CHAPTER 3

Toward a Preliminary Theory of Cyberpower

Stuart H. Starr

THIS CHAPTER represents an initial effort to develop a theory of cyberpower. First, the terms of reference that were provided to the National Defense University (NDU) team are characterized. Next, the components of a theory of cyberpower are characterized. Consistent with that characterization, key terms are identified, and straw man definitions of those terms are put forth. Specific objectives that are addressed in this theory are identified. In accord with those objectives, a holistic framework to categorize and discuss key categories is presented. The intellectual capital required to address these issues is discussed within this holistic framework.

Subsequently, theoretical dimensions of the key categories—cyberspace, cyberpower, cyber strategy, and institutional factors—are discussed. In addition, the challenges associated with connecting across these categories and anticipating future cyber activities and issues of interest are contemplated. The chapter concludes by summarizing major findings and identifying the next steps that should be taken to refine this preliminary theory of cyberpower.

Terms of Reference

In the 2006 Quadrennial Defense Review (QDR),[1] requests were made to develop theories of spacepower and cyberpower. The Institute for National Strategic Studies (INSS) and Center for Technology and National Security Policy (CTNSP) at NDU were tasked with developing, respectively, theories of spacepower[2] and cyberpower.

As stated in the terms of reference for the cyberpower task,[3] "there is a compelling need for a comprehensive, robust and articulate cyberpower theory that describes, explains and predicts how our nation should best use cyberpower in support of U.S. national and security interests." Consistent with that broad goal, the terms of reference identified four specific areas for which the theory should account:

- the Nation's increased use of and reliance upon national security, civil, and commercial cyber capabilities
- other nations' and nongovernmental actors' use of cyberspace
- direct challenges to U.S. use of cyberspace
- the changed and projected geostrategic environment.

Elements of a Theory

A theory of warfare should address five key issues.[4] First, it should introduce and define the key terms that provide the foundation of the theory. Second, it should give structure to the discussion by categorizing the key elements of the theory. Third, it should explain the elements in these categories by summarizing relevant events and introducing key frameworks or models. Fourth, it should connect the various elements of the subject so that key issues can be treated comprehensively. Finally, it should seek to anticipate key trends and activities so that policy can be germane and useful.

This framework for a theory raises one immediate issue. The terms of reference identified the need to predict, rather than anticipate, key activities. However, as described below, the cyber problem is in the midst of explosive, exponential change, creating an environment of exceptional uncertainty in which making reliable predictions is infeasible. Thus, the NDU team adopted the less challenging task of anticipating key trends and activities.

Finally, the following caveat must be stressed: since this is a preliminary effort to develop a theory of cyberpower, the emerging theory will not be complete. Furthermore, as discussed below, early efforts to develop a theory for any discipline inevitably were somewhat wrong.

To provide some context for theoretical developments, it is useful to note the challenges posed to the theories associated with physics over time. Contemporary physics theory has evolved over hundreds of years, dating back to the seminal contributions of Galileo Galilei and Isaac Newton. In this discipline, there is a common base of knowledge, although there are significant variants for specific subareas (for example, quantum mechanics, classical dynamics, and relativity). In addition, there are strong links to other hard science disciplines, such as mathematics, chemistry, and biology. Although the definitions of key terms and concepts are generally established, it should be noted that there were many false starts; a hundred years ago, for example, physicists had (incorrectly) postulated the existence of an ether through which electromagnetic waves propagated as they traversed a vacuum. Even in contemporary times, questions persist about the fundamental definitions of matter (for example, quarks with a variety of properties).

Within the subareas of physics, there is broad agreement about key categories (for example, solid, liquid, and plasma physics) for which mathematical models have generally been developed drawing on experiments and observations. Many of these mathematical models have proven to be extremely accurate and precise in explaining and predicting outcomes. However, efforts are still under way to connect many of the key subareas of physics. For example, there is considerable work ongoing in the area of string theory to develop a unified understanding of basic phenomena, although some critics have argued that this effort is likely to be a dead end.[5]

To highlight the challenges facing the “cyber theorist,” it is useful to contrast the discipline of physics with that of cyberspace. The cyberspace of today has its roots in the 1970s, when the Internet was conceived by engineers sponsored by the Advanced Research Projects Agency (ARPA). Detailed analysis of cyberspace issues often requires even broader cross disciplinary knowledge and skills than does analysis of physics. Experts with requisite skills include, inter alia, computer scientists, military theorists, economists, and lawyers. Each of these disciplines has its own vocabulary and body of knowledge. Thus, it is quite challenging for these stakeholders to communicate effectively. This difficulty is manifested in debates about the most basic of terms (for example, *cyberspace*) where key definitions are still contentious. Consistent with the heterogeneous nature of the problem, it is not surprising that prior efforts to characterize this space have not been successful. At present, there is no agreed taxonomy to support a comprehensive theory.

As noted above, key attributes of a theory include its ability to explain and predict (or at least anticipate). Among the many reasons why prior cyber theory efforts have foundered are the facts that key facets of the field are changing exponentially, there is little or no agreement on key frameworks, and the social science element of the discipline (for example, understanding of cognition and human interactions in virtual societies) makes it difficult to develop models that reliably explain or anticipate outcomes. Finally, the disparate elements of the field cannot be connected because a holistic perspective of the discipline has not yet been created.

Objectives

This chapter addresses the five elements of a military theory: define, categorize, explain, connect, and anticipate. In the areas of *explain* and *anticipate*, the focus is on identifying and characterizing rules of thumb and principles for cyber elements. More extensive explanations of and anticipation for cyber elements will be found elsewhere in this book.

The scope of the chapter is restricted to two major areas. First, the national security domain is the focus of attention. Changes in cyberspace are having a major effect on social, cultural, and economic issues, but they are addressed only tangentially. Second, attention is limited to the key cyberpower issues confronting the national security policymaker. Thus, no attempt is made to generate a comprehensive theory of cyberpower that touches on broader issues.

Approach

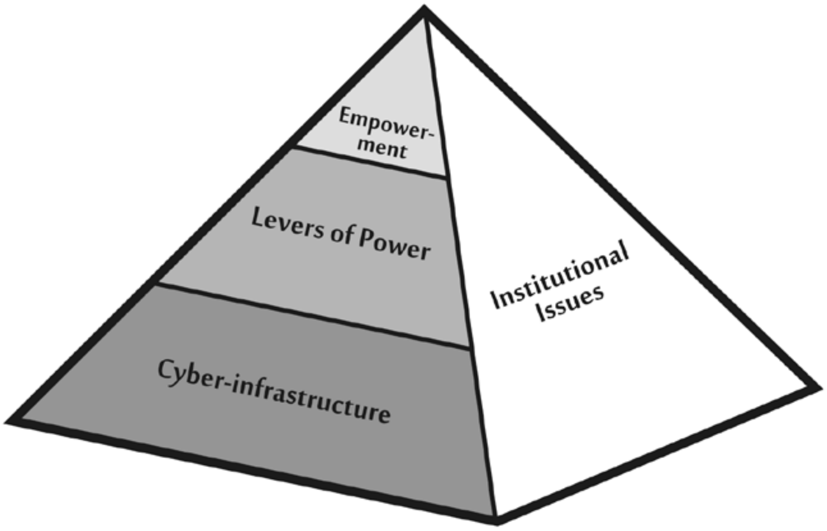
To achieve these objectives, the NDU team employed the following approach. First, we drew insights from observations of cyber events, experiments, and trends.[6] Second, we built on prior national security methods, frameworks, theories, tools, data, and studies germane to the problem. Finally, we formulated and hypothesized new methods, frameworks, theories, and tools to deal with unexplained trends and issues.

We implemented this approach through a series of workshops that drew upon world-renowned leaders in the areas of interest. This included representatives from government, industry, academia, and think tanks. At each workshop, the author of a chapter presented preliminary thoughts and conjectures to the participants. Based on feedback from the participants and reactions from the NDU team, the authors generated the material that is contained in this book.

The NDU team has adopted the holistic cyber framework depicted in figure 3–1. This framework is patterned after the triangular framework that the military operations research community has used to deconstruct the dimensions of traditional warfare. In that framework, the base consists of systems models, upon which rest more complex, higher orders of interactions (for example, engagements, tactical operations, and campaigns). Historically, the outputs from the lower levels provide the feedback to the higher levels of the triangle.

By analogy, the bottom of the pyramid consists of the components, systems, and systems of systems that comprise the cyber infrastructure. The output from this cyber infrastructure enhances the traditional levers of power: political/diplomatic, informational, military, and economic (P/DIME). These levers of power, in turn, provide the basis for empowerment of the entities at the top of the pyramid. These entities include, among others, individuals, terrorists, transnational criminals, corporations, nation-states, and international organizations. While nation-states have access to all of these levers of power, the other entities generally have access to only a subset of them. In addition, initiatives such as deterrence and treaties may provide the basis for limiting the empowerment of key entities. The pyramid suggests that each of these levels is affected by institutional issues that include factors such as governance, legal considerations, regulation, information-sharing, and consideration of civil liberties. This framework is merely one of many that could be constructed to conceptualize the cyber domain. However, it has proven useful to the NDU team in deconstructing the problem and developing subordinate frameworks to address key cyber issues.

Figure 3-1: Broad Conceptual Framework



Key Definitions

As noted above, there is a continuing discussion about the appropriate definitions for key cyber terms. For example, in its study of the "Convergence of Sea Power and Cyber Power,"[7] the Strategic Studies Group (SSG) identified 28 candidate definitions of the term *cyberspace*. To categorize and compare those terms, the group introduced a two-dimensional space that featured the axes *focus* (present-day versus future) and *centricity* (technology versus human). They observed that the definition posed by William Gibson, in his 1984 book *Neuromancer*,[8] fell in the upper right quadrant of this space (futurist with some consideration of the human dimension): "A consensual hallucination . . . a graphic representation of data abstracted from banks of every computer in the human system."

For the purposes of this theory, the NDU team adopted a variant of the formal definition of cyberspace that the Joint Staff employed in the *National Military Strategy for Cyberspace Operations*: "An operational domain 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 interconnected and internetted information systems and their associated infrastructures."[9] This definition does not explicitly deal with the information and cognitive dimensions of the problem. To do so, the NDU team has introduced two complementary terms: cyberpower and cyber strategy.

Cyberpower is defined as the ability to use cyberspace to create advantages and influence events in the other operational environments and across the instruments of power. In this context, the instruments of power include the elements of the P/DIME paradigm. For the purposes of this preliminary theory, primary emphasis is placed on the military and informational levers of power.

Similarly, *cyber strategy* is defined as the development and employment of 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. Thus, one of the key issues associated with cyber strategy deals with the challenge of devising tailored deterrence to affect the behavior of the key entities empowered by developments in cyberspace.

The definition that the NDU team has adopted for cyberspace begins with the phrase *an operational domain*. This raises an issue that is hotly debated by the military Services: Is cyberspace a domain?

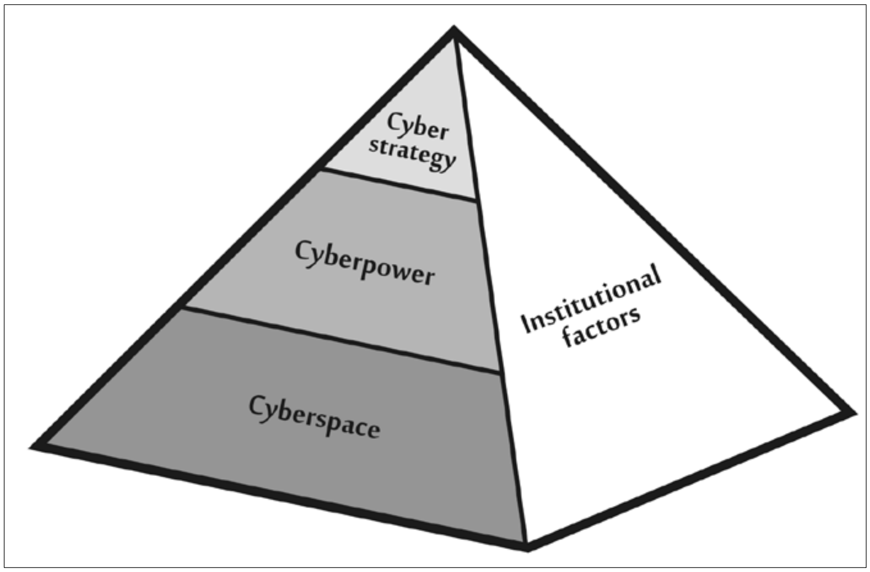
The term *domain* is not defined formally in key national security and military products. However, it is cited in selected policy documents. For example, the 2004 National Military Strategy states that "the Armed Forces must have the ability to operate across the air, land, sea, space, and cyberspace domains of the battlespace.[10] Furthermore, the 2006 QDR notes that "the [Department of Defense] will treat cyberspace as a domain of warfare." Joint Publication 3–0, *Joint Operations*, identifies several key features of a domain: it can be described physically; there are distinctions in means, effects, and outcomes; and military and combat operations can be conducted in and through the domain.[11]

One can make the argument that cyberspace is a domain through the following logic. It is widely accepted that (outer) space is a domain. In comparison to space, cyberspace has the following bounding attributes that suggest that it is a military domain: it is subject to ongoing levels of combat (see below); it is characterized by greater ease of access; and it is more difficult to identify and track military operations within it.

The acceptance of cyberspace as a domain has significant practical implications for the requirement to allocate resources to support organization, training, and equipping of "cyberforces," the need to develop a culture that is consistent with cyber activities, and the development of a professional cadre and establishment of a structured career progression.

Thus, for the purposes of this preliminary theory, cyberspace will be assumed to be "an operational domain" (as stated in the NDU team definition). Consistent with that definition, the elements of the holistic framework can be recast as depicted in figure 3–2.

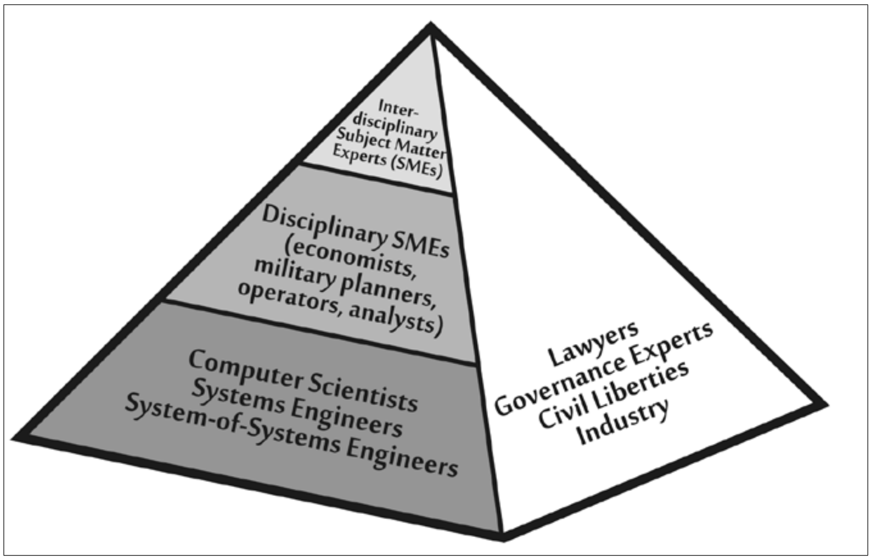
Figure 3-2: Cyberspace, Cyberpower, CyberStrategy, and Institutional Factors



Required Intellectual Capital

Dealing with the rich array of cyber policy issues that confront senior decision- makers will require a diverse set of intellectual capital. Figure 3–3 suggests the differing types of knowledge needed to address issues within and across the categories of interest.

Figure 3-3: Required Intellectual Capital


Inter-disciplinary Subject Matter Experts (SMEs)
Disciplinary SMEs (economists, military planners, operators, analysts)
Computer Scientists
Systems Engineers
System-of-Systems Engineers
Lawyers
Governance Experts
Civil Liberties
Industry

For example, in the realm of cyberspace, there is a need for physicists, electrical engineers, computer scientists, systems engineers, and system-of-systems engineers. These professionals will play key roles in developing the hardware components (such as microprocessors and hard drives), software protocols and standards (for example, implementing Internet Protocol version 6 [IPv6]), applications and services, and the systems that exploit this hardware and software (command, control, and communications systems).

In the realm of cyberpower, subject matter experts who are qualified to deal with P/DIME issues are needed. This implies extensive reliance on micro- and macroeconomists and social scientists with training in such diverse fields as sociology, cultural anthropology, psychology, and demographics. Furthermore, in the area of military knowledge, participation by military planners, operators, and analysts is necessary.

In the realm of cyber strategy, interdisciplinary experts are required who are able to deal with the full range of political, military, economic, social, informational, and infrastructure (PMESII) issues associated with entities empowered by changes in cyberspace. In particular, analysts are needed who have had experience in addressing deterrence among these entities.

Finally, in the realm of institutional factors, the key skills needed are legal, governance, civil liberties, and industrial experience.

Cyber policy decisionmakers are expected to be among the main users of this intellectual capital. They will also need operations analysts to help orchestrate and harness this heterogeneous intellectual capital and futurists to help conceptualize possibilities that require unfettered imaginations.

Theoretical Perspectives

Three of the major objectives of a theory of cyber are to help explain, connect, and anticipate key aspects of the problem for the decisionmaker. Doing so will require the formulation of conceptual models for the various categories introduced above. In formulating these conceptual models, it is useful to recall the famous saying by the statistician George Box: "All models are wrong; some are useful."[12] The challenge for the theorist is to suggest and apply appropriate models that are useful for the decisionmaker and to delineate the range of their utility.

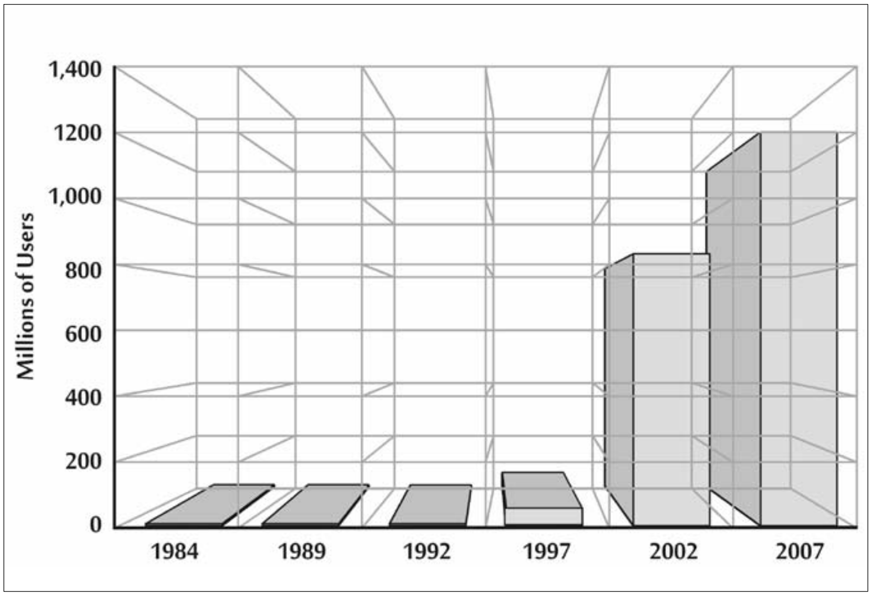
This section systematically introduces a variety of models that are germane to the many policy questions associated with cyber issues. Structurally, a bottom-up approach is pursued and cyberspace, cyberpower, cyber strategy, and institutional factors are addressed.[13] For each area, we introduce a variety of models and frameworks that help the decisionmaker explain key observables and conceptualize the issues of interest. This is followed by an articulation of rules of thumb and principles that highlight major issues of interest.

Theoretical Aspects of Cyberspace[14]

This section briefly explains key cyberspace trends in five main areas: growth in users, features of major components (such as microprocessors and hard drives), architectural features (for example, Internet protocols), and military systems of systems.

Growth in users. The most remarkable aspect of the Internet has been the exponential growth in users worldwide. Figure 3–4 illustrates that growth over a 33-year period. User population increased from approximately 1 million users in 1992 to 1.2 billion users in 2007.

Figure 3-4: Number of Internet Users



It is projected that the Internet will have 2 billion users by 2010. This number is projected to grow substantially if the One Laptop Per Child project, which aims to get millions of low-cost laptops to children in underdeveloped countries, is brought to fruition.

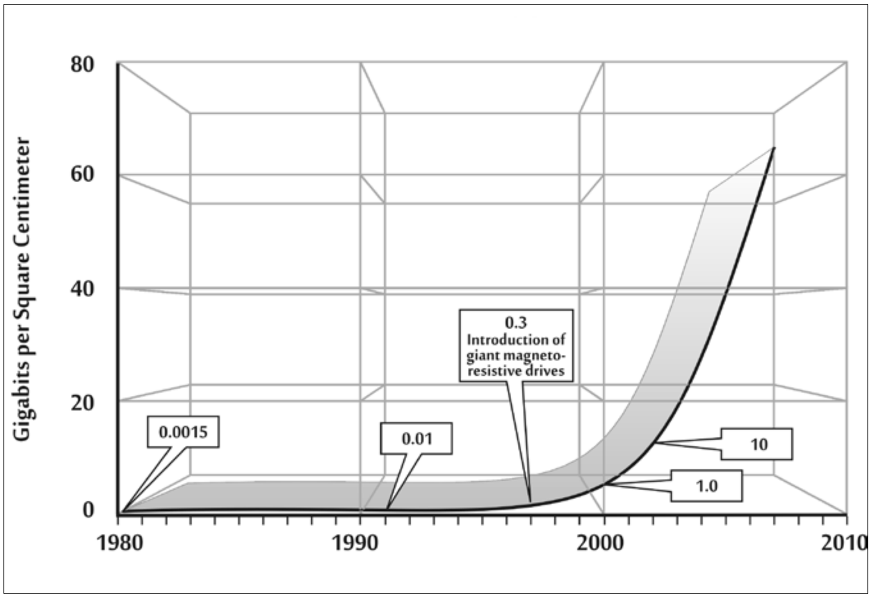
The SSG report depicted this growth from another perspective. The researchers set 50 million users as a benchmark for penetration of a mass medium. That level was achieved by radio in 38 years, television in 13 years, and the Internet in 6 years (beginning with the introduction of the World Wide Web).

Another key element of cyberspace is cellular telephony. As a point of reference, the first cell phone call was made in 1973. It is estimated that today, 35 years later, approximately 3.3 billion cell phones are in use worldwide.

Components. From a theoretical perspective, the physics of the hardware that supports cyberspace has a significant impact on its performance. This is particularly manifested in the design of microprocessors and hard drives.

Microprocessors. Clock cycles of modern microprocessors exceed 2 gigahertz (GHz). Therefore, under ideal circumstances, electrons can move a maximum of 0.15 meters in a single processor clock cycle, nearing the size of the chip itself. With clock cycles going even higher,[15] electronic signals cannot propagate across a chip within one clock cycle, meaning elements of the chip cannot communicate with other elements on its other side. Thus, this limitation maximizes the effective size of a single integrated microprocessor running at high clock speeds. Addressing this limitation is one of the reasons that various processor manufacturers have moved chip architectures toward multicore processors, where multiple, semi-independent processors are etched on a single chip. Current chips have two or four cores, with substantial increases expected for the future.

Figure 3-5 Hard Drive Capacity



Hard drives. Figure 3–5 depicts computer hard drive storage capability (in gigabits per square centimeter) over the last 25 years. It is notable that the improvement in memory was negligible for the first 20 until IBM engineers applied the phenomenon of giant magnetoresistance.[16] Currently, improvements in memory are manifesting exponential improvement, making it feasible to create portable devices, such as iPods, with extremely high storage capability. These two examples suggest that a careful technology assessment is needed to determine if and when bottlenecks in technology that limit current performance will be overcome.

Architectural features. Figure 3–6 schematically depicts the architecture of the existing Internet. The key innovations of this architecture revolve around the protocols and standards instantiated in the transmission control protocol/ Internet protocol (TCP/IP) stack and the use of a router to transmit packets from the sender to the user.

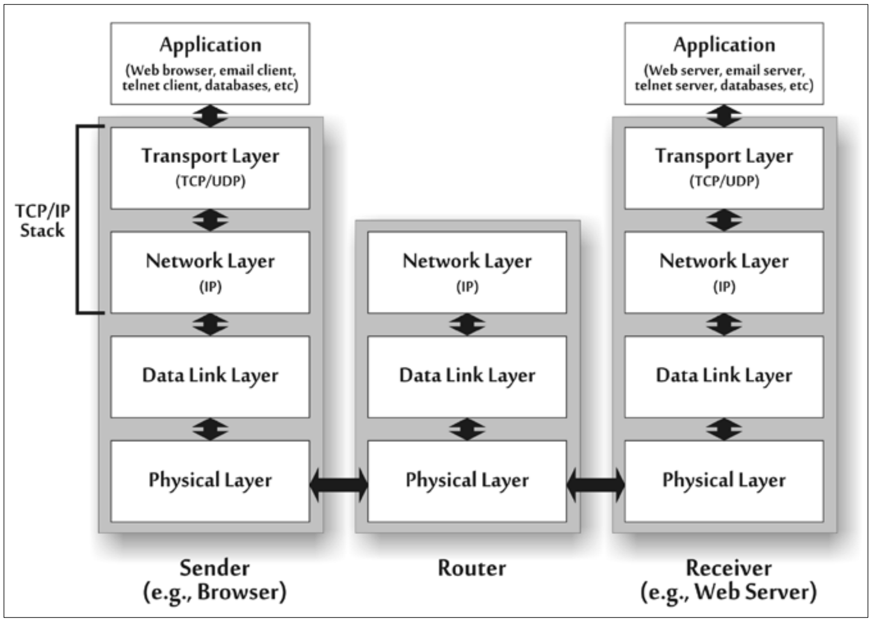
Originally, this architecture was devised by a group for whom security was a secondary issue. Thus, the primary emphasis was to implement an architecture that facilitated the interoperability among heterogeneous networks. In addition, a decision was made to implement IP addresses that consisted of 32 bits (or approximately 4 billion addresses).

These two decisions have led to several major limitations in the current architecture. In light of the security shortfalls in the existing architecture, there is interest in alternative architectures designed around different priorities (for example, highest priority being security, second priority being connectivity among highly mobile users). Consistent with those revised priorities, new architectural efforts are under way at the National Science Foundation and Defense Advanced Research Projects Agency (DARPA).

Second, the constraint on IP addresses (as well as concern about enhanced security and mobility) has led to the adoption of IPv6. Since it allocates 128 bits to IP addresses, it will give rise to an extraordinarily large number of IP addresses.[17]

Both of these innovations pose a problem to the cyberspace community: how can one transition from the current architecture to an alternative architecture efficiently and effectively without creating new security vulnerabilities? This is an ongoing challenge that the computer science community must confront over the next decade.

Figure 3-6: Protocol Layering and Routing Packets across a Network



Military systems-of-systems. The military community has embraced the underlying computer science principles associated with the Internet, although it has enhanced security for classified systems by developing airgapped networks (such as the Secret Internet Protocol Router Network and the Joint Worldwide Intelligence Communications System). Figure 3–7 provides an illustration of that implementation for the notional global information grid (GIG).

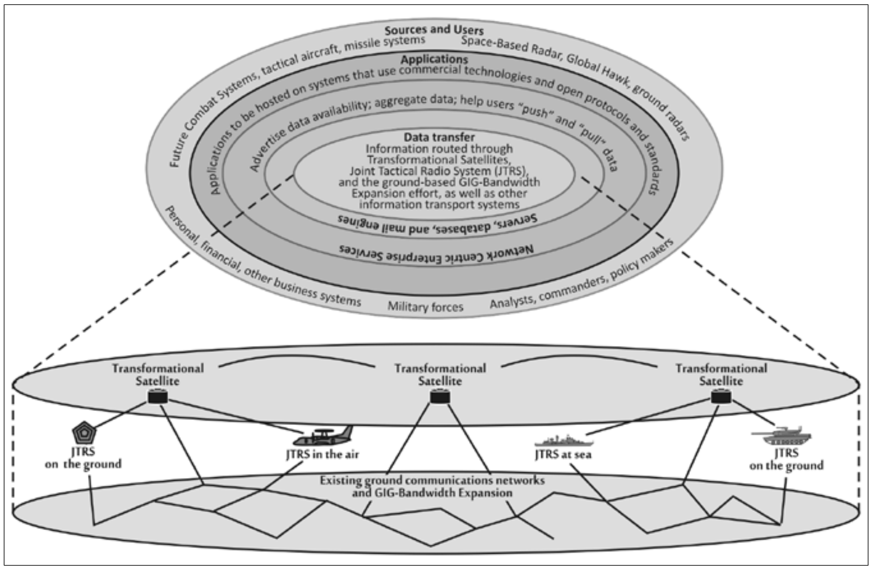
There are several distinctive aspects of the evolving GIG. First, for the transport layer, the plan is to employ a heterogeneous mix of satellite (for example, transformational satellites), airborne (selected joint tactical radio systems), and surface (fiber optic) telecommunications media. As a side note, the military is finding it difficult to develop many of these elements within acceptable levels of performance, schedule, and cost.

Second, there is interest in employing a service-oriented architecture to provide loose coupling among key systems. Third, the military has developed communities of interest to address the challenges associated with the data that will flow through the systems (for instance, specify metadata; deal with issues of pedigree). The military wishes to transition from the principle of "need to know" to "need to share." Finally, it hopes to assimilate the Services' visions of future systems into the GIG (for example, the Army LandWarNet, Navy ForceNet, and Air Force Command and Control [C^2] Constellation). Achieving this vision will require the concerted efforts of the military's system-of-systems engineers.[18]

Cyberspace rules of thumb and principles. To help explain the various trends in cyberspace, one can provide several rules of thumb and straw man principles. Several broad guidelines employed in the community are incorrectly characterized as laws. For example, Moore's "law" indicates that the number of transistors on a chip approximately doubles every 18 months.[19] This growth has contributed to the production of smaller, less expensive devices that have enhanced computational power. Although this trend is generally representative of past behavior, there is concern that it may be extremely difficult to sustain in the indefinite future without a fundamental, expensive change in the underlying technology (such as transition to nanotechnology). Second, as noted in figure 3–5, recent breakthroughs in physics have put the growth in hard drive capacity on an exponential versus a conservative linear curve. Ultimately, this curve will reach a level of saturation (an "S-curve") that is representative of a mature technology. Lastly, the current limitation in IP addresses will be dramatically overcome once the transition to IPv6 is implemented.

Several straw man cyberspace principles can be articulated. First, the offense has the advantage, in part because of the target-rich environment that an adversary faces.

Figure 3-7: A Framework to Characterize the Global Information Grid


Sources and Users
Future Combat Systems, tactical aircraft, missile systems
Space-Based Radar, Global Hawk, ground radars
Applications
Applications to be hosted on systems that use commercial technologies and open protocols and standards
Advertise data availability; aggregate data; help users "push" and "pull" data
Data transfer
Information routed through Transformational Satellites, Joint Tactical Radio System (JTRS), and the ground-based GIG-Bandwidth Expansion effort, as well as other information transport systems
Servers, databases, and mail engines
Network Centric Enterprise Services
Personal, financial, other business systems
Military forces
Analysts, commanders, policy makers
Transformational Satellite
Transformational Satellite
Transformational Satellite
JTRS on the ground
JTRS in the air
JTRS at sea
JTRS on the ground
Existing ground communications networks and GIG-Bandwidth Expansion

This situation makes it difficult for defense to prioritize and defend selected targets. In addition, the existing architecture makes it challenging to attribute an attack if an adversary seeks anonymity. If cyberspace is to be more resistant to attack, it will require a new architecture that has "designed-in" security. However, it will be a challenge to transition effectively and efficiently from the current legacy system to a more secure objective system.

Theoretical Aspects of Cyberpower

This section briefly explains key trends in the military and information dimensions of cyberpower.[20] It focuses on changes in the principles of war, environmental theories of power and risk, net-centric operations (NCO), and the mission-oriented approach to influence operations.

Principles of war. Historically, military intellectuals have developed a set of principles of war to support the planning and execution of operations. These principles have evolved over hundreds of years through the writings of key military analysts.[21] Although the precise set of elements in these principles of war is variable, most lists would include unity of command, objective, offensive, mass, maneuver, economy of force, security, surprise, and simplicity. In general, a contemporary general officer would regard these factors as essential dimensions of a plan and subsequent operations. Thus, he would test his straw man plan by thinking deeply about each of these principles.

It is argued that a revised set of modernized principles of war is appropriate for 21st-century operations. One of the participants in this debate has updated the list to include perceived worthiness, informed insight, durability, engagement dominance, unity of effort, adaptability, and culminating power.[22] As illustrated in table 3–1, most of these revised principles represent combinations of and linkages to the classical set of principles of war.

This preliminary theory of cyberspace has not focused extensively on the issue of the appropriate principles of warfare in an information age. However, it does acknowledge that the impact of changes in cyberspace may warrant a basic reassessment of the appropriate principles of contemporary warfare. Thus, it identifies this area as one worthy of continued research.

Table 3-1: Evolving Principles of War

Modernized	Relationship to Traditional Principles
Perceived worthiness	Morale: what makes it worthwhile to risk one's life in combat?
Informed insight	Sensemaking, cognition, surprise
Strategic anchoring	Concentration on and prominence of the offensive
Durability	Incorporate security into plan; depends on logistics
Engagement dominance	Incorporates and simplifies maneuver; impose/ oppose surprise
Unity of effect	Draws on unity of command; reinterprets economy of force, mass, maneuver
Adaptability	Presupposes flexibility but does not mandate simplicity
Culminating power	Power needed to attain satisfactory closure at a given level of conflict

Source: Charles Dunlap, "Neo-Strategicon: Modernized Principles of War for the 21st Century," *Military Review* (March-April 2006).

Environmental theories of warfare. In the discussions that led to this study, the observation was made that the naval theories of Alfred Thayer Mahan played a major role in shaping U.S. perspectives and strategies on naval power. It was suggested that cyberpower needed a comparable perspective to shape its strategy in cyberspace. Consistent with that interest, this study reevaluated the various environmental theories of power. These included analyses of land power,[23] naval power,[24] airpower,[25] and spacepower.[26] Based on these analyses, four common features of environmental power theories were identified: technological advances, speed and scope of operations, control of key features, and national mobilization.

Consistent with each of these features, the following implications were drawn for a theory of cyberpower. With respect to technological advances, it was observed that dependency on cyberspace has given rise to new strategic vulnerabilities. This vulnerability has been dramatized by the specter of a "cyber Pearl Harbor" and the realization that the existing cyberspace is vulnerable to a variety of adversary attacks (for example, denial-of-service attacks, exfiltration of sensitive but unclassified information, or potential corruption of sensitive data). In addition, due to the diffusion of low-cost cyberspace technology, the power of nonstate actors (such as individuals, terrorists, transnational criminals, and corporations) has been greatly enhanced (see below).

Improvements in cyberspace have also enhanced the speed and scope of operations. These upgrades are manifested in the speed at which global operations can be conducted (for example, the ability to successfully engage time-sensitive targets anywhere in the world). In addition, they have led to improvements in the ability to automate command and control, dramatically decreasing the classic observe-orient-decide-act loop process.

In the environmental theories of power, emphasis was placed on controlling key features. For example, in naval theories, this entailed the domination of chokepoints (such as the Straits of Malacca), while in spacepower theory, there was interest in controlling geosynchronous orbit locations. In the case of cyberspace, the key features are manmade. Thus, for example, there is interest in defending “cyber hotels” where information and communications technology systems are concentrated. In addition, while the chokepoints in the physical world tend to be immutable, they may change relatively rapidly in cyberspace (for example, the location of extensive server farms).

Finally, national mobilization is a vital measure of cyberpower. To ensure that it is available when needed, the United States must assure access to a cadre of cyberspace professionals. This argues for reexamining career progression for cyberspace professionals in the military Services. In addition, it is important to establish links to the private sector where the bulk of cyberspace professionals reside. This suggests that a reservoir of Reservists should be established to provide access to this intellectual capital in the event of national need.

It is argued in this book that the U.S. Government has tended to focus on the opportunities offered by changes in cyberspace rather than the risks assumed. To summarize that dichotomy, table 3–2 identifies the opportunities and risks associated with military activities at the strategic, operational, and tactical levels.

Table 3-2: Military Opportunities and Risks in Cyberspace

Level	Opportunities	Risks
Strategic	Net-centric warfare– enabled New centers of gravity opportunities (for example, deterrence, virtual conflict)	Loss of technical advantage Rapidly changing operating environment Military dependence on key systems (for example, the global information grid)
Operational	Phasing of operations Enhanced force structure mix (for example, cheaper, more precise)	Loss of advantage in operational pace
Tactical	Discover and track adversaries using cyberspace	New front for adversaries to build resources

The risks at the strategic level include loss of technical advantage (due to the diffusion of cyberspace technology), potential rapid change in the operating environment (such as the possibility that nations such as China could leapfrog the United States by transitioning rapidly to IPv6), and the vulnerabilities associated with military dependence on key systems (for example, the GIG). At the operational level, the diffusion of cyberspace technology could result in the U.S. loss of advantage in operational pace. Finally, at the tactical level, advances in cyberspace could generate a new front for adversaries to build resources. These observations suggest that the U.S. Government might be assuming significant, unknown risks by failing to take a balanced perspective of key cyberspace trends. It also implies the need to undertake more extensive risk assessments to understand the potential downside of key dependencies.

To begin to deal with these risks, steps should be taken at the strategic, operational, and programmatic levels. At the strategic level, actions should be taken to ensure the resilience of supporting critical infrastructures, such as electric power generation and transmission. At the operational level, it is vital to plan for operations against an adversary that is highly capable of cyberwarfare. This should include the creation of an opposing force that would be employed extensively in experiments and exercises. Finally, at the programmatic level, emphasis should be placed on addressing cyberspace implications in the development process. This should include placing higher priority on the challenges of information assurance. Overall, an improved analytic capability is required to address each of these issues.

Net-centric operations. As one aspect of the analytic capability, work is needed to enhance and apply the existing conceptual framework for NCO. As illustrated in figure 3–8, the NCO process involves consideration of the interactions among the physical, information, cognitive, and social domains.[27] There is a need to develop better analytic tools for all aspects of this process, particularly in the cognitive and social domains. One potential source of intellectual capital is the forthcoming initiative by the Director of Defense Research and Engineering in the Office of the Secretary of Defense (OSD) to improve human, social, and cultural behavior models and simulations. This issue is discussed later in this chapter.

Mission-oriented approach to influence operations. In the area of influence operations, a straw man framework has been developed to help the community plan for and implement influence operations (see figure 3–9). This framework represents an extension of the mission-oriented approach developed and applied to a variety of C^2 issues in the 1980s.[28]

This approach begins with the articulation of the nature of the problem of interest. It then poses a sequence of questions. First, what is the operational objective of the mission? A reasonable objective may be to establish a trust relationship with the indigenous population (versus “winning hearts and minds”). Second, how should this operational objective be accomplished? Again, a decision was made to work with surrogate audiences, including the local media, religious leaders, educational leaders, political leaders, and tribal leaders, in order to reach the undecided population. Organizations and processes were established to reach out to those audiences effectively. At this point, one can characterize the existing doctrine, organization, training, materiel, leadership and education, personnel, and facilities (DOTMLPF) activities and compare them to the operational needs. This will give rise to DOTMLPF shortfalls and the articulation of options to mitigate them. It may also prompt the operator to reevaluate the operational goals and the operational activities to support them.

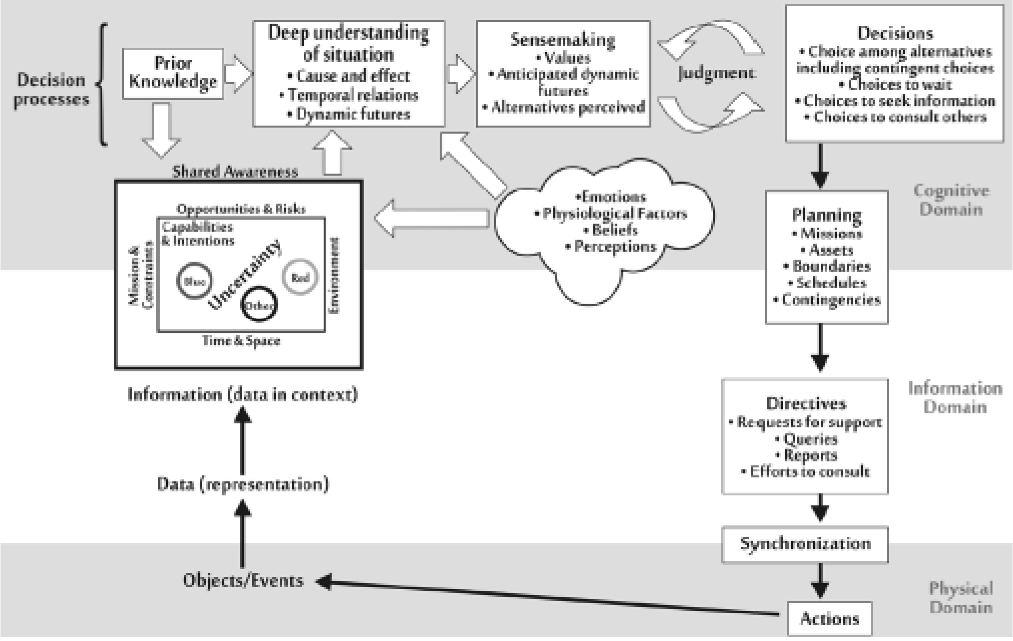
This process should be refined and applied to a broader variety of strategic, operational, and tactical influence operations. In particular, it can be used to explore the utility of employing new options in cyberspace (media such as the Internet and social networks) to improve future influence operations.

Cyberpower rules of thumb and principles. One of the so-called laws of cyber-power was formulated by Bob Metcalfe.[29] He postulated that the value of a telecommunications network is proportional to the square of the number of users of the system (n^2). However, there is no empirical data to support this law. A recent article suggested that the value is closer to nlog(n).[30]

From an analytical perspective, the former Office of Force Transformation has supported a number of studies to relate the impact of net-centricity on enhancements in cyberpower (primarily in the military domain). These ongoing studies have demonstrated that net-centricity can have a substantial impact on mission effectiveness for selected mission areas. For example, the use of jam-resistant Link 16 radios by airborne interceptors in M-on-N combat can enhance air-to-air loss exchange ratios by approximately 2.5.[31] However, the complexity of modern conflict is such that it is difficult to assess the effect of net-centricity on complex missions (for example, air-land operations or stability and reconstruction operations). This suggests that additional experiments will be needed to assess the quantitative value of net-centricity for complex missions, in which better control is exercised over potentially confounding variables.

Theoretical Aspects of Cyber Strategy[32]

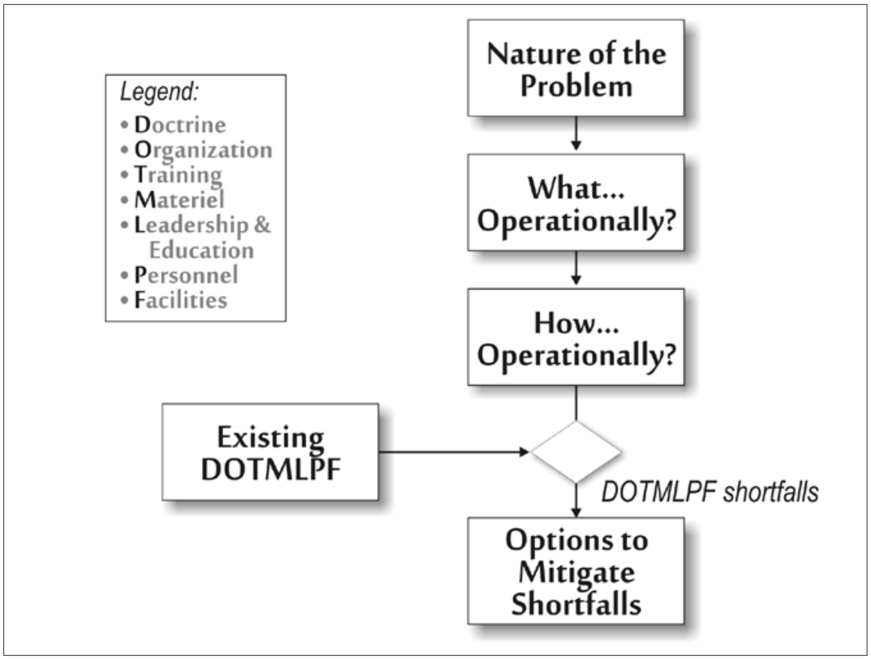
Figure 3-8: Conceptual Framework for Netcentric Operations



The NDU team has identified an extensive list of entities that are being empowered by changes in cyberspace that includes individuals, "hacktivists,"[33] nongovernmental organizations (such as the Red Cross), terrorists, transnational criminals, corporations, nation-states, and international governmental organizations (such as the United Nations).

For the purposes of this study, attention has been focused on a subset of these entities that includes terrorists, transnational criminals, and certain nation- states (China and Russia). From a U.S. Government national security perspective, two issues stand out. First, is it feasible to achieve tailored cyber deterrence? Second, what steps should be taken to deal with cyber espionage?

Figure 3-9 Straw Man Framework for Analyzing Influence Operations



Terrorist use of cyberspace. Terrorists are empowered substantially by changes in cyberspace. With the loss of physical sanctuary in key areas (such as Afghanistan), they have been turning to the sanctuary of cyberspace to perform important interrelated functions that include recruiting malleable candidates, raising resources to support operations, planning operations (employing such open-source tools as Google Earth), commanding and controlling operations, conducting influence operations (for example, disseminating their perspectives of operations in Iraq to sympathetic and uncommitted audiences), and educating and training supporters on a variety of subjects (such as interpreting the Koran and building and deploying improvised explosive devices).

Terrorists have found cyberspace an attractive milieu for several reasons. First, the cost of entry is low. One can acquire the latest cyber technology for hundreds to thousands of dollars and exploit key open-source software. In addition, terrorists can take full advantage of the extraordinary sums that have been invested by the commercial sector in cyber infrastructure (including communications and navigation systems). Second, cyberspace provides rapid, worldwide reach. Thus, terrorists are able to transcend the limited geographic reach of their prior physical sanctuary and perform the key functions cited above. Third, it has been posited that the next generation of terrorists is being radicalized by online interactions.[34] Finally, there is concern that terrorists are developing linkages with transnational criminals who are able to provide terrorists with cyber knowledge while profiting from the relationship.

Recent reports suggest strategies for the U.S. Government to counter the terrorists' use of cyberspace. For example, a special report on Internet-facilitated radicalization formulated five recommendations to address the cyber threat posed by terrorists:

- craft a compelling counternarrative for worldwide delivery in multimedia, at and by the grassroots level
- foster intra- and cross-cultural dialogue and understanding to strengthen the ties that

bind communities at the local, national, and international levels

- recognize and address the need for additional behavioral science research into the process of radicalization both online and offline
- deny or disrupt extremist access to, and extremist efforts through, the Internet via legal and technical means and covert action, where appropriate
- remedy and resource capability gaps in government.[35]

The many actions associated with these recommendations are summarized in table 3–3. From the perspective of this chapter, some of the more interesting actions involve developing a strategic communication plan based on a compelling narrative, implementing an innovative program on behavior science research, and addressing U.S. Government shortfalls in knowledge of culture and language.

Nation-state use of cyberspace. From a nation-state perspective, different combinations of levers of power are employed to generate desired effects. From a theoretical perspective, these nations formulate their strategy through a mix of P/DIME activities. The effects of these activities are manifested in the areas of PMESII. Tools are being created to explore how alternative P/DIME activities can give rise to differing PMESII effects.

The United States. Using the P/DIME–PMESII paradigm, one can begin to characterize how cyber changes have empowered the United States. In the political dimension, changes in cyberspace have encouraged democratic participation by the population. The Internet has provided a forum for individuals to articulate their views through blogs and contributions to wikis. In addition, political candidates are finding the Internet to be a useful vehicle for raising resources from grassroots supporters. Furthermore, Internet sites such as YouTube have enhanced the accountability of candidates.

Table 3-3: Options to Counter Terrorist Use of Cyberspace

Recommendations	Proposed Actions
Craft compelling multimedia counternarrative for worldwide delivery	Challenge extremist doctrine Offer compelling narrative Use graphics Deliver message through authentic sources Amplify, augment grass-roots nonextremist voices
Foster intra- and cross-cultural dialogue at all levels	Address perceptions, realities of American Muslim alienation, marginalization Enhance civic engagement Increase people-to-people exchanges Deal appropriately with the media
Address need for behavioral science research	Deepen understanding of radicalization process Apply social networking theory
Deny or disrupt extremist use of Internet	Employ legal means Undermine trust that binds adversary networks Exploit convergence of human intelligence and cyberspace
Address capability gaps in U.S. Government	Address cultural and linguistic deficiencies Reclaim high ground Develop strategic communications plan Expand community policing programs

In the military dimension, the concept of NCO has enhanced effectiveness in selected operational domains (for example, air-to-air combat). Efforts are still required to quantify the military benefits that are achievable for more complex military operations (such as air-land maneuver).

Economically, the commercial sector has seen dramatic improvements in industrial productivity (for example, Boeing's use of computer-aided design tools to support the development of the 777 and 787 aircraft). These cyber-based advancements are giving rise to considerable improvements in responsiveness by reducing time to market and cost reductions (for example, by outsourcing “backroom operations” to other nations).

The development of cyberspace has increased social interactions in several ways. Tens of millions of users participate in social networking sites such as MySpace and FaceBook. In addition, millions of users worldwide participate in virtual reality environments such as Second Life. In fact, terrorist organizations are rumored to be using virtual reality environments to explore prototypical operations.

In the information dimension, the Internet has increased dissemination of information worldwide. The argument can be made that the U.S. dominant position in entertainment and advertising provides a strong forum for promoting soft power.[36]

Finally, many critical infrastructures have been using the Internet to facilitate more efficient and effective operations. However, this constitutes a double-edged sword because of the potential vulnerability of supervisory control and data acquisition systems.

Overall, it must be stressed that empowerment is more than the sum of the individual PMESII factors.

Near-peer use of cyberspace. Nations such as China and Russia use a different vocabulary in discussing cyberspace and cyberpower. For example, Chinese writings on the subject focus on stratagems, objective and subjective reality, and dialectic (that is, “reasoning that juxtaposes opposed or contradictory ideas and seeks to resolve conflict”).

Two key aspects of the Chinese view of the revolution in military affairs are particularly germane: “War with the objective of expanding territory has basically withdrawn from the stage of history, and even war with the objective of fighting for natural resources is now giving way to war with the objective of controlling the flow of financial capital.” Furthermore, “If we go our own path to develop military theory, weapons, and equipment, we will develop something never seen before in places that no one has ever thought of before; others will be unable to anticipate or resist our ‘self-accommodating systems.’”

As an illustration of “self-accommodating systems” against a superior foe, three ways are cited for making a cat eat a hot pepper: “Stuff it down his throat, put it in cheese and make him swallow it, or grind it up and spread it on his back. The latter method makes the cat lick itself and receive the satisfaction of cleaning up. The cat is oblivious to the end goal. This is strategy.”

Cyber deterrence. A vision for tailored deterrence was articulated in the 2006 QDR. Consistent with that vision, a recent strategy paper identified three aspects of tailoring:

- tailoring to specific actors and specific situations. This recognizes that tailored deterrence is “context specific and culturally sensitive.”
- tailoring capabilities. One dimension of this factor deals with the associated resource implications.
- tailoring communications. This relates to the kinds of messages that the United States would send in words or actions to deter specific actors in peacetime and crisis situations.[37]

Table 3-4: The Calculus of Tailored Deterrence

- What are the nation's or group's values and priorities? How are they affected by its history and strategic culture?
- What are their objectives in the particular situation?
- What factors are likely to influence their decisionmaking?
- Who makes decisions, how does the leadership think, what is their worldview and experience with and view of the United States?
- How do they calculate risks and gains?
- What do they believe their stakes to be in particular situations?
- How risktaking is the leadership?
- How much latitude does the leadership have (to provoke, conciliate, and so forth)?
- What are their alternative courses of action?
- What do they believe the costs and benefits of constraints to be?
- What do they perceive America's answers to these questions to be?

Source: M. Elaine Bunn, *Can Deterrence Be Tailored?* Strategic Forum 225 (Washington, DC: National Defense University Press, January 2007).

To deal with the various dimensions of tailored deterrence, a variety of questions must be addressed that include the social, cultural, and historical aspects of the adversary, including his calculation of risks and gains. As noted in table 3–4, a critical element of this calculus deals with the adversary's perception of the U.S. position on these key questions.

There is a debate within the analytic community as to whether tailored deterrence is a viable concept for the full spectrum of U.S. adversaries.[xxxviii] That issue represents an important element of the research agenda for the community. However, the NDU study team believes that the full set of P/DIME options should be considered in developing a course of action to respond to a cyber attack.[xxxix]

Cyber strategy rules of thumb and principles. Three key insights emerged during the course of this study. First, low-end users (such as individuals, hacktivists, terrorists, and transnational criminals) have enhanced their power considerably through recent cyberspace trends. A tailored deterrence strategy will be needed to keep these entities in check.

Second, potential near-peer adversaries are aggressively exploring options to exploit attributes of cyberspace. In the near term, this exploitation is being manifested through acts of espionage that have resulted in the exfiltration of massive amounts of sensitive governmental and industrial data. In the longer term, the United States must be prepared to deal with unique "cyber stratagems" that reflect the particular cultural and military history of important nations such as China and Russia.

To deal with the emerging cyber threat, the United States must conduct experiments and exercises that feature a creative and aggressive cyber opposing force. It would be naïve and dangerous to assume that future adversaries will not seek to negate the benefits that the United States hopes to achieve through net-centric warfare.

Theoretical Aspects of Institutional Factors

This section focuses on two critical institutional factors: governance of cyberspace and the legal dimensions of the problem. The section concludes by identifying key institutional issues and principles.[xl]

Table 3-5: Governance of Cyberspace

Function Group	Domain names	Int’l domain names	Core Internet functions	Telecomms standards	World Wide Web standards	Product standards	Development	Cyber security**
Internet Corporation for Assigned Names and Numbers (ICAAN)	X	X						X
Internet Society*			X					X
International Telecommunication Union (ITU)		X		X		X		
Organization for Economic Co-operation and Development (OECD)							X	X
Council of Europe								X
European Union (EU)							X	X
International Organization for Standardization						X		X
International Electrotechnical Commission						X		X
Institute of Electrical and Electronics Engineers						X		
World Wide Web Consortium					X			
United Nations (UN)							X	

*Internet Society and related organizations (Internet Engineering Task Force, Internet Engineering Steering Group, Internet Architecture Board)

** As well as national governments

Governance. Table 3–5 characterizes key governance functions in cyberspace and the organizations that participate in them. The mechanisms for governance of the Internet are exceedingly complex. Organizational activities often overlap or fit end-to-end, requiring the expenditure of considerable resources in multiple forums to achieve objectives. Consequently, a core set of participants (generally in the private sector) is involved in several of these organizations.

In an effort to evaluate the performance of Internet governance, the following criteria are introduced: open, democratic, transparent, dynamic, adaptable, accountable, efficient, and effective. When measured against these criteria, recent Internet governance has performed remarkably well.

However, in the future, the U.S. Government will be challenged to alter its position on

Internet governance. Preliminary views on this subject are being articulated at the ongoing Internet Governance Forums (IGFs). In fact, a recent white paper on the subject observed:

> Internet Governance is an isolating and abstract term that suggests a nexus with an official government entity. The term also implies a role for the U.S. Congress in Internet decision-making. It is a misnomer because there is no true governance of the Internet; only a series of agreements between a distributed and loosely connected group of organizations and influencers. A more fitting term may be "Internet Influence," or for long-term strategy purposes, "Internet Evolution."[xli]

Cyber law. One of the most challenging legal issues confronting the cyber community is whether cyber attack is an act of war. Legalistically, the answer is often presented as one of three possible outcomes: it is not a use of force under United Nations (UN) Article 2(4); it is arguably a use of force or not; it is a use of force under UN Article 2(4).

Several frameworks are being considered by the legal community to address this issue. Michael Schmitt has formulated a framework that defines and addresses seven key factors: severity, immediacy, directness, invasiveness, measurability, presumptive legitimacy, and responsibility. Once one has assessed each of those factors, one should employ multi-attribute utility theory to weight each of them and come to a determination. As an example, the application of this framework in chapter 22 of this volume, "International Law and Information Operations," implies that the recent attack against Estonia was not a use of force under Article 2(4). An associated challenge is to formulate responses to that attack consistent with the legal tenet of proportional response.

Overall, the area of cyber law is in its infancy. Although there have been preliminary rulings on sharing of music, there are major issues on the questions of sovereignty, intellectual capital, and civil liberties. These issues will be areas for research for the foreseeable future.

Institutional principles. Based on the insights developed during the course of this study, four major straw man principles have emerged in the arena of institutional factors.

First, given the complexity of the governance mechanisms, one should seek influence over cyberspace versus governance. Second, the legal community has barely addressed the key issues that must be resolved in the cyber arena. For example, considerable research is needed to assess the following questions:

- What is an act of (cyber)war?
- What is the appropriate response to an act of (cyber)war?
- What is the appropriate way to treat intellectual property in the digital age?
- How can nations resolve differences in sovereign laws associated with cyber factors?

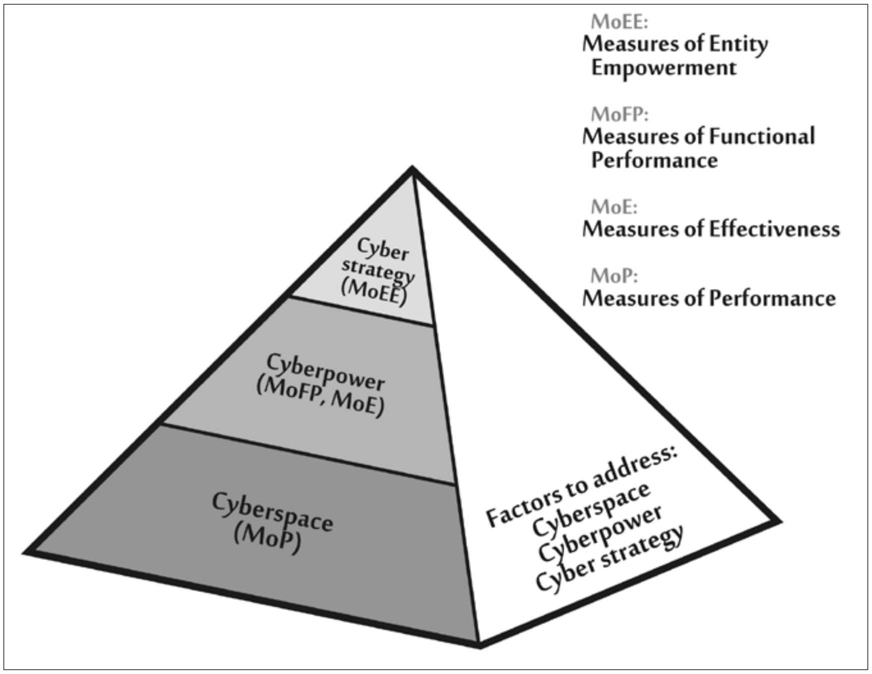
Third, there is a need for a framework and enhanced dialogue between champions of civil liberties and proponents of enhanced cyber security to establish an adequate balance. Finally, guidance and procedures are required to address the issue of sharing cyber information between the U.S. Government and industry. This approach should be based on the concept of risk management.

Connections

At the beginning of this chapter, it was noted that one reason for a theory was the need to connect diverse elements of a body of knowledge. In general, the community is focusing on the issue of connecting the knowledge within a stratum of the pyramid. Even though this is challenging, it generally involves communicating among individuals with a common background and lexicon.

It is far more difficult to have individuals connect across the different strata of the pyramid. This effort requires individuals from different disciplines to work effectively together. Doing so requires a holistic perspective on the measures of merit for cyber issues. Figure 3–10 suggests a potential deconstruction of the measures of merit associated with the cyber problem. It identifies four linked sets of measures: performance, functional performance, effectiveness, and measures of entity empowerment (MOEEs). Since this field of endeavor is still in its infancy, the material is meant to be illustrative and not exhaustive.

Figure 3-10: Measures of Merit



Measures of performance are needed to characterize the vital computer science and electrical engineering dimensions of the problem. A key measure is the amount of bandwidth available to representative users of cyberspace. As the bandwidth increases to the megahertz/second range, the user is able to access advanced features such as imagery and video products. A second measure is connectivity. For circumstances in which the cyber-infrastructure is fixed, a useful measure is the percent of people in a country who have access to the Internet. However, in many military operations, the cyber-infrastructure and the users are mobile. Under those circumstances, a more useful measure is the performance of mobile ad hoc network users (for example, their ability to stay connected). Third, one can introduce measures of the "noise" that characterizes the cyber-infrastructure. For example, the extent to which the quality of the Internet is degraded can be characterized by the unwanted email that it carries, which can subsume a considerable subset of the network's capacity. In early 2007, approximately 90 percent of the traffic on the Internet was estimated to have been spam.[xlii]

In addition, the integrity of the information is further compromised by phishing exploits in which criminal elements seek to employ the Internet to perpetrate economic scams. Finally, measures of performance can be introduced to characterize resistance to adversary actions, including denial-of-service attacks, propagation of viruses or worms, and illicit intrusion into systems.

It is useful to introduce measures of functional performance that characterize how successfully selected entities are able to perform key functions, taking advantage of cyberspace. In the case of the U.S. military, the concept of net- centricity is to employ advances in cyberspace to perform essential functions, which include the ability to enhance the performance of increasing levels of information fusion (for example, at level one, the ability to generate a timely, complete, accurate picture of blue forces). Similarly, a basic tenet of net-centricity is to propagate commander's intent so that the participants in the operation can synchronize and self-synchronize their actions.

Measures of effectiveness are needed to characterize how successful entities can be in their key missions, taking advantage of cyberspace. In the context of major combat operations, measures of effectiveness are required to characterize the ability to exploit cyberspace in multiple dimensions. At one extreme, enhancements in cyberspace have the potential to reduce the time to conduct a campaign and the casualties associated with the campaign. At the other extreme, enhancements in cyberspace may substantially enhance blue force loss exchange ratios and the amount of ground gained and controlled.

From the perspective of cyber strategy, there is interest in characterizing the extent to which enhancements in cyberspace can empower key entities. In the case of nation-states, potential measures of entity empowerment might include selected PMESII variables. As an example, it might address the ability to leverage cyberspace to influence a population, shape a nation at strategic crossroads, and deter, persuade, and coerce an adversary.

Table 3–6 suggests some candidate measures of merit that may be employed in future analyses of cyber issues.

Anticipation

From the perspective of the decisionmaker, the primary challenge is to anticipate what will occur next in the cyber domain and to formulate coherent policy to cope with those developments. To begin to address that challenge, this section deals with four aspects of anticipation. First, it identifies key trends expected to characterize cyberspace. Second, it identifies the research activities that should be conducted to address those trends. Third, it briefly identifies the major policy issues that decisionmakers will need to address. Finally, it discusses the assessment needs that must be addressed to support the formulation and analysis of policy options.

Cyber Trends

To anticipate key changes in cyberspace, various chapters of this book have identified several key trends. However, it is difficult to provide quantitative estimates as to how rapidly these trends will be manifested. Thus, the following should be regarded as a partial, qualitative list of some of the most significant potential changes.

Table 3-6: Selected Measures of Merit

Measures	Representative Measures
Cyberstrategy—entity empowerment	Political reforms (for example, participation in democratic elections) Military efforts to enhance security (for example, reduction in number, severity of insurgent, terrorist attacks) Economic reforms (for example, reconstruction projects completed) Social reforms (for example, reconciliation of warring parties) Information (for example, gaining trust of host nation population) Infrastructure (for example, improvement in delivery of electric power, clean water)
Effectiveness (against targeted groups)	Informational • Media: number of positive/negative stories • Clerics: tone of mosque sermons Military: loss exchange rates
Functional performance	Informational • Time to create, validate, disseminate influence messages • Number of meetings held with surrogate groups
Performance	System performance (for example, latency, bandwidth, reliability) Resistance to adversary attack (for example, ability to withstand a denial-of-service attack)

First, there is an increased move to adoption of IP-based systems. As a consequence, one can anticipate a convergence of telephone, radio, television, and Internet. As one example, there is a dramatic use of voice over Internet protocol (with attendant security issues) in the area of telephony. Second is the emergence of sensor networks that feature an extremely large number of heterogeneous sensors. One manifestation is the netting of enormous numbers of video cameras in urban areas, raising issues in the civil liberties community. Third is an inexorable trend toward proliferation of broadband and wireless. An example of this trend was the plan to have citywide deployment of worldwide interoperability for microwave access. However, this trend suggests the difficulty in predicting when a trend becomes a reality. Nextel had made this objective the key to its strategy; however, the company has recently observed that the technology has not matured sufficiently to implement it in the near term.[xliii] Fourth is the enhancement of search capabilities, both for local systems and the entire Internet. A driver for this trend has been industrial competition to develop improved search engines (in part, to enhance advertising revenue). Fifth are extraordinary efforts to enhance human/machine connectivity. One example is the development of direct nerve and brain connections to computers or prostheses, arising from efforts to treat soldiers injured by improvised explosive devices in Iraq.[xliv] Finally, there are dramatic increases in user participation in information content. This trend is manifested through the proliferation of blogs, contributions to wikis, participation in social networks, and involvement in virtual reality environments.

Table 3-7: Areas Where Additional Theoretical Research is Required

Area	Research Areas
Cyberspace	Perform technology projections to identify key breakthroughs Develop techniques to protect essential data from exfiltration, corruption Formulate an objective network architecture that is more secure and identify options to transition to it
Cyberpower	Extend analyses to other levers of power (diplomatic, economic) Perform risk assessments to address cyber-dependence Quantify the blue-red information duel
Cyber strategy	Conduct research on “tailored deterrence” Explore options to address cyber espionage
Institutional factors	Perform research on cyber influence; legal frameworks; balance between security and civil liberties
Cyber assessment	Develop analytical methods, tools, data, and intellectual capital to assess cyber issues

Opportunities for Cyber Research

As an application of the emerging theory of cyber, table 3–7 identifies the major areas where cyber research should be pursued.

Cyberspace research. In the area of cyberspace, improved technology projections are needed to identify major breakthroughs (comparable to the discovery of giant magnetoresistance) that may substantially affect measures of performance for cyberspace. Second, malevolent actors inevitably will gain access to the

U.S. Government and defense industrial base cyberspace. This suggests that research is needed to protect the essential data in cyberspace from exfiltration or corruption. Finally, additional research is needed to formulate an objective architecture for cyberspace that is inherently more secure than the existing architecture. Consistent with that effort, there is a need to address the challenging issue of transitioning from the existing to the objective architecture.

Cyberpower research. Due to resource constraints, this preliminary assessment of cyber theory has not adequately addressed the political, diplomatic, and economic levers of power, and assessments should be completed for them. Second, existing assessments of the military lever of power have focused almost exclusively on the potential benefits that can accrue by creatively employing cyberspace. It is equally important to perform risk assessments to understand the potential downside of relying extensively on cyberspace. This includes conducting experiments and developing the methodology, tools, data, and intellectual capital required to perform military risk assessments. Similarly, it is important to conduct research into the potential benefits and risks associated with leveraging cyberspace developments for non-U.S. military capability (for example, North Atlantic Treaty Organization [NATO] allies that are pursuing network-enabled capabilities). Finally, in the area of information, additional research is needed to quantify the information duels likely to occur with potential adversaries.

Cyber strategy research. To deal with the challenges posed by the full array of entities empowered by enhancements in cyberspace, it is vital that information- enabled societies conduct research on tailored deterrence. This concept suggests that important alliances (such as NATO) must develop a holistic philosophy that understands the goals, culture, and risk calculus of each of the potential adversaries, develops and plans for capabilities to deter these adversaries, and devises a strategy to communicate these concepts to the potential adversaries.

Institutional factors research. Theoretical research is needed to address critical gaps in institutional knowledge in the areas of governance, legal issues, sharing of information, Internet regulation, and civil liberties.

First, in the area of governance, the U.S. Government must reassess the role of the Internet Corporation for Assigned Names and Numbers in the governance of the Internet. In the future, the United States clearly must be more adroit in the area of cyber influence versus governance. This will require a thorough reexamination of all the institutional bodies that affect cyber governance and the development of a Government strategy to interact with them.

Second, cyber legal issues are in their infancy. The current situation is non-homogeneous, with inconsistent laws in various sovereign nations (for example, German hate crime laws) and limited signatories to the Council of Europe Convention on Cybercrime.[xlv] In particular, there is a need to clarify the issue of espionage in cyberspace—what it is and what rights of response are left to the victims. In addition, a consistent model must be adopted that can be applied to determine whether a cyber attack is an act of war.

Third, controversy continues about the sharing of information between the U.S. Government and the private sector. Research is needed to determine what information should be shared and under what circumstances.

Fourth, regulatory agencies, such as the Federal Communications Commission, have the authority to regulate Internet service providers to redress selected cyber security issues. However, to date, regulatory agencies have been reluctant to address these issues.

Fifth, the recent debate about the Foreign Intelligence Surveillance Act court has mobilized the civil liberties community to raise the specter of "Big Brother." As a consequence of the actions of civil liberties organizations, major Government programs have been terminated or modified (for example, DARPA's Total Information Awareness and the Department of Homeland Security's Multi-state Anti-terrorism Information Exchange). Research is needed to clarify the appropriate balance among actions to deal with adversaries while still protecting civil liberties.

Cyber assessment research. As discussed below, our ability to perform cyber assessments is extremely uneven. As a consequence, research efforts are required to develop analytical methods, tools, data, and intellectual capital to address issues in the areas of cyberpower, cyber strategy, and infrastructure issues.

Cyber policy issues. During the course of the NDU cyber project, several major policy issues were singled out that required further attention. For the purposes of this preliminary cyber theory, these issues have served to focus the boundaries of this study, although we have also addressed a number of lower priority policy issues. Consequently, emphasis has been placed on assembling the intellectual capital required to illuminate those issues.

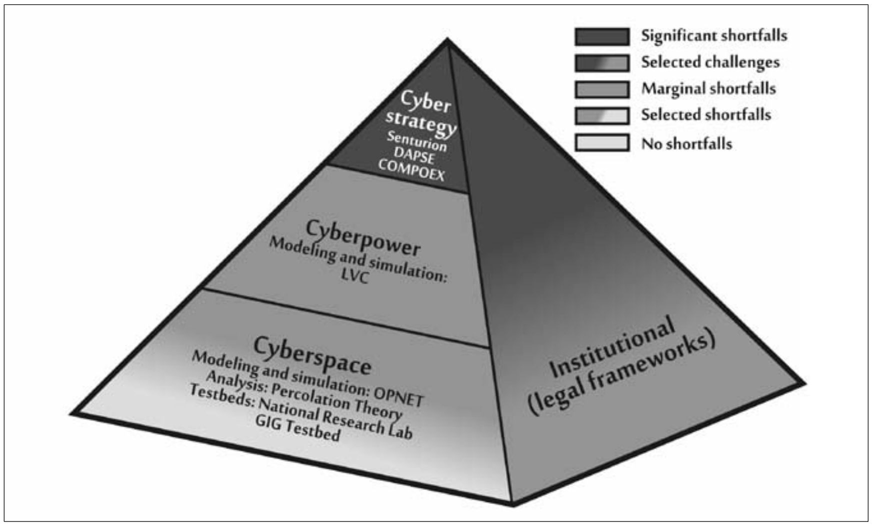
Table 3-8: Selected Policy Recommendations

Category	Area/Recommendations
Cyberspace	Security: U.S. Government should adopt "differentiated security" approach Resources: establish national cyber laboratories; substantially increase research and development funding for governmental agencies; enhance private sector activities
Cyberpower	Net-centric operations: address risks (for example, exercise against highly capable cyber warriors) Computer network attack: review definitions, classification level, integration into operations Influence operations: adopt a holistic, multidisciplinary, interagency approach Stability, security, transition, reconstruction: adopt I-power approach
Cyber strategy	Organization: create a new interagency cyber policy council Deterrence: U.S. Government should adopt a more robust deterrence policy (for example, generate capabilities, undertake political action) Espionage: conduct policy/legal review
Institutional	Governance: develop strategy for Internet influence Legal: clarify definitions, reconcile international and sovereign law Critical infrastructure protection: implement effective public- private partnership

In table 3–8, these issues have been aggregated into the categories of cyber-space, cyberpower, cyber strategy, and institutional factors. However, most of these issues are extremely broad and contentious; consequently, additional analyses will be required to address them adequately.

Cyber assessment. One of the major challenges confronting the analysis community is to develop the methods, tools, and data needed to support cyber policy decisionmakers. Figure 3–11 suggests the relative maturity of key tools in the areas of cyberspace, cyberpower, cyber strategy, and institutional factors.

Figure 3-11: Subjective Assessment of Modeling, Simulation, and Analysis for Cyber Policy Analyses



In the areas of cyberspace, the community is employing several tools to address computer science and communications issues. Perhaps the best known is the OPNET simulation widely employed to address network architectural issues.[xlvi] From an analytic perspective, techniques such as percolation theory enable one to evaluate the robustness of a network.[xlvii] Looking to the future, the National Research Laboratory has developed a GIG Testbed to explore the myriad issues associated with linking new systems and networks.

In the area of cyberpower, the community has had some success in employing live, virtual, and constructive simulations. For example, in assessments of air-to- air combat, insights have been derived from the live air intercept missile evaluation– air combat evaluation experiments, virtual experiments in the former McDonnell Air Combat Simulator, and constructive experiments using tools such as the TAC BRAWLER air combat simulator. However, the community still requires better tools to assess the impact of advances in cyberspace on broader military and informational effectiveness (for example, land combat in complex terrain).

In the area of cyber strategy, a number of promising initiatives are under way. In response to recent tasking by U.S. Strategic Command, a new methodology and associated tools are emerging (the Deterrence Analysis and Planning Support Environment).[xlviii] However, these results have not yet been applied to major cyber strategy issues. In addition, promising tools are emerging from academia (for example, Senturion predictive analysis software and George Mason University's Pythia modeling software) and DARPA (Conflict Modeling, Planning, and Outcomes Experimentation). However, these are still in early stages of development and application.

Finally, only primitive tools are available to address issues of governance, legal issues, and civil liberties. Although some tools are being developed to explore the cascading effects among critical infrastructures (National Infrastructure Simulation and Analysis Center system dynamics models),[xlix] they have not yet undergone rigorous validation.

Conclusion

Consistent with the macro framework that has been adopted to characterize the cyber problem, this section summarizes the key insights in the areas of cyberspace, cyberpower, cyber strategy, and institutional factors. The section concludes by identifying the next steps that should be taken to refine the theory of cyberpower.

Key Insights

Cyberspace. Cyberspace is a manmade environment experiencing exponential growth in important measures of performance. There is an extraordinary diffusion of knowledge among all the stakeholders of cyberspace, including malevolent users. As a consequence of this diffusion of knowledge, cyberspace is being degraded by noise (such as spam) and a broad variety of cyber attacks. The most troubling of these attacks includes denial of service, exfiltration of data, and the potential for corruption of data. In each instance, recent experience has demonstrated that these attacks are relatively easy to implement technically and financially and are extremely difficult to attribute.

These vulnerabilities arise from the basic architecture that has evolved from the original ARPANET. A new cyberspace architecture may be required to halt the perceived erosion of security. However, there will be substantial difficulties in transitioning from the current architecture to one that is more robust against adversary action.

Cyberpower. As cyberspace evolves, it has the potential to enhance each of the levers of national power. This chapter has focused on two of these levers: military and information.

In the area of military power, studies are under way to characterize the extent to which enhancements in cyberspace can enhance key measures of effectiveness. These studies tend to be unambiguous in the area of air-to-air combat where experiments suggest that enhanced digital communications can enhance loss-exchange ratios by a factor of approximately 2.5. Although studies of other military operations have also been undertaken, the results are generally confounded by other factors such as mobility and protection.

To complement these experiments, an assessment of theories of environmental warfare was undertaken that critically reassessed the theories of land, sea, air, and space theory. Based on that assessment, it was concluded that a theory of cyberpower should focus on four factors: technological advances, speed and scope of operations, control of key features, and national mobilization.

From the perspective of information, the chapter has addressed influence operations from a strategic and tactical perspective. Based on prior experiences and an adaptation of earlier analytical frameworks, an approach was developed for linking operational objectives and processes to DOTMLPF requirements. These assessments suggest that developments in cyberspace can substantially affect future efforts to enhance influence operations (for example, to implement precision-guided messages).

Cyber strategy. The evolving theory of cyber has identified a range of entities that will be empowered by enhancements in cyberspace. These include terrorist groups, which are employing cyberspace to recruit, raise money, propagandize, educate and train, plan operations, and command and control operations; hacktivists, who are employing cyberspace to conduct "cyber riots" and implement exploits in cyberspace; transnational criminals, who pursue a variety of techniques (such as phishing and denial-of-service attacks) to raise substantial funds (reputed to be more than the money derived from drug trafficking); and nation-states, the most advanced of which are employing cyberspace to enhance all dimensions of PMESII activities.

However, changes in cyberspace have given rise to unintended consequences. Many of the entities at the low end of the spectrum (terrorists, hacktivists, transnational criminals) are making life more dangerous for information-enabled societies. In particular, these entities tend to be much more adaptable than nation- states, causing the latter to respond, belatedly, to the initiatives of the former. In addition, research about selected near-peers (China, Russia) suggests that they have new perspectives on cyber strategy that will present information-enabled societies with new challenges in cyberspace.

Institutional factors. From an institutional perspective, issues are emerging that will affect all aspects of cyber theory. This chapter has high-lighted the challenges that exist in cyber governance, legal issues, exchange of cyber information between governments and industry, and the balance between national security and civil liberties. From a theoretical perspective, one of the major challenges emerges from the difficulty in characterizing and responding to an attack in cyberspace. As demonstrated by recent events, it is extremely difficult to attribute an attack to an adversary that chooses to act anonymously. In light of that ambiguity, it is difficult to formulate a coherent response to such an attack. For example, it is still unclear how an alliance, such as NATO, might respond to a cyber attack against one or more of its members. It is anticipated that these issues will be addressed in subsequent analyses.

Next Steps

As stated earlier, this effort constitutes a preliminary theory of cyberpower. To refine this product, it is recommended that the following steps be pursued.

Define. Although there is still confusion about the definitions for the key terms in a theory of cyberpower, the community should find it relatively straight-forward to go from the current base to agreement on terms. However, additional work is still required to establish the linkage between cyber terms and the terms associated with information operations.

Categorize. The cyber pyramid has proven to be a useful taxonomy in "binning" major concepts. However, there is still a need to develop specific cyber frameworks and models to explore policy issues that confront senior decision- makers.

Explain. This theory of cyberpower was anticipated to be incomplete. Additional efforts are needed to address issues beyond the scope of this book. In the area of cyberpower, there is a need to assess how potential changes in cyberspace will affect political, diplomatic, and economic functionality and effectiveness. In the area of cyber strategy, the extent to which key entities are empowered by advances in cyberspace and cyberpower must be assessed. These entities include individuals, nongovernmental organizations, transnational corporations, selected nation-states, alliances, and international organizations. Finally, in the area of institutional factors, there is a pressing need to assess the effect of changes in cyberspace on the balance between civil liberties and national security. In assessing these issues, it would be useful to employ a risk management approach.

Connect. Currently, we have relatively little understanding about the appropriate measures of merit to employ in cyber assessments or the relationships among them. For example, we do not have a clear understanding about how changes in cyberspace affect U.S. levers of power or empowerment. At a minimum, it is important to develop preliminary relationships so that a decisionmaker can understand the implications of how potential changes in cyberspace or institutional factors will affect cyberpower and cyber strategy.

Anticipate. Cyberspace is in the midst of explosive, nonlinear change. It is vital that more detailed technology assessments be undertaken to anticipate and understand potential breakthroughs in cyberspace. Furthermore, efforts should be made in the development and application of models, simulations, and analyses to assess the impact of these changes on cyberpower and cyber strategy. These developments in methodologies, tools, and data should provide decisionmakers with the analytic support needed to explore the long-range effect of alternative cyber options.

Appendix: Timeline of Key Cyber Events

This appendix summarizes several of the key events associated with the evolution of cyberspace, cyberpower, cyber strategy, and institutional factors. These observations have affected the formulation of the preliminary theory of cyberpower.

Figure 3-12: Evolution of Cyberspace

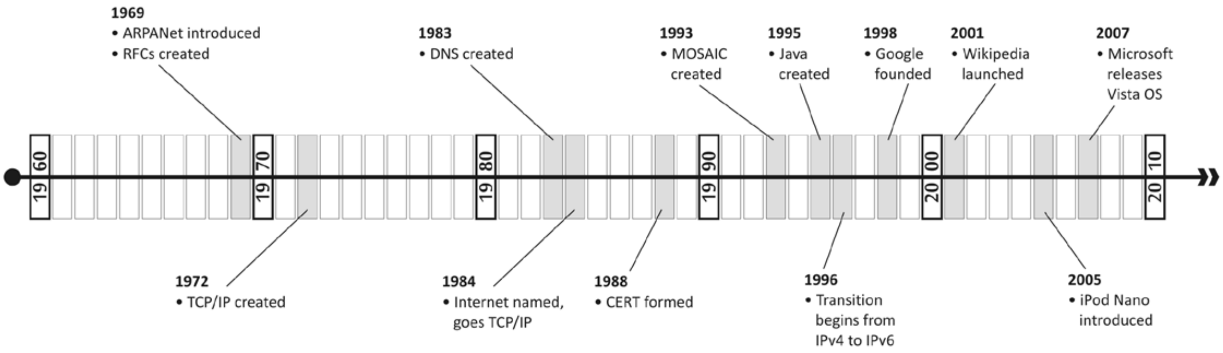


Figure 3–12 provides a timeline of recent events that have shaped cyberspace. It is notable that this timeline is scarcely 40 years old. Among the events of interest are the creation of the Internet (and the associated development of the TCP/ IP) and the evolution of the domain name service (DNS). A major enabler was the proliferation of inexpensive personal computers with operating systems that made it relatively simple for any user to employ the technology. Other seminal events include the creation of the World Wide Web and the Mosaic browser that made the information easily accessible to individual users.

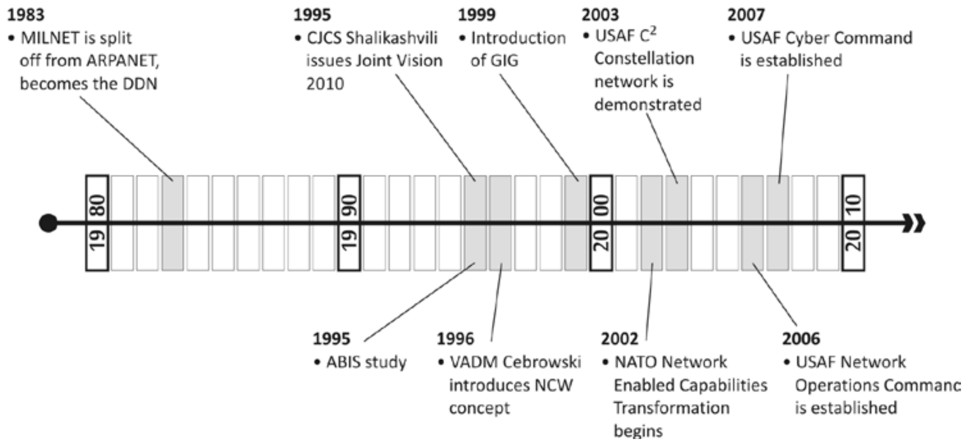
Google, founded in 1998, has become the world leader in popular search engines. By virtue of its advertising revenue, it has developed a viable business model.

Another important development involves the launch of the Wikipedia in 2001. Its open-source software is widely used by government entities (for example, Intellipedia and the Joint Data Systems of the Office of the Secretary of Defense).

In 2001, Apple began to sell the iPod, a device able to provide high capacity in an extremely small package due to the discovery of giant magnetoresistance.

Finally, in 2007, Microsoft released Vista, a new operating system. The oft-delayed product was revised to deal with the many security problems that afflict cyberspace.

Figure 3-13: Evolution of Cyberpower – a Military Perspective


1983
• MILNET is split off from ARPANET, becomes the DDN
1995
• CJCS Shalikashvili issues Joint Vision 2010
1999
• Introduction of GIG
2003
• USAF C2 Constellation network is demonstrated
2007
• USAF Cyber Command is established
1980
1990
2000
2010
1995
• ABIS study
1996
• VADM Cebrowski introduces NCW concept
2002
• NATO Network Enabled Capabilities Transformation begins
2006
• USAF Network Operations Commanc is established

The timeline in figure 3–13 identifies events that have shaped the military's perspectives on the use of cyberspace. The timeline begins in 1983, when MILNET split off from ARPANET (subsequently becoming the Defense Data Network). Subsequently, the intellectual underpinnings of military cyberpower were refined by the publication of *Joint Vision 2010*.[l] That was complemented by the Advanced Battlespace Information System, which was cosponsored by Vice Admiral Arthur Cebrowski, Director, J6, Joint Staff, and Anita Jones, Director of Defense Research and Engineering, to orchestrate evolving network concepts of operations and science and technology investments.[li] Subsequently, Vice Admiral Cebrowski and John Garstka wrote a seminal paper introducing the concept of net-centric warfare.[lii] Building on that base, OSD launched the concept of the Global Information Grid, and the individual Services formulated their visions of subordinate networks (LandWarNet, ForceNet, and C^2 Constellation). In addition, selected NATO and Partnership for Peace nations developed tailored strategies to implement variants of net-enabled capabilities. More recently, the Air Force has modified its mission space to include operations in cyberspace and reorganized to create an Air Cyber Command.[liii]

Although the current NDU effort has not specifically addressed the economic and diplomatic levers of power, these issues are being actively discussed elsewhere. For example, Thomas Friedman has identified 10 critical steps on the road to increased economic globalization.[liv] As shown in figure 3–14, these steps have their roots deep within the use of information technology (for example, the age of the personal computer, the advent of the Internet, and the revolution in Internet search engine capabilities). The extent and impact of globalization are being actively debated in the academic community.

Similarly, the diplomatic community is beginning to assess the impact of cyberspace on its operations. The global availability of information has affected the roles of Embassies. Whereas the Embassy was once the primary source of indigenous information, the capital city frequently has access to information not easily available to the Embassy. Furthermore, the Department of State has begun to explore "blog" diplomacy to provide "digital outreach."[lv]

Evolution of Cyber Strategy

The cyber strategy timeline in figure 3–15 emphasizes selected attacks and responses in cyberspace. At the onset of the timeline, the key elements of malware included worms (1979) and viruses (1983). An early example of an attack on sensitive but unclassified U.S. Government systems occurred in 1998 with Solar Sunrise. Although this was ultimately attributed to two California teenagers (linked to a subject matter expert in Israel), it dramatized the vulnerability of selected Government databases to intrusion. Subsequently, events such as Moonlight Maze (beginning in 1999 and attributed to sources in Russia) and Titan Rain (beginning in 2003 and attributed to sources in China) suggested the vulnerability of U.S. Government and defense industrial base data sources to cyber espionage. In the case of Titan Rain, Chinese sources were estimated to have exfiltrated on the order of 10 terabits of data.

More recently, attacks have featured distributed denial of service, drawing on herds of penetrated zombies or bots. As examples, in February 2007 there was a generally unsuccessful attack on the core DNS servers[lvi] and a reasonably successful "cyber riot" against government agencies, the financial sector, and media outlets in Estonia.[lvii] In many of these events, it has proven exceedingly difficult to attribute the source of the attack.

Figure 3-14 Evolution of Cyberpower – Economic Perspective

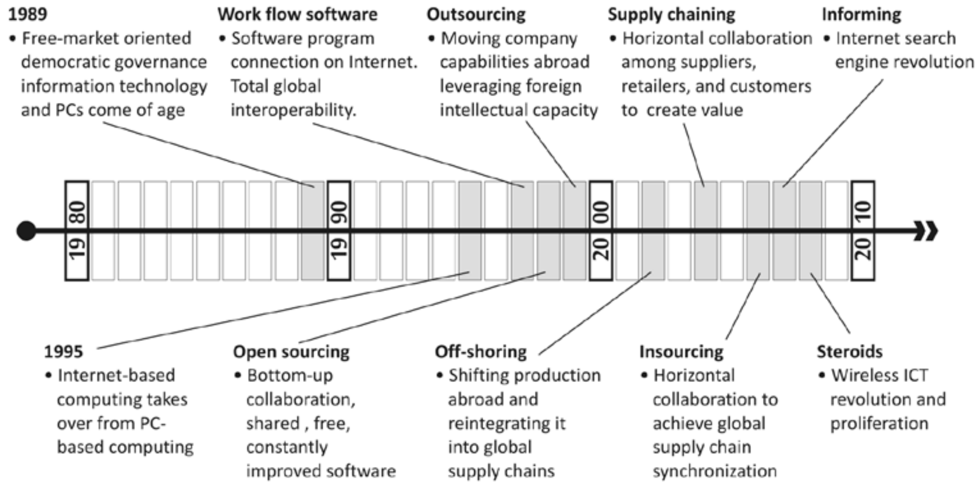
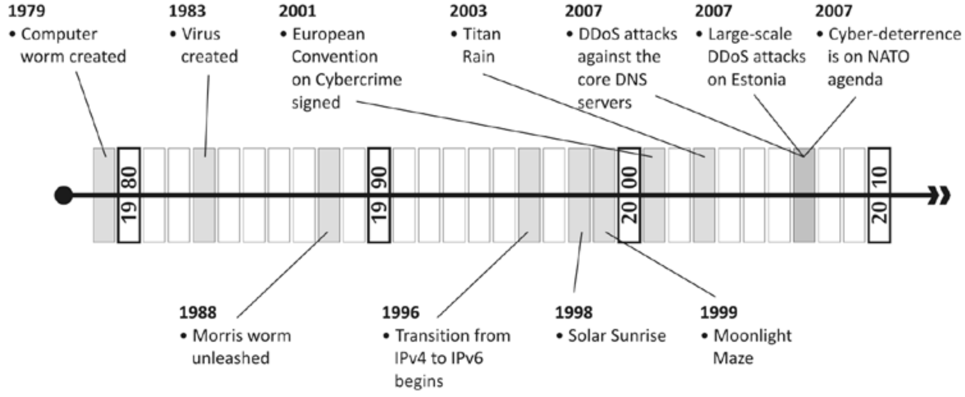
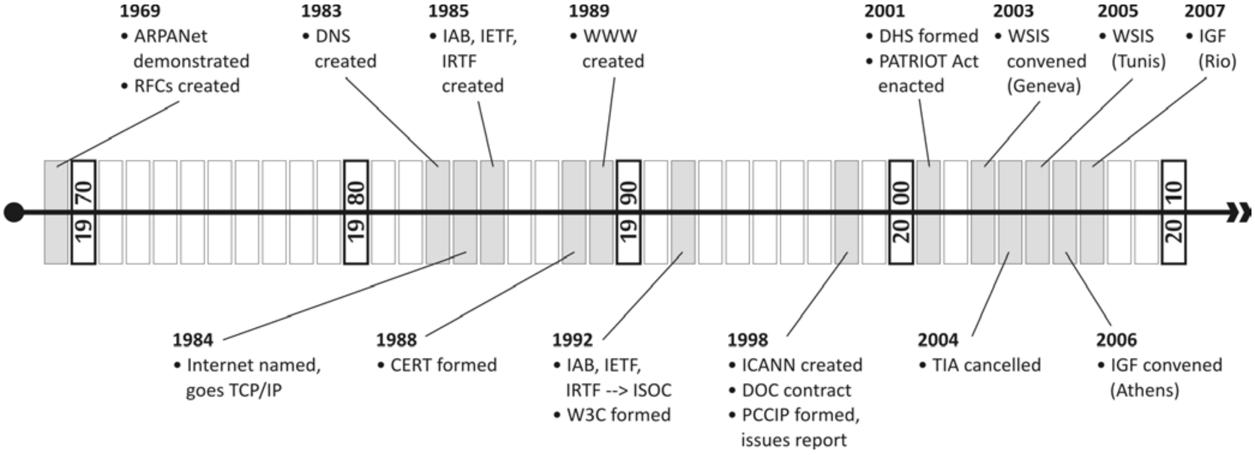

1989
• Free-market oriented democratic governance information technology and PCs come of age
Work flow software
• Software program connection on Internet. Total global interoperability.
Outsourcing
• Moving company capabilities abroad leveraging foreign intellectual capacity
Supply chaining
• Horizontal collaboration among suppliers, retailers, and customers to create value
Informing
• Internet search engine revolution
19 80
19 90
20 00
20 10
1995
• Internet-based computing takes over from PC-based computing
Open sourcing
• Bottom-up collaboration, shared , free, constantly improved software
Off-shoring
• Shifting production abroad and reintegrating it into global supply chains
Insourcing
• Horizontal collaboration to achieve global supply chain synchronization
Steroids
• Wireless ICT revolution and proliferation

Figure 3-15 Evolution of Cyber Strategy – Selected Attacks and Responses


1979
• Computer worm created
1983
• Virus created
2001
• European Convention on Cybercrime signed
2003
• Titan Rain
2007
• DDoS attacks against the core DNS servers
2007
• Large-scale DDoS attacks on Estonia
2007
• Cyber-deterrence is on NATO agenda
19 80
19 90
20 00
20 10
1988
• Morris worm unleashed
1996
• Transition from IPv4 to IPv6 begins
1998
• Solar Sunrise
1999
• Moonlight Maze

The attack against Estonia has prompted NATO to reevaluate its position on cyber defense. For example, Estonia is in the process of establishing a Computer Defense Center of Excellence, and NATO is addressing cyber deterrence in senior meetings. With respect to the latter, there is ongoing discussion about the implications of a cyber attack against a NATO Ally (Is an attack against one an attack against all? Does it have ramifications for Articles 4 and 5?).

Figure 3-16: Timeline of Key Institutional Events



Evolution of Institutional Factors

Figure 3–16 provides a timeline of key institutional events. Several of the early events (demonstration of the ARPANET, introduction of TCP/IP into the Internet, creation of the DNS) were discussed above.

In the 1980s and 1990s, organizations were created to provide governance for the Internet: the Internet Engineering Task Force and the Internet Research Task Force. In 1992, they morphed into the Internet Society, and the World Wide Web Consortium was formed.

Subsequently, the Internet Corporation for Assigned Names and Numbers was created in 1998.

In 1998, the President's Commission on Critical Infrastructure Protection was formed under the leadership of Tom Marsh. That effort focused public attention on the issues associated with critical infrastructure protection.

Institutionally, the events of September 11, 2001, gave rise to significant organizational and legal activities. These included the creation of the Department of Homeland Security and the passage of the USA PATRIOT Act. One unintended consequence was the formation and cancellation of the Total Information Awareness program at DARPA, due in part to concerns voiced by civil liberties advocates.

In recent years, the future governance of the Internet has been affected by two meetings of the World Summit on the Information Society in Geneva and Tunis. These have been followed by two Internet Governance Forum meetings in Athens and Rio de Janeiro.

[1] Department of Defense, *2006 Quadrennial Defense Review Report* (Washington, DC: Department of Defense, February 6, 2006.

[2] Charles D. Lutes, "INSS Project Summary: Towards a Theory of Spacepower," August 28, 2007.

[3] Terms of Reference for study of "A Theory of Cyberpower," March 2006.

[4] Harold R. Winton, "An Imperfect Jewel," presentation to Institute for National Strategic Studies workshop on theory of warfare, National Defense University, Washington, DC, September 2006.

[5] Jim Holt, "Unstrung," *The New Yorker*, October 2, 2006.

[6] An enumeration of key cyber events is provided in the appendix to this chapter.

[7] Strategic Studies Group XXVI, "Convergence of SeaPower and CyberPower," July 24, 2007.

[8] William Gibson, *Neuromancer* (New York: Ace Science Fiction, 1984).

[9] *National Military Strategy for Cyberspace Operations* Washington, DC: The Joint Staff, December 2006). More recently, Chairman of the Joint Chiefs of Staff Admiral Michael G. Mullen has proposed an alternative definition of *cyberspace*: "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" (Joint Staff Action Processing Form, Action Number J–7A 00067–08, May 30, 2008).

[10] Chairman of the Joint Chiefs of Staff, *The National Military Strategy of the United States of America—A Strategy for Today, A Vision for Tomorrow* (Washington, DC: The Joint Staff, 2004).

[11] Joint Publication 3–0, *Joint Operations* (Washington, DC: The Joint Staff, September 17, 2006, incorporating change 1, February 13, 2008).

[12] George E.P. Box, "Robustness in the Strategy of Scientific Model Building," in *Robustness in Statistics*, ed. R.L. Launer and G.N. Wilkinson (New York: Academic Press, 1979).

[13] For each category, we briefly cite the chapters of the book that are relevant. Furthermore, in the appendix to this chapter, we introduce a brief timeline of major events that characterize each category.

[14] In-depth theoretical discussions of cyberspace are provided in the following chapters of this book: chapter 4, "A Graphical Introduction to the Structural Elements of Cyberspace"; chapter 5, "Cyberspace and Infrastructure"; chapter 6, "Evolutionary Trends in Cyberspace"; chapter 7, "Information Security Issues in Cyberspace"; and chapter 8, "The Future of the Internet and Cyberpower."

[15] As a bounding case, note that the fastest U.S. computer, Roadrunner (built by IBM and Los Alamos National Laboratory), is capable of more than 1 petaflop (1 quadrillion floating point calculations per second). John Markoff, "Military Supercomputer Sets Record," *The New York Times*, June 9, 2008.

[16] The Nobel Prize in Physics for 2007 was awarded to Albert Fert of France and Peter Grunberg of Germany, who independently discovered this phenomenon.

[17] IPv6 will provide 2^{128} addresses. This would provide $5x10^{28}$ addresses for each of the 6.5 billion people alive today.

[18] See Jeremy M. Kaplan, *A New Conceptual Framework for Net-centric, Enterprise-wide, System- of-systems Engineering*, Defense and Technology Paper 29 (Washington, DC: Center for Technology and National Security Policy, National Defense University, July 2006).

[19] To put this change in context, note that in 1971, processor speeds were on the order of $4x10^5$ hertz (or 400 kilohertz) and the cost of 1 megabyte of dynamic random access memory (DRAM) was approximately $400 (in

2006 dollars). By 2006, commercial processor speeds were on the order of $4x10^9$ hertz (or 4 gigahertz) and the cost of 1 megabyte of DRAM was $0.0009. Sally Adee, "37 Years of Moore's Law," *IEEE Spectrum* (May 2008).

[20] In-depth theoretical discussions of the military and informational dimensions of cyberpower are provided in the following chapters of this book: chapter 10, "An Environmental Approach to Understanding Cyberpower"; chapter 11, "Military Cyberpower"; chapter 14, "Cyber Influence and International Security"; chapter 15, "Tactical Influence Operations"; and chapter 17, "Facilitating Stability Operations with Cyberpower."

[21] Carl von Clausewitz, *On War*, ed. and trans. Michael Howard and Peter Paret (Princeton: Princeton University Press, 1975).

[22] Charles J. Dunlap, "Neo-Strategicon: Modernized Principles of War for the 21st Century," *Military Review* (March-April 2006).

[23] Halford J. Mackinder, "The Geographical Pivot of History," *The Geographical Journal* (1904).

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

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

[26] Colin S. Gray and Geoffrey Sloan, eds., *Geopolitics, Geography, and Strategy* (London: Routledge, 1999).

[27] David S. Alberts and Richard E. Hayes, "Power to the Edge," Command and Control Research Program, June 2003. Note that the figure does not explicitly depict the social domain.

[28] David T. Signori and Stuart H. Starr, "The Mission Oriented Approach to NATO C^2 Planning," *Signal* (September 1987), 119–127.

[29] George Gilder, "Metcalfe's Law and Legacy," *Forbes ASAP*, September 13, 1993.

[30] Bob Briscoe, Andrew Odlyzko, and Benjamin Tilly, "Metcalfe's Law is Wrong," *IEEE Spectrum* (July 2006). To illustrate the differences in these results, assume that one has a network of 100 users. According to "Metcalfe's Law," the "value" of the network is on the order of 10,000. However, the revised "law" suggests that the value is on the order of 100 x 2 = 200.

[31] Daniel Gonzales et al., "Network-centric Operations Case Study: Air-to-Air Combat with and without Link 16" (Santa Monica, CA: RAND/National Defense Research Institute, 2005).

[32] In-depth theoretical discussions of cyberspace are provided in the following chapters of this book: chapter 13, "Deterrence of Cyber Attacks"; chapter 18, "Cyber Crime"; chapter 19, "Cyber Terrorism: Menace or Myth?"; and chapter 20, "Nation-state Cyber Strategies: Examples from China and Russia."

[33] *Hacktivism* (a portmanteau of *hack* and *activism*) is often understood as the writing of code, or otherwise manipulating bits, to promote political ideology. "Hacktivism," *Wikipedia*, available at <http://en.wikipedia.org/wiki/Hacktivism>.

[34] Marc Sageman, "The Homegrown Young Radicals of Next-Gen Jihad," *The Washington Post*, June 8, 2008, B1.

[35] Frank Cilluffo et al., "NETworked Radicalization: A Counter-Strategy," Homeland Security Policy Institute and Critical Incident Analysis Group Task Force on Internet-facilitated Radicalization, Washington, DC, May 2007, available at <www.gwumc.edu/hspi/reports/NETworked%20Radicalization_A%20Counter%20Strategy.pdf>.

[36] Joseph S. Nye, Jr., *Understanding International Conflicts: An Introduction to Theory and History* (New York: Pearson-Longman, 2005).

[37] M. Elaine Bunn, *Can Deterrence Be Tailored?* Strategic Forum No. 225 (Washington, DC: National Defense University Press, January 2007).

[xxxviii] AFEI Conference on Cyber Deterrence, Tysons Corner, VA, November 1–2, 2007.

[xxxix] For example, the United States might respond to a cyber attack through a variety of levers of power including diplomacy (for example, a demarche) or economic actions (restricting the flow of technology).

[xl] In-depth theoretical discussions of institutional factors are provided in the following chapters of this book: chapter 21, "Internet Governance"; chapter 22, "International Law and Information Operations"; chapter 23, "Cyberpower and Critical Infrastructure Protection: A Critical Assessment of Federal Efforts"; and chapter 24, "Cyberpower from the Presidential Perspective."

[xli] OASD (NII)/DOD CIO Globalization Task Force, "Development of an Internet Influence/Evolution Strategy for the Department of Defense," October 19, 2007.

[xlii] John Soat, "IT Confidential: Is There Anything That Can Be Done About E-mail?" *Information Week*, February 17, 2007.

[xliii] Audi Lagorce, "Clearwire, Sprint Nextel Scrap WiMax Network Agreement," *Market Watch*, November 9, 2007.

[xliv] Michael J. Riezenman, "Melding Mind and Machine," *The Institute*, June 2008, available at

<www.ieee.org/portal/site/tionline/menuitem.130a3558587d56e8fb2275875bac26c8/index.jsp?&pName=institute_level1_article&TheCat=2201&article=tionline/legacy/ inst2008/jun08/featuretechnology.xml&>.

[xlv] Council of Europe, Convention on Cybercrime, November 23, 2001, available at <http://conventions.coe.int/Treaty/en/Treaties/Word/185.doc>.

[xlvi] Emad Aboelela, *Network Simulation Experiments Manual*, 3d ed. (San Francisco: Morgan Kaufmann, June 2003).

[xlvii] Ira Kohlberg, "Percolation Theory of Coupled Infrastructures," presentation at 2007 Homeland Security Symposium, "Cascading Infrastructure Failures: Avoidance and Response," National Academy of Sciences, Washington, DC, May 2007.

[xlviii] Strategic Multi-Layer Analysis Team, "Deterrence in the 21st Century: An Effects-Based Approach in an Interconnected World, Volume I," sponsored by USSTRATCOM Global Innovation and Strategy Center, October 1, 2007.

[xlix] William Wimbish and Jeffrey Sterling, "A National Infrastructure Simulation and Analysis Center (NISAC): Strategic Leader Education and Formulation of Critical Infrastructure Policies," Center for Strategic Leadership, U.S. Army War College, August 2003.

[l] Chairman of the Joint Chiefs of Staff, *Joint Vision 2010* (Washington, DC: The Joint Staff, July 1996).

[li] Arthur Cebrowski and Anita Jones, "Advanced Battlespace Information System: Volume I," 1996.

[lii] Arthur Cebrowski and John Garstka, "Network Centric Warfare: Its Origin and Future," U.S. Naval Institute *Proceedings* (January 1998).

[liii] Josh Rogin, "Air Force to Create Cyber Command," *FCW.COM*, November 13, 2006.

[liv] Thomas L. Friedman, *The World Is Flat: A Brief History of the Twenty-first Century* (New York: Farrar, Straus and Giroux, 2005).

[lv] Walter Pincus, "State Department Tries Blog Diplomacy," *The Washington Post*, November 19, 2007, A15.

[lvi] ICANN Factsheet, "Root Server Attack on 6 February, 2007," March 1, 2007.

[lvii] Joshua Davis, "Hackers Take Down the Most Wired Country in Europe," *Wired* 15, no. 9 (August 22, 2007).