Building a Conceptual Framework for Cyber's Effect on National Security

FJ Cilluffo[1], JR Clark[2]

[1]*Center for Cyber and Homeland Security*
The George Washington University
E-mail: cilluffo@gwu.edu

[2]*College of Liberal Arts*
Towson University
E-mail: jrclark@towson.edu

Abstract: *Cyber changes everything; cyber changes nothing. That important, yet unhelpful, truism captures the state of debate concerning the effects of cyber technologies on national security. This 'either/or' pathology stems from the lack of a conceptual framework. Thankfully, this is changing. The Department of Defense's 2015 cyber strategy presents an understanding of the strategic environment. Admiral Rogers' 2015 vision and guidance for U.S. Cyber Command captures how cyber changes military art. Herein lies the foundation for building a conceptual framework. Based on these documents and general strategic theory, seven dicta for the further development of a conceptual framework are offered.*

Keywords: *Cyber, War, Warfare, Strategic Theory*

Introduction

Arguments about the effects of cyber technologies on national security often resemble a Rorschach test—more telling in regard to the professional background and personality of the author than the actual ramifications of cyber technologies. Like cyber technologies themselves, such arguments are ubiquitous, occurring in academia, in policy circles, among practitioners, and on the Internet (where a nascent version of the argument presented here first appeared on the blog *Lawfare*).

Despite a wide range of substantive positions, past works can be generally divided into two camps. Authors in one camp, including Lucas Kello (2013) and Paul Rosenzweig (2013), foresee the independent delivery of decisive strategic advantage via cyber technologies. For Kello, Rosenzweig, and other members of this camp, cyber changes everything. Authors in the other camp, including Erik Gartzke (2013) and Thomas Rid (2013), contend that there is not, nor will there be, any strategic advantage singularly produced by cyber technologies. For Gartzke, Thomas, and other members of this camp, cyber changes nothing.

This divide is no surprise, given the quick pace of technological development and ambiguities in regard to the second- and third-order effects of cyber technologies on national security. The stakes are, however, more significant than professional ego or academic bragging rights. Cyber technologies—defined here as the vast array of information and communication technology

devices that create, support, define, access, and use cyberspace (Shafqat & Masood 2016)—now permeate American society. Cyber technologies are interwoven into every aspect of United States national security: political, military, and economic. With some variance, similar conditions exist in every modern nation-state: peers, allies, and adversaries. As a result, both camps are right, and both camps are wrong.

Despite collectively arriving at the unhelpful truism (that cyber changes everything; cyber changes nothing), each camp is to be commended for advancing the state of the debate. Since the publication of John Arquilla and David Ronfeldt's 1993 article 'Cyberwar is coming!', the camps' combined theorizing about the potential effects of existent or prospective cyber technologies outline a range of possible scenarios (Arquilla and Ronfeldt 1993). Their 'what-if' arguments serve as catalysts for discussions about the policies and capabilities needed for national security in the 21st century.

Nonetheless, their arguments are insufficient for the implementation of policy or for the operationalization of capabilities. The U.S. cannot plan for and/or equip itself for the full range of theoretical scenarios. Resource limitations prohibit this approach. Nor is this approach necessary, given the strategic environment. The environment is defined by the range of motives and capabilities of real actors and the specifics of existing U.S. vulnerabilities and dependencies. These conditions create a hierarchy of cyber-based risks to national security.

To move beyond the everything/nothing debate, a conceptual framework for cyber is needed. Such a framework would allow policymakers and practitioners to understand, evaluate, plan for, and manipulate cyberspace and cyber technologies in the pursuit of national security. To do this, however, any conceptual framework for cyber must (1) be predicated on strategic theory; (2) be informed by the existing (or likely future) political motivations of key actors; and (3) be based on an appreciation of the current (or likely future) operational context—including its physical, political, and technological aspects.

The foundations for crafting such a framework are, thankfully, emerging. In April 2015, the Department of Defense published its cyber strategy. This document provides a baseline understanding of the political motivations of the United States and a general appreciation of the strategic environment (Department of Defense 2015). Two months later, Admiral Michael Rogers released 'Beyond the build', his vision and guidance for Cyber Command. In it, he outlines how cyber technologies change military art—including how militaries fight and defend, how and when militaries come into contact with one another, and how military force is generated and sustained (Rogers 2015).

It is time to develop a conceptual framework for understanding cyber's effect on national security. What follows is an important first step in doing so. It outlines the core tenets of the cyber debates, reviews the foundations provided by 'The DoD cyber strategy' (Department of Defense 2015) and by 'Beyond the build' (Rogers 2015), and uses both to set the parameters of a conceptual framework. From this, two things become clear. First, as an operational domain, cyberspace has much in common with the maritime domain. Second, much work lies ahead. To that end, seven dicta are offered for the further development of a conceptual framework that

predicts, tracks, categorizes, responds to, and addresses the effects of cyber technologies on national security.

State of the Debate—Two Camps

In crafting a conceptual framework for cyber, it is important to start by revisiting the debate between the two cyber camps. The core tenets of their arguments demarcate the key points that any framework must successfully address. Their collective arguments also illustrate the importance of strategic theory, the consideration of political motivations, and an awareness of the operational context. These three elements help resolve many of the differences between the camps and often increase the utility of their work.

Four tenets are at the center of the disagreement between the everything/nothing camps. The first tenet addresses the level of societal vulnerability created by cyber technology's central role in modern infrastructure. The second tenet addresses how cyber technologies affect the balance between offensive and defensive military capabilities. The third tenet addresses the effects of weaponized cyber technologies on warfare. The fourth tenet addresses the potential for cyber technologies to inflict significant damage in the physical domain.

The first tenet, the issue of whole-of-society vulnerability, is directly connected to the operational environment of the 21st century. Empirically, the claim that modern infrastructures—including those systems of executive departments and agencies, military command and control systems, critical infrastructure, and key aspects of civilian society—are dependent on cyber technologies is unquestionably valid. For the United States and every other advanced nation-state, modern life requires cyber technologies. The economic, social, and political shock of reverting to a pre-cyber world would be devastating. In practical terms, it is simply inconceivable.

This whole-of-society vulnerability, authors in the everything-camp contend, is a product of the "sub-structure of technology" that ultimately comingles civilian and military infrastructures (Cavelty 2011, p. 13). For the everything-camp, this sub-structure creates a situation in which the ability to target either the military or civilian realms creates the ability to target the other (Cavelty 2011; Colarik & Janczewski 2012; Rosenzweig 2013). Attack one and, inherently, the other is attacked. Take down one, and the other is dragged down. As cyber technologies become ever more prevalent through the 'Internet of things', the potential attack surface expands. Furthermore, the everything-camp argues, societal vulnerability is produced by coercive threats to attack civilian infrastructure that may force the target's government to comply with the attacker's will—regardless of the level of cybersecurity present in a government's own systems (Brantly 2014; Hjortdal 2011; Rosenzweig 2013).

Authors in the nothing-camp contend that cyber technologies have little effect on the vulnerability of nation-states. This is the case, they argue, because the effects of computer network attacks or computer network exploits are fleeting (Lindsay 2014b; Rid 2013). Furthermore, the nothing-camp notes, attacks or exploits are one-off events—given the ability of the target to patch or to modify their systems. They believe this condition mitigates any great vulnerability (Clark & Levin 2009; Gartzke 2013; Rid 2013). In addition, members of the nothing-camp see a lack of motive for attacks with societal level effects. They argue that state

and non-state actors who employ cyber technologies, whether for noble or nefarious purposes, have no reason to bring down the system they are leveraging for their own gain (Gartzke 2013; Lindsay 2014a; Lindsay 2014b).

The second tenet, how cyber technologies affect the balance between offensive and defensive military capabilities, also speaks to the operational environment of the 21st century. Members of the everything-camp posit the idea that cyber technologies are offense dominant. Their logic is this: the speed with which cyber technologies act and transit distances renders defenses ineffective. Speed, they contend, not only shrinks geographic barriers but reduces reaction time—negating the ability of defenses to respond (Cavelty 2011; Colarik & Janczewski 2012; Farwell & Rohozinski 2012; Rosenzweig 2013). Predicated on the assumption that cyber technologies could disarm the target before it could react, members of the everything-camp envision a cyber based ability to introduce strategic paralysis (Cavelty 2011; Colarik & Janczewski 2012; Farwell & Rohozinski 2012; Rosenzweig 2013; Sharma 2010). As a result, members of the everything-camp contend that cyber technologies may achieve Sun Tzu's objective of "[s]eizing the enemy without fighting" (Sharma 2010, p. 62). Cyber technologies' offensive dominance is further supported, they argue, by the difficulty of attribution. Without the ability to identify their attackers, targets are unable to threaten, either pre or post event, to retaliate after their paralysis has passed (Brantly 2014; Kello 2013). For authors in this camp, deterrence is foreclosed and attacks can be carried out with little fear of retribution.

Members of the nothing-camp acknowledge the speed of cyber technologies but reject the assumption that speed inherently favors the offense or overcomes key geographic barriers. Authors in the nothing-camp note that successful attacks or exploits are not, in fact, instant events. To be successful, they require undetected probing and reconnaissance, overcoming air-gapped systems not connected to the Internet, and (increasingly) getting past active cyber defenses (Gartzke 2013; Jacobsen 2014; Lindsay 2014a; Lindsay 2014b; Rid 2013). Jeppe Jacobsen and others note that the capabilities of cyber defenses are catching up to those of cyber offenses, a point supported by work being conducted by the Defense Advanced Research Projects Agency (aka DARPA)—including its Active Cyber Defense, High-Assurance Cyber Military Systems, and PLAN X projects (Babb 2015; Fraser 2016; Freedberg 2016; Heinl 2014; Jacobsen 2014; Keromytis 2016; Richards 2016). As a result, Jacobsen contends that there is no reason to believe that cyber technologies inherently or permanently favor the offense (Jacobsen 2014).

The third tenet addresses the effects of cyber technologies on warfare, specifically on disarming one's enemy in the Clausewitzian sense (Clausewitz 1976, p. 77). Authors in the everything-camp claim that cyber technologies dramatically lower the expense and difficultly of doing so, by presenting the opportunity for the most dramatic expression of asymmetric warfare since David versus Goliath. This is their logic: advanced militaries are dependent on highly complex Internet technologies for command and control and employ equally complex technologies for navigation and targeting, each of which is dependent on millions of lines of computer code. These two conditions multiply the available points of entry for a computer-based attack against these systems (Kello 2013; Rosenzweig 2013). Members of the everything-camp argue that, because the warfighting function of advanced militaries are dependent upon such technologies, even a temporary interruption in militaries' ability to use these technologies strategically

weakens those militaries' ability to wage war (Colarik & Janczewski 2012; Hjortdal 2011; Kello 2013). This, members of this camp contend, allows the relatively weak to leverage a few lines of malicious code in order to move the decisive actions of a confrontation into a sphere in which they can exploit their advantage (Farwell & Rohozinski 2012; Libicki 2009; Lupovici 2011).

Members of the nothing-camp challenge the notion that cyber technologies favor the weak, and thus represent an asymmetric leveling of the battlefield. They argue that cyber alone will not compel a nation-state to accept the political demands of the attacker. Authors in the nothing-camp believe that, absent the synchronous or sequential use of kinetic force, cyberattacks or exploits are, and will be, politically ineffective (Gartzke 2013; Jacobsen 2014; Lindsay 2014a; Rid 2013). They contend that if computer network attacks or exploits are unable to achieve the political objective of the weaker actor, they are more like vandalism or a criminal enterprise, than like warfare (Gartzke 2013; Lindsay 2014b; Rid 2013). In fact, authors in the nothing-camp argue that cyber technologies benefit Goliath, not David. They contend that cyber technologies overwhelmingly benefit advanced militaries, which are likely the stronger power in any conflict (Gartzke 2013; Rid 2013). This condition is a product of the precise and complex targeting necessary to launch a successful attack or exploit, and the fact that such must be used in conjunction with the use of force in the physical domains (Gartzke 2013; Jacobsen 2014; Lindsay 2014b; Rid 2013). Russia's use of hybrid warfare against Estonia and Georgia illustrate their point, even if some members of the nothing-camp question the effectiveness or sources of the attacks directed at Tallinn and Tbilisi (Gartzke 2013; Rid 2013).

The fourth tenet of the debate between the cyber-changes-everything-/nothing-camps revolves around the ability of cyber technologies to inflict damage. Members of the everything-camp argue that weaponized cyber technologies will have the potential, if not yet fully realized, to do significant damage in the physical domains—if not directly, then via second- or third-order effects (Applegate 2013; Kello 2013; Reed 2005; Rosenzweig 2013; Sharma 2009). Members of the nothing-camp disagree. In their work, they argue that only one known cyberattack—Stuxnet—has led to physical damage; moreover, in that case, such was neither the direct result, nor even the primary objective of the attack (Gartzke 2013; Lindsay 2014a; Rid 2013). Although the December 2015 cyberattack that brought down the Ukrainian electrical grid represents a second case, it is unlikely to alter the logic of the nothing-camp's assessment of the efficacy of such attacks (Zetter 2016). Thomas Rid captures the essence of their position; he views Stuxnet as primarily a psychological operation aimed at the confidence of Iran's nuclear scientists and technicians (Rid 2013). It is reasonable to assume that Rid and other members of the nothing-camp would view the Ukrainian attack similarly.

In regard to the question of damage, the disagreement between the two cyber camps is more definitional than substantive. In short, it depends on how damage is defined. The nothing-camp equates damage to physical damage, the direct destruction of a specific physical item: a generator, a weapon system, or the direct death of a human (Gartzke 2013; Lindsay 2014a; Lindsay 2014b; Rid 2013; Samaan 2010). The effects of cyber technologies on the capabilities, or on the relative distribution of capabilities, is discounted by the nothing-camp. The everything-camp, however, views damage in a broader, more long-term sense. Authors in the everything-camp include damage to capabilities, as well as indirect or deferred damage to such, and contend that both are strategically important. For example, authors in the everything-camp contend that

deaths or financial losses from an attack against the electrical grid, or changes in the balance of military strength as a result of the theft of intellectual property, ultimately count as damage in the physical domains (Brantly 2014; Hjortdal 2011; Kello 2013; Rosenzweig 2013).

The state of the debate between the two camps makes it clear that a conceptual framework for cyber must address how such technologies affect the relative vulnerability of nation-states, how they affect the balance between the use of offensive and defensive military force, how adversaries attempt to array force to their advantage, as well as what constitutes strategically significant damage. These are the tenets of the camps' disagreement; resolving them has merit. The importance of doing so, however, lies elsewhere. It has to do with setting the parameters of the conceptual framework.

A conceptual framework for cyber only has value if it helps policymakers and practitioners understand, evaluate, plan for, and manipulate cyberspace and cyber technologies in the pursuit of national security. In short, the value of a strategic framework is directly connected to practical concerns. Setting the parameters for what constitutes a practical concern is therefore critical. The foundations for setting such have begun to emerge, not from academics—but from the practitioners.

Foundations for a Framework

'The DoD cyber strategy' (2015) presents an assessment of the realities facing the United States, including its vulnerabilities, and a broad strategy for national security. Admiral Rogers' 'Beyond the build' (2015) offers practical guidance, rather than esoteric theorizing, regarding the role Cyber Command must execute to secure U.S. interests in the cyber domain and in preparing, and supporting, those commands primarily operating in the physical domains. Together these two documents address the four tenets of the cyber debate. More importantly, these documents provide a foundation for setting the parameters for a conceptual framework.

'The DoD cyber strategy' (2015) makes it clear that cyber technologies expand the range of actors with the potential to threaten U.S. national security. Secretary of Defense Ash Carter argues in his introductory letter that the U.S. now faces a litany of state and non-state actors that desire to use cyber technologies against it (Department of Defense 2015). The strategy notes that state and non-state actors are motivated by a desire to leverage cyber technologies to "achieve a variety of political, economic, or military objectives" against the United States, her allies, and other members of the international community (Department of Defense 2015, p. 1). As state and non-state actors seek to carry out such, the strategy highlights the fact that these actors may "strike at a nation's values as well as its interests or purposes" (Department of Defense 2015, p. 1). As 'The DoD cyber strategy' (2015) makes clear, this is no longer abstract theorizing; North Korea's attack against Sony Pictures, China's theft of intellectual property, the use of cyber technologies by the Islamic State in Iraq, and the Levant for recruitment and the dissemination of propaganda are realized, not hypothetical, threats (Department of Defense 2015).

'The DoD cyber strategy' (2015) expresses an appreciation of how cyber increases the range of actors and motives that threaten the U.S. This sentiment is mirrored by authors in each of the cyber debates camps. It represents an area of agreement between the two camps. Working from the perspective of the everything-camp, Lucas Kello writes: "more important than the nature of a

new weapon are the nature of its possessor and the purposes that instigate its use" (Kello 2013, p. 32). Jon Lindsay, working from the perspective of the nothing-camp, argues that, in assessing threats, the motivations and nature of the actors, organizations, or nation-states possessing cyber capabilities are more important than the efficacy of cyber technologies (Lindsay 2014a). How 'The DoD cyber strategy' treats the range of actors and motives is more important than simple observation or the forging of academic agreement. The strategy's appreciation of how cyber is altering the operational environment provides a way to evaluate the first and fourth tenets of the cyber debate—and to derive the implications of these tenets.

The empowerment via cyber technologies of an increased range of actors with varied motives is itself a function of cyber's ubiquity in modern life. The architecture of the Internet and the World Wide Web increase the number of connections between potential attackers and potential targets—regardless of the respective natures of either. 'The DoD cyber strategy' (2015) makes it clear that as a result, the level of societal vulnerability is increased by cyber technologies. The ubiquity of cyber technologies and their position at the center of modern infrastructure increases the ability of nation-states to act against the U.S. government. These same conditions increase the ability of nation-states to act against corporations and, potentially, against individual citizens. Similarly, cyber technologies have empowered criminals, terrorists, and hacktivists to act against governments, private-sector corporations, universities, non-governmental organizations, and individuals. 'The DoD cyber strategy' (2015) makes it clear that the presence of cyber in modern life creates the ability to circumvent the protective barriers of national borders and defenses and potentially nullifies the ability of national militaries to serve as effective protectors for their societies. The result is increased societal vulnerability.

The issue of cyber-inflicted damage, the fourth tenet, addresses the implications of this societal vulnerability. From the outset, 'The DoD cyber strategy' (2015) presents the argument that cyber can, and does, inflict damage. Nonetheless, the strategy's view of damage is more nuanced than that of the everything-camp. 'The DoD cyber strategy' (2015) posits the idea that by undermining the material sources of American instruments of power—the U.S.'s technological and military advantages, its economy, and its infrastructure—cyberattacks and exploits do inflict damage upon the United States (Department of Defense 2015). The strategy also puts forth the idea that cyberattacks and exploits can be used to damage the United States by undermining the social sources of American power, including the value of American intellectual property, the country's level of social cohesion, and the political will of the American people (Department of Defense 2015). In short, 'The DoD cyber strategy' (2015) finds that cyber technologies present opportunities to weaken the material strength and resolve of the United States.

In addressing the mechanisms by which cyber technologies might inflict harm upon the U.S., the 'The DoD cyber strategy' (2015) engages the second and third tenets of the cyber debate—those regarding the balance between offense and defense, and the degree to which cyber technologies offer new opportunities for asymmetric warfare. The strategy rejects the notion that cyber technologies inherently favor the offense or defense. Instead, it argues that cyber technologies will be inherent in both the offense and defense. As a result, it states that the DoD "must be able to secure its own networks against attack and recover quickly" (Department of Defense 2015, p. 4). Furthermore, the strategy makes it clear that the cyber domain will be contested space; and although the DoD plans to dominate it, U.S. forces must be prepared to operate without the

benefit of modern technologies for communications and navigation (Department of Defense 2015, p. 4). 'The DoD cyber strategy' (2015) calls upon American armed services to be prepared to operate without the technologies upon which the everything-camp believes them to be dependent. In short, the strategy calls upon the U.S. military of the 21st century to be prepared to, if necessary, fight and win using the tools of the mid-20th century (Department of Defense 2015, p. 5).

In reality, each of the services has already begun working to ensure that it can do just that. Each of the services is preparing to fight within contexts in which future enemies attempt to leverage their technological strengths while simultaneously attempting to avoid or nullify those of the United States (Freedberg 2015; United States Air Force Curtis E. Lemay Center for Doctrine Development and Education 2011; United States Army Training and Doctrine Command 2010). Each of the services is incorporating this into their operations and planning. They are also incorporating this into their procurement processes; the services have added red-team cyberattacks into their equipment and weapons' development processes (Reuters 2012; Keller 2015; Osborn 2015). With these actions, the services are operationalizing 'The DoD cyber strategy' (2015)—by neither ceding the cyber domain, nor being wholly dependent upon it.

In regard to the second and third tenets of the cyber debates, 'The DoD cyber strategy' (2015) acknowledges that cyber technologies are changing modern warfare. At the same time, it attempts to ensure that cyber technologies offer no asymmetric advantage to the adversaries and/or enemies of the United States. If successful, the strategy will, as predicted by the nothing-camp, provide advantages to the United States. The capability to operate, even dominate, all the domains, offers the best mechanism for selecting and shaping the battlespace in a manner most advantageous to the United States and its political objectives.

Admiral Michael Rogers' 'Beyond the build' (2015) offers his command vision regarding Cyber Command's role in the cyber domain and its role in preparing other commands for how cyber will affect their operations. Like 'The DoD cyber strategy' (2015), 'Beyond the build' (2015) addresses the increased vulnerabilities posed by cyber technologies and how they could damage the United States, the first and fourth tenets of the cyber debate. Rogers' vision puts forth the idea that the sinews of the U.S. economy, its political and social systems, its governmental communication conduits, and its military's command and control systems all now reside in the cyber domain (Rogers 2015). Rogers argues that this creates vulnerabilities for the United States, but that the U.S. is not alone in this: "All nations have vulnerabilities that can be exploited in and through cyberspace" (Rogers 2015, p. 2).

Central to the commander's vision is the notion that cyber technologies alter the application of military force; they change how militaries fight (Rogers 2015). Beginning with the opening sentence—"As cyberspace has grown and become more pervasive, military art has changed"—and continuing throughout the document, Rogers argues that cyber technologies must be integrated into the full spectrum of military operations; from peacetime preparation, through war, and into recovery operations (Rogers 2015, p. 2). Similar to claims in 'The DoD cyber strategy' (2015) are Rogers's contentions that cyber is neither offense nor defense dominant, and that it does not organically favor the weak or the strong. Rogers (2015) argues that cyber will benefit those who employ it best. For Rogers, the objective is to leverage cyber technologies to build capacity and capability (Rogers 2015, p. 2). For this reason, 'Beyond the build' (Rogers 2015)

contends that cyber must be part of planning, training, and execution. Furthermore, rather than being held as something distinct, Rogers argues that cyber technologies must be folded into the traditional terminology, operational concepts, tactics, techniques, and procedures of existing military mission sets (Rogers 2015, p. 7).

As one would expect, Admiral Rogers's vision is that of a warfighter (2015). It highlights how cyberspace alters three foundational elements of war: (1) how militaries fight and defend, (2) how and when militaries come into contact with one another, and (3) how military force is generated and sustained. As a result of cyber technologies, Rogers argues that the exercise of military force will be more integrated, collaborative, and driven by information-sharing to unite national and allied efforts (Rogers 2015). Rogers argues that the fight will be predicated on agility and innovation (Rogers 2015). Like 'The DoD cyber strategy', Rogers argues that the fight will occur within and beyond cyberspace (2015). As a result, Rogers's vision makes it clear that he too expects cyberspace to be a contested domain: "We must train and exercise to operate with degraded systems, because digital connectively should never be taken for granted" (Rogers 2015, p. 1.). Because cyber technologies create situations in which the pursuit of political objectives and the maintenance of military readiness are no longer confined to the physical world, Rogers (2015) believes cyber technologies expand how and when militaries come into contact with one another. 'Beyond the build' (Rogers 2015) outlines a new reality. In addition to locations identified by grid coordinates, national militaries now deploy to, reconnoiter, and fight upon locations defined by IP-addresses in order to defend or attack networks, or to integrate cyber operations with joint-force operations. Unlike their physical counter-parts, cyber operations are constant. As a result, adversarial militaries are simultaneously and constantly in contact with one another (Rogers 2015). Changes in how militaries fight and how and when they come into contact with one another necessitate changes in how military force is generated and sustained. Rogers (2015) argues that to build and sustain a military capable of meeting the demands of the modern world,

> The nation needs a motivated, fully-trained, and well-led cyber workforce that understands evolving technologies and adversary TTPs. The workforce—military (both active and reserve), civilian, and contractor—is the Command's greatest resource. (Rogers 2015, p. 10)

In addition, he argues that procurement processes must be made more agile and efficient so that forces can be properly equipped. As the Admiral makes clear, both of these tasks require commitment to an operational mindset whereby U.S. cyber capabilities are led, not administered (Rogers 2015).

Based on the 'The DoD cyber strategy' (2015), cyber technologies have clearly increased societal vulnerability. The strategy makes it clear that cyber technologies can inflict damage, especially long-term damage, against the foundations of national power. 'The DoD cyber strategy' (2015) also makes clear that cyber technologies are affecting, and will affect, warfare. Similarly, Admiral Rogers' 'Beyond the build' (2015) puts forward the idea that cyber technologies are catalyzing an evolution in warfare. For Rogers (2015), cyber technologies alter how military force is generated, sustained, and brought into contact with other forces.

Together, 'The DoD cyber strategy' (2015) and 'Beyond the build' (2015) set the foundations for the parameters of a conceptual framework for cyber. They suggest that the military employment

of cyber technologies will affect the vulnerability of nation-states and the societies they represent. From these documents comes the notion that it is not the technology itself, nor even the degree to which it is ingrained within a society, but rather how cyber technologies affect force employment that matters.

Strategic Theory, Political Motivation, Operational Environment

Strategy is about consequences (Freedman 2013; Gray 2015). Strategy is the means by which a particular end—in the context of national security, a political end—is sought. The means are selected based on assumptions about their level of appropriateness and/or on assumptions about their likely success (Gray 2015). Strategic effect is not, therefore, about the nature of the means itself. Strategic effect, properly understood, is about the consequences of a given means in regard to the desired end.

To support risk assessment, policy selection, and the crafting of strategy, a conceptual framework for understanding the effects of cyber technologies on national security must be predicated on strategic theory. Regardless of the level of damage inflicted, force employment, even the employment of cyber force, is only strategic if it generates effects on an identified political end. Until recently, this point went largely ignored: "Cyber is now recognized as an operational domain, but the theory that should explain it strategically is very largely missing" (Lovelace 2013, p. iii). Thus, the first strategically important question is this: which ends might the means of cyber technologies affect?

The preliminarily answer to that question is contained in 'The DoD cyber strategy' (2015). Cyber technologies can and do affect the American economy. They can and do affect American values. They can and do affect the sovereign functioning of the American government. In short, cyber technologies affect three of the most primary U.S. political objectives: the sustainment and promotion of free market economics, the expression and protection of individual freedom and liberty, and the expression and protection of political independence.

Cyber technologies provide the backbone for the modern global economy. The expansion of the free market economy to include the global exchange of goods and services was produced by, and depends on, cyber technologies. Cyber technologies cut the cost of international communication, and allow for the high levels of coordination and cooperation necessary for the distributed production of goods, efficient supply chains, and increased business productivity. Cyber technologies have done for America's economy what maritime technologies did for Britain's—put it atop the global economy. This situation, this end, pays dividends to the United States, both in terms of material benefit and in socializing the world to America's economic principles.

Cyber technologies support the expression and protection of American values, including freedom of the press, freedom of assembly, and political activism. They support science and research; in fact, they were created to support these endeavors. They also support art and literature. Americans connect to their communities, and even forge communities, via cyber technologies. From the boardroom to the classroom, from the town hall to the high-school dance hall, evidence of these connections abounds. In the 21st century, cyber technologies give life to "We the people…"—our defining political end.

From the mundane to the critical, cyber technologies facilitate the execution of local, state, and federal governments' sovereign authority. Tax records, the control of traffic in the air and on the ground, emergency-response systems, and court proceedings are all executed via cyber technologies. As 'The DoD cyber strategy' (2015) makes clear, so too are the command and control systems of America's armed services—not to mention its intelligence enterprise. Cyber technologies play a critical role in the protection and exercise of U.S. independence, the end that guarantees the previous two roles.

The second strategically important question is: how might cyber means affect those ends? Admiral Rogers provides the logic of the answer—by contesting America's ability to use cyber technologies to those ends (Rogers 2015). Rogers's argument that cyber technologies alter how militaries fight and defend, how and when militaries come into contact with one another, and how military force is generated and sustained suggests that the strategic effects of cyber technologies will be a product of their effect on an actor's use of cyberspace (2015). 'Beyond the build' (2015) presents a world in which the strategic effects of the use of cyber technologies are the result of actions on the part of an adversary to deny the U.S. use of cyberspace to achieve the three political ends listed above.

Based on Rogers' logic, a conceptual framework for understanding cyber ought to be informed by an inventory and evaluation of those actors that would seek to challenge U.S. political objectives (2015). Challenges might be inherent, the product of a fundamental disagreement about the ideological or normative value of the objective. Challenges might also be based on a desired redistribution of the benefits of the political objectives, born out of a desire to capture a larger portion of the gains currently enjoyed by the United States. Thus the crafting of a conceptual framework and the use of said framework to understand the strategic environment both involve answering a third strategically important question: what ends do various nation-states, international governmental organizations, non-governmental organizations, corporations, criminals, hacktivists, terrorists, and other actors in the international system seek?

An appreciation of the operational context is the final component of the needed conceptual framework. As is clear from the cyber debates, 'The DoD cyber strategy' (2015), and 'Beyond the build' (Rogers 2015), the operational context is complex and interwoven. Appreciating it, however, reduces to a single measure—the distribution of cyber power. Based on Rogers's logic and a definition provided by Colin Gray, cyber power is the ability to use cyberspace to achieve one's objectives or deny others the ability use cyberspace to achieve their objectives (Rogers 2015; Gray 2013). Cyber power is and will be a product of the cyber capabilities of a potential attacker, its target, and the characteristics of the cyber domain in which they interact. Understanding the operational context requires an assessment of how cyber technologies affect the relative capabilities of various actors in relation to their identified objective.

When 'The DoD cyber strategy' (2015) and 'Beyond the build' (Rogers 2015) are connected to strategic theory, a general conceptual framework (one based on the need to reference the political motivations of key actors and the specifics of the operational context) takes form. What emerges is a model in which the cyber domain shares significant commonalities with the maritime domain. The strategic effects of cyberspace mirror the strategic effects of the seas. Like the seas, cyberspace represents a resource, a medium for transport and exchange, a medium for

information and the spread of ideas, and a medium upon which and from which to project power (Till 2009). Like the seas, cyber at some point affects every aspect of modern life. Like the seas, cyber has a direct effect on economic health and prowess; access to cyber for digital trade also mirrors the use of sea lanes for physical trade. Like the use of the seas, the use of cyber for the achievement of national security objectives requires committed investment in the resources and skills necessary to outperform others. Equating the cyber domain to the maritime domain anchors the conceptual framework for understanding cyber's effects on national security. It also suggests that much work is left to be done to fully develop the needed conceptual framework.

Dicta to Build Upon

This article does not provide a finished conceptual framework for understanding the effects of cyber technologies. It does, however, attempt to move the process forward. In the spirit of continuing that process, the following dicta are offered. Built on the insights of the cyber debates, the foundation provided by 'The DoD cyber strategy' (2015), Admiral Rogers' 'Beyond the build' (2015), and the argument above, these dicta seek to sketch out the strategic core of the framework and highlight where it ought to be more fully developed.

- Dicta 1: Cyber is its own domain; but, at the same time, it transcends and affects the other domains. Success/victory/security will go to those who marshal and integrate their efforts.
- Dicta 2: Cyber does not change the nature of competition, conflict, or war. Each is about an actor's pursuit of an identified objective.
- Dicta 3: Cyberspace does not alter strategic theory. The strategic effects of cyber technologies are based on their consequences for the actors that use them.
- Dicta 4: As an operational domain, cyber is analogous to the maritime domain. Power may be employed in, projected from, or projected into cyberspace.
- Dicta 5: Weaponized cyber technologies are and will be significant at the operational and tactical levels. They are enablers of other weapons and affect force employment.
- Dicta 6: Cyber technologies have no immediate and little short-term strategic effects, but they do have the potential for dramatic long-term, standalone strategic effects.
- Dicta 7: Cyber power is a function of relative capabilities and is expressed as an actor's ability to use cyber to pursue its objectives or to deny others the ability to use cyber to achieve theirs.

Conclusion

Conrad Crane, Chief of Historical Services for the Army Heritage and Education Center at the Army War College, argues there are two types of warfare—asymmetrical and stupid (Crane 2014). Cyber technologies do nothing to change that. Nor do they do anything to alter the fundamental nature of conflict, including war, in the international system. Crafting a conceptual framework for understanding the effects of cyber technologies on national security helps to ensure that the U.S. successfully employs cyber technologies to win the asymmetrical wars of the future.

Crafting a framework to understand, evaluate, plan for, and manipulate cyberspace and cyber technologies in the pursuit of national security is critical—but it is not enough. It does not guarantee success. The preliminary conceptual framework offered here captures the

overwhelming complexity of the role cyber technologies play in national security. As the conceptual framework is further developed, and as cyber technologies become ever more prevalent (considering the coming 'Internet of things'), the complex, interwoven dynamics faced by policymakers and practitioners will expand exponentially. Thus, even with the best framework for cyber, it will still be possible to engage in the second type of warfare, the stupid variety.

To help avoid this potential for stupidity, it is important to consider how the U.S. can synchronize, integrate, and de-conflict those national-security policies and activities that affect or are affected by the cyber domain. To that end, simultaneous to the crafting of a conceptual framework, the crafting of the Title 10 authorities and command structures to execute within it ought to occur— including the elevation of U.S. Cyber Command to a full combatant command.

References

Applegate, S 2013, 'The dawn of kinetic cyber', *Proceedings of the 5th International Conference on Cyber Conflict*, eds. K. Podins, M. Maybaum, J. Stinissen, NATO, Tallinn, viewed 03 April 2016, < https://ccdcoe.org/cycon/2013/proceedings/d2r1s4_applegate.pdf>.

Arquilla, J & Ronfeldt, D 1993, 'Cyberwar is coming!', *Comparative Strategy*, vol. 12, no. 2, pp. 141-65.

Babb, C 2015, 'New military cyber program visualizes invisible attacks', Voice of America, viewed 31 March 2016, <http://www.voanews.com/content/military-program-visualizes-invisible-attacks/2853093.html>.

Brantly, A 2014, 'Cyber actions by state actors: motivation and utility', *International Journal of Intelligence and CounterIntelligence*, vol. 27, no. 3, pp. 465-84.

Cavelty, M 2011, 'Unraveling the Stuxnet effect: of much persistence and little change in the cyber threats debate', *Military and Strategic Affairs*, vol. 3, no. 3, pp. 11-19.

Clark, W & Levin, P 2009, 'Securing the information highway: how to enhance the United States' electronic defenses', *Foreign Affairs*, vol. 88, no. 6, pp. 2-10.

Clausewitz, C 1971. *On War*, eds. M Howard & P Paret, Princeton University Press, Princeton, NJ, U.S.A.

Colarik, A & Janczewski, L 2012, 'Establishing cyber warfare doctrine', *Journal of Strategic Security*, vol. 5, no. 1, pp. 31-48.

Crane, C 2014, 'Observations on the long war', War on the Rocks, viewed 05 April 2016, <http://warontherocks.com/2014/09/observations-on-the-long-war/>.

Department of Defense 2015, 'The DoD cyber strategy', Washington, viewed 18 March 2016, <http://www.defense.gov/Portals/1/features/2015/0415_cyberstrategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf>.

Farwell, J & Rohozinski, R 2012, 'Stuxnet and the future of cyber war', *Survival: Global Politics and Strategy*, vol. 53, no. 1, pp. 23-40.

Fraser, T 2016, 'Automated program analysis for cybersecurity', Defense Advanced Research Projects Agency, viewed 31 March 2016, <http://www.darpa.mil/program/automated-program-analysis-for-cybersecurity>.

Freedberg, S 2015, 'Navy rolls out CYBERSAFE: "Our operational network is under fire"', Breaking Defense, viewed 05 April 2016, <http://breakingdefense.com/2015/04/navy-rolls-out-cybersafe/>.

——2016, 'Faster than thought: DARPA, artificial intelligence, & the third offset strategy', Breaking Defense, viewed 31 March 2016, <http://breakingdefense.com/2016/02/faster-than-thought-darpa-artificial-intelligence-the-third-offset-strategy/>.

Freedman, L 2013. *Strategy, a history*. Oxford University Press, Oxford, U.K.

Gartzke, E 2013, 'The myth of cyberwar: bringing war in cyberspace back down to earth', *International Security*, vol. 38, no. 2, pp. 41-73.

Gray, C 2013, *Making sense of cyber power: why the sky is not falling*, U.S. Army War College, Carlisle Barracks, PA, U.S.A.

——2015. *The future of strategy*, Polity, Malden, MA, U.S.A.

Heinl, C 2014, 'Artificial (intelligent) agents and active cyber defense: policy implications', *Proceedings of the 6th International Conference on Cyber Conflict*, eds. P. Brangetto, M. Maybaum, and J. Stinissen, NATO, Tallinn, pp. 3-66.

Hjortdal, M 2011, 'China's use of cyber warfare: espionage meets strategic deterrence', *Journal of Strategic Security*, vol. 4, no. 2, pp. 1-24.

Jacobsen, J 2014, 'The cyberwar mirage and the utility of cyberattacks in war: how to make real use of Clausewitz in the age of cyberspace', Danish Institute for International Studies, viewed 02 April 2016, <https://www.ciaonet.org/attachments/25101/uploads>.

Keller, J 2015, 'Air Force seeks to shield military avionics from computer hackers', Military and Aerospace Electronics, viewed 05 April 2016, <http://www.militaryaerospace.com/articles/print/volume-26/issue-5/news/news/air-force-seeks-to-shield-military-avionics-from-computer-hackers.html>.

Kello, L 2013, 'The meaning of the cyber revolution: perils to theory and statecraft', *International Security*, vol. 38, no. 2, pp. 7-40.

Keromytis, A 2016, 'Active cyber defense', Defense Advanced Research Projects Agency, viewed 31 March 2016, <http://www.darpa.mil/program/active-cyber-defense>.

Lindsay, J 2014a, 'Correspondence: a cyber disagreement', *International Security*, vol. 39, no. 2, pp. 181-192.

——2014b, 'The impact of China on cybersecurity: fiction and friction', *International Security*, vol. 39, no. 3, pp. 7-47.

Libicki, M 2009. *Cyberdeterrence and Cyberwar*, RAND, Santa Monica, CA, U.S.A.

Lovelace, D 2013, 'Forward', *Making sense of cyber power: why the sky is not falling*, by C Gray, U.S. Army War College, Carlisle Barracks, PA, U.S.A.

Lupovici, A 2011, 'Cyber warfare and deterrence: trends and challenges in research', *Military and Strategic Affairs*, vol. 3, no. 3, pp. 49-62.

Osborn, K 2015, 'Army weapons developers think about how future enemies will attack', Scout Warrior, viewed 05 April 2016, <http://www.scout.com/military/warrior/story/1608274-army-acquisition-think-like-the-enemy>.

Reed, T 2005, *At the abyss: an insider's history of the Cold War*, Random House, New York, U.S.A.

Reuters 2012, 'Naval hackers broke into the F-35 logistics system exposing more huge weaknesses', *Business Insider*, 16 November 2012, viewed 05 April 2016, <http://www.businessinsider.com/naval-hackers-broke-into-the-f-35-logistics-system-exposing-more-huge-weaknesses-2012-11>.

Richards, R 2016, 'High-assurance cyber military systems', Defense Advanced Research Projects Agency, viewed 31 March 2016, <http://www.darpa.mil/program/high-assurance-cyber-military-systems>.

Rid, T 2013, 'Cyberwar and peace', *Foreign Affairs*, vol. 92, no. 6, pp. 77-87.

Rogers, M 2015, 'Beyond the build: delivering outcomes through cyberspace: the commander's vision and guidance for US cyber command', United States Cyber Command, Fort George Meade, viewed 18 March 2016, <http://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/docs/US-Cyber-Command-Commanders-Vision.pdf>.

Rosenzweig, P 2013, *Cyber warfare: how conflicts in cyberspace are challenging America and changing the world*, Praeger, Santa Barbara, CA, U.S.A.

Samaan, J 2010, 'Cyber command: the rift in US military cyberstrategy', *The RUSI Journal*, vol. 155, no. 6, pp. 16-21.

Shafqat, N & Masood, A 2016, 'Comparative analysis of various national cyber security strategies', *International Journal of Computer Science and Information Security*, vol. 14, no. 1, pp. 129-36.