CHAPTER 2

From Cyberspace to Cyberpower: Defining the Problem

Daniel T. Kuehl

THIS CHAPTER has several ambitious objectives that are critical for this book: to lay out the central concepts for what we mean by *cyberspace* and *cyberpower*; to suggest definitions that capture the logic behind these concepts; and to establish a set of foundations upon which future work can build. *Cyberspace* has been in our lexicon for two decades, since William Gibson used it to describe "a consensual hallucination" in his science fiction novel, *Neuromancer*, but there certainly is no consensus on its meaning in the world of the 21st century.[1] While organs of government attempt to define its meaning in the real, operational world— Gibson's approach obviously will not suffice—the approaches we develop toward this domain will shape how it interacts with other domains and affects relationships among the other elements and instruments of power, especially how humans and the organizations we create use that power.

The march of technology and progress guarantees that even while we debate this definition—regardless of exactly how we define it now and refine it in the future—our use of cyberspace has already reached the point where an increasingly wide range of social, political, economic, and military activities are dependent on it and thus are vulnerable to both interruption of its use and usurpation of its capabilities. This chapter offers definitions of both *cyberspace* and *cyberpower*, suggests some of the ways they relate to and impact other domains, and explores how they are shaping new operational concepts such as information operations, new technological combinations such as the global information grid, and other instruments of power. It suggests an approach for a national cyber strategy and provides links to this book's following chapters, which explore key topics and issues in greater detail.

Cyberspace: A New Domain

From the start of recorded history until about a century ago, mankind had only two physical domains in which to operate, the land and the sea, each of which had dramatically different physical characteristics. The sea was usable by humans only with the aid of technology—the galley, sailing ship, steamship, nuclear submarine—because we could swim for only so long. Other than by simply walking, the land was usable only through the exploitation of technology—the wheel, the plow, the war chariot (up to and including the modern main battle tank). The great change was a century ago, when we added a third physical domain—the aerospace—to the mix,[2] and while its military aspects outweighed its commercial applications for many years, the economic, social, and political aspects of air travel and transportation for the 21st-century are enormous. In 1957, we added a fourth to our mix, and while outer space is not yet as militarily or commercially pervasive as the air, it has deep and essential links to operations and activities in all other environments. Each of these four physical domains is marked by radically different physical characteristics, and they are usable only through the use of technology to exploit those characteristics.

To these domains we have now added a fifth: cyberspace. Joint Publication 1–02, *Department of Defense Dictionary of Military and Associated Terms*, had a definition of cyberspace dating to the early 2000s, but there was almost universal agreement that it was insufficient: "the notional environment in which digitized information is communicated over

computer networks."[3] Cyberspace is hardly "notional," and confining it to the realm of being "digitized and computerized" is far too limiting, failing to reflect the massive technological and social changes with which cyberspace is interwoven.

Defining Cyberspace

Since the mid-1990s, a number of authors (see table 2–1) have offered useful insights that have helped shaped thought on this issue, and the definition proposed in this chapter draws heavily from them. Several consistent threads run through these insights, including the role of electronics, telecommunications infrastructures, and information systems.[4] A crucial and useful perspective was offered by the 2003 *National Strategy to Secure Cyberspace*, which defined cyberspace as the "nervous system—the control system of the country . . . composed of hundreds of thousands of interconnected computers, servers, routers, switches, and fiber optic cables that allow our critical infrastructures to work."[5] The Joint Staff in early 2006 initiated an important and much-needed effort to develop the *National Military Strategy for Cyberspace Operations*, and when it was approved in December 2006 by Chairman of the Joint Chiefs of Staff General Peter Pace, it included a definition that closely mirrored the one suggested by this book: "Cyberspace is a domain characterized by the use of electronics and the electromagnetic spectrum to store, modify and exchange information via networked information systems and physical infrastructures."[6]

Two additional official definitions were issued in early 2008. One came out of the White House, with President George W. Bush's signature of National Security Presidential Directive (NSPD) 54/Homeland Security Presidential Directive 23, "Cybersecurity Policy," on January 8, 2008. While NSPD 54 itself is classified, its definition of cyberspace is not: "Cyberspace means the interdependent network of information technology infrastructures, and includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers in critical industries." Whatever the strengths and weaknesses of this definition, it is important to consider that it was issued within the context of a specific issue, the safety and security of military and government information networks.

Table 2-1. Definitions of Cyberspace

- Greece: *kybernetes* (the steersman) or *cybernetics*, the study of control processes, which was the basis for Tom Rona's concept (1976) of "information warfare."
- William Gibson, *Neuromancer* (1984): "a consensual hallucination."
- Edward Waltz, *Information Warfare: Principles and Operations* (1998): The "cyberspace dimension" refers to the middle layer—the information infrastructure—of the three realms of the information warfare battle-space. These three realms are the physical (facilities, nodes), the information infrastructure, and the perceptual.
- Google: "The electronic medium of computer networks, in which online communication takes place. . . . a metaphor for the non-physical terrain created by computer systems. . . . the impression of space and community formed by computers, computer networks, and their users. . . . the place where a telephone conversation appears to occur. . . . the place between the phones."
- Winn Schwartau, *Information Warfare: Chaos on the Electronic Superhighway* (1994): "That intangible place between computers where information momentarily exists on its route from one end of the global network to the other. . . . the ethereal reality, an infinity of electrons speeding down copper or glass fibers at the speed of light. . . . Cyberspace is borderless . . . [but also] think of cyberspace as being divided into groups of local or regional cyberspace—hundreds and millions of smaller cyberspaces all over the world."
- Winn Schwartau, *Information Warfare*: *Chaos on the Electronic Superhighway* (2d ed., 1996): "[National] cyberspace are distinct entities, with clearly defined electronic borders. . . . Small-C cyberspaces consist of personal, corporate or organizational spaces. . . . Big-C cyberspace is the National Information Infrastructure. . . . add [both] and then tie it all up with threads of connectivity and you have all of cyberspace."
- *Oxford English Dictionary* (1997): "The notional environment within which electronic communication occurs."
- Walter Gary Sharp, *CyberSpace and the Use of Force* (1999): "The environment created by the confluence of cooperative networks of computers, information systems, and telecommunication infrastructures commonly referred to as the Internet and the World Wide Web."
- Dorothy Denning, *Information Warfare and Security* (1999): "The information space consisting of the sum total of all computer networks."
- Gregory Rattray, *Strategic Warfare in Cyberspace* (2001): "A physical domain resulting from the creation of information systems and networks that enable electronic interactions to take place. . . . Cyberspace is a man-made environment for the creation, transmittal, and use of information in a variety of formats. . . . Cyberspace consists of electronically powered hardware, networks, operating systems and transmission standards."
- *Merriam-Webster Third New International Dictionary* (2002): "The on-line world of computer networks."
- *National Military Strategy for Cyberspace Operations* (2006): "A domain characterized by the use of electronics and the electromagnetic spectrum to store, modify and exchange information via networked systems and physical infrastructures."
- National Security Presidential Directive 54 (2008): "The interdependent network of information technology infrastructures, and includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers in critical industries."
- Deputy Secretary of Defense Gordon England (2008): "A global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers."

Just over 4 months later, in May 2008, the Department of Defense (DOD) expanded this definition in a memorandum from Deputy Secretary of Defense Gordon England that defined cyberspace as "a global domain within the in- formation environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers."[7] The memo also advises that DOD will use this definition "until further notice," a wise acknowledgment that the rapidly evolving nature of the field will likely generate further refinement. This memo thus nullified the definition contained in the 2006 *National Military Strategy for Cyberspace Operations*, which will incorporate the new definition whenever it is formally revised. While both definitions are useful and advance our conceptual understanding of cyberspace, they lack a critical piece of information: what makes cyberspace unique? If cyberspace is a domain alongside land, sea, air, and outer space, what are its unique and defining physical characteristics?

All of these various approaches combine to suggest that cyberspace is more than computers and digital information. This chapter offers a definition that builds upon those threads cited above and yet is different in some crucial regards: cyberspace is *a global domain within the information environment whose distinctive and unique character is framed by the use of electronics and the electromagnetic spectrum to create, store, modify, exchange, and exploit information via interdependent and interconnected networks using information-communication technologies*.[8]

This definition blends the best elements of both Secretary England's approach and that contained in the *National Military Strategy for Cyberspace Operations*. These interdependent and interconnected information networks and systems reside simultaneously in both physical and virtual space and within and outside of geographic boundaries. Their users range from entire nation-states and their component organizational elements and communities down to lone individuals and amorphous transnational groups who may not profess allegiance to any traditional organization or national entity.[9] They rely on three distinct yet interrelated dimensions that in the aggregate comprise the global information environment as outlined in Joint Publication 3–13, *Information Operations*, and to which (hopefully) Secretary England's memo was referring: the physical platforms, systems and infrastructures that provide global *connectivity* to link information systems, networks, and human users; the massive amounts of informational *content* that can be digitally and electronically sent anywhere, anytime, to almost anyone, a condition that has been enormously affected and augmented by the convergence of numerous informational technologies; and the human *cognition* that results from greatly increased access to content and can dramatically impact human behavior and decisionmaking.[10]

From Cyberspace to Cyberpower

While the fundamental technological aspects of cyberspace that require the use of manmade technology to enter and exploit seem to support an argument that cyberspace is a manmade environment, this situation is actually no different from any of the other four domains. We also need manmade technologies to enter and exploit the other domains, the only difference being that we can more easily see and sense those domains.[11] It is, however, important to note that while the physical characteristics of cyberspace can be delineated and come from forces and phenomena that exist and occur in the natural world, in a real sense cyberspace is also a designed environment, created with the specific intent of facilitating the use

and exploitation of information, human interaction, and intercommunication.[12]

At the risk of being reductionist, it might be useful to break down the definition offered in this chapter and examine some of its key elements. First, cyberspace is an *operational* space where humans and their organizations use the necessary technologies to act and create effects, whether solely in cyberspace or in and across the other operational domains and elements of power.[13] In this sense it is like any of the other four physical domains—land, sea, air, and outer space—in which we operate, and one of the explicit objectives of this definition is to place cyberspace firmly within the bounds of the operational domains and elements of power within which the national security community operates. The business community uses cyberspace to facilitate global trade, exchange funds, manage far-flung enterprises, and do innumerable other vital things. In a real sense, cyberspace is where we create and use the digital information that fuels the global economy. Every day, the global business community exchanges trillions of dollars via cyberspace, transactions in which not a single dime or euro of hard currency is moved. The political strategist cannot ignore cyberspace, because its effective use may well mean the difference between victory and defeat in the electoral process.[14]

In the effort to influence—whether focused on an individual, an organization, or an entire society—cyberspace is a key operational medium through which "strategic influence" is conducted, and daily we see increased references to "Jihad.com" and other ways in which the terrorists and so-called jihadists and irhabists are using cyberspace as a critical medium for their operations.[15] Warfare of the 21st century involving opponents possessing even a modicum of modern technology is hardly possible without access to cyberspace, and entire new operational concepts such as network-centric warfare or fighting in an "informationized battlespace" would be impossible without cyber-based systems and capabilities.[16] The ability to reprogram the targeting data within a weapon on its way to the target, then rely on real-time updates from a global positioning system satellite to precisely strike that target, is possible only through the use of cyberspace. In many ways, the entire debate on whether DOD is "transforming" itself revolves around efforts to better employ and exploit cyber-based capabilities.[17]

The second part of the definition is what truly makes cyberspace unique and distinguishes it from the other environments, for it is the use of *electronic* technologies to create and "enter" cyberspace and use the energies and properties of the *electromagnetic spectrum* that sets cyberspace apart. Even without detailed definitions and analyses, we can clearly see that the physical characteristics of these different domains are what differentiate them from each other.[18] The argument that cyberspace is a manmade environment is only half-true. The electronic technologies that we create and employ to use cyberspace are its counterparts to the vehicles, ships, airplanes, and satellites that we have created to exploit the other domains, but the unique characteristics of each domain are naturally occurring phenomena of the physical world.[19] Any definition of cyberspace that omits this fundamental condition—the blending of electronics and electromagnetic energy—is thus flawed by not recognizing the central features that make cyberspace distinct.

This brings us to the third aspect of our definition, because we exploit those characteristics and properties not to sail the seas or orbit the earth, but rather to "*create, store, modify, exchange, and exploit*" information via those electronic means. This may seem self-evident, but that may be because we see so many different trees around us that we do not realize the extent of the forest. The way that cyberspace has changed (some would argue is expanding astronomically)

how we can create, store, modify, exchange, and exploit information has transformed how we operate in the other domains and use the instruments of national power. We literally can capture any kind of information—the human voice on a cell phone, the contours of a fingerprint, the contents of the *Encyclopedia Britannica*, or the colors of ice and dust as "seen" by a spacecraft on the planet Mars—store that information as a string of bits and bytes, modify it to suit our purposes, and then transmit it instantly to every corner of the globe.[20]

It is the fourth aspect of our definition, the *networking of interdependent and interconnected networks using information-communication technologies* that are the backbone of those systems, that has brought cyberspace to the forefront of debates over its impact on and importance to national security and international affairs.[21] We began to network and interconnect modern, technologically based information systems with the invention of the telegraph, which has been called the "Victorian Internet," before we began using the air, the subsurface of the sea, or outer space.[22] The telegraph functions by the use of small amounts of electricity (the early ones were powered by battery) to transmit information in the form of dots and dashes over a wire, a process remarkably similar to today's use of fiber optic cables to perform the same basic function—albeit in a form and volume that Samuel Morse could not have imagined. The extension of these dots and dashes into the ether came with the invention of the wireless, which had followed by not many years the telephone, and preceded by even fewer years the transmission of voice over wireless—radio.

All of these functions were uses of cyberspace, even though the invention of the electronic computer was decades away. Once the microchip was developed, all the elements were present for what we have come to call the information revolution, and even though this revolution took place in an evolutionary manner—as do almost all revolutions—we now see that in myriad ways, our daily life is essentially inseparable from cyberspace. The definition of cyberspace proffered in this chapter thus begins with those physical characteristics that make cyberspace unique before emphasizing the key interaction of communications to exchange information. It is the inseparable linkage of the technology, the human users, and the impact of the interconnectivity in the modern world that differentiates these kinds of information networks from earlier ones—such as the Pony Express of the 1860s—and that hints at cyberspace's future impact.

What does this definition of cyberspace offer us that the other definitions do not? Two key issues manifest themselves. First is its foundation in the physical world: it is based not on any list of activities that take place within that domain but rather on the unique physical characteristics that set it apart from the other domains. What makes cyberspace neither aerospace nor outer space is the use of the electromagnetic spectrum as the means of "movement" within the domain, and this clear distinction from other physical environments may be crucial to its further development within the national security structure.

This leads to the second key issue: clarity. As contrasted with some of the definitions surveyed earlier, the definition presented here clearly focuses on the technologies that exploit cyberspace's unique characteristics and their resultant effects. If the information being "created, stored, modified, exchanged, or exploited" depends on the use of electronics and electromagnetic energy, then it is being done in cyberspace; if the information is carried by a rider on a pony or a messenger riding a motorcycle, it is not. A computer connected to an area network or a broadcast platform transmitting television signals to a set of receivers is exploiting cyberspace, regardless of whether that computer or transmitter is being carried in a ship, an airplane, the international space station, or by a Special Forces Soldier riding a horse.[23]

Cyberspace and Information Operations

One issue that has engaged DOD in a surprisingly contentious debate is the relationship between cyberspace and information operations (IO). Joint Publication 3–13 defines *IO* as: the integrated employment of the core capabilities of Electronic Warfare, Computer Network Operations, Psychological Operations [PSYOP], Military Deception, and Operational Security in concert with specified supporting and related capabilities, to influence, disrupt, corrupt or usurp adversarial human and automated decision making while protecting our own.[24]

This definition does not particularly help sharpen this debate, because it constitutes a list of activities, whereas cyberspace is a domain within which those activities are often conducted. To add another element of potential confusion to the debate, Joint Publication 3–13 provides an insightful and useful description of the information environment, as discussed earlier in this chapter: three separate but related and synergistic dimensions, which in this chapter are termed *connectivity, content*, and *cognition*. The first of these, the physical/interconnected dimension, is the primary means by which cyberspace touches and shapes the information environment, because the technological aspects of an interconnected world are dominated by cyberspace.

However, there are other forms and means of connectivity that do not come from cyber capabilities and are outside the definition of cyberspace: the posting of broadsides of the Declaration of Independence that were distributed by horse, hand, or post throughout the 13 colonies in 1776 was an example of connectivity, as is an American battalion commander sitting down to meet with a group of tribal elders in a province in Iraq. The printed material on the broad- side, or the subject of the conversation with the tribal elders, would be an example of the content. A PSYOP leaflet may be printed on a hand-operated printing press in Afghanistan, and when the battalion PSYOP officer meets with that leaflet's intended audience to gauge its impact, content has been exchanged without any help from cyberspace. But content is also created in cyberspace: a growing amount of the information that is carried and delivered via the interconnectivity just discussed is created, modified, and stored via electronic/cyber means. Thus, it is erroneous to equate cyberspace with IO. Instead, the most accurate view of cyberspace is to see it as one critical aspect of the overall information environment within which IO is conducted, but not the entire environment, a view that coincides with Secretary England's definition of cyberspace as "a global domain within the information environment."[25]

While information operations include all three dimensions of the information environment, cyberspace comprises only a part—albeit perhaps a large part—of the connectivity and content dimensions.[26] Cyberspace is thus shaping and changing the three dimensions of the information environment: how we create information content itself (a Web page, for example), how we share that content through new forms of connectivity (the Internet links that make that Web page accessible to over a billion people), and how human interaction and communication are affected.

Another way of looking at this is to portray cyberspace as having multiple layers. At the foundation is the set of physical characteristics that create the basic frameworks of how we enter and use cyberspace. The next layer consists of the platforms and technological systems that we create and employ to create, store, modify, exchange, and exploit information in all its myriad

forms. This is where we design and build cyberspace, because each of these cyber platforms is created with a purpose, and we combine them to create even newer and more complex/capable systems and networks. The next layer is the information itself. Finally, and most importantly, is the human element—the people who use the connectivity and the content to affect cognition and do the different things that people do with information. Each layer is important, and each is affected and shaped by the others.[27]

If cyberspace is but one element of the information environment—albeit perhaps the most important one in many cases—are there other issues that arise from this relationship? There are likely many, but two that immediately come to mind are the organizational and doctrinal aspects as related to warfare and the military component of power. Even as the U.S. military comes to grips with a definition of cyberspace, the Services and the joint force are responding with organizational and doctrinal adaptations. Both the Navy and Air Force took action in 2006 to improve their abilities to operate in cyberspace. In October 2006, Admiral Mike Mullen, then Chief of Naval Operations, tasked his Strategic Studies Group at the Naval War College to develop a concept for "Fighting in Cyberspace in 2030" and to examine the operational, procedural, and technological improvements needed for the Navy to master the cyberspace warfighting realm. Admiral Mullen called cyberspace a "new dimension in warfare," and he wanted to determine the relationships between cyberspace and the traditional realms such as the maritime environment. What will warfare be like in cyberspace, he asked, and how will a "1,000 ship Navy go to cyberspace?"[28]

The group's report, which examined the "Convergence of Sea Power and Cyber Power," surveyed nearly 30 definitions of cyberspace and attempted to plot them on an x-y scale that measured each definition against two metrics: its degree of human versus technical centricity, and its present-day versus future focus. It assessed the definition in the 2006 *National Military Strategy for Cyberspace Operations* as quite present-day and tech-centric, then offered its own definition of cyberspace as:

> an unconstrained interaction space . . . for human activity, relationships, and cognition . . . where data, information, and value are created and exchanged . . . enabled by the convergence of multiple disciplines, technologies, and global networks . . . that permits near instantaneous communication, simultaneously among any number of nodes, independent of boundaries.[29]

While there is much wisdom and perceptive insight in this approach, it has two problems. One is that it is unwieldy and suffers from the understandable attempt to include detailed examples and explanations. The other is that it is not grounded in what makes cyberspace unique—namely, electronic technologies and the electromagnetic spectrum.

The Air Force's move into cyberspace attracted much greater attention because of the more visible and public manner in which it was accomplished. On the anniversary of the bombing of Pearl Harbor in 2005, Air Force Chief of Staff General Michael Moseley and Secretary of the Air Force Michael Wynne signed a new Air Force mission statement declaring that the mission of the Air Force was to "fly and fight in the Air, Space, *and Cyberspace* [emphasis added]." Early in 2006, General Moseley established a task force to explore concepts for how the Air Force should respond to the emergence of this new warfighting environment. In September 2006, General Moseley and Secretary Wynne signed a joint memo directing the creation of an "Operational Command for Cyber- space" that would "enable the employment of

global cyber power across the full spectrum of conflict."

Two months later, on November 1, General Moseley designated the 8th Air Force as the Air Force Cyber Command and gave it the added mission of extending the Service's reach and capability into the "domain of electronics and the electromagnetic spectrum." The eventual goal was to develop a plan to "organize, train, and equip" the Air Force as a fully capable cyber force, and for the 8th Air Force to become the cyber equivalent of the Air Force's major commands for air and space sometime in the future (2007 was the target for an "initial operational capability"). The Air Force established a goal of "full operational capability" by late 2009, and was building cyberspace into its programs and budget plans a decade into the future.[30] The Cyber Command's "Strategic Vision" described the cyber domain and strategic environment and established the goal of "dominating cyberspace" so that the Air Force would be able to "establish, control, and use" the domain. Talking about developing capabilities is one thing, but putting resources—money, people, and organizations—into cyberspace is another, and it appeared that the Air Force was not only "talking the talk" about cyberspace, but "walking the walk" as well.[31]

However, suspicion arose among the other Services that the Air Force's movement was a grab for cyber turf, and in the wake of Secretary of Defense Robert Gates' relief of both Secretary Wynne and General Moseley in early summer 2008, the new Air Force Chief of Staff, General Norton Schwartz, called a halt to all actions on Air Force Cyber Command: "Transfers of manpower and resources, including activation and re-assignment of units, shall be halted." While it is unclear how much influence Secretary Gates and Chairman of the Joint Chiefs of Staff Admiral Mullen had on this action, it will certainly have a negative impact of the development of cyber capabilities in the Air Force and perhaps across DOD.[32]

The Army and the Marine Corps are also developing concepts and capabilities for cyber operations, albeit to less of a degree than the Navy and Air Force. The Army sees cyberspace not so much as its own unique warfighting domain but rather as a critical enabler for two vital functions: intelligence and command and control of forces and operations, or "networked enabled battle command." Army Field Manual 3.0, *Operations*, reorganized a series of five tasks related to information and cyber, none of which are cyber-specific, which is congruent with the Army's institutional reluctance to consider cyberspace as an operational domain.[33] But in June 2008, the Army established a Network Warfare Battalion (Provisional), which may herald a more aggressive approach to cyberspace. The Marines' cyber concept is somewhat similar and looks at cyberspace from the perspective of command, control, communications, and computers.

In 2002, a change to the Unified Command Plan assigned responsibility for information operations to U.S. Strategic Command (USSTRATCOM), which undertook a wide-ranging reorganization that included the creation of several joint task forces (including one for global network operations) and joint functional component commands (including one for network warfare). The former includes important elements of the Defense Information Systems Agency and emphasizes protecting and defending military cyber capabilities, while the latter includes capabilities for that aspect of IO known as computer network attack. These changes were made to improve USSTRATCOM's ability to operate in cyberspace and carry out critical missions in support of military and national security strategy, but they also hint at an inherent tension between offense and defense, with the offensive and defensive components divided into two entirely different organizations.[34] This particular and somewhat unusual organizational structure reflected the desire of then USSTRATCOM Commander General James Cartwright

to push the authority and responsibility for conducting IO away from the central headquarters and out to the organizations that actually had capabilities and resources. Whether this organizational structure endures in its present form or is modified is perhaps less important than the continued development of real capabilities to plan and conduct IO.

Alliance Perspective

Since cyberspace is global in nature, it is fitting to include the perspective of our single most important alliance, the North Atlantic Treaty Organization (NATO). In 2008, NATO issued its final draft of "Policy on Cyber Defence." Its intent was to enhance NATO's protection against cyber attacks on communication and information systems of "critical importance to the Alliance," meaning those that support military and political decisionmaking. Data processing systems and supporting services needed for functioning and consultations of Allied nations, intelligence-sharing, decisionmaking, and planning and conduct of NATO missions are the most critical functions to be protected.[35] This interest in cyberspace was intensified by the events in Estonia in mid-2007, which contributed to the creation of several organizations to support this protection. These included NATO's Computer Incident Response Capability, the Cyber Defence Management Authority, and the NATO Cooperative Cyber Defence Centre of Excellent, to be located in Tallinn, Estonia.[36]

These efforts will almost certainly receive added impetus as a result of the "cyberwar" waged as part of the Russian-Georgian confrontation in August 2008. While Russian conventional military operations were conducted in Georgia during the crisis, there reportedly was a "coordinated Russia versus Georgia cyber attack in progress" as well. But there was probably far more smoke than actual fire in this situation. While someone acted to deface and otherwise interfere with a wide range of Georgian governmental Web pages and sites, there was no attribution of these actions to the Russian government, nor were there any cyber attacks against actual Georgian infrastructure or systems critical to the life and well being of the populace or the capability of its military forces. Rather crude defacements of Georgian government Web pages—replacing the image of Georgian President Mikheil Saakashvili with one of Adolf Hitler, for example—or denial of service attacks against other Georgian governmental Web sites appeared to be the extent of the "cyberwar."[37] This limited action should not, however, be interpreted as a lack of Russian capability. Far more likely was the lack of appropriate targets in Georgia, along with the reluctance to expose what might have been very specialized and hard to acquire capabilities. Instead of focusing on cyber attacks against infrastructure, the confrontation featured widespread use of cyberspace by both sides for influence and propaganda purposes, activities that are just as real and strategically vital as potential actions against cyber-connected supervisory control and data acquisition systems.

Cyberspace is slowing finding its way into the doctrinal lexicons of all the Services, and one of the issues that will be contentious is the meaning of *superiority*. Unfortunately, Joint Publication 3–13 defines *information superiority* as "the operational advantage derived from the ability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same." This definition uses a measurement of effort, not impact, and has a communications or intelligence flavor to it. The Air Force developed a significantly different approach, describing *superiority* as "that degree of information advantage of one force over another that permits the conduct of operations at a given time and place without prohibitive opposition."[38] While this definition has a decidedly

martial tone, this approach is better because it is based upon an effect—"degree of advantage"—rather than a sterile and perhaps misleading measurement of effort.

An even better approach was offered in the 2004 edition of Joint Publication 1–02, *Department of Defense Dictionary of Military and Associated Terms*, which defined *information superiority* as "that degree of dominance in the info domain which permits the conduct of operations without effective opposition." If one substitutes the word *aerospace* or *maritime* for *information*, General Hap Arnold or Admiral Chester Nimitz would have understood and agreed. Taking the next step and substituting *cyberspace* for *info realm* produces a workable definition of *cyber superiority*: "the degree to which one can gain advantage from the use of cyberspace while if necessary preventing one's adversaries from gaining advantage from it. Cyber superiority includes offensive/proactive and defensive/protective operations."

The question that immediately comes to mind, however, is whether such a concept is at all appropriate to or workable in cyberspace. If cyberspace inherently includes all of the practically endless networks and information systems that are globally interconnected, how can one speak of having "superiority" in it or "dominating" it? If cyberspace has become part of the global commons that the entire world has access to—such as the aerospace or the sea—how can one speak of controlling it? A materially based view is clearly inappropriate, because the issue is not controlling electrons or electromagnetic forces, but rather influencing the use of cyberspace, in the same way that air or naval superiority is not about controlling molecules of air or water but rather controlling how the physical domain is used. It is a measure of effect or impact on human affairs and processes. Attaining operational superiority requires action at both ends of the spectrum: offensive or proactive efforts to use cyberspace and perhaps actively negate someone else's use of it, while simultaneously defending our uses of it and taking protective measures to prevent as much as possible anyone else from interfering with our use.

Cyberpower

This brings us to a second major objective of this chapter: to define and explore cyberpower. Earlier, this chapter drew a strong analogy among the domains of air-land-sea and outer space and cyberspace, and those same analogies hold true for a concept of cyberpower as drawn from seapower or airpower. Surprisingly, however, although much has been written about airpower and seapower, simple and clean definitions of them are lacking. The "father of American seapower," Admiral Alfred Thayer Mahan, wrote extensively about the factors that led to naval supremacy and how a government could spur national attitudes toward power on the seas, but he never clearly and simply defined what he meant by the term.[39] A definition of *seapower* published by two professors at the U.S. Naval Academy shortly after World War I—"a nation's ability to enforce its will upon the sea"—was clearly influenced by Mahan's thinking and emphasized effects rather than means, although it ignores seapower's relationship to other aspects of power, such as national economic strength.[40] Obviously, the professors were not referring to controlling the sea itself but rather to controlling human and national activities on the sea and how that physical medium was used to affect events and operations.

Giulio Douhet, the man most closely associated with the concept of airpower, also did not clearly define it, although he created elaborate scenarios to demonstrate its impact on future warfare. Nor did Billy Mitchell, one of the pioneers of American airpower, define it in detail, although his pithy statement that "airpower is the ability to do something in the air"

captures several critical aspects of any form of power. Yet it, too, suffers from the same narrow perspective as Mahan's definition and ignores, for example, the huge economic impact of American dominance of the civilian airliner market for many years.[41] But all of these pioneers would have understood—and likely agreed with— an approach that concentrated on the ability to use and exploit the physical environments, "the ability to use the sea to advantage," or "the ability to use the air for our purposes." This leads to the definition of *cyberpower* as "the ability to use cyberspace to create advantages and influence events in all the operational environments and across the instruments of power."[42] This definition is broader than the Mahanian or Douhetian approaches to seapower or airpower because it includes explicit reference to other forms of power and is meant to emphasize cyberpower's synergistic impact on and integration with other forms and instruments of power.

This instrument of power is shaped by multiple factors. While cyberspace as an environment simply "is," cyberpower is always a measure of the ability to use that environment. Technology is one obvious factor, because the ability to "enter" cyberspace is what makes it possible to use it. That technology is constantly changing, and some users—countries, societies, nonstate actors, and the like—may be able to leap over old technologies to deploy and use new ones to dramatic advantage. Organizational factors also play an important role, because the organizations we create reflect human purposes and objectives, and their perspectives on the creation and use of cyberpower will be shaped by their organizational mission, be it military, economic, or political. All of these different factors shape how we employ cyberpower to impact and influence the elements of power.

The element that is most closely tied to cyberpower is information. Cyberspace and cyberpower are clearly dimensions of the informational instrument of power under the PIME (political, informational, military, economic) model, one of several current approaches to elements of power, and we can see myriad ways that cyberpower links to, supports, and enables the creation and exercise of the other instruments. Cyberpower is playing an increasingly vital role in economic strength. The National Security Strategies published by the Reagan administration in the 1980s were laced with insights and references to the role that information and the new information technologies would play in strengthening the American economy. In the global economy of the 21st century—the economy of a globalized and interconnected "flat world"—cyberspace is perhaps the single most important factor linking all the players together, boosting productivity, opening new markets, and enabling management structures that are simultaneously flatter yet with a far more extensive reach.[43]

Cyberpower's impact on political and diplomatic affairs is hardly less extensive. The world's most ubiquitous influence medium remains satellite television, which is carried by systems and networks that connect via cyberspace. The influence campaigns waged by the U.S. Government or by the shadowy terrorist nets of al Qaeda are both using cyperpower as a crucial capability in the struggle for minds and ideas.[44] Militarily, cyberpower has been perhaps the most influential instrument of the past two decades. From the Russian concept of the "military technical revolution" in the 1980s to the development of net-centric concepts and defense transformation in the U.S. military, cyberspace and cyberpower have been at the heart of new concepts and doctrines. Across the levels of conflict, from insurgency to main-force conventional warfare, cyberpower has become an indispensable element of modern technologically based military capability.

Cyberpower is exerting itself as a key lever in the development and execution of national policy, whether it be counterterrorism, economic growth, diplomatic affairs, or one of myriad

other governmental operations. In state and even local affairs, cyberpower is shaping how governments connect with their citizens to provide services in ways that could not have been imagined a decade ago. It does the same for the development of new technologies, in their creation, exploitation, and measurement of success. One is hard pressed to think of a technology today that is not affected or improved by a cyber component; just look at the number of computers and information systems embedded within the typical new automobile for an example of how cyber capabilities are improving technologies that at first glance seem to have no connection to cyberspace at all. As cyberpower has exerted increasingly widespread impact across society during the past two decades, we are forced to adapt to those impacts in new ways, as seen in the current debate over how to draw the limits on government surveillance of the citizenry and access to their personal information, from financial records to communications.

Cyberpower creates synergies across the other elements and instruments of power and connects them in ways that improve all of them. Cyberspace is literally transforming how we create data itself, the raw material that fuels our economy and society. Because of new forms of content—images, sounds, information in a thousand and one forms—and the connectivity that we use to transmit and exchange that content, we are transforming how we exert influence and employ "smartpower" in the pursuit of strategic goals, whether as part of the war of ideas against violent extremism or to enable a traditional town hall meeting. These latter uses hint at what is perhaps the most significant and transformative impact cyberspace and cyberpower are having, that of linking people and organizations in new ways in an increasingly wired world in which traditional borders and boundaries are being altered and new relationships among people being forged. Where once only governments spoke to other governments, now we see governments and individuals interacting with each other, often across national borders. Listing all of the many ways (some of which are not yet known) that cyberspace and cyberpower will drive and facilitate change is impossible, but they are already driving it. The whole of the cyber revolution is greater than the sum of its parts, and not only will its impact be nearly ubiquitous, but also it will increase.

A National Strategy for Cyberspace

The existence of cyberspace as a new global domain presents fresh opportunities for its employment and vulnerabilities to be defended against, as discussed previously, and the strategist will be challenged to integrate its capabilities with other elements and instruments of power. In short, it demands the crafting of strategy—a *cyber strategy* that looks to enable and exploit the capabilities that cyberspace offers while protecting and defending against the vulnerabilities it simultaneously presents. To do this, we must first define our terms: what is a cyber strategy? The Joint Staff defines *strategy* as "the art and science of developing and employing instruments of national power in a synchronized and integrated fashion to achieve theater, national, and/or multinational objectives." This is a good starting point, but the approach toward defining any strategy in terms of an operational realm, such as an *air strategy*, must be grounded in that realm. Thus, the approach this chapter uses is that "cyber strategy is the development and employment of strategic capabilities to operate in cyberspace, integrated and coordinated with the other operational domains, to achieve or support the achievement of objectives across the elements of national power in support of national security strategy." To develop a national strategy for cyberspace, therefore, is to simultaneously create cyber resources and procedures that can contribute to the achievement of specific national

security objectives. Those means/resources might be technological (Internet Protocol Version 6), or organizational (the Joint Functional Component Command–Network Warfare or a Computer Emergency Response Team), or even human (trained and certified chief information officers.) At a foundational level, those objectives might focus on the creation of the resources and procedures themselves in the same sense that an airpower strategy must first consider what airpower means are available or needed, then examine how those resources could be used. This is a fundamental first step in the sense that one could not have an air or space strategy without first having the airplane or satellites that enabled the use of those realms; the concepts and doctrines for the use of those planes and satellites follow. This must be a strategy of partnership, given the definition of cyberspace presented in this chapter, because the private sector is inseparable from government and the military in cyberspace. Indeed, in many crucial ways—at least in the United States—the government and Armed Forces are heavily and increasingly dependent on the private sector for the development, maintenance, and security of cyberspace capabilities.[45]

This perspective is no different from the way that we view seapower or airpower. Mahan enumerated several factors necessary for the development of national seapower, among them geography, industry, populace, national character, and governance. While Douhet did not do the same for airpower, others have, such as Stefan Possony, who listed no fewer than 15 elements, including industry, research and development, aircraft, and manpower.[46] These attributes are closely tied to the private sector and national industry, and this is as, if not more, true of cyberspace as these other forms of power. There are important parallels to—and differences from—cyberspace. While no modern nation possessing and employing seapower or airpower has lacked any of these attributes, this might not always hold true for cyberspace. Small nations may be able to create significant cyber capabilities—look at the example of Estonia, which has infused cyberspace throughout much of its daily life, to significant economic and societal benefit—and the human side of the equation does not requires thousands of trained troops, perhaps only dozens or hundreds.[47]

A large part of the cyber strategy issue concerns the ends for which these cyber capabilities might be used. These ends are part of the larger military, political, economic, diplomatic, and national security objectives being sought. Cyberpower is not created simply to exist, but rather to support the attainment of larger objectives. Nations do not expend national resources to create seapower or airpower or spacepower except in the expectation that those efforts will help to achieve strategic goals across the elements of national power—political, diplomatic, informational, military, and economic—as a means of satisfying the vital national needs and interests of national security strategy. The national security strategies of the Reagan administration in the 1980s made explicit reference to the links between information and economic power, including specific recommendations concerning computers and advanced information technologies. Toward the end of the Clinton administration in the 1990s, the role of information in diplomatic, military, and economic affairs was explicitly recognized and explored. While the George W. Bush administration did not make these connections in its two national security strategy documents, lower level strategies such as the *National Strategy to Secure Cyberspace* or the *National Military Strategy for Cyberspace Operations* did. The key contribution for a national strategy for cyberspace will be to clearly demonstrate how it makes possible the support of all the other strategies, especially the national security strategy, and the achievement of their critical and interrelated objectives. This is the challenge for the future.

---

[1] The research for this effort provided a wide range of approaches to this definition, some of which are

summarized in table 2–1.

[2] While some in the U.S. Air Force have argued that the aerospace is a seamless environment that extends from the Earth's surface to infinity, the fact is that the air and outer space are subject to not only differing legal regimes—overflying a nation's sovereign airspace could be a violation of international law, while orbiting the Earth in space is not—but physical ones as well. Movement in the air is governed by lift, while in space, the laws of orbital mechanics rule. Thus, air and space are two very different domains.

[3] Joint Publication 1–02, *DOD Dictionary of Military and Related Terms* (Washington, DC: The Joint Staff, dated April 12, 2001, and amended through November 9, 2006), available at <www.dtic.mil/doctrine/jel/new_pubs/jp1_02.pdf>.

[4] See, in roughly chronological order: Winn Schwartau, *Information Warfare: Chaos on the Electronic Superhighway*, 2d ed. (New York: Thunder's Mouth Press 1996); Ed Waltz, *Information Warfare: Principles and Operations* (Boston: Artech House, 1998); Walter Gary Sharp, *Cyberspace and the Use of Force* (Falls Church, VA: Aegis Research, 1999); Dorothy Denning, *Information Warfare and Security* (Reading, MA: Addison-Wesley, 1998); and Gregory Rattray, *Strategic Warfare in Cyberspace* (Cambridge: MIT Press, 2001).

[5] The White House, *The National Strategy to Secure Cyberspace* (Washington, DC: The White House, 2003).

[6] During the initial meeting of the task force that wrote this book, a representative of the Joint Staff (J6X) effort to develop the *National Military Strategy for Cyberspace Operations* presented a concept for cyberspace that was unacceptable to almost everyone in attendance. To their credit, the J6X team—of which the author of this chapter was a member—reworked its approach, perhaps influenced by concepts presented by this author at that initial meeting, to the point where the final J6X effort was very similar to that presented during the meeting and to that suggested in this chapter. While this author had some minor quibbles with the definition that was used in the final product, it comes so close to many of the key points he offered during the drafting process that we were clearly on the same sheet of music. The same is essentially true of the 2008 definition of cyberspace signed by Deputy Secretary of Defense Gordon England and Chairman of the Joint Chiefs of Staff Admiral Mike Mullen.

[7] Both definitions are contained in the Deputy Secretary of Defense Memorandum to the Military Departments et al., "The Definition of Cyberspace," May 12, 2008, and its accompanying staff papers.

[8] The term *domain* has taken on a near-theological significance in the Department of Defense, with intelligent and well-intended people trying to parse differences between words such as *domain*, *realm*, and *environment*. This can be seen in the Deputy Secretary of Defense definition, which characterizes cyberspace as a domain within an environment.

[9] The role of the human element in cyberspace is the subject of an ongoing debate as to whether humans are an integral part of cyberspace, or whether we are merely the users— some would add creators—of cyberspace. While this author feels that the importance of the human element can hardly be overemphasized, we are no more "part" of cyberspace than we are of the aerospace or outer space, since the essence of the definition of these different environments flows from their unique physical characteristics.

[10] The current (February 2006) Joint Publication 3–13, *Information Operations*, available at <www.dtic.mil/doctrine/jel/new_pubs/jp3_13.pdf>, defines this environment as "the aggregate of individuals, organizations, and systems that collect, process, or act on information," then further refines this definition with the observation that this environment functions via the interrelated effects of three dimensions: the physical (which is described in this chapter as connectivity), the informational (content), and the cognitive. This author finds the approach toward the three dimensions the most instructive and thus has concentrated on them.

[11] The debate about whether cyberspace is a "place we go" stems from the need to use manmade technologies to operate in cyberspace. But this is no different than most of our other physical environments in that we require technologies such as motors to use those environments. Submarines, airliners, and spacecraft—and computers—operate in different physical environments, yet all use motors in the process of "entering" and operating in those environments.

[12] The author is indebted to Dave Clark for suggesting this perspective on cyberspace. His point about interconnectivity cannot be stressed too strongly.

[13] *Operational* is being used in the sense of it being practical and useful, a place where things actually happen, and not as one of the levels of war such as *tactical* or *strategic*.

[14] The observation was made during the 2008 Democratic Presidential primary, that while Senator Hillary Clinton told supporters to visit her Web page, Senator Barack Obama told supporters to text-message their five closest friends and thus gained advantages through his exploitation of "viral networking."

[15] We are seeing an enormously increased use of cyberspace and the Internet by the terrorists and radical Islamist organizations. See, for example, Gabriel Weimann, "Hezbollah Dot Com: Hezbollah's Use of the Internet During the 2006 War," presented at the International Institute for Counterterrorism's "International Conference on Terrorism's Global Impact," Herzliya, Israel, September 2006, or Weimann's book *Terror on the Internet: The New Arena, the New Challenges* (Washington, DC: U.S. Institute of Peace Press, 2006). Even terminology has come into play, with some specialists suggesting that we use the wrong terms to describe the enemy and that calling terrorists "jihadists" legitimizes them, while words such as "irhabists" speak to Islamic audiences in different ways. See the work of Jim Guirard and the "Truespeak Institute," available at <www.truespeak.org/> or Douglas E. Streusand at Marine Corps Command and Staff College for more. Also see Irving Lachow and Courtney Richardson, "Terrorist Use of the Internet: The Real Story," *Joint Force Quarterly* 45 (2d Quarter 2007), available at <www.ndu.edu/inss/Press/ jfq_pages/editions/i45/24.pdf>.

[16] The U.S. concept of network-centric warfare dates to 1998 and the pathbreaking article by Arthur K. Cebrowski and John J. Garstka, "Network-Centric Warfare: Its Origin and Future," United States Naval Institute *Proceedings* (January 1998), available at <www.usni. org/Proceedings/Articles98/PROcebrowski.htm>. The Chinese have been prolific writers about "informationized" warfare for at least a decade; see Michael Pillsbury, *Chinese Views of Future Warfare* (Washington, DC: National Defense University

Press, 1998), available at <www.ndu.edu/inss/Press/NDUPress_Books_Titles.htm>.

[17] See, for example, David C. Gompert, Irving Lachow, and Justin Perkins, *Battle-Wise: Seeking Time-Information Superiority in Networked Warfare* (Washington, DC: National Defense University Press, 2006); also Myriam A. Dunn, "The Cyberspace Dimension in Armed Conflict," *Information and Security* 7 (2001), 145–158, available at <www.isn.ethz. ch/crn/_docs/ACF18D.pdf>.

[18] Some radio waves are blocked by dense material such as water or earth, while other waves are best transmitted via those dense materials. It depends on the type of radio waves and their frequency ranges.

[19] In 2007, a team sponsored by Carnegie Mellon University's Software Engineering Institute published a compendium of papers titled *Preparing to Fight in Cyberspace*. The first paper, "On the Security of the Cyber Battlefield," by William L. Fithian, suggested that "cyberspace is just as much a physical space as air, sea, land, or outer space." That is precisely the same argument made in this chapter.

[20] There are obvious limits to this: we have not yet learned how to express the emotion of the human heart or the intellect of the human mind as a string of ones and zeroes, until they are turned into observable phenomena in the physical world—at which point we can capture those phenomena in multiple ways. Another question that arose during the writing of this definition concerned the words *exchange* and *transmit*. *Exchange* was chosen as being more inclusive: you cannot have an exchange of information without its transmission, and transmission without reception is meaningless.

[21] The term *information-communication technology* (ICT) has been in use worldwide for more than a decade, and our failure to use it is a strange omission. ICT neatly blends two critical dimensions of cyberspace—the information itself and its exchange.

[22] See Tom Standage, *The Victorian Internet* (New York: Walker, 1998), and Daniel R. Headrick, *The Invisible Weapon* (New York: Oxford, 1991). While it is true that we had earlier ways of transmitting information—balloons, signal fires, flags—the origins of modern information technology began with the telegraph little more than a century and half ago. The same holds true for the use of the subsurface of the sea: while the *Turtle* dates to the Revolutionary War, and the CSS *Hunley* to the Civil War, they were powered by hand cranks and hardly permitted useful employment of the subsurface.

[23] Dave Clark has observed that in India, WiFi base stations have been mounted in vehicles that are then driven from village to village, to enable local cyber cafes to make temporary connection to the Internet. What is interesting is not the form of physical transport—the WiFi station could even have been elephant-mounted, perhaps—but the astronomical expansion of connectivity that results in each separate location when that WiFi base arrives.

[24] This definition of information operations was first published in the *Information Operations Roadmap* approved by the Secretary of Defense in October 2003 and became part of the formal joint doctrinal lexicon with the issuance of Joint Publication 3–13, *Information Operations*, in February 2006; available at <www.dtic.mil/doctrine/jel/new_pubs/jp3_ 13.pdf>.

[25] If one tried to capture this visually as a Venn diagram, the connectivity dimension would include three related and touching yet separate elements, reflecting technologies dependent on cyberspace (the Internet or television), technologies not dependent on cyberspace (the office "snail mail" distribution system), and human interaction. The content dimension would also include three distinct yet related and touching elements, again reflecting technologies dependent on cyberspace (a Web page), technologies not dependent on cyberspace (the content of an office memo tacked to the bulletin board), and human interaction.

[26] See David T. Fahrenkrug, "Cyberspace Defined," in *The Wright Stuff* (Maxwell Air Force Base, AL: Air University Press, May 17, 2007), available at <www.au.af.mil/au/aunews/ archive/0209/Articles/CyberspaceDefined.html>. The Air University portal has a number of viewpoints on cyberspace; see <www.au.af.mil/info-ops/cyberspace.htm> for a list.

[27] The author is indebted to Dave Clark, who suggested this "layered" approach to cyberspace.

[28] See Rati Bishnoi, "Navy Eyes Fighting in Cyberspace," *InsideDefense.com*, November 29, 2006.

[29] Naval War College Strategic Studies Group XXVI briefing, "Convergence of Sea Power and Cyber Power," July 13, 2007.

[30] See Sebastian M. Convertino II, Lou Anne DeMattei, and Tammy M. Knierim, *Flying and Fighting in Cyberspace*, Maxwell Paper 40 (Maxwell Air Force Base, AL: Air University Press, July 2007); and "Cyber-Commander: Preparing Combat Forces for the Electromagnetic Spectrum," *Military Information Technology* 12, no. 3 (April 2008), 25–27.

[31] Michael Wynne and General T. Michael Moseley, "Establishment of an Operational Command for Cyberspace," memorandum, September 6, 2006; General Moseley, "Operational Cyberspace Command 'Go Do' Letter," memo to 8th Air Force Commander, November 1, 2006; John T. Bennett and Carlo Munoz, "Wynne, Moseley Tap 8th Air Force as First-Ever 'Cyberspace Command," *Inside the Air Force*, November 3, 2006; Marcus Weisgerber, "Cybercommand Expected to Reach IOC in May," *Inside the Air Force*, January 26, 2007.

[32] Bob Brewin, "Air Force Suspends Cyber Command Program," *Nextgov.com,* August 12, 2008, available at <www.nextgov.com/nextgov/ng_20080812_7995.php>.

[33] Until early 2008, in fact, the Army's institutional position was that cyberspace was NOT a distinct warfighting domain.

[34] The U.S. Strategic Command Web page at <www.stratcom.mil/organization-fnc_comp. html> has a thumbnail sketch of each of these organizations and others, including the Joint Information Operations Warfare Command.

[35] Executive Working Group, "NATO Policy on Cyber Defence," C–M (2007) 0120, December 20, 2007.

[36] NATO press release, "NATO opens new centre of excellence on cyber defence," May 14, 2008, available at <www.nato.int/docu/update/2008/05-may/e0514a.html>. As an indicator of the level of interest in the topic, a quick Google search on the combined terms *NATO* and *cyber* yielded over a million hits.

[37] Dancho Danchev, "Coordinated Russia vs. Georgia cyber attack in progress," *ZDNet. com*, August 11, 2008, available at <http://blogs.zdnet.com/security/?p=1670>. Also see John Markoff, "Before the Gunfire, Cyberattacks," *The New York Times*,

August 13, 2008, and David Ho, "Web Sites Hit as War Uses Bytes and Bullets," *Atlanta Journal- Constitution*, August 15, 2008.

[38] Air Force Doctrine Document (AFDD) 2–5, *Information Operations*, January 11, 2005, 7. A planned revision to this doctrine was shelved until the entire issue of cyberspace and the Air Force is clearer. AFDD 2–11, *Cyberspace Operations*, is in development, although it may not be completed until 2009.

[39] Alfred Thayer Mahan, *The Influence of Sea Power upon History, 1660–1783* (Boston: Little, Brown and Company, 1890).

[40] William Oliver Stephens and Allan Westcott, *A History of Sea Power* (New York: Doubleday, 1920), 443.

[41] Although Douhet used the terms *aerial power* and *air power* within the first few pages of *The Command of the Air* (originally published in 1921, reprinted by the Office of Air Force History in 1983), he never clearly defined the term. In his editor's introduction to the 1983 reprint, Air Force historian Richard Kohn described airpower as "the use of space off the surface of the earth to decide war on the surface." The very first use of the term actually came with the onset of powered flight, in H.G. Wells' futuristic novel *The War in the Air*, published in 1908, which predicted some of the massed aerial attacks on cities and civilians seen later in the 20th century.

[42] While the concept of cyber superiority offered here is clearly a comparison between competitors, the concept of cyberpower offered here is by no means a comparison and is not intended to be seen in a zero-sum context. Indeed, one of the oft-cited attributes of cyberspace is its ability to augment and empower many users simultaneously.

[43] See Thomas L. Friedman, *The World is Flat: A Brief History of the Twenty-first Century* (New York: Farrar, Straus and Giroux, 2005); it is curious that the term *cyberspace* is not listed in the index, because cyberspace's impact on the 21st century drips from every page of this marvelous analysis of the future.

[44] One of the assignments the author gives students at the National Defense University is to watch international and non-U.S. television to gain a perspective on how information is being used by others in the global battle for ideas. How do they access television from dozens of countries all over the globe? Via the Internet, of course, and by going to Web sites such as <www.yourglobaltv.com/portal.htm>, they can access television programming from all over the Earth.

[45] Indeed, one of the criticisms that can be made of the National Security Presidential Directive 54–type approach is that it focuses too narrowly on military and governmental information networks without sufficient appreciation of their growing reliance on civilian networks and infrastructures.

[46] Mahan, 25; for Possony's list, see Charles M. Westenhoff, *Military Air Power* (Maxwell Air Force Base, AL: Air University Press, 1990), 24.

[47] For a cogent analysis of the cyber event in Estonia in May 2007, see Joshua Davis, "Hackers Take Down the Most Wired Country in Europe," *Wired* 15, no. 9 (August 22, 2007), available at <www.wired.com/print/politics/security/magazine/15-09/ff_estonia>.