The Utility of Cyberpower

Lt. Col. Kevin L. Parker, U.S. Air Force

AFTER MORE THAN 50 YEARS, the Korean War has not officially ended, but artillery barrages seldom fly across the demilitarized zone.[1] U.S. forces continue to fight in Afghanistan after more than 10 years, with no formal declaration of war.[2] Another conflict rages today with neither bullets nor declarations. In this conflict, U.S. adversaries conduct probes, attacks, and assaults on a daily basis.[3] The offensives are not visible or audible, but they are no less real than artillery shells or improvised explosive devices. This conflict occurs daily through cyberspace.

To fulfill the U.S. military's purpose of defending the nation and advancing national interests, today's complex security environment requires increased engagement in cyberspace.[4] Accordingly, the Department of Defense (DOD) now considers cyberspace an operational domain.[5] Similar to other domains, cyberspace has its own set of distinctive characteristics. These attributes present unique advantages and corresponding limitations. As the character of war changes, comprehending the utility of cyberpower requires assessing its advantages and limitations in potential strategic contexts.

Lt. Col. Kevin L. Parker, U.S. Air Force, is the commander of the 100th Civil Engineer Squadron at RAF Mildenhall, United Kingdom. He holds a B.S. in civil engineering from Texas A&M University, an M.A. in human resource development from Webster University, and an M.S. in military operational art and science and an M.Phil. in military strategy from Air University. He has deployed to Saudi Arabia, Kyrgyzstan, and twice to Iraq.

Defining Cyberspace and Cyberpower

A range of definitions for cyberspace and cyberpower exist, but even the importance of establishing definitions is debated. Daniel Kuehl compiled 14 distinct definitions of cyberspace from various sources, only to conclude he should offer his own.[6] Do exact definitions matter? In bureaucratic organizations, definitions do matter because they facilitate clear division of roles and missions across departments and military services. Within DOD, some duplication of effort may be desirable but comes at a high cost; therefore, definitions are necessary to facilitate the rigorous analyses essential for establishing organizational boundaries and budgets.[7] In executing assigned roles, definitions matter greatly for cross-organizational communication and coordination.

No matter how important, precise definitions to satisfy all viewpoints and contexts are elusive. Consider defining the sea as all the world's oceans. This definition lacks sufficient clarity to demarcate bays or riverine waterways. Seemingly inconsequential, the ambiguity is of great consequence for organizations jurisdictionally bound at a river's edge. Unlike the sea's constant presence for millennia, the Internet is a relatively new phenomenon that continues to expand and evolve rapidly. Pursuing single definitions of cyberspace and cyberpower to put all questions to rest may be futile. David Lonsdale argued that from a strategic perspective, definitions matter little. In his view, "what really matters is to perceive the infosphere as a place that exists, understand the nature of it and regard it as something that can be manipulated and used for strategic advantage."[8] The definitions below are consistent with Lonsdale's viewpoint and suffice for the purposes of this discussion, but they are unlikely to satisfy practitioners who wish to apply them beyond a strategic perspective.

Cyberspace: the domain that exists for inputting, storing, transmitting, and extracting information utilizing the electromagnetic spectrum. It includes all hardware, software, and transmission media used, from an initiator's input (e.g., fingers making keystrokes, speaking into microphones, or feeding documents into scanners) to presentation of the information for user cognition (e.g., images on displays, sound emitted from speakers, or document reproduction) or other action (e.g., guiding an unmanned vehicle or closing valves).

Cyberpower: The potential to use cyberspace to achieve desired outcomes.[9]

U.S. Cyber Command held a joint cyberspace training exercise during November 2011, primarily conducted at the Air Force Red Flag Facility at Nellis Air Force Base, Nev. The exercise brought together approximately 300 cyber and information technology professionals, 2 November 2011. (U.S. Army)

Advantages of Wielding Cyberpower

With these definitions being sufficient for this discussion, consider the advantages of operations through cyberspace.

Cyberspace provides worldwide reach. The number of people, places, and systems interconnecting through cyberspace is growing rapidly.[10] Those connections enhance the military's ability to reach people, places, and systems around the world. Operating in cyberspace provides access to areas denied in other domains. Early airpower advocates claimed airplanes offered an alternative to boots on the ground that could fly past enemy defenses to attack power centers directly.[11] Sophisticated air defenses developed quickly, increasing the risk to aerial attacks and decreasing their advantage. Despite the current cyberdefenses that exist, cyberspace now offers the advantage of access to contested areas without putting operators in harm's way. One example of directly reaching enemy decision makers through cyberspace comes from an event in 2003, before the U.S. invasion of Iraq. U.S. Central Command reportedly emailed Iraqi military officers a message on their secret network advising them to abandon their posts.[12] No other domain had so much reach with so little risk.

Cyberspace enables quick action and concentration. Not only does cyberspace allow worldwide reach, but its speed is unmatched. With aerial refueling, air forces can reach virtually any point on the earth; however, getting there can take hours. Forward basing may reduce response times to minutes, but information through fiber optic cables moves literally at the speed of light. Initiators of cyberattacks can achieve concentration by enlisting the help of other computers. By discretely distributing a virus trained to respond on command, thousands of co-opted botnet computers can instantly initiate a distributed denial-of-service attack. Actors can entice additional users to join their cause voluntarily, as did Russian "patriotic hackers" who joined attacks on Estonia in 2007.[13] With these techniques, large interconnected populations could mobilize on an unprecedented scale in mass, time, and concentration.[14]

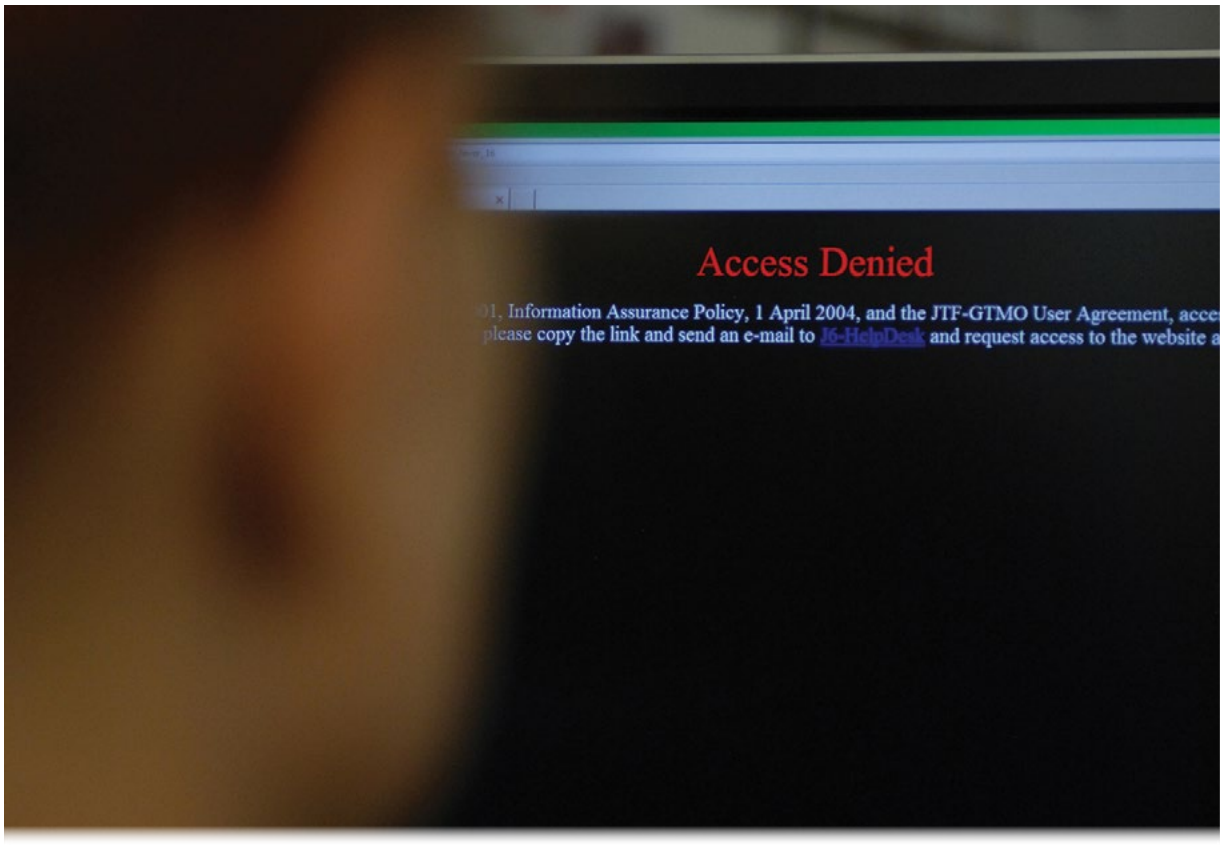
Cyberspace allows anonymity. The Internet's designers placed a high priority on decentralization and built the structure based on the mutual trust of its few users.[15] In the decades since, the number of Internet users and uses has grown exponentially beyond its original conception.[16] The resulting system makes it very difficult to follow an evidentiary trail back to any user.[17] Anonymity allows freedom of action with limited attribution.

Cyberspace favors offense. In Clausewitz' day, defense was stronger, but cyberspace, due to the advantages listed above, currently favors the attack.[18]

Historically, advantages from technological leaps erode over time.[19] However, the current circumstance pits defenders against quick, concentrated attacks, aided by structural security vulnerabilities inherent in the architecture of cyberspace.

Cyberspace expands the spectrum of nonlethal weapons. Joseph Nye described a trend, especially among democracies, of antimilitarism, which makes using force "a politically risky choice."[20] The desire to limit collateral damage often has taken center stage in NATO operations in Afghanistan, but this desire is not limited to counterinsurgencies.[21] Precision-guided munitions and small-diameter bombs are products of efforts to enhance attack capabilities with less risk of collateral damage. Cyberattacks offer nonlethal means of direct action against an adversary.[22] The advantages of cyberpower may be seductive to policymakers, but understanding its limitations should temper such enthusiasm. The most obvious limitation is that your adversary may use all the same advantages against you. Another obvious limitation is its minimal influence on nonnetworked adversaries. Conversely, the more any organization relies on cyberspace, the more vulnerable it is to cyberattack. Three additional limitations require further attention.

Cyberspace attacks rely heavily on second order effects. In Thomas Schelling's terms, there are no brute force options through cyberspace, so cyberoperations rely on coercion.[23] Continental armies can occupy land and take objectives by brute force, but success in operations through cyberspace often hinges on how adversaries react to provided, altered, or withheld information. Cyberattacks creating kinetic effects, such as destructive commands to industrial control systems, are possible. However, the unusual incidents of malicious code causing a Russian pipeline to explode and the Stuxnet worm shutting down Iranian nuclear facility processes were not ends.[24] In the latter case, only Iranian leaders' decisions could realize abandonment of



Access Denied! J-6 Information Assurance runs proxies to protect Joint Task Force Guantanamo servers from malicious websites. Information Assurance defends joint task force servers from internal and external threats while ensuring they comply with Defense Information Systems Agency, U.S. Army, and U.S. Southern Command procedures and policies, Guantanamo Bay, Cuba, 8 July 2008. (U.S. Navy)

nuclear technology pursuits. Similar to strategic bombing's inability to collapse morale in World War II, cyberattacks often rely on unpredictable second order effects.[25] If Rear Adm. Wylie is correct in that war is a matter of control, and "its ultimate tool … is the man on the scene with a gun," then operations through cyberspace can only deliver a lesser form of control.[26] Evgeny Morozov quipped, "Tweets, of course, don't topple governments; people do."[27]

Cyberattacks risk unintended consequences. Just as striking a military installation's power system may have cascading ramifications on a wider population, limiting effects through interconnected cyberspace is difficult. Marksmanship instructors teach shooters to consider their maximum range and what lies beyond their targets. Without maps for all systems, identifying maximum ranges and what lies beyond a target through cyberspace is impossible.

Defending against cyberattacks is possible. The current offensive advantage does not make all defense pointless. Even if intrusions from sophisticated, persistent attacks are inevitable, certain defensive measures (e.g., physical security controls, limiting user access, filtering and anti-virus software, and firewalls) do offer some protection. Redundancy and replication are resilience strategies that can deter some would-be attackers by making attacks futile.[28] Retaliatory responses via cyberspace or other means can also enhance deterrence.[29] Defense is currently disadvantaged, but offense gets no free pass in cyberspace.

Expectations and Recommendations

The advantages and limitations of using cyberpower inform expectations for the future and several recommendations for the military.

Do not expect clear, comprehensive policy soon.[30] Articulating a comprehensive U.S. strategy for employing nuclear weapons lagged 15 years behind their first use, and the timeline for

clear, comprehensive cyberspace policy may take longer.[31] Multiple interests collide in cyberspace, forcing policy makers to address concepts that traditionally have been difficult for Americans to resolve. Cyberspace, like foreign policy, exposes the tension between defaulting to realism in an ungoverned, anarchic system, and aspiring to the liberal ideal of security through mutual recognition of natural rights. Cyberspace policy requires adjudicating between numerous priorities based on

Defending against cyberattacks takes more than firewalls.

esteemed values such as intellectual property rights, the role of government in business, bringing criminals to justice, freedom of speech, national security interests, and personal privacy. None of these issues is new. Cyberspace just weaves them together and presents them from unfamiliar angles. For example, free speech rights may not extend to falsely shouting fire in crowded theaters, but through cyberspace all words are broadcast to a global crowded theater.[32]

Beyond the domestic front, Internet access creates at least one significant foreign policy dilemma. While it can help mobilize and empower dissidents under oppressive governments, it also can provide additional population control tools to authoritarian leaders.[33] The untangling of these sets of overlapping issues in new contexts is not likely to happen quickly. It may take several iterations, and it may only occur in crises. Meanwhile, the military must continue developing capabilities for operating through cyberspace within current policies.

Defend in depth—inner layers. Achieving resilience requires evaluating dependencies and vulnerabilities at all levels. Starting inside the firewall and working outward, defense begins at the lowest unit level. Organizations and functions should be resilient enough to sustain attacks and continue operating. In a period of declining budgets, decision makers will pursue efficiencies through leveraging technology.[34] Therefore, prudence requires reinvesting some of the savings to evaluate and offset vulnerabilities created by new technological dependencies.[35] Future war games should not just evaluate what new technologies can provide, but also they should consider how all capabilities would be affected if denied access to cyberspace.

Beyond basic user responsibilities, forces providing defense against cyberattacks require organizations and command structures particular to their function. Martin van Creveld outlined historical evolutions of command and technological developments. Consistent with his analysis, military cyberdefense leaders should resist the technology-enabled urge to centralize and master all available information at the highest level. Instead, their organizations should act semi-independently, set low decision thresholds, establish meaningful regular information reporting, and use formal and informal communications.[36] These methods can enhance "continuous trial-and-error learning essential to collectively make sense of disabling surprises" and shorten response times.[37] Network structures may be more appropriate for this type of task than traditional hierarchical military structures.[38] Whatever the structure, military leaders must be willing to subordinate tradition and task-organize their defenses for effectiveness against cyberattacks.[39] After all, weapons "do not triumph in battle; rather, success is the product of man–machine weapon systems, their supporting services of all kinds, and the organization, doctrine, and training that launch them into battle."[40]

Defend in depth—outer layers. Defending against cyberattacks takes more than firewalls. Expanding defense in depth requires creatively leveraging influence. DOD has no ownership or jurisdiction over the civilian sectors operating the Internet infrastructure and developing computer hardware and software. However, DOD systems are vulnerable to cyberattack through each of these avenues beyond their control.[41] Richard Clarke recommended federal regulation starting with the Internet backbone as the best way to overcome systemic vulnerabilities.[42] Backlash over potential legislation regulating Internet activity illustrates the problematic nature of regulation.[43] So, how can DOD effect change seemingly beyond its control? Label it "soft power" or "friendly conquest of cyberspace," but the answer lies in leveraging assets.[44]

One of DOD's biggest assets to leverage is its buying power. In 2011, DOD spent over $375 billion on contracts.[45] The military should, of course, use its buying power to insist on strict security standards when purchasing hardware and software. However, it also can use its acquisition process to reduce vulnerabilities through its use of defense contractors. Similar to detailed classification requirements, contracts should specify network security protocols for all contract firms as well as their suppliers, regardless of the services provided. Maintaining stricter security protocols than industry standards would become a condition of lucrative contracts. Through its contracts, allies, and position as the nation's largest employer, DOD can affect preferences to improve outer layer defenses.[46]

Develop an offensive defense. Even in defensive war, Clausewitz recognized the necessity of offense to return enemy blows and achieve victory.[47] Robust offensive capabilities can enhance deterrence by affecting an adversary's decision calculus.[48] DOD must prepare for contingencies calling for offensive support to other domains or independent action through cyberspace.

The military should develop offensive capabilities for potential scenarios but should purposefully define its preparations as defense. Communicating a defensive posture is important to avoid hastening a security-dilemma-inspired cyber–arms race that may have already started.[49] Over 20 nations reportedly have some cyberwar capability.[50] Even if it is too late to slow others' offensive development, controlling the narrative remains important.[51] Just as the name Department of Defense sends a different message than its former name–War Department–developing defensive capabilities to shut down rogue cyberattackers sounds significantly better than developing offensive capabilities that "knock [the enemy] out in the first round."[52]

Do not expect rapid changes in international order or the nature of war. Without question, the world is changing, but world order does not change overnight. Nye detailed changes due to globalization and the spread of information technologies, including diffusion of U.S. power to rising nations and nonstate actors. However, he claimed it was not a "narrative of decline" and wrote, "The United States is unlikely to decay like ancient Rome or even to be surpassed by another state."[53] Adapting to current trends is

Secretary of the Army John McHugh receives an update briefing from staff members of U.S. Army Cyber Command, Fort Belvoir, Va., 2 April 2012. (U.S.Army)

necessary, but changes in the strategic climate are not as dramatic as some proclaim.

Similarly, some aspects of war change with the times while its nature remains constant. Clausewitz advised planning should account for the contemporary character of war.[54] Advances in cyberspace are changing war's character but not totally eclipsing traditional means. Sir John Slessor noted, "If there is one attitude more dangerous than to assume that a future war will be just like the last one, it is to imagine that it will be so utterly different that we can afford to ignore all the lessons of the last one."[55] Further, Lonsdale advised exploiting advances in cyberspace but not to "expect these changes to alter the nature of war."[56] Wars will continue to be governed by politics, affected by chance, and waged by people even if through cyberspace.[57]

Do not overpromise. Advocates of wielding cyberpower must bridle their enthusiasm enough to see that its utility only exists within a strategic context. Colin Gray claimed airpower enthusiasts "all but invited government and the public to ask the wrong questions and hold air force performance to irrelevant standards of superheroic effectiveness."[58] By touting decisive, independent, strategic capabilities, airpower advocates often failed to meet such hyped expectations in actual conflicts. Strategic contexts may have occurred where airpower alone could achieve strategic effects, but more often, airpower was one of many tools employed.

Cyberpower is no different. Gray claimed, "When a new form of war is analyzed and debated, it can be difficult to persuade prophets that prospective efficacy need not be conclusive."[59] Cyberpower advocates must recognize not only its advantages, but also its limitations applied in a strategic context.

Conclusion

If cyberpower is the potential to use cyberspace to achieve desired outcomes, then the strategic context is key to understanding its utility. As the character of war changes and cyberpower joins the fight alongside other domains, military leaders must make sober judgments about what it can contribute to achieving desired outcomes. Decision makers must weigh the opportunities and advantages cyberspace presents against the vulnerabilities and limitations of operations in that domain. Sir Arthur Tedder discounted debate over one military arm or another winning wars single-handedly. He insisted, "All three arms of defense are inevitably involved, though the correct balance between them may and will vary."[60] Today's wars may involve more arms, but Tedder's concept of applying a mix of tools based on their advantages and limitations in the strategic context still stands as good advice. ***MR***

NOTES

1. See Chico Harlan, "Korean DMZ troops exchange gunfire," *Washington Post*, 30 October 2010, <http://www.washingtonpost.com/wp-dyn/content/article/2010/10/29/AR2010102906427.html>. Bullets occasionally fly across the demilitarized zone, but occurrences are rare.

2. See *Authorization for Use of Military Force*, Public Law 107-40, 107th Cong., 18 September 2001, <http://www.gpo.gov/fdsys/pkg/PLAW-107publ40/html/PLAW-107publ40.htm>. The use of military force in Afghanistan was authorized by the U.S. Congress in 2001 through Public Law 107-40, which does not include a declaration of war.

3. "DOD systems are probed by unauthorized users approximately 250,000 times an hour, over 6 million times a day." Gen. Keith Alexander, director, National Security Agency and Commander, U.S. Cyber Command (remarks, Center for Strategic and International Studies Cybersecurity Policy Debate Series: US Cybersecurity Policy and the Role of US Cybercom, Washington, DC, 3 June 2010, 5), <http://www.nsa.gov/public_info/_files/speeches_testimonies/100603_alexander_transcript.pdf>.

4. "The purpose of this document is to provide the ways and means by which our military will advance our enduring national interests … and to accomplish the defense objectives in the *2010 Quadrennial Defense Review*." Joint Chiefs of Staff, *The National Military Strategy of the United States of America, 2011: Redefining America's Military Leadership* (Washington, DC: United States Government Printing Office [GPO], 8 February 2011), i.

5. DOD, *DOD Strategy for Operating in Cyberspace* (Washington, DC: GPO, July 2011), 5.

6. Daniel T. Kuehl, "From Cyberspace to Cyberpower: Defining the Problem," in *Cyberpower and National Security*, eds. Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz (Dulles, VA: Potomac Books, 2009): 26-28.

7. Staff Report to the Senate Committee on Armed Services, *Defense Organization: The Need for Change*, 99th Cong., 1st sess., 1985, Committee Print, 442-44.

8. David J. Lonsdale, *The Nature of War in the Information Age: Clausewitzian Future* (London: Frank Cass, 2004), 182.

9. See Joseph S. Nye, Jr., *The Future of Power* (New York: PublicAffairs, 2011), 123. This definition is influenced by the work of Nye.

10. "From 2000 to 2010, global Internet usage increased from 360 million to over 2 billion people," *DOD Strategy for Operating in Cyberspace*, 1.

11. Giulio Douhet, *The Command of the Air* (Tuscaloosa, AL: University of Alabama Press, 2009), 9.

12. Richard A. Clarke and Robert K. Knake, *Cyber War: The Next Threat to National Security and What To Do About It* (New York: HarperCollins Publisher, 2010), 9-10.

13. Nye, 126.

14. Audrey Kurth Cronin, "Cyber-Mobilization: The New *Levée en Masse*," *Parameters* (Summer 2006): 77-87.

15. Clarke and Knake, 81-84.

16. See Clarke and Knake, 84-85. Trends in the number of Internet-connected devices threaten to use up all 4.29 billion available addresses based on the original 32-bit numbering system.

17. Clay Wilson, "Cyber Crime," in *Cyberpower and National Security*, eds. Franklin D. Kramer, Stuart H. Starr, Larry Wentz (Washington, DC: NDU Press, 2009), 428.

18. Carl von Clausewitz, *On War*, ed. and trans. Michael Howard and Peter Paret (Princeton, NJ: Princeton University Press, 1976), 357; John B. Sheldon, "Deciphering Cyberpower: Strategic Purpose in Peace and War," *Strategic Studies Quarterly* (Summer 2011): 98.

19. Martin van Creveld, *Command in War* (Cambridge, MA: Harvard University Press, 1985), 231.

20. Nye, 30.

21. Dexter Filkins, "US Tightens Airstrike Policy in Afghanistan," *New York Times*,

21 June 2009, <http://www.nytimes.com/2009/06/22/world/asia/22airstrikes.html>.

22. "We will improve our cyberspace capabilities so they can often achieve significant and proportionate effects with less cost and lower collateral impact." Chairman of the Joint Chiefs of Staff, *The National Military Strategy of the United States of America 2011: Redefining America's Military Leadership,* (Washington, DC: GPO, 2011), 19.

23. Thomas C. Schelling, *Arms and Influence* (New Haven, CT: Yale University, 2008), 2-4.

24. For Russian pipeline, see Clarke and Knake, 93; for Stuxnet, see Nye, 127.

25. Lonsdale, 143-45.

26. Rear Adm. J.C. Wylie, *Military Strategy: A General Theory of Power Control* (Annapolis, MD: Naval Institute Press, 1989), 74.

27. Evgeny Morozov, *The Net Delusion: The Dark Side of Internet Freedom* (New York: PublicAffairs, 2011), 19.

28. Nye, 147.

29. Richard L. Kugler, "Deterrence of Cyber Attacks," *Cyberpower and National Security*, eds. Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz (Washington, DC: NDU Press, 2009), 320.

30. See United States Office of the President, *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World*, May 2011.

31. See Clarke and Knake, 155. International strategy for cyberspace addresses diplomacy, defense, and development in cyberspace but fails to outline relative priorities for conflicting policy interests. 31.

32. First Amendment free speech rights and their limits have been a contentious issue for decades. "Shouting fire in a crowded theater" comes from a 1919 U.S. Supreme Court case, Schenck v. United States. Justice Oliver Wendell Holmes' established context as relevant for limiting free speech. An "imminent lawless action" test superseded his "clear and present danger" test in 1969, <http://www.pbs.org/wnet/supremecourt/capitalism/landmark_schenck.html>.

33. Morozov, 28.

34. "Today's information technology capabilities have made this vision [of precision logistics] possible, and tomorrow's demand for efficiency has made the need urgent." Gen. Norton Schwartz, chief of staff, U.S. Air Force, "Toward More Efficient Military Logistics," address on 29 March 2011, to the 27th Annual Logistics Conference and Exhibition, Miami, FL, <http://www.af.mil/shared/media/document/AFD-110330-053.pdf>.

35. Chris C. Demchak, *Wars of Disruption and Resilience: Cybered Conflict, Power, and National Security* (Athens, GA: University of Georgia Press, 2011), 44.

36. Van Creveld, 269-70.

37. Demchak, 73.

38. Antoine Bousquet, *The Scientific Way of Warfare: Order and Chaos on the Battlefields of Modernity* (New York: Columbia University Press, 2009), 228-29.

39. See R.A. Ratcliff, *Delusions of Intelligence: Enigma, Ultra, and the End of Secure Ciphers* (Cambridge, UK: Cambridge University Press, 2006), 229-30. Allied World War II Enigma code-breaking offers a successful example of creatively task-organizing without rigid hierarchy.

40. Colin S. Gray, *Explorations in Strategy* (Westport, CT: Praeger, 1996), 133.

41. *DOD Strategy for Operating in Cyberspace*, 8.

42. Clarke and Knake, 160.

43 Geoffrey A. Fowler, "Wikipedia, Google Go Black to Protest SOPA," *Wall Street Journal*, 18 January 2012, <http://online.wsj.com/article/SB10001424052970204555904577167873208040252.html?mod=WSJ_Tech_LEADTop>; Associated Press, "White House objects to legislation that would undermine 'dynamic' Internet," *Washington Post*, 14 January 2012, <http://www.washingtonpost.com/politics/courts-law/white-house-objects-to-legislation-that-would-undermine-dynamic-internet/2012/01/14/gIQAJsFcyP_story.html>.

44. "Soft power," see Nye, 81-82; "friendly conquest," see Martin C. Libicki, *Conquest in Cyberspace: National Security and Information Warfare* (Cambridge, UK: Cambridge University Press, 2007), 166.

45. U.S. Government, USASpending.gov official Web site, "Prime Award Spending Data," <http://www.usaspending.gov/explore?carryfilters=on> (18 January 2012). "2011" refers to the fiscal year.

46. DOD Web site, "About the Department of Defense," <http://www.defense.gov/about> (18 January 2012). DOD employs 1.4 million active, 1.1 million National Guard/Reserve, 718,000 civilian personnel.

47. Clausewitz, 357.

48. Kugler, "Deterrence of Cyber Attacks," 335.

49. "Many observers postulate that multiple actors are developing expert [cyber] attack capabilities." Ibid., 337.

50. Clarke and Knake, 144.

51. "Narratives are particularly important in framing issues in persuasive ways." Nye, 93-94.

52. Quote from Gen. Robert Elder as commander of Air Force Cyber Command. See Clarke and Knake, 158; Defense Tech, "Chinese Cyberwar Alert!" 15 June 2007, <http://defensetech.org/2007/06/15/chinese-cyberwar-alert>.

53. Nye, 234.

54. Clausewitz, 220.

55. John Cotesworth Slessor, *Air Power and Armies* (Tuscaloosa, AL: University of Alabama Press, 2009), iv.

56. Lonsdale, 232.

57. Clausewitz, 89.

58. Gray, 58.

59. Colin S. Gray, *Modern Strategy* (Oxford, UK: Oxford University Press, 1999), 270.

60. Arthur W. Tedder, *Air Power in War,* (Tuscaloosa: University of Alabama Press, 2010), 88.