General Dempsey hosts question-and-answer session with Peter W. Singer, director of Center for 21st Century Security and Intelligence, in Washington, DC, June 2013 (DOD/Daniel Hinton)

Expanding Combat Power Through Military Cyber Power Theory

By Sean Charles Gaines Kern

We need a theory for cyberspace operations that will allow us to understand the implications of employing cyberspace capabilities at the tactical, operational, and strategic levels.[1]

—Major General Brett T. Williams, USAF

Military theory is a primary component of operational art. Early military theorists such as Alfred Thayer Mahan, Giulio Douhet, and B.H. Liddell Hart reasoned about the maritime, air, and land domains respectively, generating frameworks, models, and principles for warfare. Today, these theories help strategists and planners think about, plan for, and generate joint combat power. Unfortunately, no standard military theory for cyberspace operations exists, although elements for such a theory do. If a codified theory for military cyber power existed, it would greatly aid the joint force com-

Lieutenant Colonel Sean Charles Gaines Kern, USAF, is assigned to U.S. Cyber Command.

mander (JFC) in integrating cyberspace operations with joint operations, resulting in expanded combat power.

Although JFCs have many years of practical experience and military education in employing joint forces, they are not as experienced with cyberspace operations.[2] There is a lack of shared cyberspace knowledge and an agreed operational approach to link cyberspace missions and actions and place them in the larger context of joint operations.[3] Military cyber power theory is the foundation for such knowledge.

The JFC requires a cyberspace component commander who, through education and experience, has developed the requisite expertise to apply military cyber power theory at a level equivalent to his or her peers in the other domains. However, joint doctrine does not describe such a leadership role. Without the equivalent of a joint force cyberspace component commander (JFCCC), it is unlikely that the JFC would be able to effectively integrate cyberspace operations within the construct of joint operations. This results in a perpetual adjunct role for cyberspace operations and suboptimal combat power, as the Chairman of the Joint Chiefs of Staff himself noted as a key operational problem in the *Capstone Concept for Joint Operations: Joint Force 2020*.[4]

Toward a Preliminary Theory

The most challenging aspect of developing cyber operational art is devising a military theory for cyber power, which is essential for assessing the operational environment and making predictive judgments that will then guide strategy and plan development. By viewing the operational environment through the lens of military cyber power theory, the JFCCC will be in the position to provide his or her best military advice to the JFC, resulting in integrated cyberspace operation and expanded combat power.

A framework advances understanding and provides a basis for reasoning about the current and potential future environment by incorporating a number of elements. The framework identifies and defines key terms and structures discussion by categorizing the elements of the theory. It explains the categorized elements by summarizing relevant events and introducing additional frameworks and models. It allows the members of the cyber community to connect diverse elements of the body of knowledge to comprehensively address key issues. Finally, the predictive nature of the framework will enable the practitioner to anticipate key trends and activities to test the validity of the theory.[5] Although Major General Brett Williams called for a theory of cyberspace operations that addresses cyberspace operations at the strategic, operational, and tactical levels, the focus here is at the strategic and operational levels since the JFCCC's responsibility will be to translate strategic direction into operational plans.

Early cyber power theorists generally identified and defined three key terms: *cyberspace*, *cyber power*, and *cyber strategy*. Under the guise of military cyber power theory, this author offers four additional terms: *military cyber power*, *military cyber strategy*, *key cyber terrain*, and *military cyberspaces*.

Military cyber power is defined as the application of operational concepts, strategies, and functions that employ cyberspace operations (offensive cyberspace operations [OCO], defensive cyberspace operations [DCO], and Department of Defense [DOD] information network [DODIN] operations) in joint operations to expand combat power for the accomplishment of military objectives and missions.[6]

Military cyber strategy is defined as the development and employment of operational cyberspace capabilities integrated with other operational domain capabilities to expand combat power and accomplish the military objectives and missions of the JFC. These definitions reflect an emphasis on cyberspace operations mission areas and their contributions to joint operations and joint force combat power.

Given the pervasive and ubiquitous nature of the cyberspace domain and the fact that the military relies heavily on the commercial sector for interconnectivity, the concept of key terrain becomes especially critical in the context of military cyber power theory. *Key cyber terrain* forms the foundation from which the joint force preserves and projects military cyber power and represents the attack surface that adversaries would likely target. It is defined as any physical, logical, or persona element of the cyber space domain, including commercial services, the disruption, degradation, or destruction of which constricts combat power, affording a marked advantage to either combatant.

Defining cyberspace as a global domain suggests a homogeneity that does not exist in reality. There is not one cyberspace, but many cyberspaces.[7] These cyberspaces are in most cases interconnected by privately owned infrastructure. DOD has over 15,000 networks, or cyberspaces, interconnected by commercial infrastructure that the department does not own or control. This has two significant implications. First, unlike in other domains, the joint force is not solely capable of generating its required military cyber power; it relies on commercial services. Second, not all key cyber terrain will be under control of the joint force. For example, there is no current equivalent in cyberspace to the way in which the United States fully militarized its airspace immediately following the 9/11 terrorist attacks. Thus, *military cyberspaces* are defined as networks or enclaves wholly owned and operated by DOD, interconnected by means that are outside the control or direct influence of DOD.

With key terms identified and defined, military cyber power theory must conceptually consider the relationships of these terms as well as other relevant domain characteristics. The JFCCC must consider his or her efforts in the context of the three layers of cyberspace: physical, logical, and persona layers.[8] Figure 1 depicts the relationships between the terms (left) and the relation of the cyberspace layers in the context of the overall friendly or adversary attack surface (right).

Based on these relationships, the JFCCC can then conceptualize the weighted effort of the cyberspace operations mission areas. These operations comprise the ways and means for the JFCCC's cyber strategy and planning.

Figure 1. Elements of Military Cyber Power Theory and Cyberspace Domain Layers

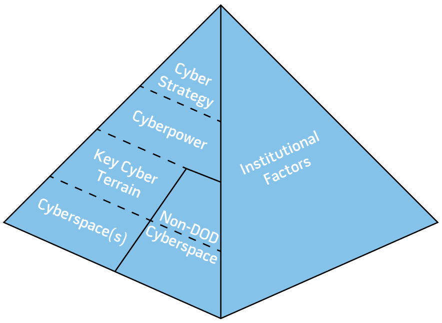


Figure 2. Weighted Effort for Cyberspace Operations

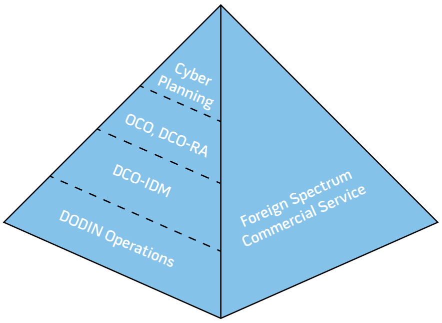


Figure 3. Cyber Adversary Characterization

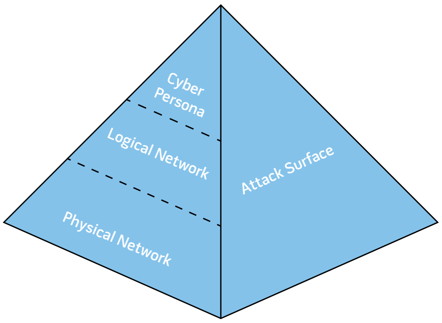
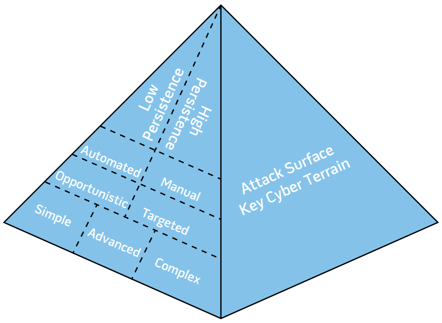


Figure 4. Cyber Kill Chain



The weighted effort, in priority order, would be DODIN operations, DCO–Internal Defense Measures (DCO-IDM), DCO–Response Actions (DCO-RA), and OCO (see figure 2).

The joint force conducts cyberspace operations, like all joint operations, with the adversary in mind. This leads to a final structured discussion to characterize cyberspace adversaries and conceptualize adversarial operational planning and execution. Ultimately, this discussion gives the JFCCC the framework to assess risks associated with generating combat power.

The JFCCC and staff assess cyberspace adversaries similar to adversaries in other domains in terms of intent and capability. It takes two types of capabilities in the cyberspace domain to conduct cyberspace operations: technical and analytical. *Analytical capability* refers to the ability to analyze a potential target to identify its critical nodes and vulnerabilities and potentially its connections to other targets. *Technical capability* refers to knowledge of computer software and hardware, networks, and other relevant technologies.[9] The JFCCC can further categorize cyber adversaries as simple, advanced, and complex, based in part on the scope and scale of operations and potential effects achieved.

In addition to being simple, advanced, or complex, military cyber power theory categorizes adversary operations as either opportunistic or targeted. The former is usually cybercrime-related, automated, and rarely attempts to maintain persistent presence. Targeted attacks are oriented against friendly key cyber terrain and are likely to be persistent and stealthy. In targeted attacks, cyber operators may be manually interacting with target systems. These categories are not mutually exclusive, as opportunistic attackers may gain access to high-value systems and in turn seek to sell access to these systems to adversaries seeking targeted access (for example, the nexus of cybercrime and state-sponsored cyber operations). Figure 3 shows the relationships among adversary capability, targeting type, and level of persistence.

Cyberspace adversaries share common strategic and operational concepts with adversaries in other domains, one of which is the concept of a kill chain. Conceptualizing a cyber kill chain enables the JFCCC to understand how the adversary plans and conducts cyber operations. The cyber kill chain depicted in figure 4 provides an excellent framework for the JFCCC to develop the appropriate strategy and corresponding operational plans to mitigate the adversarial threat. The ultimate goal is to detect and defend against the adversary as early as possible in the chain, ideally at or prior to the adversary developing access.

Military Cyber Power Principles

A theory of military cyber power includes principles that would inform the JFCCC's operational art. The true test of a theory is how well these principles hold over time. The principles examined here are not exhaustive and should serve as a foundation for future expansion of military cyber power theory.

Stealth and Utility. A cyberspace capability is effective as long as it can go undetected and exploit an open vulnerability. If the adversary detects the cyber capability or mitigates the targeted vulnerability, the cyber capability is perishable. These characteristics may drive the timing of cyber operations based on the perceived utility.[10]

Convergence, Consolidation, and Standardization. In peacetime, efficiency is valued over effectiveness. Core services are converging to Internet Protocol technologies. Smaller bandwidth network interconnections are converging to fewer massive bandwidth interconnections. DOD is consolidating data centers and Internet access points, resulting in streamlined, consolidated service architectures. DOD is also standardizing hardware and software. Convergence, consolidation, and standardization create an efficient, homogenous military cyberspace environment that reduces the DOD attack surface overall and better postures cyber defenders to preserve combat power. However, these efforts reduce system redundancy, limit alternative routes, and increase the number of chokepoints, making it easier for an

Joint Service and civilian personnel concentrate on exercise scenarios during Cyber Guard 2015 (DOD/Marvin Lynchard)

adversary to identify and target friendly key cyber terrain.

Complexity, Penetration, and Exposure. Systems are becoming increasingly complex by almost every measure. Higher complexity begets a growth in vulnerabilities. Internet penetration is expanding in terms of people and devices connected to cyberspace. People and organizations are integrating an increasing number of services delivered through cyberspace into their daily lives and operations, creating significant cyberspace exposure. Complexity, penetration, and exposure increase the attack surface by creating broader and deeper technical and process vulnerabilities, putting joint combat power at risk.

Primacy of Defense. History shows that militaries are prone to favor offensive operations.[11] Yet Colin Gray, Brett Williams, and Martin Libicki argue that DCO, not OCO, should be the JFC's primary effort in cyberspace. Since the joint force constructs cyberspace, Gray contends that cyberspace operators can repair the damage. Each repair hardens the system against future attacks. Offense can achieve surprise, but response and repair should be routine. Cyberspace defense is difficult, but so is cyberspace offense.[12] As systems are hardened, an attacker must exploit multiple vulnerabilities to achieve the same effect as compared to prior attacks that only required a single exploit.[13]

Speed and Global Reach. Cyberspace exhibits levels of speed and reach uncharacteristic of the other domains. Like other domains, cyberspace operations, especially offensive ones, require significant capability development, planning, reconnaissance, policy, and legal support prior to execution. However, once the JFC decides to act, cyberspace effects can be nearly instantaneous. The global cyberspace domain relegates geography to a subordinate consideration.

Arranging Operations. The *Joint Operational Access Concept* states that the critical support provided by cyberspace operations generally must commence well in advance of other operations as part of efforts to shape the operational area. Even in the absence of open conflict, operations to gain and maintain cyberspace superiority will be a continuous requirement since freedom of action in cyberspace is critical to all joint operations.[14] Chris Demchak offers a cautionary consideration, suggesting that if kinetic operations eventually take place, the United States may see the results of several decades of cyber "preparation of the battlefield," ranging from tainted supply chains to embedded malware.[15]

Resilience. Resilience is the ability to continue operations in a degraded cyber environment while mitigating quickly the impact of any attack. Much like the Quick Reaction Force construct in the physical domain, cyberspace operations require robust DCO-IDM capacity oriented in support of friendly key cyber terrain to respond quickly to mitigate the effects of adversarial cyberspace operations. In concert with these DCO-IDM efforts, the total force will need to implement people, process, and technology measures, such as network minimize procedures or increasing bandwidth capacity, to continue to operate in the degraded environment.

Cyber-Physical Interface. To gain efficiencies, critical infrastructure owners and operators have increasingly connected their once-closed systems to the Internet. As a result, industrial control systems and supervisory control and data acquisition systems are increasingly easy to exploit. These systems are the two primary means for cyber adversaries to achieve direct physical effects through cyberspace.

Decision Integrity. Assuring integrity of operational information is essential to maintaining trust and confidence in the quality of decisionmaking, since making decisions based on wrong information could degrade joint combat power. Without a baseline of what is normal, it is impossible to discern if an adversary has made unauthorized changes to operational information. As Charles Barry and Elihu Zimet observe, "The possession of accurate and timely knowledge and the unfettered ability to distribute this as information have always been the sine qua non of warfighting."[16]

Speed, Not Secrets. Ninety-eight percent of all information is digitized.[17] Adversaries have proved adept at compromising and extracting information from closed networks. In this environment, how long is it reasonable to expect secrecy? The days of having a high degree of confidence that secrets will remain secure are fleeting. Overclassification exacerbates this problem and negatively affects key cyber terrain analysis. The joint force should place value on the ability to make decisions before the adversary compromises key information.

Strategic Attribution. From a strategic perspective, it may be more important to know "Who is to blame?" than "Who did it?"[18] This shift in perspective changes focus from technical attribution, which is difficult, to one of assigning responsibility to a nation-state—more pointedly, to national decisionmakers—for either ignoring, abetting, or conducting cyberspace operations against the United States, its allies, and key partners.

Increase Security, Decrease Freedom of Movement. In other domains, increased security usually implies greater freedom of movement and action. This same concept is not true for cyberspace since increased cybersecurity usually restricts options in cyberspace.

Scope and Scale of Effects. The most sophisticated cyber adversaries have the means to create a regional disturbance for a short period or a local disturbance for a sustained period.[19] The intelligence functions should continually assess the intent and capabilities of potential adversaries to predict the potential scope and scale of effects.

Increased Reliance on Commercial Services. U.S. Central Command's March 2014 posture statement noted the command is "heavily reliant on host nation communications infrastructure across the Central Region."[20] Whereas a JFC can easily partition and militarize the other domains into internationally and nationally recognized contiguous operational areas, cyberspace largely exists via private sector Internet service providers connecting national and military network enclaves.[21] The JFCCC will have to consider this dynamic when attempting to define his cyber joint operational area.

Perpetual, Ambiguous Conflict. Cyberspace is in a perpetual state of conflict that crosses geographic boundaries. Unlike the other domains where one can physically discern unambiguous threat indications and warning, operations in cyberspace are inherently ambiguous. Ambiguity can make war more or less likely. Timothy Junio suggests this is the case because ambiguity "may lead states to overestimate their potential gains, overestimate their stealth, and/or underestimate their adversary's skill."[22] Demchak warns that actions by nonstate actors could lead to unintended escalation as one state misinterprets the action or uses it as cover for its own actions.[23]

Cyber Intelligence. Cyber intelligence—scanning for things that just do not look right by sifting through chatter to discern patterns of intelligence—can become close to police work.[24] When DCO operators detect an adversary, it is difficult to assess adversarial intent. Is the adversary conducting reconnaissance, exfiltrating information, or instrumenting the network for a follow-on operation? A JFCCC must be able to assess cyber situational awareness beyond the joint operational area to understand fully the scope and scale of cyber risks to the theater of operations.

Centralized Control, Centralized Execution. Because any point in cyberspace is equidistant to any other, cyber forces are capable of deploying and surging virtually without the required mobilization time and physical proximity to theater operations. This characteristic is a contributing factor to the centralized control, centralized execution model employed by U.S. Cyber Command. This model affects the development of cyberspace experience across the joint force.

Precedence. There are currently no universally accepted norms of behavior in cyberspace. As such, employment of a cyberspace capability may result in a de facto precedence that other nation-states and nonstate actors may use as a barometer for how they may choose to act in cyberspace. Currently, some senior leaders view offensive cyberspace operations as a last resort, restricting the ability to develop cyberspace experience.

Uncertainty. Whereas the physical characteristics of the other domains are well understood and defined, cyberspace is a constantly changing, dynamic domain that is difficult to model due to its ubiquity and complexity. Unlike the precision of kinetic weapons, there is a level of doubt regarding the use of cyber capabilities in terms of understanding what effects cyber forces can achieve in cyberspace and assessing the success of cyberspace operations. This uncertainty is compounded by a lack of cyber experience and education in the senior ranks, thus creating a circle of uncertainty, reluctance to employ, and lost opportunities

Soldiers training with first fully immersive virtual simulation for infantry at 7th Army Joint Multinational Training Command in Grafenwoehr, Germany, December 2013 (U.S. Army/Markus Rauchenberger)

to gain cyber experience, leading to even greater uncertainty.

The combination of key terms, frameworks, and principles serves as a foundation for an evolving military cyber power theory, which serves as a building block to enhance both the explanatory and predictive power of the JFCCC's recommendations to the JFC. Application of the theory improves the soundness and timeliness of these recommendations. With expert understanding and application of this preliminary military cyber power theory, the JFCCC will be better prepared to provide the JFC recommendations to integrate cyberspace operations in joint operations to preserve and project joint combat power.

Cyberspace Operations as Combat Power

Practitioners validate military theory through application. A successful military theory expertly applied should result in increased combat power for the practitioner. Given the lack of cyberspace operations experience and education in the joint force, it may be difficult to consider how cyberspace operations could contribute to combat power. It does not help that joint doctrine is silent regarding the direct relationship between cyberspace operations and combat power.

Joint Publication (JP) 1-02, *Department of Defense Dictionary of Military and Associated Terms*, defines *combat power* as the total means of destructive and disruptive force that a military unit or formation can apply against an opponent at a given time.[25] The two key words are *destructive* and *disruptive*. Although JP 3-12(R), *Cyberspace Operations*, does not refer to combat power, it implies it by describing direct denial effects achieved through cyberspace attack, which include, in part, the ability to destroy and disrupt adversary targets. The primary doctrinal source for combat power is JP 3-0, *Joint Operations*, in which the JFC is the central focus.

The JFC seeks decisive advantage using all available elements of combat power to seize and maintain the initiative, deny the enemy the opportunity to achieve its objectives, and generate a sense of inevitable failure and defeat in the enemy.[26] Joint doctrine leaves the reader with a sense that there is a bias to operations and effects in the physical domains. For example, JP 3-0 discusses the relative combat power that military forces can generate in terms of delivering forces and materiel. It describes the roles of long-range air and sea operations as effective force projection when timely or unencumbered access to the area of operations is not available. It also

Vice Admiral Jan E. Tighe, commander of Fleet Cyber Command and commander of U.S. 10th Fleet, right, discusses educational requirements for cyber and course matrices that support those requirements (DOD/Javier Chagoya)

discusses combat power in the context of mass, maneuver, economy of force, and surprise. Like JP 3-12(R), JP 3-0 does not reference cyberspace operations in relation to combat power, although it does note that cyberspace superiority may enable freedom of action throughout the operational area. There is clearly an opportunity to link cyberspace operations and combat power in joint doctrine.

In addition to doctrinal references to combat power, the Chairman also publishes operational concepts that provide broad visions for how joint forces will operate in response to specific challenges. For example, the Chairman's *Joint Operational Access Concept* (JOAC) calls for cross-domain synergy to overcome emerging antiaccess/area-denial (A2/AD) challenges. Cross-domain synergy seeks to employ complementary capabilities in different domains such that each enhances the effectiveness and compensates for the vulnerabilities of others.[27] To this end, the JOAC specifically addresses the need for greater and more flexible integration of cyberspace operations into the traditional land-sea-air battlespace. It identifies two combat power–related tasks required to gain and maintain access in the face of armed opposition. The first is overcoming the enemy's A2/AD capabilities through the application of combat power. The second is moving and supporting the necessary combat power over the required distances. Cyberspace operations play a critical role in accomplishing both of these tasks. Fifteen of the 30 capabilities required in the concept are either directly or indirectly associated with the conduct of cyberspace operations, with significant requirements in command and control, intelligence, and fires capabilities. The A2/AD challenge is an excellent operational problem to validate and expand the preliminary military cyber power theory discussed herein.

Conclusion

Stanley Baldwin asserted in 1932 that the "bomber will always get through." History has shown that he was wrong. However, the adoption of this theoretical airpower perspective did drive acquisition, organization, and doctrine leading into World War II. Cyberspace operations share some similarities with the interwar years. Much remains undetermined about the role of cyberspace operations in joint operations and their impact on joint combat power. Yet there are historic examples, key trends, and operational problems that call for increased attention to the need for a military cyber power theory and, consequently, the need for updates to doctrine, organization, and education to inculcate the military cyber power principles presented here.

The Joint Staff should update doctrine to reflect the growing importance of effectively integrating cyberspace operations in joint operations to expand joint combat power. It should update JP 3-12(R) to reflect the need for a JFCCC and incorporate aspects of the preliminary military cyber power theory presented here. Likewise, the Joint Staff should update JP 3-0's description of combat power to broaden and deepen the relationship between cyberspace operations and combat power. Moreover, professional military education and advanced studies programs should include military cyber power theory in the curricula and challenge students to conduct research to evolve the theory.

Organizationally, the JFC should designate a JFCCC for most task force operations. However, depending on the forces assigned, it may be difficult for the JFC to identify a JFCCC candidate that has the preponderance of cyber forces and the best means to command and control those cyber forces. Furthermore, organizations that must address A2/AD in their strategies and operational plans should conduct extensive exercises with a heavy emphasis on cyberspace capabilities.

With expert understanding and application of military cyber power theory, the JFCCC is poised to develop strategic and operational recommendations for the JFC to integrate and synchronize cyberspace operations in joint operations and achieve expanded combat power. The need for integrated cyberspace operations and its contribution to joint combat power is clearly illustrated in one of the most significant operational challenges the joint force will likely face in the future, which is gaining and maintaining operational access in the face of enemy A2/AD capabilities.

The *Joint Operational Access Concept* notes three trends in the operating environment that will likely complicate the challenge of opposed access, one of those being the emergence of cyberspace as an increasingly important and contested domain. The implication is that the JFCCC and his staff are becoming ever more central in assisting the JFC in generating combat power to disrupt, degrade, and defeat enemy A2/AD capabilities. If the joint force is going to be successful in future advanced A2/AD operations, the JFC must fully integrate cyberspace operations into joint operations. A prerequisite for success is the designation of a JFCCC with the requisite professional development, to include expert understanding of and experience applying military cyber power theory. JFQ

Notes

[1] Brett T. Williams, "The Joint Force Commander's Guide to Cyberspace Operations," *Joint Force Quarterly* 73 (2nd Quarter 2014), 12–20.

[2] Brett T. Williams, "Ten Propositions Regarding Cyberspace Operations," *Joint Force Quarterly* 61 (2nd Quarter 2011), 11–17.

[3] Williams, "The Joint Force Commander's Guide."

[4] *Capstone Concept for Joint Operations: Joint Force 2020* (Washington, DC: The Joint Staff, September 10, 2012), 7, available at <www.dtic.mil/doctrine/concepts/ccjo_jointforce2020.pdf>.

[5] Stuart H. Starr, "Toward a Preliminary Theory of Cyberpower," in *Cyberpower and National Security*, ed. Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz (Washington, DC: National Defense University Press/Potomac Books, Inc., 2009), 43–90.

[6] Adapted from Elihu Zimet and Charles L. Barry, "Military Service Overview," in *Cyberpower and National Security*, 285–308.

[7] Colin Gray, *Making Strategic Sense of Cyber Power: Why the Sky Is Not Falling* (Carlisle Barracks, PA: U.S. Army War College, April 2013).

[8] Joint Publication (JP) 3-12(R), *Cyberspace Operations* (Washington, DC: The Joint Staff, February 5, 2013).

[9] Irving Lachow, "Cyber Terrorism: Menace or Myth?" in *Cyberpower and National Security*, 437–464.

[10] Robert Axelrod and Rumen Iliev, "Timing of Cyber Conflict," *Proceedings of the National Academy of Science* 111, no. 4 (January 28, 2014), available at <www.pnas.org/content/111/4/1298.abstract>.

[11] Timothy J. Junio, "How Probable Is Cyber War? Bringing IR Theory Back into the Cyber Conflict Debate," *Journal of Strategic Studies* 36, no. 1 (February 2013).

[12] Gray.

[13] Kim Zetter, *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon* (New York: Crown Publishing, 2014).

[14] *Joint Operational Access Concept* (Washington, DC: The Joint Staff, January 17, 2012).

[15] Peter Dombrowski and Chris C. Demchak, "Cyber War, Cybered Conflict, and the Maritime Domain," *Naval War College Review* (April 2014), available at <www.readperiodicals.com/201404/3271362101.html>.

[16] Zimet and Barry.

[17] Joel Brenner, *America the Vulnerable: Inside the New Threat Matrix of Digital Espionage, Crime, and Warfare* (New York: Penguin Press, 2011).

[18] Jason Healey, *Beyond Attribution: Seeking National Responsibility for Cyber Attacks*, Issue Brief (Washington, DC: The Atlantic Council, 2011), available at <www.fbiic.gov/public/2012/mar/National_Responsibility_for_CyberAttacks,_2012.pdf>.

[19] Armed Forces Communications and Electronics Association 2013 Spring Intelligence Symposium, available at <www.afcea.org/events/globalintelforum/13/welcome.asp>.

[20] *Commander's Posture Statement* (Tampa, FL: U.S. Central Command, March 5, 2014), available at <www.centcom.mil/en/about-centcom-en/commanders-posture-statement-en>.

[21] *Capstone Concept for Joint Operations.*

[22] Junio, 125–133.

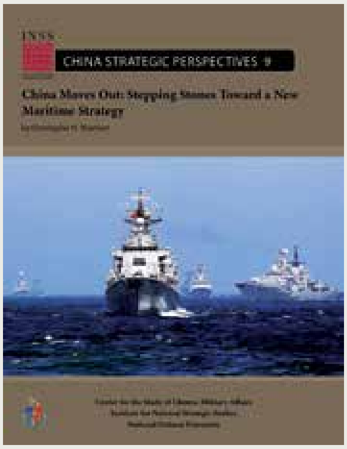
[23] Chris Demchak and Peter Dombrowski, "Cyber Westphalia: Asserting State Prerogatives in Cyberspace," *Georgetown Journal of International Affairs* (Special Issue 2013).

[24] Mark Lowenthal, *Intelligence: From Secrets to Policy*, 5th ed. (Washington, DC: Sage Press, 2013). This is adapted from Lowenthal's description of the intelligence challenge posed by terrorism.

[25] JP 1-02, *Department of Defense Dictionary of Military and Associated Terms* (Washington, DC: The Joint Staff, November 15, 2014).

[26] JP 3-0, *Joint Operations* (Washington, DC: The Joint Staff, August 11, 2011).

[27] *Joint Operational Access Concept, Version 1.0* (Washington, DC: Department of Defense, January 17, 2012), foreword.


INSS
CHINA STRATEGIC PERSPECTIVES 9
China Moves Out: Stepping Stones Toward a New Maritime Strategy