Naval War College Review

Volume 67
Number 2 *Spring*

Article 7

2014

Cyber War, Cybered Conflict, and the Maritime Domain

Peter Dombrowski

Chris C. Demchak

CYBER WAR, CYBERED CONFLICT, AND THE MARITIME DOMAIN

Peter Dombrowski and Chris C. Demchak

It has been well over a decade since the first "prophets" of information warfare proclaimed a new age of conflict fought not just on air, sea, and land but with electrons in what came to be known as "cyberspace."[1] Since these early predictions, many incidents have confirmed that criminals, random hackers, and government-sanctioned specialists can wreak havoc on governments, military communications systems, and corporations. The Stuxnet worm alone helped delay—by months, perhaps years—the long-standing efforts of Iran to acquire sufficient nuclear material to build nuclear weapons.[2] Recent revelations of hacking campaigns against such publications as the *Wall Street Journal* and *New York Times* have broadened concerns to include even the integrity of American democratic institutions.[3] Meanwhile, the commander of U.S. Cyber Command has characterized cyber attacks designed to gain access to the intellectual property of American corporations as the "greatest transfer of wealth in human history."[4]

How cyber assaults and government responses have been interpreted is not uniform, however, especially with regard to whether the world will eventually engage in "cyber war."[5] There is a community of scholars and analysts who argue that cyber war will not happen or that the impact of cyberspace on armed conflict will be limited.[6] Others in the broad field of security studies, traditional computer science, or corporate communities claim that while some form of conflict is happening, government officials, military officers, and legislators are suffering from "threat inflation." They argue that hyperbolic projections are leading to bad policy decisions, especially with regard to specific adversaries, and that there has been overinvestment in offensive cyber weapons rather than prudent defensive measures.[7] A best-selling nonfiction book has been criticized for contributing

Naval War College Review, Vol. 67 [2014], No. 2, Art. 7

unnecessarily to public fears about the potential for cyber warfare.[8] Many of these critics argue that what are being called "cyber attacks" are really instances of espionage, allowed by international law, or simply crime, which is not the mission area of the nation's military services.[9] Some analysts detect the influence of the military-industrial complex on policy debates. If hackers, official or not, from China and Russia, terrorists, and criminals use the Internet to penetrate U.S government systems, contractors see opportunities for increased revenue. As two observers of cyberspace argue, "There's an arms race in cyberspace, and a massively exploding new cyber-industrial complex that serves it."[10]

Our position on this ongoing debate is that neither side has it right. Those who have hyped cyber war as a completely new phenomenon or insist that cyber threats are impossible to anticipate have missed key continuities with the past. Especially missing is an underlying understanding about how humans and technologies have evolved and how the ways in which we analyze the cyber arena will contribute to future conflicts. Despite the complexity of cyberspace, it is possible to understand the broad trends in conflict and institutional responses. Those who dismiss cyber war as mere hype or as driven by potential profits dismiss much too quickly growing evidence of the importance of cyber operations for the Navy and the nation.

Many participants in the debates on cyber conflict demonstrate insufficient understanding of cyberspace. In particular, they do not demonstrate sufficient command of the level of integration across public and private systems, across sectors from economic to defense, and across levels of criticality in key societal functions. For example, in earlier eras, one or even many bank heists could not have taken down significant portions of the American financial system. In contrast, what has been characterized as a single-digit mistake crashed the New York Stock Exchange for several hours in 2010.[11] In August 2013, the Amazon "cloud" suddenly stopped working for hours, with no public explanation; the best estimate is that during that period 40 percent of the Internet vanished in the United States—that is, there was simply 40 percent less activity.[12] What is labeled espionage by observers seeing only a few incidents at a time can have cumulative effects on deeply integrated national systems. Distinguishing between what is crime and what espionage is not easy, nor is determining what actually represents a long-term campaign of deceptive attacks. To make such distinctions clearly requires recognition, in the first place, of the implications of extreme integration for security in modern society. Critics often have considerable difficulty with this cognitive leap—which is particularly unfortunate, as many of these critics have considerable influence in national and international policy.

In this article we will attempt to explain the challenges and opportunities of cyberspace for U.S. national security, especially naval forces. First, we will

examine how cyberspace has affected conflict over the last decade and how it will do so in the coming decades. Next, we will review how the U.S. government has responded to the increasing number and variety of attacks on its own institutions and on the private sector at home and abroad. Third, we will focus on the institutional evolution of the U.S. Navy as it attempts to fulfill the responsibilities assigned to it by national-level strategies within the framework of its traditional missions, capabilities, and culture. Finally, we will examine the specific systemic operational challenges and opportunities posed by cyber operations. Our intent is to help naval scholars, analysts, and operators begin understanding the new world of cybered conflict in the maritime environment.[13]

CONFLICT AND CYBERSPACE

Cyberspace has opened up new avenues of conflict, added layers of complexity to existing tactics and operations, and become increasingly influential in the strategic calculus of several major powers in the international system. Cyberspace is neither totally new nor totally out of control, but it is now a global socio-technical-economic system with major effects on the physical, economic, and societal security of nations. Cyberspace has made it much too easy for aggressive states and nonstate actors to reach remotely into other societies, threaten critical government systems, and affect essential operations of both public and private institutions.[14] The question is how to characterize this new reality.

Although "cyber war" has entered into the common lexicon, we generally avoid the term, because it misleads more than it illuminates. Instead, we prefer the term "cybered conflict."[15] The phrase characterizes the essential nature of modern military operations, from peacetime to high-intensity warfare. Cyber activities by military forces (and often intelligence agencies, law-enforcement organizations, and associated departments) take place in all types of conflict, during all phases of military operations, and at all levels of war. From our perspective, cybered conflict characterizes the whole spectrum of old and new forms of conflict born of, enabled through, or dramatically altered by cyberspace.

All Phases of Military Operations Are Now Cybered

U.S. joint doctrine posits a notional six-phase model of joint and combined military operations, ranging from Phase Zero ("Shaping") through Phase III ("Dominate," or "breaking the enemy's will for organized resistance or, in non-combat situations, control of the operational environment") to Phase V ("Enable Civil Authority").[16] For our purposes here, the details of what occurs in each phase are less important than the fact that cyber tools, skills, units, and perceptions play roles in all of them. Whether shaping the future operating environment by preparing for long-running conflicts of varying tempos and effects or for cybered conflicts ranging from disruptions of critical systems to cyber-enabled

Naval War College Review, Vol. 67 [2014], No. 2, Art. 7

destruction of military forces, American military specialists (including naval officers and sailors) and their civilian counterparts from the intelligence agencies and the Departments of Justice and Homeland Security use a wide range of offensive and defensive tools to support actions in the physical world. At each stage they also have to defend against the efforts of adversaries—whether official state representatives, terrorists, or criminals—trying to thwart American or allied operations or to exploit them for their own ends.

All Levels of War Are Now Cybered

Classic national-security scholarship as taught at institutions of professional military education in the United States divides thinking about war into three levels: tactics, operations, and strategy. According to joint doctrine, "strategy is a prudent idea or set of ideas for employing the instruments of national power in a synchronized and integrated fashion to achieve theater and multinational objectives." By contrast, "tactics is the employment and ordered arrangement of forces in relation to each other." For its part, "the operational level links strategy and tactics by establishing operational objectives needed to achieve the military end states and strategic objectives. It sequences tactical actions to achieve objectives."[17]

Our position is again straightforward. Cybered conflict enters into play at all three levels and connects them iteratively and systemically. At the strategic level, national policies must provide commanders with the goals for cyberspace (and to which cyber operations must contribute) and guidance regarding how cyber instruments may be used consistent with national law, as well as means to acquire and operate those tools. At the tactical level, commanders must fight battles using not only kinetic means but also offensive and defensive cyber instruments. As joint doctrine observes, all three levels overlap during the execution of a military operation; therefore, "commanders and their staffs at all levels must anticipate how their plans, operations, and actions may impact the other levels (those above and those below)."[18]

All Types of Conflict Are Now Cybered

Typologies of conflict are many. The Department of Defense defines nineteen types of warfare, ranging from acoustic to undersea.[19] These various definitions usually speak to the environment, factors, and conditions that must be understood to apply combat power successfully, protect the force, or complete the mission. These elements might include enemy and friendly armed forces, infrastructure, weather, terrain, and the electromagnetic spectrum within operational zones and areas of interest.[20]

U.S. military forces now prepare to fight in five domains:[21] land, sea, air, space, and cyber. In 2011 "cyber" was added—not without some modest resistance—as the fifth domain, a nonphysical arena of military conflict.[22]

We believe, however, that for security and military purposes cyberspace is not a domain but a substrate. In our usage, a "substrate" is an underlying layer on which modern society is built. Cyberspace uniquely underpins all four other war-fighting domains. This substrate has a topology that is largely and (surprisingly to some) territorial. Our argument that cyberspace is a substrate is thus contrary to official usage and to increasingly commonplace assertions that cyberspace is a domain.[23] One reason that cyberspace is in fact not strictly a domain is that it is a built environment—imagined, created, developed, sustained, and extended by human intentions and actions. One analyst has noted "the generative capacity for unrelated and unaccredited audiences to build and distribute code and content through the Internet."[24] As Michael Hayden, a retired Air Force general and former director of the Central Intelligence Agency, once pointed out to an audience of technologists, "God made the other four [domains]. You made the last one. God did a better job."[25]

One implication of cyberspace's being a built environment is that it can be unbuilt, remodeled, and perhaps in an extreme case even destroyed (say, by electromagnetic pulse), at least temporarily and within spatial limits. This logic, then, allows for the notion that an Internet "kill switch" exists or can be created. No less an authority than the founder and chairman of Microsoft, Bill Gates, acknowledges that the Internet can be "switched off": "It's not that hard to shut the Internet down if you have military power where you can tell people that's what's going to happen," Gates said. "Whenever you do something extraordinary like that you're sort of showing people you're afraid of the truth getting out, so it's a very difficult tactic, but certainly it can be shut off."[26] In several recent conflicts, governments, including those of Egypt and Syria, have in effect flipped the switch to turn off Internet access, however imperfectly, for their societies. The strategic, operational, and tactical objectives of these acts are unclear at this point. Moreover, the effects have been temporary, as experts inside and outside the countries work to make alternative connections.

Since World War II, the trajectory of U.S. military planning has favored joint operations, with the services fighting together from their respective domains. As we will discuss below, the services and a number of government agencies (for example, the National Security Agency, or NSA) share responsibility for operating in cyberspace, defending military and civilian systems and infrastructure, and, ultimately, conducting cyber operations as part of kinetic operations. But unlike the four other official war-fighting domains recognized by the government, cyberspace, as a substrate, as we have noted, intersects with all the others, and it is vulnerable to widespread disruption. This makes cyberspace all the more valuable; it is in effect the technological high ground, for not only the military and intelligence services but government, civilian, and commercial sectors as well.

Naval War College Review, Vol. 67 [2014], No. 2, Art. 7

Cyberspace is thus not a separate conflict space or host to a particular type of conflict. Cybered conflict occurs along a spectrum that includes conflicts from large to small—total war, small wars, wars of choice, and a host of others. In the next twenty years, the tools of cyberspace will become so ubiquitous that we prefer to use the adjective "cybered," since "cyber" is likely to be taken for granted and abandoned. In the meantime, cyberspace is changing how governments and their militaries and nonstate actors fight wars and conflicts. Organizing and operating in joint, interagency, and combined (with friends, partners, and allies) terms for cybered conflicts are not only sensible but strategically and operationally essential for success.

NATIONAL RESPONSES TO THE CHALLENGES OF CYBERSPACE

Given their decades-old and growing dependence on information and communications technologies for economic dominance and military power, the U.S. military and government agencies have slowly developed policies, strategies, and organizations to meet the challenges and possibilities of cyberspace. High-level recognition of threats emanating from "cyber" began as early as the 1990s. In 1996 President William Clinton's Executive Order 13010 created the President's Commission on Critical Infrastructure Protection, which included threats to the nation's economic and national security from cyber attacks within the scope of its activities.[27] Two years later, on the basis of the commission's recommendations, Presidential Decision Directive 63 established several cyber security–related organizations, largely focused on malicious hackers or criminals who could threaten critical national infrastructure.

The full extent of cyber threats became pressing after 9/11. That terrorists could use the web to organize themselves to attack the United States and other adversaries was becoming clear. In one high-profile example, documents found in abandoned Al Qaeda houses after the U.S. invasion of Afghanistan included guidance from Osama Bin Laden on how to use electronic means to continue the jihad and suggesting that 90 percent of Al Qaeda's future efforts would involve cyberspace.[28]

Chinese strategists have begun to develop their own concepts of cyber conflict, focusing on major state adversaries, including the United States.[29] The Persian Gulf War of 1991 demonstrated to China (and other close observers) how high-technology militaries could defeat adversaries who had advantages in troop strength. The stunning results of U.S. operations against numerically superior forces presented a major challenge to China's perception of its own advantages in future conflict—massed assets ranging from manpower to ships and missiles. According to some scholars, China's search for a compensating strategy to match the United States led it to rediscover Sun Tzu's understanding of "indirect warfare."[30]

Several Chinese colonels even proposed a concept of "unconstrained warfare," a campaign that begins long before any armed conflict is apparent. This "warfare" seeks to disrupt potential enemies using the vulnerabilities of their (real or potential) information systems, without regard for international norms or laws. As a Western analyst concludes, "China [now] has the most extensive and most practiced cyber-warfare capabilities in Asia, although the technical expertise is very uneven."[31]

By 2003, President George W. Bush signed several strategy documents focusing specifically on cyberspace. Rather than subsuming specific issues under a general concern for critical infrastructure, as President Clinton had done, the *National Strategy to Secure Cyberspace* and the *Comprehensive National Cybersecurity Initiative* specifically addressed the need to secure cyberspace and presented that mission as a systemic challenge. These documents divided responsibility for national cyber security among the Department of Defense (DoD), the newly established Department of Homeland Security, and the White House itself. While the White House retained overall policy authority, Homeland Security was given the task of ensuring "critical infrastructure protection" of the homeland—but in terms of a "coordinating," not regulating or operating, mission. DoD was charged with protecting its own global grid of computers and communications systems but received no authority to inform or protect anyone else's network, even if their health determined whether the DoD's own Global Information Grid could be protected. The Department of Defense and its subagencies rely heavily on commercial networks to transfer data across the globe;[32] nevertheless, individual federal agencies, states, and private corporations were left by and large to defend themselves.[33]

Even with the increased attention by the Bush administration to cyber security, the breadth of the nation's vulnerability was not yet fully apparent. In 2003 only 60 percent of the American population owned computers, and only 50 percent had personal access to an Internet connection.[34] Pressure on officials and policy makers would increase as more citizens, businesses, and government activities came to depend on uninterrupted information and assured access to cyberspace, to include the Internet, the World Wide Web, and over time, peer-to-peer computer networks.

Toward the end of the first decade of the 2000s, the unsettling successes of the cyber penetrations, extractions, and remote "backdoor" operations mounted steadily across DoD and other agencies.[35] Existing ("legacy") information-assurance policies, programs, and tools were failing to stem the tide of attacks. To make matters worse, a growing portion of publicly revealed data on cyber attacks pointed toward the existence of a small but global population of highly skilled, determined, and persistent "wicked actors."[36] Their successes were often

discovered only months or years later, long after the damage had been done. In 2006, the Bush administration issued another series of documents to clarify top-level policies, procedures, and responsibilities. The *National Security Strategy* and *Quadrennial Defense Review* outlined the broad bases for U.S. government policies for dealing with cyber war and cyber threats more generally, within the wider context of conventional threats and the evolving international environment.[37]

Most notably, the Department of Defense published its *National Military Strategy for Cyberspace Operations,* which assigned U.S. Strategic Command (STRATCOM) and the Joint Staff to develop an implementation plan for the defense of cyberspace.[38] The concept of a joint command to deal with cyberspace gradually emerged from this planning effort. The timing of the decision to create a unified cyber command was influenced by the well-intentioned miscalculation of several senior Air Force leaders who in 2005–2006 unilaterally declared their service the lead agency for cyber security. Publicity associated with an Air Force effort to develop a national cyber command may have prompted Robert Gates, then Secretary of Defense, to become involved directly in laying the foundation for a DoD-wide command for cyberspace operations.[39] Meanwhile, the other services, including the Navy, had begun preparing to create cyber-security and -warfare units of their own.[40]

During roughly the same period, 2004–2007, General James E. Cartwright, as commander of STRATCOM, was struck by the magnitude of ongoing assaults on DoD networks. He became concerned by massive losses of classified internal data and by the constant flood of attacks experienced. General Cartwright's efforts to protect STRATCOM and DoD itself from cyber threats fueled the design of a major command devoted to cyberspace. In particular, he argued that the new organization should be a "subunified" command (that is, a subordinate unified command, reporting in this case to STRATCOM) so that it would be less likely to be marginalized. General Cartwright continued to sponsor the idea of a national cyber command when he became the vice chairman of the Joint Chiefs of Staff in 2007.[41] It would, however, take more than the interest of a vice chief to create such a command.

In late 2008 a computer "worm" infected unclassified and classified American networks, traveling via USB memory sticks from infected computers in Afghanistan to DoD systems across the globe. The worm opened so-called back doors that potentially allowed adversaries to control infected systems. Upon discovering the breach, DoD rapidly closed down networks and restricted the use of USB sticks and most removable media, to stop reinfection.[42] This infection was followed closely by the "Conficker" worm, which targeted the Microsoft Windows operating system used by the armed services of many NATO members, including the United States. Conficker spread quickly and opened new back

doors accessible to unknown attackers.[43] For a period, someone, somewhere, had remote access to computer networks on NATO warships in port and to systems used by combat units in the field.[44] These back-to-back infections changed the priority given cyber security by the White House and DoD.[45]

By the spring of 2009, experts generally accepted that protecting the government, and particularly DoD, against Conficker and a host of other cyber threats would require major new steps.[46] During the first year of President Barack Obama's administration, the urgency increased substantially; investigative reporting has revealed that the president and his closest national-security team were not only working on defensive measures but contemplating offensive actions using cyber weapons.[47] Upon taking office the Obama administration ordered a "60-Day Cyberspace Policy Review," spearheaded by Melissa Hathaway, a former Bush administration cyber-security expert, to shape the fundamentals for future cyber-security strategic and organizational changes.[48] In May 2009, with the review complete, President Obama declared cyberspace to be a first-tier priority for national security. The White House *Cyberspace Policy Review* stated that "America's failure to protect cyberspace is one of the most urgent national security problems facing the new administration."[49]

In June 2009, Secretary of Defense Gates announced the formation of a new U.S. Cyber Command (CYBERCOM) as a subunified command subordinate to STRATCOM and collocated it with the government's main source of computer and electronic expertise, the NSA. To ease the flow of information between the two organizations, the director of NSA was to be "dual-hatted" as the commander of CYBERCOM. The arrangement allowed at least one clear point where authorities granted by Title 10 and Title 50 of the *U.S. Code* could be balanced and decisive actions taken.[50] Furthermore, a single leader could review all operations, emerging trends, and long-range effects to develop and coordinate comprehensive tactics, operations, and strategies. In principle, then, the organizational structure allowed the new command to deal with the complexity of cybered conflict. "Cyber warriors" in Cyber Command and the intelligence and information experts of the National Security Agency would in this way more readily collaborate to detect, track, thwart, or stop adversaries crippling DoD's operational readiness.[51]

The individual military services had equally important roles in foreseeing threats, defending their mission areas and forces, and disrupting cyber attacks "forward." In a June 2009 DoD memorandum, Secretary Gates asked each of the service secretaries to establish a component to support Cyber Command, a component that "possesses the required technical capability [to secure freedom of action in cyberspace] and remains focused on the integration of cyberspace operations. Further, this command must be capable of synchronizing war-fighting

effects across the global security environment as well as providing support to civil authorities and international partners."[52] Each service was to stand up an interim command by 1 October 2009 and to have it fully operational by 1 October 2010.

The services were allowed to design their own organizations and to incorporate skills, tools, and units as they saw fit, as long as all were able to contribute to the mission of U.S. Cyber Command. The Navy and Air Force in particular had already made considerable progress, in anticipation of the order. Meanwhile, the Department of Homeland Security was instructed to reinvigorate its efforts to persuade the critical infrastructure community—largely privately held—to improve its defenses against remote attacks. By midsummer of 2010, all the services had established rudimentary cyber commands. The process of reconciling differences in structure, guidance, and mission then began in earnest. This process continues unabated today, and we will later discuss its implications for the Navy.

In May 2011 the Obama administration outlined its publicly releasable, external policies in the *International Strategy for Cyberspace;*[53] the Secretary of Defense issued the *Department of Defense Strategy for Operating in Cyberspace* two months later.[54] Each statement aimed to inform the American public and the publics of allied states that the United States is taking cyber threats seriously. These documents also signaled to adversaries that preying on American targets would no longer be easy or risk-free. The U.S. government would defend itself and strike back as necessary.[55]

THE NAVY AND CYBERSPACE

At the time of the July 2009 Gates memo, the Navy was already designing new organizations capable of meeting cyber challenges. The Navy had spent most of the 2000–2008 period trying to understand the threats posed by cyber attacks and intrusions.[56] It had established a task force to study how attacks through cyberspace were affecting Navy assets and operational readiness. The task force's members understood early that the service needed to identify cyber-capable personnel with skill sets ranging from intelligence techniques to network systems and electronic warfare. In the fall of 2009, Admiral Gary Roughead, then Chief of Naval Operations, stood up Fleet Cyber Command and Tenth Fleet.[57]

The new cyber-focused command needed to provide the entire Navy with the specific missions, guidance, technical tools, and unit-level organizational structures necessary for cyber defense and offense. However, in doing so it had to work within the traditional fleet structure, to be compatible with the structures and missions of existing numbered fleets, and to serve as the Navy component supporting U.S. Cyber Command as a whole. The task force's members had also known—drawing on the longtime, well-established relationship between the U.S. Navy intelligence community and the National Security Agency—that the

complexity of cyberspace as an operational environment would demand rapid, accurate responses at tempos commensurate with the scale and harm of the threats. These qualities would be exceptionally difficult to achieve if cyber was not mainstreamed across the service. These responses would be nearly impossible to execute rapidly if bureaucratic "silos" were left in place between the Navy and joint intelligence, electronic warfare, network administration, and cryptology, among other specialized organizations.[58]

In January 2010, when Fleet Cyber Command (known as FCC, or Fleet Cyber) was declared operational as the Navy's component of CYBERCOM, its organization was unique among its service counterparts. Rather than splitting combat-support functions, such as intelligence, from operational combat missions as other services have done, its structure integrates them and thereby supports both U.S. Cyber Command and the Navy's own requirements. A single flag officer leads not only FCC, an Echelon 2 command (i.e., reporting directly to the Chief of Naval Operations), but also the newly recommissioned Tenth Fleet, as a subordinate Echelon 3 command—an institutional design intended to allow the Navy to act quickly in a hostile and deeply cybered world.[59]

Nonetheless, and despite the best efforts of their designers, leaders, and champions, Fleet Cyber Command and Tenth Fleet have not found it easy to meet the challenges of cyberspace. First, both have themselves been assaulted from cyberspace even as they experience the normal growing pains of a new command structure. Second, long-standing internal divisions in the naval service have complicated their manning, training, equipment, employment, and assessment. Inside and outside the Navy numerous debates are ongoing about what constitutes the cybered conflict space and even whether it is truly a "domain," as designated by DoD. Among its critics are some who fear change, some (a small number) who understand computer systems, and even optimists convinced that a fully integrated approach to cyberspace would achieve nearly everything that might be done in the physical world. In brief, like much of the U.S. government, CYBERCOM, and its counterparts in the other services, Fleet Cyber Command is still learning its own missions, strengths, weaknesses, and evolving opportunities.[60]

In late November 2012 the Navy took several other steps toward sustaining cyber capabilities. The Deputy Chief of Naval Operations for Information Dominance / Director of Naval Intelligence (Vice Admiral Kendall L. Card) and Commander, U.S. Fleet Cyber Command / Tenth Fleet (Vice Admiral Michael S. Rogers) signed three documents:

- *Navy Strategy for Achieving Information Dominance 2013–2017*[61]
- *Navy Cyber Power 2020*[62]
- *Navy Information Dominance Corps Human Capital Strategy 2012–2017*.[63]

Naval War College Review, Vol. 67 [2014], No. 2, Art. 7

Each demonstrates the evolution of Navy thinking about how to serve, survive, and excel in a cybered maritime environment. It is too soon to evaluate fully the Navy's progress in effective cybered conflict. It is time, however, to relate the Navy's thinking to what is coming in the dynamically evolving global cyberspace. Trends already evident across the digitized world will affect future military conflict, the cyber threat environment in the maritime domain, and the Navy's own efforts to establish organizational and operational frameworks for meeting cyber challenges in the near-to-medium term. Several of these trends will impact the Navy's ability to fulfill the "sailing direction" issued by the Chief of Naval Operations, Admiral Jonathan Greenert, that "cyberspace will be operationalized with capabilities that span the electromagnetic spectrum—providing superior awareness and control when and where we need it."[64]

THE CHALLENGES OF CYBERED CONFLICT IN THE MARITIME DOMAIN

What is different about the challenges facing U.S. naval forces during cybered conflicts?[65] How can naval forces contribute to combined and joint operations that include cyber operations? The problem is not just that the cyberspace substrate connects most of the world and allows intrusions from a wide range of state and nonstate actors. Rather, we argue, it is that cyberspace favors the offensive military capabilities of adversaries and enhances their potentially destabilizing effects on the nature and level of interstate conflict in the coming years.[66]

The offense/defense balance in international affairs has long been considered critical to the prospects for the reduction of conflict and the promotion of international peace.[67] Recent scholarship concludes, at least preliminarily, that "innovations in Information and Communication Technology (ICT) allow states to take greater risks and adopt more vigilant or offensive positions toward adversaries. Cyber capabilities do not cause armed conflict, but make decisions to escalate easier and cheaper."[68] Scholars are only now developing a serious research program to understand the impact of offensive cyber instruments on the future of conflict.[69] There are still scholars who remain skeptical about the utility of offense/defense theory for understanding the impact of technological change on war and peace or, more important, the effects of cyber operations. One, for example, argues, "This is not to say that cyber attacks would have no effect, only that they are extremely unlikely to prove strategically decisive. A capability to address cyber threats is then useful, but planning for cyber warfare must be conducted within the larger framework of recognition that these capabilities are not in fact a game changer."[70]

In our view, the "game changing" aspects of cyberspace do not lie in cyber warfare at the high end of the spectrum of conflict. Rather, the strategically decisive

aspects of cyberspace concern the three significant advantages that its current globally unfettered structure offers attackers: relatively risk-free opportunities in the scale, proximity, and precision of cyber "weapons." These advantages make attacks cheaper, easier, and more effective for both state and nonstate actors. While they may be temporary and transitional, they exist now, and in our judgment they will continue to exist for the next fifteen to twenty years.

First, like the superpowers of old, adversaries can readily use the web to scale attacking units from small to large, tightly organized or loosely linked. Further, attackers can use the web for communication, training, supply, and operations, even as they scale up and down and back again. For one example, they can cheaply scale up by buying, or even renting, "botnets" on the global black market. A botnet—a linked network of software hidden in millions of innocent computers—can be commanded to participate in attacks. Today there are hundreds of thousands of botnets in use, for sale, or lying dormant, on machines whose users do not know that they are infected.[71]

Second, to pose a threat, adversaries have no need to move into close physical proximity to collect critical information or to deploy long-range expensive weapons. Relatively high-quality "signals intelligence" is now available to anyone with time and an Internet connection.[72] Third, the precision in targeting is no longer constrained to line-of-sight, blue-water, or over-the-horizon military capabilities. Cyber-enabled attackers can vary the precision of their targeting from a single person to cities, regions, or entire nations.

However, these three factors, notwithstanding the offensive advantages they offer attackers, may also provide opportunities for the U.S. Navy's offensive and defensive cyber operations.

Scale

Given the reliance of global commerce; governments at all levels; and military, intelligence, and law-enforcement organizations on the communication systems and computers associated with cyberspace, the institutional scale required to cause real harm has dropped dramatically.[73] Small organizations—including criminal enterprises, terrorist groups, and subunits of national militaries—can now use the Internet to spy on, harass, and attack with relatively modest investments in personnel and equipment. States with modest cyber resources can achieve disproportionate effects with appropriate tools, skill, and organizational structures. Small states might also achieve asymmetric advantages by investing in cyber instruments or employing proxies with better capabilities.

Small, covert, and even part-time organizations scattered in large enough numbers across the globe can undercut traditional threat and warning indicators employed by U.S. intelligence agencies. The modern military's standard set of such indicators identifies emerging cyber threats much less effectively than it

Naval War College Review, Vol. 67 [2014], No. 2, Art. 7

does conventional attackers. For the Navy, as for the other services and government agencies, it will be even harder to assess the cyber capabilities and intentions of potential adversaries than to evaluate their conventional and nuclear forces. One pressing question urged by such uncertainty is how resilient the Navy can become.

Proximity

Until the modern era, most conflict was confined to visual range.[74] For most of history, the farther an attacker from physical view, the less one could know about whether a given weapon or unit was the right choice to use against it, at that time, in that place. Even during the Cold War only major powers could develop and deploy large numbers of over-the-horizon weapons; they were expensive to build, required considerable long-distance intelligence to be effective, and outstripped standard damage-assessment techniques.

Proximity thus mattered enormously for attackers.[75] Intelligence was (and is) crucial for fighting and winning. Getting up close to look, and in a timely manner, was throughout history the most straightforward way to collect usable information. Critical and timely knowledge—the "signals intelligence" of superpowers and close neighbors—has never, however, been cheap to acquire or easy to validate.[76]

With the global connectivity of cyberspace, however, no longer does an enemy need to move into physical proximity to pose and execute a threat. Now too, adversaries both actual and potential can obtain intelligence inexpensively. If hackers can access a system and gain control of key functions, they can hide successes, elude defenses, and leave behind back doors by which to reenter in the future. Hackers need not be on the same continent as, let alone physically touch, targeted computers.[77]

Often the information that cyber attackers need to target a system is already online, posted for legitimate reasons. Terrorist sites when raided are almost always found to contain caches of maps, specific data, and operationally relevant material on potential targets that had been harvested from publicly accessible Internet sites. Such information is often considered public information that must be provided to citizens, investors, and internal customers. Democratic norms and laws regarding transparency and accountability often encourage or even require government agencies and private enterprises to make available information that would be useful to cyber thieves, spies, and attackers. Public and private cyber-security experts have sought to discourage such "oversharing," but most Western democracies have a long way to go. After the attacks on the United States in September 2001, for example, much public data about nuclear power plants and nation-spanning oil pipelines were removed from public websites

in the United States; such data had already been found in Al Qaeda computers seized in Afghanistan.[78]

While great powers and some sophisticated states, like Israel, still enjoy comparative advantages in signals and various other technical means of collection and assessment, intelligence gaps between these states and their adversaries may be closing. Strategists, planners, and policy makers will eventually need to adapt to this new geostrategic reality of cyberspace.[79] For maritime powers throughout history, forward-deployed fleets have been crucial for defeating land powers. Naval forces operating in theaters far from home could quickly and independently collect information and decide whether and how to act. Only peer maritime powers, and few land-based adversaries, could challenge that powerful capability. The U.S. Navy is still in the business of long-distance power projection. In a cybered world, however, the task is more problematic. The Navy must adapt to the loss of its own proximity advantage. No longer will its bases, battle groups, forward infrastructure, and allied navies be immune just because they are over the horizon or far from the battle space. We believe that a more diffused set of threats and adversaries will be able to fight at a distance against the Navy and the nation. Another major research question for the Navy, then, is how to make proximity matter again, how to regain its traditional operational advantages against cyber-capable foes.

Precision

The history of warfare demonstrates the many physical constraints on precision in choosing how often, where, and when to attack, given the size of the target and its ability to frustrate or defeat its attackers. Historically, precision has been expensive; few polities aside from empires, superpowers, and perhaps close neighbors have had the means to target their enemies precisely, in order to achieve operational success or conserve resources. In a cyber attack or a conventional operation accompanied by cyber tactics, this constraint fades into merely a question of time, knowledge, and occasionally patience. Attackers can now choose very specific targets—for today, for this tool, for this duration, and for this or that end. They can focus on individuals—by bank account, name, citizenship, location, or entertainment preference. They can also target specific firms, cities, or nations with similarly individualized parameters, with fairly small investment in readily available computer applications.[80]

Correspondingly, adversaries can use *imprecision* strategically as well. Cyber attackers often intentionally build a certain amount of imprecision into their "weapons" to ensure they hit their intended targets. For example, to take down a particular subset of users of an innocent application, attackers can purchase destructive malicious software, such as a "Trojan," on cyber crime's global black

Naval War College Review, Vol. 67 [2014], No. 2, Art. 7

market;[81] with it they can attack the application anywhere it is installed in the world. Among the victims will be their true targets; for the attackers, the others represent either irrelevant collateral damage or extra benefit. Such wider harm is rarely a concern to cybered attackers, except perhaps when the attack is undertaken by state actors bound by international law.[82]

In fact, when precision in the form of restraint is displayed, that characteristic itself suggests that the attackers are state actors. Usually only states concerned with international legitimacy try to avoid the potential for collateral damage posed by cyber weapons (Trojans, malware, etc.) that escape "into the wild." One of the key indicators that a government had been involved in attacks on Estonia in 2007 was the degree of constraint exhibited in the timing, choice of targets, and duration. Many analysts presume that proxy actors were paid by Russian officials to attack Estonian targets but not beyond certain redlines.[83] Precision, however, may also reflect organizational maturity and a wider view of the consequences of success, of failure, or of errors that send the attack spinning out of control.[84] If true, the Russian actors behind the attacks showed restraint not because they had to but for their own reasons.[85]

For the Navy and the U.S. military more generally, the development of precision weapons, both offensive and defensive, has long been a priority—at least since the development of the Norden bombsight in World War II.[86] Precision increases the effectiveness of weapons and reduces costs (although in direct terms this is contestable, given the per-unit cost of many precise weapons). Professional militaries have often increased accuracy to decrease the volume of munitions employed, limit the number of aircraft sorties required, reduce (at least in theory) logistical expenses, and, ultimately, minimize collateral risks. At the same time, cost-effectiveness is said to lower the barriers to using coercion and reduction in collateral damage to increase the legitimacy of some forms of warfare, by some domestic and international observers.[87] One of these has argued that "precision weaponry has revolutionized contemporary warfare by multiplying the effectiveness of using air and ground power together."[88] In a similar fashion, cyber operations may, by changing the roles of scale, proximity, and precision in warfare, increase the effectiveness of air, sea, land, and space operations when employed to reduce collateral damage and avoid risk to forces undertaking legitimate action.

In the cybered world, precision targeting is not necessarily an expensive option open only to major powers. Precision can help achieve aims without crossing redlines that might provoke wider kinetic conflict. Cybered conflict can occur along a spectrum across all phases of war, and long before any kinetic exchange, adversaries can use precision cyber tools to tilt the conflict in their favor. In particular, adversaries may use precise cyber weapons to undermine the resilience of

the targeted state's military or infrastructure, or even its entire economic system, sometimes without declaring their intention or being identified as the attackers.

The critical research question here for the Navy is how to turn the offensive advantages of precision into a more costly liability for attackers. Standardization in software and hardware systems, for example, can make offensive action easy for adversaries. The now-standard obligation to reduce costs by acquiring commercial-off-the-shelf (COTS) equipment often makes systems cheaper but more vulnerable in cybered conflicts. The U.S. military, including the Navy, might avoid providing the COTS advantage to potential adversaries by revising its acquisition process, to include the design of information architectures and the procurement of system components. It will require considerable ingenuity, but increasing variation within otherwise standardized equipment; off-the-shelf software architectures; and routine-driven procedures, units, or deployment patterns may hold long-term benefits.

Twenty years ago, the proponents of a "revolution in military affairs" (RMA) led by the U.S. military made all manner of claims for the impact of precision weapons on the future of conflict. This is not the place to wade into arguments about the nature of the RMA, past or present. But the impact of cyberspace on the scale, proximity, and precision of warfare, combined with the utility of cyber instruments in all phases, levels, and types of war, suggests a far greater impact for cyber than the classic RMA. By confronting directly the advantages of scale, proximity, and precision in cyber conflict, the Navy and CYBERCOM may both increase the effectiveness of traditional air, sea, land, and space operations and prepare for the inevitable more dynamic and complex cybered threat environment. In short, the challenge to the Navy is to reduce all three systemic advantages for attackers: to make it harder for them to choose to be precise or not at their will, more difficult for their operations to be "close" though not physically close, and more expensive and personally risky for them to organize dispersed strangers or covertly to manipulate masses of distant innocent systems.

THE CURRENT AND FUTURE CYBER "LITTORAL"

Cybered conflict is here to stay and must be taken seriously even if cyber war in the conventional sense—that is, resulting in combat deaths—is not likely. Cyber operations, both offensive and defensive, will play major roles in all levels of war (from terrorism and counterinsurgency to high-intensity conflict and all the gradations between). Conflict involving cyber will neither stay wholly within networks nor prove over time to have been a fad or simply a subset of existing tactical, operational, or technological categories. From both empirical and conceptual perspectives, cybered conflict is neither a "flash in the pan" or a "lesser

included case"; it has already proved to be an evolutionary force, slowly altering the likely future conditions for interstate competition and the potentials for kinetic forms of battle. Scholars, analysts, and, most important, operators need to think systematically about how cyber operations—offensive and defensive, to the extent that distinction still makes sense—affect tactics, operations, and strategies.

Future military and security analyses of "cyber" writ large by the U.S. government, or indeed that of any state, should adopt a systemic approach adapted from the logic of complex socio-technological systems and how new developments change what can be used by defenders and abused by adversaries. For example, since such systems are in reality "patterns of artifacts, institutions, rules and norms assembled and maintained to perform economic and social activities," the Navy's scholars and strategists need to think through what current and new technologies, from 3D printing and autonomous private vehicles to new materials, will do to change those patterns.[89] Many current arguments about cyber operations in the government and policy communities are characterized by hype, false analogy, and, worse, misunderstanding of the technical, engineering, and scientific underpinning of the terms. Instead, the conversation should be about what is today being systematically lost, threatened, and penetrated on a vast scale. Furthermore, emergent technologies labeled "disruptive technologies" will change the calculus, some reducing scale, proximity, and precision obstacles even further, others offering opportunities to enhance barriers if the defenders are wise enough to see the opportunities.[90]

Cybered conflicts occur only partly inside computer and communications networks; what the Navy has viewed as the "littoral" in bounding its area of concern (traditionally the intersection of the land and sea) is increasingly difficult to identify. Large sections of what matters to the maritime services now overlap with traditional military, intelligence, and even commercial operations across the nation and the globe. Furthermore, the internationally accepted rules of war are difficult to apply in cyber war. However, in the context of a broader notion of conflict (i.e., as cybered conflict), these rules would find resonance with much of what happens before and during a kinetic conflict.[91] Other well-known forms of conflict, such as hybrid warfare, asymmetric conflicts, and counterterrorism, are also cybered conflicts to the extent that key events depend on the cyberspace substrate.[92]

The U.S. government has struggled since the Clinton administration to adapt to the policy, legal, organizational, and operational demands of conflict in cyberspace. Progressing by fits and starts, key policy makers have reached a consensus that cyberspace is an important arena for conflict, one worthy of resources, specialized organizations, different interagency relationships, and eventually perhaps legislative action.[93] Much remains to be done, especially with

regard to domestic policies, organizational implementation, and resourcing, but since the establishment of CYBERCOM and its service equivalents the defense and intelligence communities have become better equipped to meet external cyber challenges and take advantage of American cyber technologies to protect national interests.

Two of the most likely and challenging scenarios for future crises, perhaps even shooting wars, will clearly involve cyber operations: Iran and North Korea.[94] In each case, Phase Zero operations involving both sides, as well as third parties, already appear to involve cyber attacks of various types. If kinetic operations eventually take place, we may see the results of several decades of cyber "preparation of the battlefield," ranging from tainted supply chains to embedded malware. For the time being, serious assessments and many details are obscure and will likely remain so until leaks and eventual declassification reveal the full extent of cyber operations.[95] In the interim, a more systemic view will enable the United States, with its already-demonstrated considerable cyber capabilities in disruption work, to balance those capabilities with the resilience needed for robust "cyber power."

The Navy will be an integral part of that cyber power. The Navy has led service-level efforts in developing, deploying, operating, and sustaining complex electronic systems in the past.[96] Thanks to innovative institutional changes, it may be the service best positioned to integrate cyber fully into its culture, organizational structure, and operations.[97] As a maritime force, it has a long-established cultural acceptance of the deception, masking, mobility, and improvised independent operations that deployed ships have needed for survival in peace as well as war. At present, however, an assumption of uninterrupted communications has diminished its institutional capacity to sail resiliently under the cyber "radar," despite millions of opportunistic "hunters." The newer forms of conflict enabled by cyberspace require a rediscovery of inclinations buried in the Navy's history and culture and a repurposing of them for the new—much more complex, deceptive, and sensor-rich—environment. The "littoral" may be defined more in terms of what one keeps the enemy from easily knowing and how abruptly one can emerge in the enemy's near proximity than of what beach needs to be crossed. The sociotechnical systems the service depends on today need to change, at the hands of officers and sailors who understand the basics of the cyber substrate as it is today and as it is evolving. We argue—though only time and trial by fire will confirm the proposition—that the Navy may be uniquely qualified to adapt to cybered conflict, if the research is done and the new sociotechnical lines of evolution are identified.

A systemic understanding of cyber and research along lines identified above are needed not only for the Navy but also for the nation as a whole, if the Navy

Naval War College Review, Vol. 67 [2014], No. 2, Art. 7

is to develop its portion of national cyber power. In the coming transitional cybered conflict age, cyber power will rest on a balance between the resilience of the system being attacked and that system's ability to reach forward and disrupt in advance the small numbers of very skilled wicked actors able to overcome that resilience. This balance of resilience and disruption will apply to the Navy as well as the nation as a whole. When it is achieved, the nation will have in effect pursued an overarching cyber "security resilience" strategy redressing the advantages that today cyberspace gives the offense. Effective and robust cyber power diminishes the value of any adversary's "counterresilience" strategies intended to wear down deceptively the resilience of the defender's whole socio-technical-economic system.

Today the United States has allies who are well intentioned but simply cannot find the economic resources to invest in the cyber security that they know their economic, critical infrastructure, and national-security systems require. When a service or nation becomes a cyber power, it will have greater freedom of choice in the coming transitional era and better chances of maintaining that power in the era that will follow. The more the Navy is able to answer the systemic cyber challenges and reduce the scale, proximity, and precision advantages attackers enjoy today, the better prepared it will be for the bordered, encrypted, and technologically diverse future international system. The more systemically the Navy contributes to its own cyber security, the more critical a player it will be in ensuring the cyber power and the well-being of the nation as a whole, as the cybered world gradually restructures itself in response to global economic, demographic, technological, and security challenges.

NOTES

The authors thank Emily Goldman, Ron Deibert, John Mallery, Paul Cornish, Nigel Inkster, Sandro Gayken, Daniel Ventre, Sue Eckert, Catherine Lotrionte, Patrick James, Melissa Hathaway, Erik Gartske, Catherine Kelleher, and Joe Nye for providing comments, suggestions, and forums for discussing our ideas. Chris Demchak would also like to thank the officers and officials she interviewed in the course of her research in the United States and Europe.

1. For early research on cyber war see John Arquilla and David Ronfeldt, "Cyberwar Is Coming!," *Comparative Strategy* 12, no. 2 (1993), pp. 141–65; Arquilla and Ronfeldt, *The Advent of Netwar* (n.p.: RAND, 1996); Arquilla and Ronfeldt, eds., *In Athena's Camp: Preparing for Conflict in the Information Age* (Washington, D.C.: National Defense Univ., 1997); Martin C. Libicki, *What Is Information Warfare?* (Washington, D.C.: National Defense Univ. Press, 1995), chap. 9; Chris Demchak and Patrick D. Allen, "Cyber Hot War: The Palestinian/Israeli Hacker Conflict," in *Proceedings of the 69th Military Operations Research Society Symposium* (Annapolis, Md.: June 2001); T. X. Hammes, "War Evolves into the Fourth Generation," *Contemporary Security Policy* 26, no. 2 (2005), pp. 189–221; and Bruce D. Berkowitz, *The New Face of War: How War Will Be Fought in the 21st Century* (New York: Free Press, 2003).

2. See James P. Farwell and Rafal Rohozinski, "Stuxnet and the Future of Cyber War," *Survival: Global Politics and Strategy* 53, no. 1 (2011), pp. 23–40, and Chris Demchak and Peter Dombrowski, "Rise of a Cybered Westphalian Age," *Strategic Studies Quarterly* (2011), pp. 32–61.
3. Nicole Perlroth, "Hackers in China Attacked the *Times* for Last 4 Months," *New York Times,* 30 January 2013.
4. Donna Miles, "Cyber Defense Requires Teamwork, Agility, Alexander Says," American Forces Press Service, 27 October 2011, available at www.defense.gov/.
5. The United States, of course, is not alone; other nations are experiencing economic losses and widespread threats to national security. Globally, billions of dollars have been spent on defensive measures ranging from simple firewalls to the creation of such complex institutions as Great Britain's Defence Cyber Operations Group and France's Agence nationale de la sécurité des systèmes d'information. For a comparative perspective, see Chris Demchak's *Cyber Westphalia: Cyber Commands and Emergent Organizing for Cyber Security,* in manuscript. On the United States see Jean-Loup Samaan, "Cyber Command: The Rift in US Military Cyber-Strategy," *RUSI Journal* 155, no. 6 (December 2010), pp. 16–21.
6. Thomas Rid, "Cyber War Will Not Take Place," *Journal of Strategic Studies* 35, no. 1 (February 2012), pp. 5–32; Brandon Valeriano and Ryan Maness, "The Fog of Cyberwar: Why the Threat Doesn't Live Up to the Hype," *Foreign Affairs* (November 2012).
7. Gary McGraw and Nathaniel Fick, "Separating Threat from the Hype: What Washington Needs to Know about Cyber Security," in *America's Cyber Future: Security and Prosperity in the Information Age,* ed. Kristin M. Lord and Travis Sharp (Washington, D.C.: Center for a New American Security, June 2011), vol. 2, pp. 43–53.
8. Richard A. Clarke and Robert Knake, *Cyber War: The Next Threat to National Security and What to Do about It* (New York: HarperCollins, 2010).
9. For example, Tyler Moore and Ross Anderson, "Internet Security," in *The Oxford Handbook of the Digital Economy,* ed. Martin Peitz and Joel Waldfogel (New York: Oxford Univ. Press, 2011), and Ross Anderson et al., "Measuring the Cost of Cybercrime," *Workshop on Economics of Information Security 6/2012,* weis2012.econinfosec.org/.
10. Ronald Deibert and Rafal Rohozinski, "The New Cyber Military Industrial-Complex," *Globe and Mail,* 28 March 2011
11. For the "Flash Crash," Dan Goodin, "Network Attacks (Allegedly) Ravage London Stock Exchange: Open Source Trade System Breach?," *Register,* 31 January 2011.
12. See Jack Clark, "Amazon *Disappears* from Internet; Last Week Google, This Week Amazon, Next Week, El Reg?," *Register,* 19 August 2013.
13. Naval War College authors have contributed to these debates. See, for example, Derek Reveron, ed., *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World* (Washington, D.C.: Georgetown Univ. Press, 2012); Chris C. Demchak, "Resilience, Disruption, and a 'Cyber Westphalia': Options for National Security in a Cybered Conflict World," in *Securing Cyberspace: A New Domain for National Security,* ed. Nicholas Burns and Jonathon Price (Washington, D.C.: Aspen Institute, 2012), pp. 59–94; and Thomas G. Mahnken, "Cyberwar and Cyber Warfare," in *America's Cyber Future,* ed. Lord and Sharp, pp. 55–64.
14. William F. Lynn III, "Defending a New Domain: The Pentagon's Cyberstrategy," *Foreign Affairs* 89, no. 5 (September/October 2010), pp. 97–108.
15. See Chris C. Demchak, *Wars of Disruption and Resilience: Cybered Conflict, Power, and National Security* (Athens: Univ. of Georgia Press, 2011).
16. The following section draws on U.S. Joint Staff, *Joint Operation Planning,* Joint Publication 5.0 (Washington, D.C.: 11 August 2011), pp. III-41 through III-44, available at www.dtic.mil/.
17. Summarized directly by U.S. Joint Staff, *Doctrine for the Armed Forces of the United States,* Joint Publication 1 (Washington, D.C.: 25 March 2013), pp. 17–18, available at www.dtic.mil/.
18. Ibid., p. 18.

19. U.S. Joint Staff, *Department of Defense Dictionary of Military and Associated Terms,* Joint Publication 1-02 (Washington, D.C.: 8 November 2010 [as amended through 15 October 2013]), available at www.dtic.mil/.

20. For the legal dimensions of cybered conflict, see Michael Schmitt, "Classification of Cyber Conflict," *Journal of Conflict and Security Law* 17, no. 2 (June 2012), pp. 245–60.

21. Keith B. Alexander, "Warfighting in Cyberspace," *Joint Force Quarterly,* no. 46 (2007), pp. 58–61.

22. Martin C. Libicki, "Cyberspace Is Not a Warfighting Domain," *I/S: A Journal of Law and Policy for the Information Society* 8, no. 2 (Fall 2012), pp. 325–40.

23. See Lynn, "Defending a New Domain," and "War in the Fifth Domain: Are the Mouse and Keyboard the New Weapons of Conflict?," *Economist,* 1 July 2010.

24. Jonathan L. Zittrain, "The Generative Internet," *Harvard Law Review* 119, no. 7 (May 2006), p. 1975.

25. Quoted in William Jackson, "U.S. Understanding of Cyber War Still Immature, Says Former NSA Director," *GCN,* 29 July 2010, gcn.com/articles/.

26. Clarke and Knake, *Cyber War*.

27. This section draws on Kevin P. Newmeyer, "Who Should Lead U.S. Cybersecurity Efforts?," *Prism* 3, no. 2 (March 2012), pp. 116–18.

28. See the Harmony database of translated materials captured after U.S. invasion of Afghanistan, in 2001, at *Combating Terrorism Center,* www.ctc.usma.edu/.

29. For an overview of the development of China's capabilities in cyberspace since the mid-1990s, see Desmond Ball, "China's Cyber Warfare Capabilities," *Security Challenges* 7, no. 2 (Winter 2011), pp. 81–103. For another perspective see James Mulvenon, "PLA Computer Network Operations: Scenarios, Doctrine, Organizations, and Capability," in *Beyond the Strait: PLA Missions Other than Taiwan,* ed. Roy Kamphausen, David Lai, and Andrew Scobell (Carlisle, Pa.: U.S. Army War College, Strategic Studies Institute, 2009), pp. 257–59.

30. Timothy L. Thomas, *Dragon Bytes: Chinese Information-War Theory and Practice from 1995–2003* (Fort Leavenworth, Kans.: Foreign Military Studies Office, 2004). For an earlier account of Chinese views on the future of warfare see Michael Pillsbury, ed., *Chinese Views of Future Warfare* (Washington, D.C.: National Defense Univ. Press, 1997).

31. Ball, "China's Cyber Warfare Capabilities," pp. 81–103.

32. "A robust, resilient Internet is also a key enabler of DoD's ability to carry out a global, modern national defense strategy." U.S. Defense Dept., *DoD Information Enterprise Strategic Plan* (Washington, D.C.: 2012), p. 8, available at dodcio.defense.gov/.

33. Ibid., p. 117.

34. U.S. Commerce Dept., *Digital Nation: Expanding Internet Usage,* NTIA Research Preview (Washington, D.C.: National Telecommunications & Information Administration, February 2011), p. 7, available at www.ntia.doc.gov/.

35. U.S. Defense Dept., *Resilient Military Systems and the Advanced Cyber Threat,* Task Force Report (Washington, D.C.: Defense Science Board, January 2013 [research complete 2012]), available at www.acq.osd.mil/; James Clapper, Director of National Intelligence, *Worldwide Threat Assessment,* testimony to the Senate Committee on Armed Services, 18 April 2013, 113th Cong., 1st sess., available at www.intelligence.senate.gov/.

36. "Wicked" actors are a subgroup of the globe's "bad actor" community infecting cyberspace. "Wicked" is a phrase used by mathematicians; thus "wicked problems" is used to convey how difficult it is to keep these persistent and skilled individuals out of networks and why they usually require of defenders forward disruption as well as systemic resilience. Generally these actors are not easily deterred. See Demchak, "Resilience, Disruption, and a 'Cyber Westphalia,'" pp. 59–94.

37. David Sanger recounts the Bush administration's high-level efforts to come to grips with the potential for cyber operations in *The Inheritance: The World Obama Confronts and the Challenges to American Power* (New York: Broadway Books, 2010), pp. 430–41.

38. U.S. Joint Staff, *The National Military Strategy for Cyberspace Operations* (Washington, D.C.: November 2006), available at www.dod.mil/.
39. Members of the Air Staff, interviews by authors, Washington, D.C., 2009–12.
40. Members of the Navy Staff and Office of the Secretary of Defense, interviews by authors, Washington, D.C., 2009–12.
41. Gen. James E. Cartwright, USMC, interviews by authors, Washington, D.C., 2010–12.
42. Kim Zetter, "The Return of the Worm That Ate the Pentagon," *Wired,* 9 December 2011; Ellen Nakashima, "Cyber-intruder Sparks Massive Federal Response—and Debate over Dealing with Threats," *Washington Post,* 8 December 2011.
43. S. Shin, G. Gu, N. Reddy, and C. P. Lee, "A Large-Scale Empirical Study of Conficker," *IEEE Transactions on Information Forensics and Security* 7, no. 2 (2012), pp. 676–90.
44. Rendon Group, *Conficker Working Group: Lessons Learned* ([Washington, D.C.]: January 2011 [issued June 2010]), available at www.confickerworkinggroup.org/.
45. Sharon Weinberger, "Top Ten Most-Destructive Computer Viruses: Created by Amateur Hackers, Underground Crime Syndicates and Government Agencies, These Powerful Viruses Have Done Serious Damage to Computer Networks Worldwide," *Smithsonian,* 20 March 2012.
46. Senior members of the Obama staff associated with the sixty-day review, interviews by authors, Washington, D.C. See also *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure* (Washington, D.C.: White House, n.d. [2009]), available at www.whitehouse.gov/.
47. Lynn, "Defending a New Domain," pp. 97–108.
48. See Macon Phillips, "Cyber Review Underway," *White House Blog,* www.whitehouse.gov/.
49. See *Cyberspace Policy Review.*
50. For Title 10 and Title 50 authorities, see Andru E. Wall, "Demystifying the Title 10–Title 50 Debate: Distinguishing Military Operations, Intelligence Activities & Covert Action," Harvard Law School *National Security Journal* 3, no. 1 (2012), pp. 85–141, available at harvardnsj.org/.
51. Senior leaders in the transition and early teams of U.S. Cyber Command and the Joint Staff, interviews by authors, Washington, D.C., 2009–12.
52. Quoted in part at "Tenth Fleet History," *U.S. Fleet Cyber Command / U.S. Tenth Fleet,* www.fcc.navy.mil/.
53. *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World* (Washington, D.C.: White House, May 2011), available at www.whitehouse.gov/.
54. U.S. Defense Dept., *Department of Defense Strategy for Operating in Cyberspace* (Washington, D.C.: July 2011), available at www.defense.gov/.
55. Other supporting documents, many classified, have also recently been signed to support and clarify the operational authority and legal guidelines for these themes.
56. Demchak, "Resilience, Disruption, and a 'Cyber Westphalia.'"
57. The Navy foresaw the possibilities of cyberspace in the 1990s, expressing this recognition, at least in part, with its focus on network-centric warfare (NCW). The implementation of NCW concepts was largely defined by the assumption of state-level actors as adversaries; however, theorists like the late Vice Adm. Arthur Cebrowski acknowledged that NCW was scalable down to smaller, nonstate actors as well. For an accessible overview of NCW see Arthur K. Cebrowski and John J. Garstka, "Network-centric Warfare: Its Origin and Future," U.S. Naval Institute *Proceedings* (January 1998), pp. 28–35. For a wider discussion of NCW within the context of the revolution in military affairs, see Peter Dombrowski, Eugene Gholz, and Andrew Ross, *Military Transformation and the Defense Industry after Next: The Defense Industrial Implications of Network-centric Warfare,* Newport Paper 18 (Newport, R.I.: Naval War College Press, 2003), esp. pp. 5–12.
58. Senior Navy officers involved in the design of Fleet Cyber Command / Tenth Fleet, interviews by authors, Washington, D.C., 2009–12.
59. See "Tenth Fleet History."

60. Ibid.

61. U.S. Navy Dept., *Navy Strategy for Achieving Information Dominance 2013–2017: Optimizing Navy's Primacy in the Maritime and Information Domains* (Washington, D.C.: Deputy Chief of Naval Operations for Information Dominance / Fleet Cyber Command / Tenth Fleet, n.d. [2012]), available at www.public.navy.mil/.

62. *Navy Cyber Power 2020: Sustaining U.S. Global Leadership—Priorities for 21st Century Defense* (Washington, D.C.: Deputy Chief of Naval Operations for Information Dominance / Fleet Cyber Command / Tenth Fleet, November 2012), available at www.public.navy.mil/.

63. *Navy Information Dominance Corps Human Capital Strategy 2012–2017* (Washington, D.C.: Deputy Chief of Naval Operations for Information Dominance / Fleet Cyber Command / Tenth Fleet, n.d. [2012]), available at www.public.navy.mil/.

64. U.S. Navy Dept., *CNO's Sailing Directions* (Washington, D.C.: Navy Staff, n.d.), available at www.navy.mil/.

65. This section draws on Chris C. Demchak, "Dilemmas of Arms Control and Cybersecurity," in *Arms Control: History, Theory, Policy,* ed. Paul Viotti and Robert Williams (New York: Praeger / ABC-CLIO, 2012).

66. These are challenges that will continue to exist at least until the Westphalian state system adapts and states find ways to regulate cyberspace and cyber weapons. See Chris Demchak and Peter Dombrowski, "Cyber Westphalia: Asserting State Prerogatives in Cyberspace," *Georgetown Journal of International Affairs* (forthcoming).

67. For a classic overview of offense/defense theory see George H. Quester, *Offense and Defense in the International System* (Piscataway, N.J.: Transaction, 2003).

68. Ilai Saltzman, "Cyber Posturing and the Offense-Defense Balance," *Contemporary Security Policy* 34, no. 1 (2013), pp. 40–63.

69. Timothy J. Junio, "How Probable Is Cyber War? Bringing IR Theory Back into the Cyber Conflict Debate," *Journal of Strategic Studies* 36, no. 1 (2013), pp. 125–33.

70. Erik Gartzke, "The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth," *International Security* 38, no. 2 (Fall 2013), pp. 41–73.

71. See Robert Lamb, "What Are Botnets?," *Discovery News,* news.discovery.com/.

72. Ronald Deibert, John Palfrey, Rafal Rohozinski, and Jonathan Zittrain, *Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace* (Cambridge, Mass.: MIT Press, 2010).

73. One standout in the vast literature is Paul Bracken, *The Command and Control of Nuclear Forces* (New Haven, Conn.: Yale Univ. Press, 1983). For an overview of the consequences of the information revolution, more specifically the Internet and cyberspace, on international affairs generally, as well as the differing impacts on states and nonstate actors, large and small, see Joseph S. Nye, Jr., *The Future of Power* (New York: PublicAffairs, 2011), esp. pp. 114–18, and Emily O. Goldman, *Power in Uncertain Times: Strategy in the Fog of Peace* (Stanford, Calif.: Stanford Univ. Press, 2011), p. 135.

74. The emergence of cybered conflict challenges long-standing theories about the impact of geographic distance on conflict. Kenneth Boulding, for example, argued that "in the case of the state, its power of destruction is an inverse function of the distance from the source of supplies of both men and materials"; Boulding, "Economic Issues in International Conflict," *Kyklos* 6, no. 2 (May 1953), p. 99.

75. Forward observers grow in importance with the increasing range of fires on battlefields and at sea. William H. McNeill, *The Pursuit of Power: Technology, Armed Force, and Society since AD 1000* (Chicago: Univ. of Chicago Press, 1982).

76. John Keegan, *Intelligence in War: Knowledge of the Enemy from Napoleon to al-Qaeda* (London: Hutchinson, 2004).

77. Microsoft recently achieved a historical high in the number of vulnerabilities identified per month (thirty-four). Elinor Mills, "Microsoft Plugs Critical Holes in Huge Patch Tuesday," CNET.com, 8 July 2010.

78. L. Elaine Halchin, "Electronic Government in the Age of Terrorism," *Government Information Quarterly* 19, no. 3 (2002), pp. 243–54.

79. Harvey Starr, "Territory, Proximity, and Spatiality: The Geography of International Conflict," *International Studies Review* 7 (2005), pp. 387–406. Several generations of international relations and strategic studies scholars—beginning with Quincy Wright and extending to the economist Kenneth Boulding and economic geographers like John Agnew today—have analyzed the importance of geographic proximity for the nature of interstate conflict. Scholars today need to collect data and theorize carefully about how cyberspace is undermining the centrality of conflict for understanding the geostrategic environment.
80. Nathan Friess and John Aycoc, *Black Market Botnets* (Calgary, Alta.: Univ. of Calgary, Dept. of Computer Science, July 2007).
81. "What Is the Difference: Viruses, Worms, Trojans, and Bots?," *Cisco,* www.cisco.com/.
82. Susan W. Brenner and Leo L. Clarke, "Combatting Cybercrime through Distributed Security," *International Journal of Intercultural Information Management* 1, no. 3 (2009), pp. 259–74. Also see Demchak, "Dilemmas of Arms Control and Cybersecurity," pp. 219–38.
83. Heather A. Conley and Theodora P. Gerber, *Russian Soft Power in the 21st Century: An Examination of Russian Compatriot Policy in Estonia,* CSIS Europe Program Report (Washington, D.C.: Center for Strategic and International Studies, 2011), available at csis.org/.
84. "Estonia Hit by 'Moscow Cyber War,'" *BBC Online,* 17 May 2007.
85. Michael Joseph Gross, "Stuxnet Worm: A Declaration of Cyber-war," *Vanity Fair,* April 2011; Kim Zetter, How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History," *Wired,* 11 July 2011.
86. Stephen Lee McFarland, *America's Pursuit of Precision Bombing, 1910–1945* (Washington, D.C.: Smithsonian Institution Press, 1995).
87. J. Marshall Beier, "Discriminating Tastes: 'Smart' Bombs, Non-combatants, and Notions of Legitimacy in Warfare," *Security Dialogue* 34, no. 4 (December 2003), pp. 411–25.
88. Robert A. Pape, "The True Worth of Air Power," *Foreign Affairs* 83, no. 2 (March/April 2004), pp. 116–30.
89. James Manyika et al., "McKinsey Global Institute Report: Disruptive Technologies—Advances That Will Transform Life, Business, and the Global Economy," *Insights & Publications* (May 2013), available at www.mckinsey.com/. The quotation is from Frans Berkhout, Adrian Smith, and Andy Stirling, *Socio-technological Regimes and Transition Contexts,* SPRU Electronic Working Paper 106 (Falmer, Brighton, U.K.: Univ. of Sussex, Freeman Centre, June 2003), available at www.sussex.ac.uk/.
90. For an understanding of disruptive technology in common use in national security circles, see Terry Pierce, *Warfighting and Disruptive Technologies: Disguising Innovation* (New York: Routledge, reissued 2005). For an application of the concepts of disruptive and sustaining innovations to military technologies more closely related to Clayton Christensen's original research, see Peter Dombrowski and Eugene Gholz, *Buying Military Transformation: Technological Innovation and the Defense Industry* (New York: Columbia Univ. Press, 2006).
91. On the laws of armed conflict and cybered conflicts, see Michael N. Schmitt, gen. ed., *The Tallinn Manual on the International Law Applicable to Cyber Warfare* (New York: Cambridge Univ. Press, 2013), available at static.ow.ly/.
92. The preceding paragraph is adapted from Chris Demchak, "Cybered Conflict vs. Cyberwar," *Atlantic Council,* www.acus.org/.
93. Congressional and public debates over the Cyber Intelligence Sharing and Protection Act represent only the latest skirmishes between groups like the Electronic Frontier Foundation and the American Civil Liberties Union—that is, between those that fear the erosion of privacy rights and civil liberties and those concerned with providing the government and corporations the tools they believe are necessary to combat cyber espionage and attacks of all sorts.
94. Both countries have reportedly used cyber attacks over the last year and a half, although attribution remains in dispute. See Nicole Perloth, "Cyberattack on Saudi Firm Disquiets U.S.," *New York Times,* 24 October 2012, p. A1, and Choe Sang-Hun, "Computer Networks in South Korea Are Paralyzed in

Cyberattacks," *New York Times,* 20 March 2013, p. A5.

95. Neither the full story nor the full effects can be known until some time has passed. Edward Snowden's betrayal may not have the effects he imagined, as key institutions of the United States and its allies evolve in response. See T. Gjelten, "The Effects of the Snowden Leaks Aren't What He Intended," *All Things Considered,* National Public Radio, broadcast 20 September 2013, available at www.npr.org/.
96. Norman Friedman, *Network-centric Warfare: How Navies Learned to Fight Smarter through Three World Wars* (Annapolis, Md.: Naval Institute Press, 2009).
97. On the suitability of the U.S. Navy to support cyber security, see W. Alexander Vacca, "Military Culture and Cyber Security," *Survival* 53, no. 6 (2011), pp. 159–76.

Dr. Dombrowski is a professor of strategy at the Naval War College. His previous positions include chair of the Naval War College's Strategic Research Department, director of the Naval War College Press, editor of the Naval War College Review, *co-editor of* International Studies Quarterly, *associate professor of Political Science at Iowa State University, and defense analyst at ANSER, Inc. He has also been affiliated with research institutions, including the East-West Center, the Brookings Institution, the Friedrich Ebert Foundation, and the Watson Institute for International Studies at Brown University, among others. Dr. Dombrowski is the author of over forty-five articles, monographs, book chapters, and government reports. He received his BA from Williams College and an MA and PhD from the University of Maryland.*

Dr. Demchak has a PhD from Berkeley (political science) with a focus on organization theory and complex systems, security studies, and surprise in large-scale sociotechnical systems across nations. She also holds two master's degrees in, respectively, economic development (Princeton) and energy engineering (Berkeley). For over two decades, she has published numerous articles on societal security difficulties with large-scale information systems. Dr. Demchak's recent books include a coedited volume entitled Designing Resilience *(2010) and a theory-to-practice volume,* Wars of Disruption and Resilience: Cybered Conflict, Power, and National Security *(2011), as well as a prior book entitled* Military Organizations, Complex Machines, *in the Cornell Security Studies series. She is currently working on a new series of articles for a manuscript tentatively entitled* Cyber Westphalia: Cyber Commands and Emergent Organizing for Cyber Security. *She is a founding codirector of the Naval War College's Center for Cyber Conflict Studies.*

Naval War College Review, Spring 2014, Vol. 67, No. 2