CHAPTER 10

An Environmental Approach to Understanding Cyberpower

Gregory J. Rattray

CYBERSPACE has increasingly become an environment in which the United States and actors around the globe act, cooperate, and compete. Achieving their objectives will require influencing other actors by orchestrating power in this realm. We do not yet have enough historical experience to fully understand the fast-evolving nature of cyber conflict and cyberpower. However, it helps if we understand the factors that underpin it. This chapter, therefore, illuminates key aspects of cyberpower by comparing and contrasting the cyber environment in light of theories of power in other environments: land, sea, air, and space. Control of key aspects of the operating environment enhances an actor's power. Inability to obtain access or sustain control can limit the range of political, diplomatic, economic, military, and informational aspects of power. For example, control over land areas such as Asia Minor, a major bridge between Asia, Europe, and Africa through which armies and trade routes have passed for millennia, has influenced the destiny of civilizations. At sea, the ability to dominate straits such as Gibraltar or Malacca have enabled empires to ensure the rapid transit of military force and secure shipping lanes essential to their economies. For the last century, freedom to operate air forces over battlefields and provide supplies via an air bridge has been fundamental to both military operations and diplomatic successes, such as the Berlin Airlift. In space, key positions such as spots for geosynchronous orbits have become the object of competition among nations and commercial corporations because they enhance the ability to conduct communications and intelligence operations.

By analogy, we seek to understand the new environment of cyberspace. Thus, this chapter first reviews the particular characteristics of the cyberspace environment that affect its strategic features. It then summarizes previous environmental theories of land power, seapower, airpower, and spacepower. A third section reviews the sources of power in each of these environments: technological advances, changes in speed and scope of operations, control of key features, and mobilization of national resources. Two distinct features of cyberspace—offense dominance and the rapidity of change—are examined. The chapter concludes with recommendations for the United States to address challenges of generating cyberpower.

Cyberspace as an Environment

The term *cyberspace* came into broad use during the early 1990s, when cyber-space was viewed as fundamentally different than the normal physical world. However, cyberspace is actually a physical environment: it is created by the connection of physical systems and networks, managed by rules set in software and communications protocols.[1] Discussion of cyberspace in the national security realm largely evolved from the interest in information warfare, particularly computer and network warfare.[2]

The United States increasingly stresses the concept of cyberspace as an operating environment. The Nation's leaders have begun to recognize the significance of this environment for U.S. security. Since the attacks of 9/11, security objectives have changed, as recognized in this statement from the 2002 *National Security Strategy of the United States of America*: "We are menaced less by fleets and armies than by catastrophic technologies in the hands of the embittered few."[3] The *National Defense Strategy of the United States of*

America asserted the need to secure strategic access and retain global freedom of action, particularly through the control of the global commons, in order to deal with traditional, irregular, catastrophic, or disruptive threats. The National Defense Strategy of 2005 identified cyberspace, along with space and international waters and airspace, as a global commons and cyber operations as a disruptive challenge. It explicitly states that "cyberspace is a new theater of operations."[4]

U.S. national policy has recognized the need to protect U.S. cyberspace. The Clinton administration issued Presidential Decision Directive 68, "Critical Infrastructure Protection," putting protection of key U.S. assets against cyber attack on par with defense against physical strikes. The Bush administration extended this effort; its 2002 *National Strategy to Secure Cyberspace* outlined key efforts necessary to:

> reduce our vulnerabilities to these threats before they can be exploited to damage the cyber systems supporting our Nation's critical infrastructures and to ensure that such disruptions of cyberspace are infrequent, of minimal duration, manageable, and cause the least damage possible.[5]

The Defense Department, Department of Justice, Federal Bureau of Investigation, Intelligence Community, and other Federal agencies have established organizations and programs to deal with cyberspace issues and roles related to their respective national security missions. The Department of Homeland Security, in particular, is expressly charged with protecting the United States against terrorist attacks in cyberspace. The department set up a National Cyber Security Division in September 2003, and in the fall of 2006, an Assistant Secretary for Cybersecurity and Telecommunications was appointed, with responsibility for orchestrating the full range of the department's activities in this realm.

Cyberpower, as we use the term in this book, is the ability to use cyberspace to strategic advantage and to influence events in the other operational environments and across the instruments of power.[6] As with control of land masses, crucial sea lanes, airspace, or satellite orbits, cyberpower has risen as a key factor in the capacity of states and other actors in the international system to project influence:

> Successful military operations depend on the ability to protect information infrastructure and data. Increased dependence on information networks creates new vulnerabilities that adversaries may seek to exploit.[7]

Ensuring that we have adequate influence and control in the cyberspace commons and can keep it from becoming a launching ground from which our adversaries can strike with impunity has increasingly become a goal of U.S. national strategy. Military operations, economic activity, and transit of ideas across other domains—land, sea, air, and space—rely more and more on the effective functioning of cyberspace. Cyberpower has become a fundamental enabler for the full range of instruments of national power: political, diplomatic, economic, military, and informational.

Strategic Features of the Cyberspace Environment

Cyberspace comprises both physical and logical systems and infrastructures that are

governed by laws of physics as well as the logic of computer code. The principal physical laws governing cyberspace are those related to electromagnetism and light. The speed at which waves propagate and electrons move creates both advantages and challenges: global communications across cyberspace can happen nearly instantaneously, and vast amounts of data can rapidly transit great distances, often unimpeded by physical barriers and political boundaries.

This speed and freedom of movement creates challenges and advantages for individuals, organizations, and states, but at the same time it creates weaknesses that could be exploited by adversaries.

In cyberspace, like air and space, almost all activities involve the use of technology. Cyberspace is unique in that the interactions are governed by hardware and software that is manmade, so the "geography" of cyberspace is much more mutable than other environments. Mountains and oceans are hard to move, but portions of cyberspace can be turned on and off with the flick of a switch; they can be created or "moved" by insertion of new coded instructions in a router or switch. Cyberspace is not, however, infinitely malleable: limits on the pace and scope of change are governed by physical laws, logical properties of code, and the capacities of organizations and people.

The systems and infrastructures that make up cyberspace have varying degrees of interconnectivity. A home computer with a printer but no other connection utilizes cyberspace but is a very small, isolated enclave. A radio transmitter can reach a broader number of devices in its broadcast area with a one-way message. The Internet has become the prime example of a massive global network. In cyberspace, ever-increasing numbers of hardware devices have significant degrees of interconnectivity moderated by software and protocol rules. The recent explosion of digital standards for wireless transmission is leading to a fusion of wired and wireless systems, as has the convergence of transmission control protocol/Internet protocol (IP) as the most useful standards for facilitating transit of information between systems.

Although economic imperatives and the desire to widen circles of communication have led to the rapid growth of a global information infrastructure, governments, corporations, and individuals can and do control how much interconnection they establish. Boundaries are established in cyberspace by choices in how to employ hardware, software, and standards. For example, the governments that set up the International Telecommunications Union required use of certain protocols to carry telephone traffic over international circuits under their purview. Thus, states had some sovereignty over their respective telephony systems, giving them the capacity to govern the economics of international calling and to monitor the communications of their citizens.[8] The current emergence of voice over Internet protocol as an alternative for long-distance voice conversations undermines that ability and keeps governments from using standards to establish enclaves within their political-geographic borders. Still, just as governments may jam undesirable radio and television broadcasts from outside their geographic borders, now the People's Republic of China, regimes in the Middle East, and other states endeavor to employ software filters and other techniques to limit where their citizens can traverse within the global Internet.[9]

Actors in the Cyberspace Environment

The challenge of managing the technological foundations of cyberspace means that human capital is a fundamental influence on the use of this environment. Skilled people

operate the systems, engineer the infrastructures, and drive the innovations necessary for achieving advantages in cyberspace. While this is also true on land and sea and in air and space, the speed of technological change in the early 21st century ensures that, to sustain advantages in using cyberspace for military, economic, or informational purposes, nations must focus on nurturing this core resource with its constant requirement for learning and training.

The number of actors who play a significant role in cyberspace is also a distinguishing feature. States do not, and cannot, control cyberspace to the same degree as they can with land, sea, and air, or even as they could control cyberspace in the past: for example, during both World Wars, the U.S. Government took control of the operation of the Nation's predominant telephone provider, American Telephone & Telegraph (AT&T).[10] That was possible because at that time, AT&T alone provided almost all of the network hardware and determined the communications rule sets that allowed the telephone system to work (although it did so under close regulation by the government). Now, however, in the United States and elsewhere, there are myriad providers of devices, connectivity, and services in loosely woven networks with open standards. Governments would have extreme difficulty in controlling the full spectrum of telecommunications and other activities in cyberspace.

Establishing sovereignty, or deciding on rules to govern the global cyber-space commons, creates major challenges and growing national security concerns for state actors.[11] With telephone networks, governments had ways to control connectivity beyond their borders. However, over time, non-state actors— corporations, nongovernmental organizations, public interest groups—have also become influential; it is not just states that set standards or determine the rules of the road. In many respects, governance in cyberspace resembles the American "Wild West" of the 1870s and 1880s, with limited governmental authority and engagement. Users, whether organizations or individuals, must typically provide for their own security. Theories and approaches for exercising state control, and for leveraging control for national power, have not yet been developed.

Environmental Theories of Power

To understand the growing significance of cyberspace, it helps to examine how strategic theorists have addressed questions of national power in other environments. Theories related to land, sea, air, and outer space power share common elements that an environmental theory of cyberpower ought to address. We also identify unique features that distinguish these theories from one another.

Land Power

Theories of military strategy and national power have existed since the rise of civilizations, but two major, competing theories about how control over specific environments affects national power came to prominence in the late 19th century. The *heartland theory*, articulated by Halford John Mackinder, focused on the increasingly intense national competition in Europe at the turn of the 20th century. Major powers were competing globally, establishing colonies and seeking the upper hand militarily. Mackinder contrasted nations with control over the Eurasian heartland, such Germany and Russia, with nations that operated on the periphery, such as England and the United States. He noted how rapid industrialization and technologies such as the railroad and telegraph were helping transform the

speed and scale of military operations. Mackinder predicted that the ability to mobilize the resources of the heartland to utilize the new transportation and communications technologies would enable the heartland nations to establish protected lines of communication and engage in military operations quickly at places of their choosing. Thus, he wrote: "Who rules East Europe commands the Heartland; who rules the Heartland commands the World-Island; who rules the World-Island controls the world."[12]

In contrast was the *rimland theory* published by Nicholas Spykman in 1944.[13] Examining the course of World War I, with attention to the security arrangements that could ensure stability after World War II, Spykman's theory contrasted sharply with that of Mackinder. Spykman saw the key sources of power in the population and material goods on the rim of the Eurasian continent, in the Western European peninsula, and in East Asia. Developments in military operations, such as amphibious warfare and carrier- and land-based airpower, would allow rimland nations to apply power at key pressure points around the Eurasian land mass and elsewhere on the globe. Spykman explicitly restated Mackinder's propositions: "Who controls the rimland rules Eurasia; Who rules Eurasia controls the destinies of the world."[14]

British, Russian, and U.S. power would, said Spykman, play the key roles in controlling the European littoral and thereby the essential power relations of the world. External lines of communication, in his view, now provided the dominant means for nations to employ military power, secure their economic interests, and provide for global stability.

Just as Mackinder and Spykman did for land power, those who would develop a theory of cyberpower must determine the key resources and focal points for transit in cyberspace.

Seapower

Focused more on the characteristics of the environment, theories of seapower arose even prior to the land power theories of Mackinder and Spykman. In 1890, Alfred Thayer Mahan published *The Influence of Sea Power upon History, 1660–1783*.[15]

This work, widely discussed in the United States and Europe, articulated principles about the relationship between a nation's seapower and its overall power. When Mahan wrote, rapid developments in technology—steam power, screw propulsion, armor for ships, and guns with longer range and increased accuracy—were changing the nature of seapower. The growth of steam power required navies to establish far-flung coaling stations and repair facilities to sustain a global naval presence.

In Mahan's view, naval power was fundamental to a nation's grand strategy, for economic power derived from maritime trade. Defining the conditions necessary for a nation to develop seapower, he stressed that mobilization of naval power in both military and merchant fleets was a national priority in order to secure global presence, maximize trade, and enable the projection of power ashore. Mahan wrote that:

> the growth of sea power in the broad sense . . . includes not only the military strength afloat, that rules the sea or any part of it by force of arms, but also the peaceful commerce and shipping from which alone a military fleet naturally and healthfully springs and upon which it securely rests.[16]

To command sea lanes of communication, Mahan advocated a large main battle fleet equipped to fight decisive battles, to maintain naval supremacy, and to guarantee secure trade with colonies. He also stressed the natural advantages of certain nations that controlled chokepoints, such as straits between key bodies of water and the approaches to major river systems.[17]

British naval theorist Julian Corbett was influenced by Mahan as well as by the German strategist Carl von Clausewitz. Writing before World War I, Corbett attributed Great Britain's success to its integration of maritime, military, economic, and diplomatic resources.[18] Naval strategy—the operational and tactical movement of the fleet—was, he argued, a subset of maritime strategy. He looked more broadly than Mahan at the utility of maritime power, examining its role in limited wars: he argued that "he who commands the sea is at great liberty and can take as much or as little of the war as he will" by putting land forces into conflicts at chosen places and times.[19] Corbett argued that a major "fleet in being" might be sufficient to deter an adversary from attempting to disrupt or deny a nation's vital commerce.

Seapower theory dealt explicitly with how control of an environment enabled global maneuver and with the impact of technological change. We can draw lessons from it for understanding the development of cyberspace. For example, much of cyberspace relies on fiber optic cables that transit the seabed; these cables and associated facilities may constitute new chokepoints.[20] Alternative routes will exist in cyberspace, such as satellites for intercontinental connectivity, but these alternatives, too, might be potential chokepoints. As such, each offers a potential locus of national control.

Airpower

The legacy of World War I influenced the airpower theorists of the early and mid-20th century, in particular Giulio Douhet of Italy, William (Billy) Mitchell of the United States, and Hugh Trenchard of Great Britain. All three were participants in the rapid development of airpower in the Great War, and they drew similar conclusions about its future role in warfare. As the technology of the airplane rapidly improved, it would enhance the capacity of airpower to strike directly at an enemy, "smashing the material and moral resources of a people," said Douhet, "until the final collapse of all social organization."[21] Trenchard asserted that "the ratio of morale to material effect was 20:1."[22] The bomber, he claimed, would dominate the air and be effectively unstoppable by defenses. "Viewed in its true light, aerial warfare admits no defense, only offense," argued Douhet, failing to anticipate defensive technology such as radar and advanced interceptors.

Future wars, argued these three theorists, would be short, and they would be dominated by those with sufficient airpower. Large land or sea forces or extensive mobilization would be unneeded. Surprise and preemptive airstrikes would constitute the strategic imperative for all advanced nations. According to Mitchell,

> The advent of air power, which can go straight to the vital centers and neutralize or destroy them, has put a completely new complexion on the old system of making war. It is now realized that the hostile main army in the field is a false objective.[23]

The airpower theorists were not particularly concerned with broader issues of grand strategy and national power, although Mitchell stressed the need to make airpower a national priority to ensure the ability to keep up with rapid technological change.[24] Mitchell argued

that airpower could provide a cheap source of security and avoid the large expenditures, conscription, and taxes required to maintain standing armies. All three were dismissive of diplomatic interest in arms control to manage future conflicts. Douhet asserted: "All the restrictions, all the international agreements made during peacetime are fated to be swept away like dried leaves on the winds of war."[25]

New questions arose in the early 20th century with the rise of airpower, such as the significance of offense-defense interaction, the impact of a new kind of power on defense budgets and economic burdens, and the possibilities and limitations for international cooperation in securing control over a new domain. Such questions must now be explored with regard to cyberspace.

Spacepower

As technology advanced, nations and corporations extended military and commercial activity beyond the atmosphere into space. Control of space and how it could affect national power and global issues has become a focus for strategists. The advent of intercontinental ballistic missiles and the development of intelligence and communications satellites in the 1950s and 1960s led to strategic concern over space. National security strategists wrestled with the implications of an agreed ban on antiballistic missiles. Over time, the United States and others have increasingly focused on space as an arena for national competition. President Reagan established the Strategic Defense Initiative, envisioning the use of space-based assets to protect the United States from Russian intercontinental ballistic missiles.[26] The 2000 Space Commission report to Congress asserted the importance of the "security and economic well-being of the United States and its allies and friends" to "the nation's ability to operate successfully in space."[27]

The 2005 National Defense Strategy identifies space as a global commons, a shared resource and arena, like international waters, airspace, and cyberspace.[28] Space is increasingly an area of international military competition, as China's demonstration of its antisatellite capabilities in January 2007 made clear.[29]

In a 1999 review of geopolitics and strategy, Colin Gray and Geoffrey Sloan explicitly addressed the challenges of strategy in Earth, moon, and solar spaces.[30] They stressed the strategic significance of locations in space. For example, geosynchronous orbits are prized locations for satellites whose function (such as telecommunications) requires them to match the Earth's rotation in order to remain over a specific point on the Earth. Locations where the gravitational pull of the Earth and moon is equal (known as LaGrangian points) also offer operating advantages particularly useful for space transport and maintaining the growing manned presence in space.

Mark Harter recently asserted that space is the new "high ground":

> Space systems will significantly improve friendly forces' ability to strike at the enemy's heart or COGs [centers of gravity], paralyzing an adversary to allow land, sea and air forces to achieve rapid dominance of the battlespace.[31]

Space forces, he argued, will also conduct separate, parallel strategic campaigns with a global reach, such as warning and defending against ballistic missile launches. At the level of grand strategy, in his view, space systems can provide a means to exercise other "instruments of national power (diplomatic, informational, military, and economic) to force an enemy to

capitulate."[32] Increasing reliance on space for achieving national military and economic goals requires dedicated U.S. efforts to ensure access and ability to defend and control the space environment. He argues, similarly to Mahan and Mitchell, that national spacepower should be part of an overall national effort involving coordinated military, governmental, civil, scientific, commercial, allied, and international efforts.

Harter explicitly identifies linkages with cyberspace, stressing the reliance on space to carry information globally, and network warfare operations that make use of space systems.[33] Space satellites and their orbital locations are chokepoints in the cyber world.

Comparing Environment: Sources of Power

This overview of environmental theories of power provides a basis for identifying their common features. We focus on four common threads:

- technological advances
- speed and scope of operations
- control of key features
- national mobilization.

While all the existing theories deal substantially with major technological changes, many failed to see how continuing technological evolution could undermine major tenets they proposed. They also dealt with how the nature of the environment enables the use of military power. Additionally, we must keep in mind that rapid political change will affect how cyberpower evolves.

Technological Advances

A major imperative for most of the theories was to predict the political-military impact of technological advances. For Mackinder, the advent of rail transportation and telegraph communication meant that the nation or nations controlling the heartland would be in position to assert global rule. As Eurasia began to be covered by an extensive network of railroads, a powerful continental nation might be able to extend its political control over the Eastern European gateway to the Eurasian landmass. As Mahan saw it, the advent of steam meant that global trade and presence through maritime power would be the primary path to success for nations that could develop such capacities.

The airpower theorists thought that the rise of unstoppable strategic bombers would mean that direct strikes at the enemy centers of gravity would decide future conflicts. The ability of man to move into space led theorists such as Gray, Sloan, and Harter to argue that sustained space presence will be an essential enabler of both military operations and control over the global information infrastructure. The advent of the Internet, the opportunities for information exchange and social dialogue created by the World Wide Web, and the growing ubiquity of wireless and digital connectivity all have implications for the nature of political, economic, and military interactions. Use of the electromagnetic spectrum outside of visible light to achieve influence and conduct conflicts began, however, with the 19th century, not the 21st. The advent of the telegraph had major impacts on economic affairs, political reporting, and the conduct of diplomatic military operations. In both World Wars, radio broadcasts provided a major

vehicle for propaganda, and governments endeavored to block these messages through jamming. Later in the 20th century, Marshall McLuhan examined the impact of the relatively new medium of television, examining how people and governments were influenced by images broadcast from the faraway war in Southeast Asia.[34] The digital age of the Internet has provided new arenas for political struggles. Hackers with political motives have taken over Web sites and placed confrontational messages and other propaganda. In the spring of 2007, dissidents with ethnic Russian sympathies organized a disruptive series of cyber attacks that affected the Estonian government, banking, and other sectors.[35] Organizations engaged in economic competition increasingly rely on cyber-space as a source of advantage. The revolution in cost controls and just-in-time production systems by companies like Dell Computers in the 1990s was made possible by the ability to collect and process large amounts of data rapidly. New forms of e-commerce retail operations by Amazon and new markets such as those created by eBay have emerged. These activities are increasingly global; US and European firms produce and deliver complex software and hardware utilizing the output of far-flung research centers and manufacturing plants in places ranging from Redmond, Washington, to Dublin, to Beijing. Satellites and undersea fiber optic cables allow companies to take advantage of human capital available at lower costs in other countries.

The evolution of cyberspace is also enabling new forms of warfare. The extension of conflict to cyberspace began as early as the Crimean War when the telegraph was used to transmit intelligence reports and to command widely dispersed forces. In World War I, radio became another major mode of long-distance communications with far-flung military forces. Competition to control the use of the electromagnetic spectrum increasingly became a major feature of air, naval, and intelligence operations during World War II. The U.S. Department of Defense is now pushing toward net-centric operations based on digital communications and ease of access to information at all levels, down to the individual soldier on the battlefield. Special Forces units mounted on horseback operating against Taliban positions in Afghanistan called down global positioning system–guided precision airstrikes from B–52s they could not see. New U.S. fighter aircraft such as the F–22 carry sensor systems that allow them to share data in real time about activity in the electromagnetic spectrum both with higher headquarters and with other units conducting tactical operations. Global advantages accrue to those capable of creating information-enhanced forms of traditional military operations, but most require very deep pockets. However, smaller nonstate actors have also adapted to advances in cyberspace. With Iranian assistance, for example, Hizballah negated Israeli communications jamming and succeeded in their own efforts during the 2006 conflict in southern Lebanon.[36]

Reliance on cyberspace and issues of control over sensitive information and network availability present crucial risk management decisions to governments, corporations, and other actors (as described in chapter 7 of this volume, "Information Security Issues in Cyberspace"). A growing source of advantage to actors in cyberspace competition will be the capacity to evaluate tradeoffs related to operational value, connectivity, costs, vulnerabilities, and threats and to strike an effective balance.

The rise of digital connectivity will have transformative impacts. Just as the telegraph and railroads brought about major shifts in advantages in the age-old struggle to dominate land masses, key features of how digital communications operates will transform the landscape of opportunities in cyberspace. A crucial new feature of the Internet and the World Wide Web is the ease with which individuals and small groups can access them and send messages out to global audiences without revealing their location. The Internet was not designed to help track the

origin of activity, and challenges have continued to mount as actors have devised new methods of indirection and anonymization to hide their identity and location. Dissident Falun Gong groups provide communications for their members in and outside of the People's Republic of China and have even hijacked official Chinese satellite television broadcasts.[37] Sites run by Islamic extremists on the Internet incite individual acts of violence and terrorism against Western regimes and provide detailed information regarding bombmaking techniques and other ways to target the adversaries' society (as described in chapter 19 in this volume, "Cyber Terrorism: Menace or Myth?").

The new digital media are interactive, unlike earlier radio and television broadcast media. Web sites, Internet chat rooms, and text messaging are part of a wide, rapidly merging set of global services that have resulted in an explosion of new social network opportunities. The disruptive possibilities for misuse of this connectivity extend into political competition. Terrorist groups with a variety of objectives have turned to cyberspace as an environment for conducting recruitment and fundraising.[38]

The ease of achieving anonymity on the Internet also facilitates rapid orchestration of operations across wide geographic areas with less chance of tipping off adversaries that disruptive attacks are imminent. The 2004 Madrid train bombers, for example, reportedly used "a program downloaded from the Internet by which text messages could activate mobile phones simultaneously" to set off multiple explosions.[39]

Presence in cyberspace and ease of connectivity also create new vulnerabilities to attack. Accessibility and anonymity have produced an environment in which smaller organizations and political actors, especially those who seek to avoid vulnerabilities to retribution in other environments, can achieve a disproportional increase in capabilities to conduct their operations and disrupt those of adversaries.

The increasing use of the Internet and other aspects of the cyber environment by advanced states to orchestrate the operations of their energy, transportation, and other infrastructures creates new strategic vulnerabilities (described in chapter 23 in this volume, "Cyberspace and Critical Information Protection: A Critical Assessment of Federal Efforts"). Disruptive effects on economic, military, and social activities from sustained power outages or loss of confidence in transportation systems could be more severe, involving physical damage and even casualties. Attacks against digital control systems are technologically feasible.[40] Such vulnerabilities provide asymmetrical advantages to nonstate actors that are less reliant on such control systems and infrastructures. Cyberspace has emerged as a major new environment for political and military competition. New threats may arise from actors that may not be able to compete well in other realms. Intellectual property can be lost; adversaries can disrupt operations. Just as the expansion of global maritime trade required the development of colonies, naval fleets, and supporting infrastructures, cyberspace will call for political and military measures to protect economic and informational interests. New military capabilities and business enterprises require a conscious balancing of opportunity and risk; this demands a discipline of analysis that has not yet developed. The United States must learn how to protect its cyberspace presence in a cost-effective fashion. This may involve the development of large offensive forces that "roam the net" protecting commerce; the orchestration of international accords and norms might be able to limit disruptive activity by states against other states and punish nonstate actors; perhaps a new "cyber Manhattan Project" can establish more secure technological foundations for cyberspace.

Technological advances in other environments changed the terms of competition as, for

example, when the rise of steam propulsion gave advantages to those who could establish colonies and coaling stations to conduct global trade. Economic and military competitors of the United States have explicitly adopted such strategies in cyberspace, too. In the late 1990s, the Japanese set out national plans to establish the world's most advanced networks and promote the construction of ultra-high-speed Internet access for its businesses and citizens.[41] The People's Republic of China has engaged in a multifront approach: controlling public Internet access, developing proprietary operating systems for national use, and endeavoring to influence global standards evolution. Nonstate actors, too, have taken advantage of the new medium: "al Qaeda has become the first guerrilla movement in history to migrate from physical space to cyberspace."[42] Appropriately, then, the 2005 U.S. National Defense Strategy explicitly acknowledges that "disruptive challenges may come from adversaries who develop and use breakthrough technologies to negate current U.S. advantages in key operational domains."[43] Cyberspace may represent the operational domain of highest risk for the United States in the early 21st century.

Speed and Scope of Operations

The changing speed, pace, and scope of military operations were also essential concerns of each of the environmental strategists. While Mackinder and Spykman came to differing conclusions, both examined advantages based on concentrating force quickly, Mackinder advocating the dominance of interior lines of operations, Spykman exterior lines. Mahan and Corbett saw maritime power and naval operations as requiring nations to be able to generate power across the globe in order to control sea lanes of trade. For the air theorists, the speed of air operations meant that wars would be over quickly, giving dominant advantages to the party that struck first. As Douhet put it:

> Wars will begin in the air, and . . . large-scale aerial actions will be carried out even before the declaration of war, because everyone will be trying to get the advantage of surprise . . . for each side will realize the necessity . . . of ridding the air of aerial means to prevent any possible retaliation.[44]

Continuous operations with no territorial limits would be an inherent feature of the space environment, creating a new high ground that would enable those with enough spacepower to dominate operations in other environments.

The rapidity of connections offered by modern communications and information systems similarly creates both challenges and opportunities. Cyber-space can make information on new political developments across the globe available almost instantly. Commercial companies are tightening global supply chains by means of radio-frequency identification systems linked to point-of-sale electronic inventories, increasing efficiencies and lowering costs. Militarily, new forms of rapidly adaptive operations are made possible by use of these systems. Actionable intelligence can be rapidly pushed to cockpits of aircraft or other weapons systems allowing engagement of high-value targets across very wide areas, as in the U.S. strike that killed al Qaeda terrorist leader Abu Musab al-Zarqawi in Iraq.[45] More broadly, advanced militaries that can conduct network-centric operations can tightly orchestrate combined arms campaigns, pursuing full-scale combat operations at any time of the day and in any weather, so they can dominate less sophisticated militaries, as the United States did in Operations *Enduring*

Freedom and *Iraqi Freedom*.

However, global connectivity to achieve rapid strategic impact has become a tool for nonstate actors as well, as described in chapter 18, "Cyber Crime," and chapter 19, "Cyber Terrorism: Menace or Myth?" Organized criminal activity, Internet posting of terrorist videos of beheadings, and malicious disruption on a global scale can all spread rapidly.[46] Cyberspace provides opportunity for alliances between organized crime, hackers, and terrorists, multiplying the risk to governments, corporations, and other potential targets.

The development of airpower in the first half of the 20th century meant that attacks could be launched against strategic centers of gravity in hours. The advent of ballistic missiles with nuclear warheads after World War II brought timelines down to minutes, and the scale of effects rose dramatically. The cyberspace of the 21st century means key events and disruptive threats can necessitate responses in seconds. National leaders are faced with tighter timelines for decisions even as it becomes increasingly imperative to orchestrate action across wider distances more quickly.

The requirement for rapid response in cyberspace can mean higher levels of automated decisions for states and other entities. The Department of Defense net-centric warfare concepts, fusing improved sensor and communications systems, enable engagement of targets that emerge rapidly but offer very limited time periods in which to take action. Balancing the need for speed with the risks of automated responses in military and other operations will prove a growing challenge. Rules of engagement will often call for high-confidence identification of potential targets, but a commander may not fully trust automated systems to make the call regarding weapons employment. The U.S. Navy shootdown of an Iranian airliner in 1988 by the Aegis air defense system provides a cautionary tale, yet caution may also lead to missed opportunities.[47] Cyberspace presents chances to hide or mislead regarding the source of malicious activity. Automated systems can be subverted and turned against their operators or used against third parties.

Cyberspace has multiplied opportunities for small or nonstate groups to achieve large effects in getting their message to a global audience, thus increasing their geographic base for acquiring resources, whether through voluntary contributions or illicit activity; it offers occasions for disrupting even the largest state opponents through new means of attack. The challenge to such groups will be to take advantage of the potential for rapid, global operations without creating a recognizable signature in cyberspace that would render them vulnerable to retaliation and thus to deterrence. Nonstate actors will seek to make cyberspace a medium where guerrilla campaigns, orchestrated dispersal, and surreptitious disruption make large land, sea, and air forces fighting decisive battles irrelevant.

Control of Key Features

The environmental theories described above also endeavored to delineate the conditions that would allow control of key features, especially logistics and lines of communication. The early 20th century brought the ability to amass forces at chosen points around the Eurasian land mass, crucial to Mackinder's assertion of the centrality of the heartland. Straits or sea lanes could be controlled by a large fleet even without direct naval engagements. Mahan detailed the role of a network of coaling stations and repair facilities located in colonies in achieving global maritime prominence. The supremacy of the bomber, according to Douhet, Mitchell, and Trenchard, meant that counterforce strikes to eliminate an adversary's striking power were

essential for control of the air. Gray and Sloan sought to extend the strategic vision of geopolitics into space by identifying the key locations that would enable operations. Harter stressed the requirement "for multiple space ports from which to achieve orbit [in order] to eliminate ground choke points" as a foundation for spacepower.[48]

Cyberspace contains numerous activities, ranging from international financial transactions, coordination of global logistics, terrorist planning, or disruptive attacks on cyberdependent networks and operations. All of these activities require that actors establish the capacity to transit cyberspace. Crucial assets in cyberspace include the physical infrastructures that enable communications, such as undersea fiber optic cables and communications satellites, and major interconnection points for large global networks. The small numbers of such facilities mean they may be thought of as chokepoints, similar to mountain passes or straits between oceans. The limited number of physical paths for communications cables out of a major city can make bridges and tunnels chokepoints; for example, fiber optic networks were severely disrupted by the attacks of 9/11. Control or disruption of such cyber chokepoints could have a major impact on global communications connectivity and speed. In March 2007, authorities in the United Kingdom arrested individuals accused of planning terrorist attacks against key Internet infrastructure locations on the two U.S. coasts (known as Metropolitan Area Ethernet [MAE] East and MAE West).[49]

Logical systems and code shape the interactions of digital systems, telephone traffic, and other networks and systems in cyberspace. Thus, cyberspace is a manmade environment, unlike land, sea, air, or space. States, corporations, and other actors utilizing cyberspace can and do make choices about ownership, control, and operation of these key cyberspace features. Information infra- structures such as key network control facilities may be held in the private sector or instead may be owned and operated by the state. Standard-setting for communications systems can be in the hands of governments, such as with traditional telephone systems, or largely outside government control, as with much of Internet governance (see chapter 21 in this volume, "Internet Governance"). The diverse types of stakeholders that influence choices in forums such as the Internet Corporation for Assigned Names and Numbers include governments, businesses, technical groups, and civil-society organizations. Some key features of the cyberspace environment can change rapidly, as when the ownership of a major international satellite or fiber optic network operator changes, while others occur more slowly as, for example, IP-based telephony supplants circuit-switched voice telephone networks.

Large actors such as national governments, militaries, and multinational corporations have choices about which systems to emphasize—such as open, Internet-based communications or closed, proprietary systems—and about the pace of adoption of new standards. The United States must seek to understand constantly shifting opportunities and vulnerabilities and manage its cyber assets in light of its social, economic, and military concerns. In order to better protect cyberspace, the United States should pursue redundancy and diversity in undersea cable, satellites, ground stations, and fiber optic routing in order to minimize vulnerable chokepoints. We can worry less about precise mapping of all potential vulnerabilities (which have been a focus of many U.S. Federal Government efforts), given the constantly morphing cyberspace environment. Public and private sector actors who operate and use cyberspace for key national economic and security purposes should jointly conduct regular scenario analyses and exercises to focus investment and develop strategies to establish a robust cyber infrastructure.

In managing the evolution of the logical cyber environment, the United States should more aggressively engage those who establish protocols and standards, as competitors such as the

People's Republic of China have increasingly chosen to do. U.S. choices about open versus closed systems, and more defensible versus more accessible cyberspace systems at the national level, will require balancing of intelligence, military, law enforcement, commercial, and social objectives. More secure, robust protocols and systems may allow for more options in developing networks that can be both open and trusted. Investment in a separate, more securable government network for sensitive but unclassified information may be the only way to accommodate the desire to limit government control to foster economic growth and social dialogue by encouraging growth of public networks that emphasize accessibility and innovation.

The United States and its partners should also seek more vigorous mechanisms for cooperation in the governance of the global common. While notions of "arms control agreements" to seek international control over information "weapons" have surfaced, the more appropriate approach for the United States would be securing freedom of passage, similar to regimes governing the seas and space. So far, U.S. efforts in the international community to foster a "culture of cyber security" and to leave leadership over the evolution of the Internet to the private sector have been largely successful and productive in terms of pursuing its objectives.[50]

National Mobilization

The national mobilization of essential resources, including deliberate government efforts to coordinate military and commercial activities, was a central concern for many of the environmental strategists. Mahan, for example, advocated support for colonies as global bases from which to project maritime power. The sea-, air-, and spacepower theories focused on the potential synergy between a nation's commercial and military activities and the development of professionals dedicated to securing the nation's interests.

Human capital is an even more crucial resource in the cyber environment. The cyber environment still rewards pioneers. Risks in cyberspace are less physical than they were for previous explorers. The premium is on brainpower, creativity, and ability to manage complexity. Historical U.S. strengths—advanced education, systems integration, and intellectual property development and management—should offer advantages in cyberspace competition. However, the lack of requirement for major resource investments, and the ease of leveraging global access to networks, will provide more advantages to nonstate actors in cyberspace than in other environments. Knowledge of the vital characteristics of critical infrastructures, economic flows, military dependencies, operating systems, and disruptive code can be rapidly stored, duplicated, transferred, and acted upon. Such knowledge and network access permit action in cyberspace.

Building and sustaining the expertise to leverage these assets will be a lengthy and expensive process for large actors such as governments and corporations that pursue long-term objectives through the cyberspace environment. In Western nations, expertise resides mainly in the commercial sector; the government and its military and national security establishments must effectively leverage this pool. This contrasts with the other environments related to national security. Nonstate actors can leverage fairly small cadres of skilled personnel to use cyberspace for specific purposes, whether to mobilize large numbers of people for a demonstration against globalization or to launch disruptive attacks on infrastructure.

The centrality of human expertise requires the United States, like other major actors, to compete globally to create, attract, and retain the human capital needed to construct, utilize, and engage in cyberspace. These personnel must be capable of analyzing the ever-changing

opportunities and risks present in the environment, operating and protecting the large enterprises and infrastructures that sustain cyberspace, and performing other tasks ranging from forming new modes of sharing information to developing the capacity for preventing or deterring disruptive attack. For the U.S. military, the challenge is to nurture a strong cadre of cyber experts, similar to the naval, air, and space expertise that has enabled its success in other environments. This requires the vision and will to divert resources from traditional military missions to invest in the core capabilities necessary for the cyber environment.

National policy can influence the international, organizational, and individual access to and use of cyberspace. Many strategic choices exist. The People's Republic of China has begun to focus on tighter control of individual rights in cyberspace, seeking to establish a somewhat separate national cyberspace with controlled access to foster government political control and improve its ability to defend national cyber assets. The United States has taken a much more laissez faire approach: its national regulation and positions in international forums stress the economic benefits of loose control in empowering innovation and access by all to services provided via the Internet and other cyberspace media.

The impact of different national approaches on the ability to manage strategic conflict in cyberspace is not clear. A loosely controlled and diverse but robust network infrastructure may fare better than a centrally managed infrastructure with mandated barriers and defense, even if the latter retains a limited capacity for rapid adaptation in the face of new threats.

A major power such as the United States requires policy and organizational structures that can encompass the full range of interrelated economic, security, and social issues related to cyberspace. The growth of a global system of ownership and control of the technology and operation of cyberspace presents both economic opportunity and security risks. Increasingly, U.S. national security organizations and critical infrastructure providers rely on information technology and communications hardware and software that are produced by people and organizations whose loyalties and purposes are not always easy to assess, yet the Nation is part of a global economic system that has greatly fostered U.S. prosperity. National focus is required to address the challenges of coordinating multiple U.S. Government agencies and including the private sector in an orchestrated system for conducting national defense against a major threat in cyberspace.

Based on the appeals of Alfred Mahan and others, Theodore Roosevelt made the establishment of a modern blue water Navy a national priority as the United States began to become a global power at the beginning of the 20th century. Billy Mitchell's call for national effort to develop airpower was answered by Franklin Roosevelt on the eve of World War II and played a vital role in the U.S. victories in that conflict. John Kennedy launched a program to ensure the U.S. lead in space and to put a man on the moon in response to perceived Soviet challenges in this environment. Similarly, as the strategic significance of cyberspace grows, dedicated national programs may well be required to ensure that we have the capacity to achieve our national objectives.

Analysts concerned about the lack of a strategic U.S. cyber defense have called for a national focus to pull disparate efforts together.[51] The employment of national resources on the level of a "cyber Manhattan project" may be needed. Such efforts would also require the use of diplomatic capital to secure global support across nations, corporations, and civil society groups. National policy development is needed to integrate efforts by the White House, Congress, business, and civic leaders to set balanced objectives for utilizing and defending cyberspace.

Distinctive Features of Cyberspace

Cyberspace, as we have seen, has both similarities to and differences from other environments (see table 10–1). Two differences merit focused attention: offense dominance and the rapid changeability of the cyberspace environment.

Offense dominance is sometimes characteristic of other realms, but it has very different implications in cyberspace. Both the weaknesses in the technological foundations and the economic incentives for openness between networks and systems have made many key networks vulnerable to exploitation, manipulation, and disruption by digital attack. Nonstate actors derive advantages from the ability to focus on niche objectives, utilize anonymous access, rapidly leverage expertise, and make decisions more rapidly. Thus, offense is easy, and defense is difficult.

Concerns over which actor might strike first in a conflict play out differently in cyberspace than with air and ballistic missile forces. The ease of stealthy deployment of attacking forces and difficulty in attributing the source and intent of attackers mean that damage limitation through preemptive first strikes or retaliatory strikes is largely irrelevant: an actor would have little confidence in trying to attack preemptively to remove the cyber attack forces of an even moderately sophisticated adversary. Similarly, trying to use cyber counterattack to disable attacks in progress is complicated by issues of identifying and discretely targeting a complex web of electronic points of origin of the attacker, the culpability of the networks and systems from which attacks appear to originate, and the fundamental fact that disrupting these points in cyberspace may only have a limited effect. Deterrence by retaliation is also complicated by the difficulty of attributing an attack to any identifiable target for retaliation (but see chapter 13 in this volume, "Deterrence of Cyber Attacks").

National security organizations cannot simply defend the environment by increasing the size of their military cyber forces. If the attacker has a high probability of rapid success, simply pursuing current information security approaches with more vigor is unpromising. Most attention in the national security community has focused on risks from cyber espionage or a single, time- limited strategic cyber blow from a major adversary. Counterstrategies to deal with state or terrorist nonstate actors conducting an economic guerrilla campaign in cyberspace remain almost completely undeveloped. A robust, defensible infrastructure will depend on shaping the technologies employed, the obligations of operators of key networks and infrastructures, and the ability to coordinate government–private sector investment and responses to attacks.

Table 10-1: Elements with the Cyber Environment Compared with Other Environments

	Land	Sea	Air	Space	Cyber
Technological Advances	Rail and communications require focus on heartland	Steel and steam enable global power projection	Crush centers of gravity directly	Creates a new high ground	New strategic vulnerabilities; enables nonstate actors
Speed and Scope of Operations	Drives choice of preferred lines of communication	Allows global strikes against rim of heartland	Conflicts will end quickly	Continuous global operations	Extremely fast global operations; automation of command and control
Control of Key Features	Speed of mobilization crucial for heartland advantage	Requires global basing; geographic chokepoints	First strikes against adversary airfields crucial	Ensure access with lift; control key orbit points	Environment under human control; changes quickly
National Mobilization	Location of key resources crucial	Must protect trade as key element of national power	Ensure cadre of professionals; link to private sector	Ensure cadre of professionals; link to private sector	Ensure cadre of professionals; link to private sector

A second unique characteristic of cyberspace is its rapid changeability. The ability of nations to compete effectively in other environments involved technological competition; indeed, the efforts of Mackinder and Mahan were largely inspired by changes in the technologies being used to compete on land and sea. However, the fundamental physical forces and terrain of those environments do not change; scientists and technologists understood them better over time. By contrast, the manmade environment of cyberspace can change its key characteristics and dominant operating modes rapidly; for example, as the World Wide Web expands, bandwidth and memory capacities increase, and new devices become increasingly ubiquitous. Software updates and additions to networks change the ability to defend and attack many networks on a daily basis. The continually accelerating deployment of new technologies, standards, access, and legal regimes changes the landscape of technological choices, operational procedures, and risks for users, attackers, and defenders.

The mobilization of resources will require leadership, strategies, and decision- making processes that put a premium on learning and flexibility. Management and acquisition processes will need to support rapid implementation of changes to systems and networks, as well as agility in the adoption of rapidly changing rules governing access to outside networks and mission partners that balance usability and security. The conduct of military and other operations will place a premium on trusting individuals to understand the changes they see in the cyber tactical environment and adjust the execution of their operations quickly.

Moving Forward

Defense and economic institutions that are now dependent on the cyber environment cannot allow a continuing slide toward a "Wild West" of criminal and disruptive opportunities. Yet we also must strive to preserve the benefits of innovation and connectivity that have made the cyberspace environment so valuable. The United States must look for ways to embed flexibility and mechanisms for rapid change in policy, institutions, technology choices, and human capital plans. This new environment may require substantially different approaches due to its more mutable, human-driven characteristics.

Insights from biological and other complex adaptive systems might serve as useful guides to what changes might be necessary. The lesson of biology is that survival is not necessarily the reward for the biggest, strongest, or meanest but rather for the most adaptable. The ability to learn, to cooperate when fruitful, and to compete when necessary, will provide the fundamental strengths of those actors seeking cyberpower.

---

[1] Also see Gregory J. Rattray, *Strategic Warfare in Cyberspace* (Cambridge: MIT Press, 2001), 11–12.

[2] Key early works addressing information warfare and the possibilities of conflicts based on network attacks include Alvin and Heidi Toffler, *War and Anti-War: Survival at the Dawn of the 21st Century* (Boston: Little, Brown, 1993); John Arquilla and David Ronfeldt, "Cyberwar Is Coming!" *Comparative Strategy* 12, no. 2 (Spring 1993), 141–165; and Winn Schwartau, *Information Warfare: Chaos on the Electronic Superhighway* (New York: Thunder's Mouth Press, 1994).

[3] *The National Security Strategy of the United States of America* (Washington, DC: The White House, September 2002), 1.

[4] *The National Defense Strategy of the United States of America* (Washington, DC: Department of Defense, March 2005), 3.

[5] *The National Strategy to Secure Cyberspace* (Washington, DC: The White House, February 2002).

[6] See chapter 2 in this volume, "From Cyberspace to Cyberpower: Defining the Problem."

[7] National Defense Strategy, 13.

[8] See discussion of the International Telecommunication Union in chapter 21 of this volume, "Internet Governance."

[9] See, for example, Seth Mydans, "Monks are Silenced, and for Now, Internet Is Too," *The New York Times*, October 4, 2007, available at <www.nytimes.com/2007/10/04/world/ asia/04info.html?emc=etal>.

[10] Rattray, 43–44.

[11] For discussion of government control of the Internet and its limits, see chapter 21 in this volume, "Internet Governance."

[12] Halford John Mackinder, "The Geographical Pivot of History," *The Geographical Journal* 23, no. 4 (1904), 421–437.

[13] Nicholas Spykman, *Geography of the Peace* (New York: Harcourt and Brace, 1944).

[14] Ibid., 43.

[15] Alfred Thayer Mahan, *The Influence of Sea Power upon History, 1660–1783* (Boston: Little Brown, 1890), reprinted in David Jablonsky, ed., *Roots of Strategy*, vol. 4 (Mechanicsburg, PA: Stackpole Books, 1999).

[16] Ibid., 28.

[17] Ibid., 85.

[18] Julian S. Corbett, *Some Principles of Maritime Strategy* (London: Longmans, Green, 1911).

[19] Ibid., 55.

[20] Heather Timmons, "Two Communication Cables in the Mediterranean Are Cut," *The New York Times*, January 31, 2008, available at <www.nytimes.com/2008/01/31/business/ worldbusiness/31cable.html>.

[21] Giulio Douhet, *Command of the Air*, trans. Dino Ferrari (New York: Coward-McCann, 1942), 61.

[22] Hugh M. Trenchard, "Report on the Independent Air Force," January 1, 1919, 1334– 1335.

[23] William Mitchell, *Skyways: A Book on Modern Aeronautics* (Philadelphia: J.B. Lippincott, 1930), 255–256.

[24] The need for a national effort is the primary focus of William Mitchell, *Winged Defense: The Development and Possibilities of Modern Airpower—Economic and Military* (New York: G.P. Putnam's Sons, 1925).

[25] Douhet, 181.

[26] Ronald Reagan, "Address to the Nation on National Security by President Ronald Reagan," March 23, 1983,

available at <www.fas.org/spp/starwars/offdocs/rrspch.htm>.
[27] "Report of the Commission to Assess United States National Security Space Management and Organization," January 11, 2001, available at <www.fas.org/spp/ military/commission/report.htm>.
[28] National Defense Strategy, 3.
[29] William J. Broad and David A. Sanger, "China Tests Anti-Satellite Weapon, Unnerving U.S.," *The New York Times*, January 18, 2007, available at <www.nytimes.com/2007/01/18/ world/asia/18cnd-china.html>.
[30] Colin S. Gray and Geoffrey Sloan, *Geopolitics, Geography, and Strategy* (London: Frank Cass, 1999).
[31] Mark E. Harter, "Ten Propositions Regarding Space Power: The Dawn of a Space Force," *Air and Space Power Journal* 20, no. 2 (Summer 2006), 68.
[32] Ibid. , 67.
[33] Ibid.
[34] Marshall McLuhan and Quentin Fiore, *War and Peace in the Global Village* (New York: Bantam Books, 1968).
[35] Larry Greenemeier, "Estonian Attacks Raise Concern Over Cyber 'Nuclear Winter'," *Informationweek.com*, May 24, 2007, available at <www.informationweek.com/news/ showArticle.jhtml?articleID=199701774>.
[36] David Eshel, "Hezbollah's Intelligence War: Assessment of the Second Lebanon War," *Defenseupdate.com*, available at <www.defense-update.com/analysis>.
[37] "Falun Gong Hijacks Chinese TV," *Wired*, September 24, 2002, available at <www.wired. com/politics/law/news/2002/09/55350>.
[38] Gabriel Weimann, "www.terror.net: How Modern Terrorism Uses the Internet," U.S. Institute of Peace Special Report No. 116, March 2004, available at <www.usip.org/ pubs/specialreports/sr116.html>.
[39] Kathryn Westcott, "Transport Systems as Terror Targets," *BBC News*, July 7, 2005, available at <http://news.bbc.co.uk/1/hi/world/europe/4659547.stm>.
[40] Tim Wilson, "Experts: U.S. Not Prepared for Cyber Attack," *DarkReading.com*, April 26, 2007, available at <www.darkreading.com/document.asp?doc_id=122732>.
[41] Japanese Ministry of Information, "Basic Guidelines on the Promotion of an Advanced Information and Telecommunications Society," November 9, 1998, available at <www. kantei.go.jp/foreign/990209guideline-aits.html>.
[42] Steve Coll and Susan B. Glasser, "Terrorists Turn to the Web as Base of Operations," *The Washington Post*, August 7, 2005, A1.
[43] National Defense Strategy, 5.
[44] Douhet, 196–197.
[45] Ellen Knickmeyer and Jonathan Finer, "Insurgent Leader Al-Zarqawi Killed in Iraq," *The Washington Post*, June 8, 2006, available at <www.washingtonpost.com/wp-dyn/content/ article/2006/06/08/AR2006060800114.html>.
[46] The Slammer worm in 2003 caused major disruption across the Internet in less than 15 minutes. Paul Boutin, "Slammed! An Inside View of the Worm that Crashed the Internet," *Wired*, July 2003, available at <www.wired.com/wired/archive/11.07/slammer. html>.
[47] "U.S. Passes Up Chance to Strike Taliban: Predator had Suspected Fighters in its Sights, but Military Passed on Shot," *MSNBC.com*, September 13, 2006, available at <www. msnbc.msn.com/id/14823099>.
[48] Harter, 72.
[49] David Leppard, "Al-Qaeda Plot to Bring Down UK Internet," *The Sunday Times*, March 11, 2007, available at <www.timesonline.co.uk/tol/news/uk/crime/article1496831.ece>.
[50] Kenneth Neil Cukier, "Who Will Control the Internet?" *Foreign Affairs* 84, no. 6 (November-December 2005).
[51] See, for example, Wayne Rash, "Cyber-Security Office Calls for More Clout," *Eweek.com*, December 10, 2004, available at <www.eweek.com/article2/0,1895,1739061,00.asp>; and Scot Petersen, "Wanted: Cyber-Security," *Eweek.com*, October 18, 2004, available at <www.eweek.com/article2/0,1895,1675483,00.asp>.