States. A more pragmatic school of thought views cyber as an evolution in technology guided by historical international relations, norms, and strategic logic; and is forming a framework for keys concepts that stand to better inform US policy and strategy in cyber. In proposing a more strategically logical framework upon which to evaluate cyber threats, this paper suggests the United States' focus must be primarily on cyber security.

An aggressor nation or extremist group could use cyber tools to gain control of critical switches…. They could derail passenger trains, or even more dangerous, derail passenger trains loaded with lethal chemicals. They could contaminate the water supply in major cities, or shut down the power grid across large parts of the country…. [a] cyber-Pearl Harbor that would cause physical destruction and the loss of life, an attack that would paralyze and shock the nation and create a profound new sense of vulnerability.[1]

Leon Panetta,
October 11, 2012

Introduction

Sensationalist views that America is losing "the cyber war" during the current "cyber revolution" and faces a looming "cyber Pearl Harbor," are driving today's public narrative on cyber.[2] This alarmist school of thought views cyber as a new revolutionary form of warfare or strategic capability that is changing the nature of war and is molding today's public narrative through inflated threats and fear.[3] Without serious critical analysis or debate; many pundits, military strategists, and statesmen alike have bought in or contributed to the alarmist narrative that all cyber operations are created equal or if the threat can be imagined, it will probably happen.[4] Unfortunately, these senior, influential leaders and pundits are confusing the subject in a manner that may exacerbate international security challenges and delay solutions. As Healey points out; "armed with new cyber capabilities, generals and spymasters may be steering the world toward a much darker cyber future, characterized by unrestrained and unrestrainable attacks."[5] The problem with this alarmist narrative is that it may inhibit the creation of a more accurate, shared, and helpful understanding of cyber that can better inform politics, policy, and strategy. There is an alternative, but less "news worthy" school of thought that views cyber as an incremental evolution in technology and not the game changing revolution in warfare that alarmists and the security industry promise.[6] This more nuanced and pragmatic school views the cyber challenge through the lens of strategic logic and has started a more critical, cross-

functional analysis and debate that shows promise to better inform policy and strategy, while reducing exaggerated fears.

Today's narrative on cyber can be very technical, confusing, and unhelpful for the less cyber-savvy public influencing and national leaders developing policy and national security strategy. As government agencies are increasingly resourced to develop strategies that employ new cyber capabilities and defend against threats, it is important that they understand cyber power well enough to accurately identify the threats, create the right policies, and develop a coherent interagency strategy. Accepting sensationalist claims from the "experts" without rigorous analysis or debate has led to misinformed, strategically poor investments. Investments in the wrong areas can take away from other national security requirements, destabilize fragile international relations, and escalate to unnecessary armed conflict.[7]

Thesis

This research uses a qualitative approach to advance arguments that employ the logic of strategy in order to reduce confusion over the highly technical subject matter and inform more effective and efficient policy and strategy for cyber. The claim of a looming "cyber Pearl Harbor" is underwritten by a concept that cyber represents a revolutionary innovation that has changed or is changing the nature of war and is not consistent with international relations, norms, or strategic logic. This paper's thesis is that there will be no "cyber Pearl Harbor," because the claim is based on inflated threats and fears and an actor that may be capable of such an attack would be restrained by existing international relations and norms. To defend this thesis, working definitions or concepts are developed to establish a common framework that can be used to assess the argument and better understand the threats. With a common framework established, actors in cyberspace are analyzed through the lenses of capability, opportunity, and intent to

conduct a catastrophic, cyber Pearl Harbor-type attack. In closing, an area for strategic focus is provided to mitigate threats identified in analysis and synthesis of the key concepts presented.

Contested Terms and Concepts

To cut through the mystery surrounding cyber threats and to better assess alarmist claims that a "cyber Pearl Harbor" is looming, it is helpful to establish a common framework to evaluate the interrelated concepts of cyber weapons, cyber attack, cyber warfare, and cyber war. The lack of a common lexicon perpetuates misinformation or confusion on the subject and helps bolster disparate alarmist claims. A nuanced and shared understanding of these key concepts will prove helpful in evaluating threats and developing US policy and strategy in cyber.

What are Cyber Weapons?

With the entire mystique surrounding cyber weapons, one should not be surprised by the alarmist rhetoric driving public dialogue. "Few people understand the Internet, and even fewer understand the nature of cyber weapons."[8] Currently, there is no international or US Department of Defense definition for or consensus on the concept of "cyber weapon" and this makes it more difficult to build an adequate, shared understanding of threats.[9] In surveying the literature on cyber, it is clear that the well published technical and tactical capabilities of cyber are contributing to alarmist narratives that tend to exaggerate the threats and predict the looming "cyber Pearl Harbor."[10]

The realities of dealing with cyber incidents and crisis management have forced a growing school of practitioners, strategists, and scholars to approach cyber through the lens of strategic logic. This pragmatic cyber school is providing very useful definitions and concepts that are more congruent with existing international norms and show promise to stabilize the narrative and better inform policy and strategy in cyber. Rid and McBurney provide a pragmatic

framework to help establish what is and is not a cyber weapon. They define weapons as tools used, or designed to be used, in threat or use to cause physical, functional, or mental harm to structures, systems, or living beings.[11] Rid and McBurney remind us that weapons can be used to threaten, defend, to steal, protect, to break and enter, enforce the law, to flee, to destroy things, or to make war.[12]

Further, in developing a concept for cyber weapons, it is helpful to group cyber tools that could be used as weapons along a spectrum from their ability to cause low-potential to high-potential effects. Tools on the low-potential end of the spectrum are reconnaissance tools, scanning tools, or malware.[13] According to Andress and Winterfeld, reconnaissance tools are simply used to gather open source intelligence that could potentially be used for nefarious purposes.[14] Scanning tools are slightly more invasive and are used to find more information on the target environment or systems. These can include network mapping, port scanning, and enumerations tools.[15] Malware can be used to conduct a distributed denial of service (DDoS) that is relatively easy to defend against and highly visible. The disruptions caused by a DDoS are second order effects, such as shutting off website access, and there is no direct damage inflicted by the cyber tool.[16] This paper argues that cyber tools on the low-potential end of the spectrum are not weapons, except when used to damage systems or harm living beings. Codifying all cyber tools as weapons, regardless of user intent or actual use, bolsters alarmist claims that nearly any use can be considered an attack. Where an adversary scans ports, maps networks, and enumerates; alarmists may drive escalation to a kinetic response for these “attacks.” The cyber pragmatist will see these so-called “attacks” for what they are and is less likely to respond disproportionately.

At the opposite and high end of the spectrum, high-potential cyber weapons are like a fire and forget missile. This intelligent code purposely built to attack and inflict damage can autonomously assess the cyber environment it is in and react to achieve the pre-defined effect. The ideal high-potential cyber weapon differs from the low-potential tools in five important ways. First, its objective is to penetrate the system, as opposed to interrupting traffic. Second, it seeks to precisely penetrate a specific system, as opposed to any system with vulnerabilities. Third, the objective is a well defended target, such as a military network or public utilities. Fourth, if employed as a stand-alone attack to damage something, the potential for damage is created by vulnerabilities within the target itself. Finally, it influences ongoing processes in order to achieve a specific objective and not simply shut the system down. The Stuxnet Virus specifically designed to sabotage Iranian nuclear centrifuges is the best known example of a high-potential cyber weapon.[17] Where a high-potential weapon falls on this theoretical spectrum will correlate with how many of these attributes it employs.

What lies between these low-potential tools and high-potential cyber weapons is a large gray area of generic or specific intrusions that can vary in costs and damage. These medium-potential tools are used to access systems, sustain access, and hide access. In the context of cyber attack that will be presented in this paper, these cyber tools become weapons when an actor employs them with intent to open the door for an attack. These medium-potential cyber tools can present the pathway to espionage or attack when weaponized.[18]

It is important to understand that there is a fine line between what is and is not a cyber weapon. Considering cyber weapons are computer codes used to exploit unintentional or planted software, firmware, and/or hardware vulnerabilities; how they are employed and the intended effects play an important role in discriminating between what is and is not a weapon. Intended

use or effects may not be known until after the fact, but remain important in deciding an appropriate response. A cyber intrusion aimed at spying or extracting data will drive different international and domestic responses than a weapon intended to damage or harm. One use may be criminal where the other is an act of war. Using cyber weapons also carries legal responsibilities and requirements for their employment.[19] One can build upon this basic framework for cyber weapons in analyzing the concepts of cyber attack, cyber warfare, and cyber war and build a mental model to more accurately evaluate the alarmist proclaimed "cyber war" threats.

What is a Cyber Attack?

Cyber attack is a contested term or concept that further clouds the public understanding of cyber warfare and cyber war. It is important to build a shared understanding of cyber attack and cyber warfare in order to understand the range and severity of threats posed and to better understand the use of cyber in war. In 2011, the US Department of Defense defined computer network attack as; "actions taken to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computer and networks themselves."[20] This initial definition left significant room for cyber alarmists to confuse the public dialogue on "cyber war" and create fear by loosely codifying any surveillance or penetration of computers or networks as a cyber attack. As Valeriano and Maness suggest, it is unclear what a cyber attack even is, "since it now seems to mean everything from a Twitter hack to a full-scale government operation."[21]

Synthesizing the work of subject matter experts, scholars, legal experts and strategists; cyber pragmatists are building logical frameworks that help to clarify the threats and appear to be influencing policy. In February 2013, the Joint Staff defined offensive cyberspace operations in Joint Publication 3-12 (R), *Cyberspace Operations*, as; "Cyberspace operations intended to

project power by the application of force in or through cyberspace."[22] Offensive cyber operations replaced computer network attack in Joint Publication 1-02, *Department of Defense Dictionary of Military and Associated Terms,* as amended through February 2016.[23] This new definition is congruent with pragmatic thought that cyber is an evolution in technology, because similar to other domains, it does not characterize activities below the use of force as an attack. The old computer network attack doctrine provided some legitimacy to alarmist thought that activities falling below the use of force could be considered an attack. For example, alarmists have considered and continue to consider espionage in or through cyberspace as an attack.[24] One would not consider espionage an attack, or the tools used to conduct this activity weapons, under the new definition for offensive cyberspace operations, because they do not project power by the application of force in or through cyberspace. This doctrinal change from computer network attack to offensive cyberspace operations helps frame the debate between cyber alarmists and pragmatists on what is and what is not an attack or potential act of war. Congruent with the definition for offensive cyberspace operations and international law guiding the use of force, Brown and Tullos had previously developed a helpful framework to help one better understand how cyber operations lie on a spectrum and clearly illustrates that not every ping or Twitter hack is a cyber attack, the state of cyber warfare, or a potential act of war.

Brown and Tullos' framework is based on the foundation of domestic and international law and can help build a better lexicon for thinking about and discussing cyber. Their model places cyber operations on a spectrum that illustrates the differences between cyber operations in terms of level of damage and scale of effect. This framework could be very useful for policy makers, because it helps differentiate legally defined attacks via cyberspace from lesser cyber activities that require different responses.[25] Within this framework, cyber operations range from

virtually undetectable to annoying or destructive and can be divided into three broad categories: access, disruption, and attack.

Access operations provide entry to the adversary computer system in order to facilitate intelligence collection, disruption, or attack. These operations include gaining and maintaining access to the system and could be considered reconnaissance. Access is gained and maintained through social engineering, malware, defeat of security measures, or exploitation of other system vulnerabilities and does not generally affect the system's function or flow of information.[26] These more stealthy operations generally fall on the left end of the spectrum, but can move toward the right as the effects they produce become more pronounced or visible. Port scanning and network mapping would fall on the extreme left, while modifying log files or registries would move to the right. Both would fall short of disruption, because of their limited effects. These normally do not rise to the level of disruption, because they do not prevent normal system functions or deprive the user of access to information. While the access itself is not an act of war as defined by international law, these operations pose a challenge since they can be designed to facilitate espionage or up to and including destruction of the system.[27]

Cyber attack falls on the right end of the spectrum. Before the definition for computer network attack was replaced by a more helpful definition for offensive cyber operations, Brown and Tullos had crafted their own definition more congruent with what we have today in offensive cyber operations. They defined cyber attack as "actions in cyberspace whose foreseeable results include damage or destruction of property, or death or injury to persons."[28] Congruent with the strategic thought of Gray, Rid, McBurney, Valeriano, and Maness; Brown and Tullos adopted a definition that aligns "attack" in the cyber context with the way it is used in other domains.[29] In

doing so, they allow for a more precise analysis of cyber operations under international law and allow for cyber's legal integration into operations.

Within Brown and Tullos' pragmatic framework, most malicious cyber activities occur in the middle of the spectrum; cyber disruption. These include "actions that interrupt the flow of information or the function of information systems without causing physical damage or injury."[30] The greater the effect, the closer it moves toward an attack and the less stealthy it becomes. They importantly note that these cyber disruptions do not reach the level of attack or use of force; but are not always permissible and can violate other laws or standards, such as international agreements or domestic laws.[31] Where a cyber disruption violates the state non-intervention principle that "prohibits coercive or dictatorial actions that deprive a nation of the ability to control governmental matters such as economic, political, military or cultural activities;" it could drive a legally justifiable response that includes the use of force.[32] If a cyber activity does not constitute an act of force or violate this non-intervention restriction, it is generally permissible under international law.[33] The concepts of cyber warfare and cyber war can be further developed with the basic frameworks established for cyber weapons and cyber attack.

What is Cyber Warfare?

There is no governing body amongst nations that codifies the term warfare and its definition is often based on the perspective of the person using it.[34] As defined in Joint Publication 1, *Doctrine for the Armed Forces of the United States*; "warfare is the mechanism, method, or modality of armed conflict against an enemy. It is 'the how' of waging war. Warfare continues to change and be transformed by society, diplomacy, politics, and technology."[35] The cyber alarmist strays from US joint doctrine and international law by including in cyber warfare activities that fall short of the use of force.

Cyber alarmists do not distinguish between a nonviolent cyber activity and one that causes damage or physical harm to an adversary or one that intervenes in the internal affairs of the adversary nation. Their loose definition or concept of cyber warfare, that includes cyber activities below the use of force, does not align with strategic logic or the historical competition between friends and adversaries.[36] For example, states have historically spied on one another and this has not been considered warfare or war. Congruent with international laws on war, there is delineation between an act of espionage and act of war. Advancements in cyber technology do not change this fact. Alarmists are certainly correct that cyber activities below the threshold of intervention, physical harm, or damage can be illegal and present great security threats to nation states. However, characterizing all malicious cyber activity as warfare can result in an unintended escalation to armed conflict. Gray reminds us that; "All political communities understand themselves to be in different political, legal, and moral terrain when they are in a condition of war and are conducting, certainly are in receipt of, acts of warfare – as contrasted with a condition of nonwar."[37] An alarmist public dialogue can politically shape public sentiment and constrain the options of statesmen as the public demands action for the "war" the state is supposedly losing or the "attack" that just occurred – even when there is no physical damage or harm. While alarmists have good intentions, it is more helpful to distinguish between warfare and activities that fall short of warfare in order to better assess the threats, prioritize resources, and develop strategy.

Cyber pragmatists establish the threshold for cyber warfare at the use of force, similar to other domains, and do not view cyber as a revolutionary innovation that has changed the nature of war. Gray teaches us that warfare is the generic activity that occurs in war, such as land, air, sea, space, and cyber warfare.[38] Cyber pragmatists view cyber power as an evolution in

technology different from the other domains with its unique grammar, but not different in its application to the logic of war. Gray reminds us through the teachings of the master, Carl von Clausewitz, that all warfare is about "…shaping, or physically overcoming, the will of the enemy."[39] Congruent with the physical domains, international laws and norms, as well as, strategic logic; the cyber pragmatist separates cyber espionage, cyber terrorism, and cyber crime from cyber warfare.

Synthesizing the frameworks presented thus far and congruent with US joint doctrine, this paper asserts cyber warfare includes those activities that rise to the level of a use of force or attack that does physical damage or harm and includes any activity that violates the non-intervention principle defined in international law. Where cyber power contributes to the multi-domain use of force or as a use of force itself in joint warfighting, it is cyber warfare. Moving forward, the congruent frameworks presented on cyber weapons, cyber attack, and cyber warfare illustrated in figure 1 will help bring more clarity to the concept of cyber war.

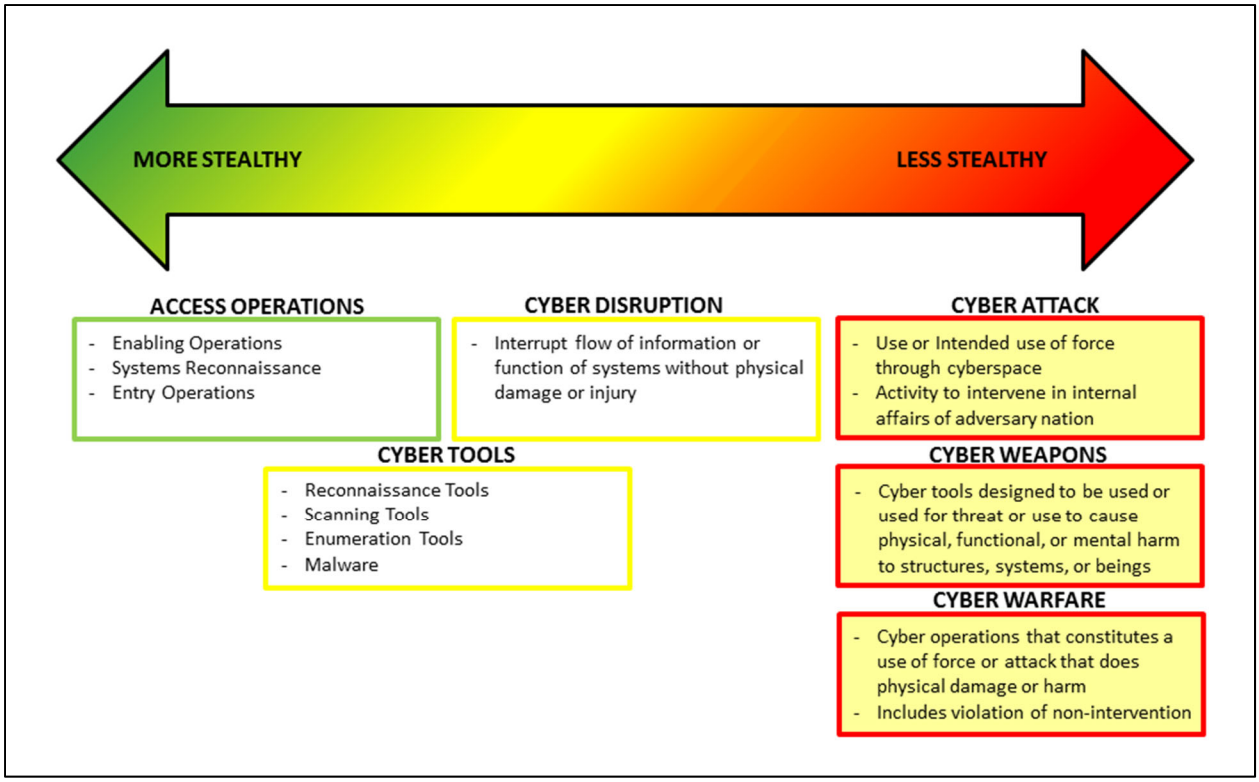

Figure 1. Cyber Operations to Cyber Warfare.[40]
(Adapted from Gary D. Brown and Owen W. Tullous, "On the Spectrum of Cyberspace Operations," *Small Wars Journal*, December 11, 2012.)

What is Cyber War?

Popular narratives from cyber alarmists consider the United States as being in a state of "cyber war" with her adversaries or anticipate a looming "cyber Pearl Harbor."[41] Some cyber alarmists view anything from a Twitter hack to network surveillance as a cyber attack, cyber warfare, and the state of cyber war. Clarke and Knake unhelpfully define cyber war as "actions by a nation-state to penetrate another nation's computers or networks for the purpose of causing damage or disruption."[42] These disparate and confusing narratives do not adequately distinguish between war, crime, terrorism, or espionage. In the physical domains, these are more clearly distinguished and drive different responses guided by domestic and international law. The public narratives on cyber war driven by alarmist claims hamper a state's ability to clearly define these

different threats and craft appropriate responses. If the response does not fit the cyber activity, there is a danger for escalation to armed conflict. As such, it is important to build a common framework and lexicon to assess and discuss the concept of cyber war.

While cyberspace and cyber power will likely continue to change the character of war, war's nature is universal and unchanging.[43] Where cyber alarmists claim the United States is at or losing the "cyber war" today; this paper asserts a cyber war is not likely to ever occur. Cyber power has been and will continue to be used in the context of multi-domain warfare as a key component or enabler, but it is highly unlikely wars will be fought or won solely in cyberspace, as is the case in any other single domain.[44] Before accepting a concept of cyber war beyond its metaphorical use; pundits, politicians, and analysts would be wise to consult the master theorist on war, Carl von Clausewitz. He reminds us, that "war is an act of force to compel our enemy to do our will."[45] Clausewitz specifically points out the fallacy in thought that there may be some ingenious way to defeat an enemy without too much bloodshed or that war will eventually rid itself of the need to use physical fighting forces.[46] Rid reminds us, there have been no cyber attacks in history that meet Clausewitz's criteria that war is violent, instrumental, and political.[47] Implying cyber war can occur in cyberspace alone defies strategic logic and what history has taught us about strategy and war. The concept of cyber war must be understood by policy makers as a metaphor or theory that stands in contrast to reality.[48] This is not to say a state should ignore cyberspace; only that it should develop a coherent national strategy for the private and public sectors to appropriately deal with different types of cyber threats. In synthesizing these concepts, a useable framework emerges and can be used to assess the potential for a catastrophic national cyber emergency described by some as a "cyber Pearl Harbor."

Is a Cyber Pearl Harbor Looming?

A "cyber Pearl Harbor" would be a massive, integrated cyber attack against the United States seeking quick strategic success in hopes to coerce America or limit her ability to fight an upcoming conventional or nuclear fight. While it may be a surprise attack, it will likely be a part of rising geopolitical tensions with an expectation of potential future combat.[49] In order to execute such an attack, the aggressor would have to have the geopolitical intent and capability to conduct such an attack, and America's vulnerabilities in cyberspace would have to be significant enough to enable the attack and provide the opportunity. The capabilities to conduct such a catastrophic attack extend well beyond what a single, or handful of attacks might require. A catastrophic attack would require significant cross-functional intelligence and targeting of many diverse supervisory and control and data acquisitions systems and the ability to sustain the attack as defenses or secondary means to operate these systems are employed.[50]

With a better understanding of what is and is not a cyber attack, cyber warfare, and cyber war, one is able to more clearly view the threat of a "cyber Pearl Harbor" by assessing the capability, opportunity, and intent of different actors in cyberspace. As per the frameworks previously provided, a "cyber Pearl Harbor" would be a significant use of force in or through cyberspace with catastrophic effects and would not include access or disruption operations that do not constitute a use of force. Access and disruptions can certainly be employed in unison with a bona fide cyber attack, just as all could be employed as a part of multi-domain warfare. At the point cyber tools and weapons are used in unison with kinetic attacks, they are simply the use of technology in terrorism or warfare. Potential adversaries in the cyber domain include; hacktivists, criminals, terrorists, and states. It is extremely important to understand the threat in order to defend against it and make better informed strategic national security investments. To

better understand the threat, each potential adversary will be analyzed based on capability, opportunity, and intent. This analysis will begin with hacktivists and follow with criminal, terrorist, and state actors.

Hacktivists are simply activists whom use the latest technology to aid their own civil disobedience, agitation, and protest in or through cyber space. For political purposes, the individual hacktivist or collective, such as Anonymous, conducts access or disruption operations to achieve their political goals. The hacktivist ranges from the script kiddie to a highly skilled operator capable of wreaking havoc in cyberspace.[51] Hacktivists do not pose a threat to conduct a "cyber Pearl Harbor" based on opportunity, capability, or intent. While the United States certainly has vulnerabilities in cyberspace, these vulnerabilities do not provide the opportunity for hacktivists to conduct significant attacks on the United States equivalent the Pearl Harbor attack. Some hacktivists have the capability to conduct damaging attacks. However, vulnerabilities limit the scope and effect of such attacks. The hacktivist generally does not have the intent to deny, degrade, or destroy heavily defended targets that represent vital US interests. Where domestic law fails to deter a hacktivist from a bona fide attack that causes significant damage or death to domestic or military targets, he or she becomes a terrorist. At worst, hacktivist activities can be criminal acts for political purposes. This argument does not include hacktivists employed as proxies of a state engaged in multi-domain warfare, as the state provides additional capabilities and intent and simply employs hacktivists to confuse attribution to the aggressor state or as a force multiplier.

When the first laws were written, the criminal was born. Harvey reminds us, "crime has adapted rapidly to exploit societies' dependence on the continued availability, accuracy and confidentiality of information. As well as significant benefits, technology has enabled old crimes

to be committed in new and more subtle ways."[52] From petty to organized crime, the intent of criminals in cyberspace is profit. These activities can range from stealing credit cards or data to a DDoS or creating and selling malware to the highest bidder. Insecure cyberspace is a crime syndicate's dream in that there is a high payoff and low risk of being caught and punished.[53] While criminals exploit vulnerabilities for profit, they do not possess the intent or all of the required capabilities to conduct a catastrophic attack equivalent a "cyber Pearl Harbor." Where domestic law fails to deter a criminal from a bona fide attack that causes significant damage or death to US domestic or military targets, he or she becomes a terrorist or state sponsored proxy engaging in cyber warfare. Cyber crime poses a challenge to national security in that it can provide the proving grounds for operators to build techniques, tactics, and procedures for later use in cyber warfare.[54] Moreover, some operators acting on behalf of the state or directed by the state gain their expertise from their day job, cyber crime.[55] It is suspected that the Russian government used hacktivists and criminal elements as proxies of the state in low-level cyber warfare in the Russian-Georgia and Estonia conflicts.[56] While this poses a threat, it is a far different threat than that posed by a catastrophic attack that would cross the threshold for the use of force and be considered an act of war.

Joint Publication 1-02, *Department of Defense Dictionary of Military and Associated Terms*, defines terrorism as "the unlawful use of violence or threat of violence, often motivated by religious, political, or other ideological beliefs, to instill fear and coerce governments or societies in pursuit of goals that are usually political."[57] Cyber terrorists are simply terrorists exploiting new technologies in cyberspace. These actors have the intent to threaten or use violence through cyberspace to instill fear or coerce the United States in pursuit of political ends. However, terrorists do not currently have the capabilities to exploit existing US vulnerabilities in

a manner to conduct a catastrophic attack, such as a "cyber Pearl Harbor." Nobody has ever died from a cyber attack.[58] Furthermore, Healey reminds us that no terrorist group has chosen cyber attack as their primary method or executed a major attack designed to cause death, destruction, or terror.[59] Terrorists employed and/or aided as proxies of a state who conduct a serious attack that causes damage or death in a target state, represent that host nation and would be engaging in an act of war between the host nation and target state. While the intent of terrorists is certainly different from that of hacktivists and criminals, their capabilities and US vulnerabilities do not indicate a serious threat for an attack that can achieve the magnitude of a "cyber Pearl Harbor."

To assess the validity of this paper's argument, it is important to consider the counter point that a "cyber Pearl Harbor" is looming. Considering US nation-state adversaries, this counter argument has merit. As history, international norms, and strategic logic suggest, state actors have and will continue to use technology to gain advantage in the conduct of adversarial international relations short of war and within war. Some state actors could have the intent, capabilities, and possibly the opportunity through US vulnerabilities in cyberspace to conduct a cyber attack equivalent a "cyber Pearl Harbor." In order to critically assess this paper's argument and counter argument, it is helpful to review the state actor's capability, opportunity, and intent through the frameworks provided on cyber weapons, cyber attack, cyber warfare, and cyber war.

At first glance, historical cyber incidents can strengthen alarmist claims that a "cyber Pearl Harbor" is looming. Building offensive cyber capabilities is explicitly stated in the doctrine of China and Russia amongst other state actors.[60] These nation-states have demonstrated advanced capabilities to establish access to US systems that could be used by adversaries to conduct an attack or legally defined use of force in or through cyberspace. Cyber alarmists assert this access extends beyond espionage and is being done to prepare for potential cyber conflicts.[61]

It is reported that Chinese military officials discuss the need to target enemy financial markets, electricity grids, and telecommunications networks by installing malware on these systems ahead of cyber attacks.[62] Since 2004, China has conducted 14 major cyber operations against international targets and the US military, to include Titan Rain and GhostNet.[63] While cyber espionage is not cyber war, these access operations do illuminate the pathway to attack when an adversary has the intent. Russia has employed cyber attack in the Russia-Georgia and Estonia conflicts.[64] While the extent of the threat is unknown, it can certainly sew fear, uncertainty, and doubt. It would be unwise for statesmen to ignore the valid threats these capabilities pose, but it would be equally unwise to overestimate their effectiveness in a sustained multi-domain conflict that would likely follow any form of significant kinetic or non-kinetic attack on the United States. Dipert reminds us that counter measures and damage repair can be executed in minutes, hours, or days by a technologically advanced country. States can also adopt less cyber reliant techniques, tactics, and procedures. Moreover, most cyber weapons employed against states with significant cyber capabilities are essentially one time use weapons whose effectiveness will rapidly diminish. [65] This does not mitigate the threat, but should temper its assessment in developing strategy. An effective strategic investment would help address access operations that enable espionage and/or attack.

While near-peer adversaries seek asymmetric advantage through cyberspace and spark fears of a "cyber Pearl Harbor," a key enabler to that threat would be US vulnerabilities in critical systems that could provide adversaries the opportunity to conduct such an attack. For an adversary to succeed, the United States "would have to create enormous vulnerabilities and cyber dependencies without concern for defending them… [and] this [would be] tantamount to a strategy of surrender."[66] Clearly, no nation would cede this advantage to their adversaries.

Nevertheless, knowingly or unknowingly, the cyber alarmists hold one of two assumptions that support a looming "cyber Pearl Harbor." First, the United States has identified vulnerabilities in critical infrastructure and is unable to mitigate them. Second, the United States does not know the vulnerabilities in critical infrastructure or systems and is thereby unable to mitigate them. If the first assumption holds true, policy makers have a better problem definition and can fund, regulate, and/or legislate mitigation to avoid the looming threat. If the second holds true, alarmist claims are based simply on fear and uncertainty about the unknowns and not facts that would substantiate the claim of a looming "cyber Pearl Harbor." Either way, vulnerabilities are the key variable in the threat equation that requires significant attention. While unchallenged alarmist claims might steer policy makers toward heavy investment in offensive cyber weapons in hopes of securing advantage in a revolutionary "cyber war," this understanding of vulnerabilities in the threat equation combined with an understanding that cyber represents an evolution in technology make it very clear that the United States must highly prioritize cyber security within her national strategy.[67] The United States has a strategic choice in deciding to take action toward reducing these vulnerabilities.

A review of evolving US policy indicates that the experts operating below the level of political rhetoric appear to understand the threats and are placing a heavy investment emphasis on cyber security in order to secure existing US advantages in joint warfighting. From Presidential Policy Directives, the 2015 National Security Strategy, the National Cybersecurity Initiative, the DOD Cyber Strategy to the Joint Operating Environment 2035 and Air Force Future Operating Concept; a prudent strategic vision that clearly identifies cyber security as a national security priority is being pursued.[68] Importantly, this reduces a rhetoric driven focus on cyber offense and the use of these capabilities against capable adversaries that could only result

in escalation. As discussed, it is wishful thinking to believe warfare will remain confined to the cyber domain. Moreover, it does not make tactical sense to engage in significant cyber attacks against opponents like Russia or China who are less vulnerable than the United States.[69]

Unknowns in near-peer capabilities and US vulnerabilities leave state actor intent as the driving variable in determining if a "cyber Pearl Harbor" is looming today. Do US adversaries have the intent or incentive to conduct a catastrophic cyber attack on the United States? Gray reminds us, "the future of warfare is not synonymous with future technology, but warfare must always have a technological dimension."[70] Based on the concepts provided on cyber warfare and cyber war, it is hard to imagine that a state actor would limit or expect to achieve a catastrophic attack on the United States using cyberspace alone. These states possess kinetic or sabotage capabilities much more effective than cyber capabilities at conducting such an attack. The same restraints that have prevented these attacks historically are likely the same international relations, norms, and restraints that prevent a "cyber Pearl Harbor." Congruent with the thought that cyber power is an evolution in technology, this author suggests state actors understand the limitations of cyber power and would not provoke a significant retaliation or escalation outside of cyberspace by conducting a catastrophic attack through cyberspace.[71] Healey reminds us the most capable cyber nations have restrained themselves well under the threshold of full scale cyber warfare and have proven just as unwilling to launch a catastrophic cyber attack as they have been in air, on land, or sea.[72]

Conclusion

In closing, cyber alarmists fail to consider the master's golden rule. Clausewitz reminds us; "The first, the supreme, the most far-reaching act of judgement that the statesman and commander have to make is to establish by that test the kind of war on which they are

embarking; neither mistaking it for, nor trying to turn it into, something that is alien to its nature."[73] Alarmists view cyber as a new revolutionary form of warfare and are shaping the public narrative through exaggerated threats and fears.[74] By loosely codifying key concepts and asserting nearly all malicious cyber activity is warfare without critical analysis or debate, these alarmist views have driven senior, influential leaders to assert a "cyber Pearl Harbor" is looming or that we are losing a "cyber war" today.[75] This narrative can cause a dangerous escalation to armed conflict and strategically hamper resolution of the true threats by steering investments to the wrong solutions.[76] Cyber pragmatists view cyber as an evolution in technology that can be used in war and codify malicious cyber activities below the use of force in a manner more consistent with existing international norms, laws, and strategic logic. In viewing cyber threats through the cyber pragmatist lens and as a function of capability, opportunity, and intent; the only serious threat is from a nation state with US vulnerabilities standing out as the key variable enabling this threat. It is clear that only nation states could have the capability to conduct the looming "cyber Pearl Harbor." However, alarmist claims overweigh the adversaries' ability to sustain effects through cyber attack and fail to account for historical international relations, norms, and strategic logic that restrain these states from conducting catastrophic attacks; especially in or through cyberspace. While cyber terrorism, cyber espionage, and cyber crime do pose serious threats, they are clearly different threats than those posed by an act of warfare and should be handled in a manner that does not lead to war. Considering US vulnerabilities drive the threat, cyber security actions taken to mitigate adversary asymmetric cyber capabilities that could be used for a catastrophic attack in multi-domain warfare, can also reduce threats from cyber terrorism or cyber crime. As such, the United States should heavily weigh investment

toward national cyber security in order to avoid escalation to real war and deny criminals, hacktivists, terrorists, and state adversaries the vulnerabilities to exploit.

Notes

1. Elisabeth Bumiller and Thom Shanker, "Panetta Warns of Dire Threat of Cyberattack on U.S.," *The New York Times Online*, October 11, 2012, http://www.nytimes.com/2012/10/12/world/panetta-warns-of-dire-threat-of-cyberattack.html?_r=0.

2. Misha Glenny and Camino Kavanagh, "800 Titles but No Policy—Thoughts on Cyber Warfare," *American Foreign Policy Interests* 34, no. 6 (November 2012): 288–89, doi:10.1080/10803920.2012.742410; Andrew F. Krepinevich, *Cyber Warfare: A "Nuclear Option"?* (Center for Strategic and Budgetary Assessments, 2012), i-iii; 2-14; 56; 79; Paul D. Shinkman, "America Is Losing the Cyber War," September 29, 2016, http://cyberattacksquad.com/america-is-losing-the-cyber-war/; Newt Gingrich, "America Lost the Cyberwar over Sony: Now What?" (Cable News Network, December 18, 2014), http://www.cnn.com/2014/12/18/opinion/gingrich-america-lost-cyberwar-sony/index.html; Colin S. Gray, *Making Strategic Sense of Cyber Power: Why the Sky Is Not Falling* (Carlisle, PA: Strategic Studies Institute and U.S. Army War College Press, 2013), 41; 49.

3. Gray, *Making Strategic Sense of Cyber Power*, 18. This is my synthesis of Gray's concern about our anxiety and even fear of cyber power and cyber warfare that can misinform how we build strategy in cyber combined with the alarmist and misleading narratives that have been consistent in the media and public discourse for the last decade or longer.

4. Gary D. Brown and Owen W. Tullos, "On the Spectrum of Cyberspace Operations," *Small Wars Journal*, December 11, 2012, 9; Brandon Valeriano and Ryan C. Maness, *Cyber War versus Cyber Realities: Cyber Conflict in the International System* (Oxford ; New York: Oxford University Press, 2015), 39–40; Jason Andress and Steve Winterfeld, *Cyber Warfare:*

Techniques, Tactics and Tools for Security Practitioners, Second edition (Amsterdam ; Boston: Elsevier, 2014), 2.

5. Jason Healey, ed., *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012*, Kindle (Vienna, VA: Cyber Conflict Studies Association, 2013), Loc 178.

6. Glenny and Kavanagh, "800 Titles but No Policy—Thoughts on Cyber Warfare," 289; Krepinevich, *Cyber Warfare: A "Nuclear Option"?*; Thomas Rid, *Cyber War Will Not Take Place* (Oxford ; New York: Oxford University Press, 2013); Thomas Rid, "Cyber War Will Not Take Place," *Journal of Strategic Studies* 35, no. 1 (February 2012): 5–32, doi:10.1080/01402390.2011.608939; Valeriano and Maness, *Cyber War versus Cyber Realities*.

7. Gal Beckerman, "Is This Really War?," *Boston Globe*, September 15, 2013, 1–2.

8. Valeriano and Maness, *Cyber War versus Cyber Realities*, 33.

9. Glenny and Kavanagh, "800 Titles but No Policy—Thoughts on Cyber Warfare," 289; Office of General Counsel, "Department of Defense Law of War Manual" (United States Department of Defense, May 2016), 994; Joint Chiefs of Staff, "Joint Publication 3-12 (R): Cyberspace Operations," February 5, 2013, http://www.dtic.mil/doctrine/new_pubs/jp3_12R.pdf.

10. Gray, *Making Strategic Sense of Cyber Power*, 40–54. These are my thoughts derived from Gray's discussion on technical and tactical driving the narrative in literature today. This has also been my experience working with cyber personnel at the tactical level.

11. Thomas Rid and Peter McBurney, "Cyber-Weapons," *The RUSI Journal* 157, no. 1 (February 2012): 7, doi:10.1080/03071847.2012.664354.

12. Ibid., 7–8.

13. Ibid.; Andress and Winterfeld, *Cyber Warfare*, 103.

14. Andress and Winterfeld, *Cyber Warfare*, 103–13.

15. Ibid., 113; Ida Mae Boyd, "The Fundamentals of Computer Hacking" (SANS Institute, December 3, 2000). "Network enumeration is a technique to identify the domain names and associated networks related to a particular organization… the type of information enumerated by hackers can be loosely grouped into the following categories: 1) network resources and shares, 2) users and groups, 3) applications and banners."

16. Rid and McBurney, "Cyber-Weapons," 8.

17. Ibid., 8–9.

18. Andress and Winterfeld, *Cyber Warfare*, 125–35, 184–190. Synthesizing the thought of Andress and Winterfeld, this author views a tool that was designed to provide access as a weapon when the intent is to go beyond data exfiltration and create damaging effects. As Andress and Winterfeld point out; reconnaissance, scanning, access, escalation of privileges, and exfiltration are precursors to assault. Capability and intent drive actions to the assault level. The target does not know if it will lead to an attack, unless the attack occurs.

19. Rid and McBurney, "Cyber-Weapons," 11.

20. Government Accountability Office, "Defense Department Cyber Efforts: Definitions, Focal Point, and Methodology Needed for DOD to Develop Full-Spectrum Cyberspace Budget Estimates," July 29, 2011, 2; 10, http://www.gao.gov/new.items/d11695r.pdf.

21. Valeriano and Maness, *Cyber War versus Cyber Realities*, 211.

22. Joint Chiefs of Staff, "JP 3-12 (R)," vii; II-2; GL-4.

23. Joint Chiefs of Staff, "Joint Publication 1-02: Department of Defense Dictionary of Military and Associated Terms," February 15, 2016, 172.

24. Gingrich, “America Lost the Cyberwar over Sony: Now What?”; Shinkman, “America Is Losing the Cyber War”; Richard A. Clarke and Robert K. Knake, *Cyber War: The next Threat to National Security and What to Do about It*, 1st ed (New York: Ecco, 2010).

25. Brown and Tullos, “On the Spectrum of Cyberspace Operations,” 1–2.

26. Ibid., 4.

27. Ibid.

28. Ibid., 5.

29. Gray, *Making Strategic Sense of Cyber Power*; Rid, “Cyber War Will Not Take Place,” February 2012; Rid, *Cyber War Will Not Take Place*, 2013; Valeriano and Maness, *Cyber War versus Cyber Realities*; Brown and Tullos, “On the Spectrum of Cyberspace Operations.”

30. Brown and Tullos, “On the Spectrum of Cyberspace Operations,” 6.

31. Ibid.

32. Ibid.; Michael Wood, “The Principle of Non-Intervention in Contemporary International Law: Non-Interference in A State’s Affairs Used to Be a Rule of International Law: Is It Still?,” 2007, 1–3, https://www.chathamhouse.org/sites/files/chathamhouse/public/Research/International%20Law/il280207.pdf.

33. Brown and Tullos, “On the Spectrum of Cyberspace Operations,” 6.

34. Andress and Winterfeld, *Cyber Warfare*, 4.

35. Joint Chiefs of Staff, “Joint Publication 5-0: Joint Operation Planning,” August 11, 2011, I-4.

36. Gray, *Making Strategic Sense of Cyber Power*, 10. Gray rightfully points out that there can be seriously harmful consequences for to defining some cyber activity as warfare and possibly war. He articulates that war and warfare are subjects of human judgment and choice. A nation that believes it is in a state of cyber war, could view things differently and more easily escalate to real war.

37. Ibid.

38. Colin S Gray, *Another Bloody Century: Future Warfare*, Kindle (London: Phoenix, 2006), 319.

39. Ibid., 327.

40. Brown and Tullos, "On the Spectrum of Cyberspace Operations"; Rid and McBurney, "Cyber-Weapons"; Rid, "Cyber War Will Not Take Place," February 2012; Rid, *Cyber War Will Not Take Place*, 2013; Andress and Winterfeld, *Cyber Warfare*; Valeriano and Maness, *Cyber War versus Cyber Realities*; Wood, "The Principle of Non-Intervention in Contemporary International Law: Non-Interference in A State's Affairs Used to Be a Rule of International Law: Is It Still?"

41. Clarke and Knake, *Cyber War*, 30–31; Krepinevich, *Cyber Warfare: A "Nuclear Option"?*, i-iii; 2-14; 56; 79; Shinkman, "America Is Losing the Cyber War"; Gingrich, "America Lost the Cyberwar over Sony: Now What?"; Gray, *Making Strategic Sense of Cyber Power*, 41, 49; Andress and Winterfeld, *Cyber Warfare*, 2.

42. Clarke and Knake, *Cyber War*, 6.

43. Colin S. Gray, *Modern Strategy* (New York: Oxford University Press, 1999); Carl von Clausewitz, Michael Eliot Howard, and Peter Paret, *On War*, First paperback printing (Princeton, N.J: Princeton University Press, 1989).

44. Gray, *Another Bloody Century*, 319; Vincent Manzo, "Deterrence and Escalation in Cross-Domain Operations: Where Do Space and Cyberspace Fit?," *Joint Force Quarterly* 66 (Quarter 2012): 10.

45. Clausewitz, Howard, and Paret, *On War*, 75.

46. Ibid., 75–76; Kevin R. Bray, "Cyber Elective: America Did Not Lose the Cyber War over Sony - The Sky Is Not Falling" (Air War College, Air University, 2016).

47. Rid, *Cyber War Will Not Take Place*, 2013, 2–3; Bray, "Cyber Elective: America Did Not Lose the Cyber War over Sony - The Sky Is Not Falling."

48. Bray, "Cyber Elective: America Did Not Lose the Cyber War over Sony - The Sky Is Not Falling."

49. Gregory Rattray and Jason Healey, "Categorizing and Understanding Offensive Cyber Capabilities and Their Use," in *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy*, ed. National Research Council (U.S.) and National Research Council (U.S.) (Washington, D.C: National Academies Press, 2010), 84.

50. "Making Sense of Cyber Course" (Max, Air War College Term 1 Elective (AY17)); Healey, *A Fierce Domain*, Loc 5209-5281.

51. P. W. Singer, *Cybersecurity and Cyberwar: What Everyone Needs to Know*, Kindle (Oxford ; New York: Oxford University Press, 2014), 76–84.

52. Shaun D. Harvey, "Determining the Utility of Cyber Power" (University of Reading, 2012), 49.

53. Jeffrey Carr, *Inside Cyber Warfare*, 2nd ed (Beijing ; Sebastopol, CA: O'Reilly, 2012), 6.

54. Ibid., 5–6; Roger Hurwitz, "Depleted Trust in the Cyber Commons," *Strategic Studies Quarterly* 6, no. 3 (Fall 2012): 38.

55. Carr, *Inside Cyber Warfare*, 5.

56. Ibid., 5; 121-130.

57. Joint Chiefs of Staff, "JP - 1-02," 241.

58. Healey, *A Fierce Domain*, Loc 468.

59. Ibid., Loc 489.

60. Sanjay Goel, "Cyberwarfare: Connecting the Dots in Cyber Intelligence," *Communications of the ACM* 54, no. 8 (August 1, 2011): 132, doi:10.1145/1978542.1978569; Arie J. Schaap, "Cyber Warfare Operations: Development and Use Under International Law," *Air Force Law Review* 64 (June 2009): 132–33.

61. Goel, "Cyberwarfare," 132; Clarke and Knake, *Cyber War*.

62. Goel, "Cyberwarfare," 134.

63. Soren Olson, "Shadow Boxing: Cyber Warfare and Strategic Economic Attack," *Joint Force Quarterly*, no. 66 (3d Quarter 2012): 19.

64. Goel, "Cyberwarfare," 132.

65. Randall R. Dipert, "The Ethics of Cyberwarfare," *Journal of Military Ethics* 9, no. 4 (December 2010): 391, doi:10.1080/15027570.2010.536404.

66. Harvey, "Determining the Utility of Cyber Power," 58.

67. Aaron Boyd, "Trump Administration Promises More Aggressive, Less Political Cyber Stance," *Federal Times Online*, November 9, 2016, http://www.federaltimes.com/articles/trump-administration-promises-more-aggressive-less-political-cyber-

stance?utm_source=Sailthru&utm_medium=email&utm_campaign=DFN%20EBB%2011.10.16&utm_term=Editorial%20-%20Early%20Bird%20Brief. Before his election, Mr. Trump, similar to others, appears to have bought-in to the disparate alarmist thoughts and has taken a position to build greater offensive capabilities in order to deter enemies from "attacking" the United States. Mr. Trump was quoted as saying; "As a deterrent against attacks on our critical resources, the United States must possess – and has to – the unquestioned capacity to launch crippling cyber counterattacks. And I mean crippling…. America's dominance in the arena must be unquestioned. Today, it's totally questioned. People don't even know if we have capability that we are supposed to have."

68. "Presidential Policy Directive (21): Critical Infrastructure Security and Resilience" (The White House, February 12, 2013), https://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil; "Presidential Policy Directive (41): United States Cyber Incident Coordination" (The White House, July 26, 2016), https://www.whitehouse.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident; "National Security Strategy" (The White House, February 2015); "The Department of Defense Cyber Strategy" (The United States Secretary of Defense, April 17, 2015); Director for Joint Force Development, "Joint Operating Environment (JOE) 2035: The Joint Force in a Contested and Disordered World" (Joint Chiefs of Staff, July 14, 2016); Headquarters, United States Air Force, "Air Force Future Operating Concept: A View of the Air Force in 2035" (United States Air Force, September 2015).

69. Healey, A Fierce Domain; Valeriano and Maness, Cyber War versus Cyber Realities.

70. Gray, *Another Bloody Century*, 98.

71. Manzo, “Deterrence and Escalation in Cross-Domain Operations: Where Do Space and Cyberspace Fit?,” 10.

72. Healey, *A Fierce Domain*, Loc 532.

73. Clausewitz, Howard, and Paret, *On War*, 88.

74. Glenny and Kavanagh, “800 Titles but No Policy—Thoughts on Cyber Warfare,” 288–89; Krepinevich, *Cyber Warfare: A “Nuclear Option”?*, i-iii; 2-14; 56; 79; Shinkman, “America Is Losing the Cyber War”; Gingrich, “America Lost the Cyberwar over Sony: Now What?”; Gray, *Making Strategic Sense of Cyber Power*, 41; 49.

75. Elisabeth Bumiller and Thom Shanker, “Panetta Warns of Dire Threat of Cyberattack on U.S.,” *The New York Times Online*, October 11, 2012, http://www.nytimes.com/2012/10/12/world/panetta-warns-of-dire-threat-of-cyberattack.html?_r=0; Gray, *Making Strategic Sense of Cyber Power*, 10.

76. Gray, *Making Strategic Sense of Cyber Power*, 10.

Bibliography

Andress, Jason, and Steve Winterfeld. *Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners*. Second edition. Amsterdam ; Boston: Elsevier, 2014.

Beckerman, Gal. "Is This Really War?" *Boston Globe*. September 15, 2013.

Boyd, Aaron. "Trump Administration Promises More Aggressive, Less Political Cyber Stance." *Federal Times Online*, November 9, 2016. http://www.federaltimes.com/articles/trump-administration-promises-more-aggressive-less-political-cyber-stance?utm_source=Sailthru&utm_medium=email&utm_campaign=DFN%20EBB%2011.10.16&utm_term=Editorial%20-%20Early%20Bird%20Brief.

Boyd, Ida Mae. "The Fundamentals of Computer Hacking." SANS Institute, December 3, 2000.

Bray, Kevin R. "Cyber Elective: America Did Not Lose the Cyber War over Sony - The Sky Is Not Falling." Air War College, Air University, 2016.

Brown, Gary D., and Owen W. Tullos. "On the Spectrum of Cyberspace Operations." *Small Wars Journal*, December 11, 2012.

Bumiller, Elisabeth, and Thom Shanker. "Panetta Warns of Dire Threat of Cyberattack on U.S." *The New York Times Online*, October 11, 2012. http://www.nytimes.com/2012/10/12/world/panetta-warns-of-dire-threat-of-cyberattack.html?_r=0.

———. "Panetta Warns of Dire Threat of Cyberattack on U.S." *The New York Times Online*, October 11, 2012. http://www.nytimes.com/2012/10/12/world/panetta-warns-of-dire-threat-of-cyberattack.html?_r=0.

Carr, Jeffrey. *Inside Cyber Warfare*. 2nd ed. Beijing ; Sebastopol, CA: O'Reilly, 2012.

Clarke, Richard A., and Robert K. Knake. *Cyber War: The next Threat to National Security and What to Do about It*. 1st ed. New York: Ecco, 2010.

Clausewitz, Carl von, Michael Eliot Howard, and Peter Paret. *On War*. First paperback printing. Princeton, N.J: Princeton University Press, 1989.

Dipert, Randall R. "The Ethics of Cyberwarfare." *Journal of Military Ethics* 9, no. 4 (December 2010): 384–410. doi:10.1080/15027570.2010.536404.

Director for Joint Force Development. "Joint Operating Environment (JOE) 2035: The Joint Force in a Contested and Disordered World." Joint Chiefs of Staff, July 14, 2016.

Gingrich, Newt. "America Lost the Cyberwar over Sony: Now What?" Cable News Network, December 18, 2014. http://www.cnn.com/2014/12/18/opinion/gingrich-america-lost-cyberwar-sony/index.html.

Glenny, Misha, and Camino Kavanagh. "800 Titles but No Policy—Thoughts on Cyber Warfare." *American Foreign Policy Interests* 34, no. 6 (November 2012): 287–94. doi:10.1080/10803920.2012.742410.

Goel, Sanjay. "Cyberwarfare: Connecting the Dots in Cyber Intelligence." *Communications of the ACM* 54, no. 8 (August 1, 2011): 132. doi:10.1145/1978542.1978569.

Government Accountability Office. "Defense Department Cyber Efforts: Definitions, Focal Point, and Methodology Needed for DOD to Develop Full-Spectrum Cyberspace Budget Estimates," July 29, 2011. http://www.gao.gov/new.items/d11695r.pdf.

Gray, Colin S. *Another Bloody Century: Future Warfare*. Kindle. London: Phoenix, 2006.

Gray, Colin S. *Making Strategic Sense of Cyber Power: Why the Sky Is Not Falling*. Carlisle, PA: Strategic Studies Institute and U.S. Army War College Press, 2013.

———. *Modern Strategy*. New York: Oxford University Press, 1999.

Harvey, Shaun D. “Determining the Utility of Cyber Power.” University of Reading, 2012.

Headquarters, United States Air Force. “Air Force Future Operating Concept: A View of the Air Force in 2035.” United States Air Force, September 2015.

Healey, Jason, ed. *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012*. Kindle. Vienna, VA: Cyber Conflict Studies Association, 2013.

Hurwitz, Roger. “Depleted Trust in the Cyber Commons.” *Strategic Studies Quarterly* 6, no. 3 (Fall 2012): 20–45.

Joint Chiefs of Staff. “Joint Publication 1-02: Department of Defense Dictionary of Military and Associated Terms,” February 15, 2016.

———. “Joint Publication 3-12 (R): Cyberspace Operations,” February 5, 2013. http://www.dtic.mil/doctrine/new_pubs/jp3_12R.pdf.

———. “Joint Publication 5-0: Joint Operation Planning,” August 11, 2011.

Krepinevich, Andrew F. *Cyber Warfare: A “Nuclear Option”?* Center for Strategic and Budgetary Assessments, 2012.

“Making Sense of Cyber Course.” Max, Air War College Term 1 Elective (AY17).

Manzo, Vincent. “Deterrence and Escalation in Cross-Domain Operations: Where Do Space and Cyberspace Fit?” *Joint Force Quarterly* 66 (Quarter 2012): 8–14.

“National Security Strategy.” The White House, February 2015.

Office of General Counsel. “Department of Defense Law of War Manual.” United States Department of Defense, May 2016.

Olson, Soren. “Shadow Boxing: Cyber Warfare and Strategic Economic Attack.” *Joint Force Quarterly*, no. 66 (3d Quarter 2012): 15–20.

"Presidential Policy Directive (21): Critical Infrastructure Security and Resilience." The White House, February 12, 2013. https://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.

"Presidential Policy Directive (41): United States Cyber Incident Coordination." The White House, July 26, 2016. https://www.whitehouse.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident.

Rattray, Gregory, and Jason Healey. "Categorizing and Understanding Offensive Cyber Capabilities and Their Use." In *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy*, edited by National Research Council (U.S.) and National Research Council (U.S.), 77–97. Washington, D.C: National Academies Press, 2010.

Rid, Thomas. "Cyber War Will Not Take Place." *Journal of Strategic Studies* 35, no. 1 (February 2012): 5–32. doi:10.1080/01402390.2011.608939.

———. *Cyber War Will Not Take Place*. Oxford ; New York: Oxford University Press, 2013.

Rid, Thomas, and Peter McBurney. "Cyber-Weapons." *The RUSI Journal* 157, no. 1 (February 2012): 6–13. doi:10.1080/03071847.2012.664354.

Schaap, Arie J. "Cyber Warfare Operations: Development and Use Under International Law." *Air Force Law Review* 64 (June 2009): 121–73.

Shinkman, Paul D. "America Is Losing the Cyber War," September 29, 2016. http://cyberattacksquad.com/america-is-losing-the-cyber-war/.

Singer, P. W. *Cybersecurity and Cyberwar: What Everyone Needs to Know*. Kindle. Oxford ; New York: Oxford University Press, 2014.

"The Department of Defense Cyber Strategy." The United States Secretary of Defense, April 17, 2015.

Valeriano, Brandon, and Ryan C. Maness. *Cyber War versus Cyber Realities: Cyber Conflict in the International System*. Oxford ; New York: Oxford University Press, 2015.

Wood, Michael. "The Principle of Non-Intervention in Contemporary International Law: Non-Interference in A State's Affairs Used to Be a Rule of International Law: Is It Still?," 1–8, 2007. https://www.chathamhouse.org/sites/files/chathamhouse/public/Research/International%20Law/il280207.pdf.