Introduction

THIS book is intended to help create a coherent framework for understanding and utilizing cyberpower in support of national security. Cyberspace and cyber- power are now critical elements of international security. Yet, as was noted during the course of the Department of Defense's (DOD's) 2006 Quadrennial Defense Review (QDR),[i] DOD lacks a coherent framework to assess cyber-power policy issues. To redress that shortfall, the Under Secretary of Defense for Policy directed the Center for Technology and National Security Policy (CTNSP) at the National Defense University to undertake a study of the subject area. As the study's terms of reference stated, "There is a compelling need for a comprehensive, robust, and articulate cyber power theory that describes, explains, and predicts how our nation should best use cyber power in support of United States (U.S.) national and security interests."

The book is a result of that study. It is divided into six broad areas. The first part provides a foundation and overview of the subject by identifying key policy issues, establishing a common vocabulary, and proposing an initial version of a theory of cyberpower. The second part identifies and explores possible changes in cyberspace over the next 15 years by assessing cyber infrastructure and security challenges. The third part examines the potential impact of changes in cyberspace on military use and deterrence. The fourth part analyzes informational levers of power. The fifth part addresses the extent to which changes in cyberspace serve to empower key entities such as transnational criminals, terrorists, and nation- states. The final part looks at key institutional factors, which include issues concerning governance, legal dimensions, critical infrastructure protection, and organization.

The chapters for this book were the product of several workshops at which experts from government, think tanks, industry, and academia presented their views on the major subject areas. Based on the feedback from those discussions, each presenter developed a chapter for this book. This introduction provides a bottom-up perspective of these chapters, summarizes the major themes of each, and identifies potential next steps.

Foundation and Overview

Part I is designed to provide a holistic perspective of the cyber domain by identifying and discussing major policy issues, providing key definitions, and formulating a preliminary theory of cyberpower.

In chapter 1, "Cyberpower and National Security: Policy Recommendations for a Strategic Framework," Franklin D. Kramer identifies and explores many of the key policy issues that senior decisionmakers will have to confront over the next decade. He aggregates these issues into the categories of structural issues (security, human capital and research and development, governance, and organization) and geopolitical issues (net-centric operations, computer network attack, deterrence, influence, stability operations, and doctrine, organization, training, materiel, leadership and education, personnel, and facilities [DOTMLPF]).

In chapter 2, "From Cyberspace to Cyberpower: Defining the Problem," Daniel T. Kuehl establishes a common vocabulary for the cyber realm. These include the following key definitions:

Cyberspace is a global domain within the information environment whose distinctive and unique character is framed by the use of electronics and the electromagnetic spectrum to create, store, modify, exchange, and exploit information via interdependent and interconnected networks using information-communication technologies.[ii]

Cyberpower is the ability to use cyberspace to create advantages and influence events in all the other operational environments and across the instruments of power.

Cyber strategy is the development and employment of strategic capabilities to operate in cyberspace, integrated and coordinated with the other operational domains, to achieve or support the achievement of objectives across the elements of national power in support of national security strategy.

In addition, Kuehl discusses two related terms: *information operations* and *influence operations*.

In chapter 3, "Toward a Preliminary Theory of Cyberpower," Stuart H. Starr develops an initial version of the theory of cyberpower, which was requested in the 2006 QDR. This preliminary theory addresses five key areas: it *builds* on the key definitions provided in chapter 2; it gives structure to the discussion by *categorizing* the key elements of the theory; it *explains* the elements in these categories by summarizing relevant events and introducing key frameworks; it seeks to *anticipate* key trends and activities so that policy can be germane and useful; and it *connects* the various elements of the subject so that key issues can be treated comprehensively.

Cyberspace

The six chapters in part II characterize the structure of cyberspace, identify evolutionary trends (particularly in the area of security), describe the relationship of cyberspace and critical infrastructures, and explore potential revolutionary changes to cyberspace.

In chapter 4, "A Graphical Introduction to the Structural Elements of Cyberspace," Elihu Zimet and Edward Skoudis display and explain ways in which the different layers of cyberspace interact with each other and how elements interact within each individual layer. In addition, they identify and discuss major trends in cyberspace (for example, convergence and the increased move to Internet protocol [IP] version 6; merging of hardware and software and the rise of embedded "computers" with hard-wired programming; and broadband and wireless proliferation).

In chapter 5, "Cyberspace and Infrastructure," William D. O'Neil identifies and discusses the vulnerabilities that characterize our critical infrastructures. To counter those vulnerabilities, he recommends that the United States create a more reliable and robust grid for electrical transmission and distribution and implement directive regulations for infrastructure firms at the process level.

In chapter 6, "Evolutionary Trends in Cyberspace," Edward Skoudis focuses on the private-public relationship of how cyberspace is maintained and run. He identifies and discusses key trends in computers and networks (broadband proliferation, wireless proliferation, the transition from IP version 4 to IP version 6) and major social trends (worldwide technological development with localized emphases, and the rise of online communities, collaboration, and information-sharing).

In chapter 7, "Information Security Issues in Cyberspace," Edward Skoudis explores the various technology-related Internet security issues from the viewpoints of both attackers and defenders. He focuses on those forms of attacks that are associated with current Internet technologies and are most likely to continue to present a substantial challenge in the near future. He cautions that the security concerns associated with the use of the Internet today have originated from the application of technologies in ways unanticipated by their original designers.

In chapter 8, “The Future of the Internet and Cyberpower,” Marjory S. Blumenthal and David D. Clark raise eight policy issues that they deem relevant to the future of cyberspace. These policy issues include security, object provenance, identity, location-aware computing, location sensing, open sensor networks, open vehicle networks, and networks in times of crisis. In particular, they note that future networks may focus on an architecture for information-handling services built out of distributed servers and staged delivery. Attention to architecture at these higher levels may provide an alternative to today’s focus on common packet formats and allow the lower layers of a future network to more directly exploit features of diverse technology.

In chapter 9, “Information Technology and the Biotech Revolution,” Edward Skoudis explores the blurring of lines between the computer and the human. Trends suggest that innovative interfaces are possible that will enable humans to effectively and efficiently harness machine computing power (for example, enhanced prostheses, or mental control of computers).

Cyberpower: Military Use and Deterrence

In part III, the potential impact of changes in cyberspace on the military and for deterrence is explored in four chapters.[iii]

In chapter 10, “An Environmental Approach to Understanding Cyber-power,” Gregory J. Rattray provides a historical perspective by assessing the common features of environmental power theories (for example, Alfred Thayer Mahan on naval power; Giulio Douhet on airpower; Halford J. Mackinder on land power; Colin Gray and Geoffrey Sloan on spacepower). Based on these earlier efforts, he identifies four common features of environmental power theories that are germane to cyberpower: technological advances, speed and scope of operations, control of key features/bottlenecks, and national mobilization.

In chapter 11, “Military Cyberpower,” Martin C. Libicki addresses the question of whether networking operators permit a measurable improvement in operational effectiveness. Currently, the picture is ambiguous. In selected cases (such as air-to-air engagements), experiments demonstrate that networking can give rise to appreciable improvements in loss exchange ratios.[iv] However, in more complex ground-based operations (for example, the Stryker Brigade Combat Team), networking appears to be of value, but more experimentation will be needed to assess quantitatively how much it helps.[v]

Chapter 12, “Military Service Overview,” by Elihu Zimet and Charles L. Barry, provides an overview of Service initiatives in cyberspace and cyberpower.

In chapter 13, “Deterrence of Cyber Attacks,” Richard L. Kugler asserts that although the U.S. Government is aware of the risks, it does not currently have a well-developed, publicly articulated strategy for deterring cyber attacks. As attacks may be launched as part of an adversary’s strategic agenda, deterrence is a matter of not only defensive and offensive capabilities, but also the capacity to influence the adversary’s motives, cost-benefit calculations, and risk-taking propensities. Recognizing the various actors and agendas that are likely to pose a cyber threat, the author proposes that a policy of “tailored deterrence” as cited in the 2006 QDR is needed to prevent attack. He concludes by noting that the message of a declaratory policy must be tailored for the types of adversaries likely to be faced. U.S. objectives, as well as an actor's specific motives and capabilities, will determine the response to an attack (which may use levers of power outside of the cyber realm).

Cyberpower: Information

Complementing the perspectives on the military lever of power are four chapters in part IV that address the informational lever of power and discuss the role of military and influence levers of power in a whole-of-government approach to stability, security, transition, and reconstruction (SSTR) operations.

Chapter 14, "Cyber Influence and International Security," by Franklin D. Kramer and Larry K. Wentz, explores the strategic and operational levels of influence. The authors identify three key elements of influence operations: expertise in the application of principles of influence; domain experience in arenas where the principles are to be applied; and experience in the use of cyberspace. They conclude that if the United States is to enhance its influence in cyberspace, it will require a multifaceted strategy that differentiates the circumstances of the message, key places of delivery, and sophistication with which messages are created and delivered, with particular focus on channels and messengers.

In chapter 15, "Tactical Influence Operations," Stuart H. Starr introduces a framework that links operational influence objectives to DOTMLPF initiatives. Two perspectives illustrate this framework. Looking backward, the activities of Colonel Ralph Baker, USA, former Brigade Combat Team leader in Baghdad, are mapped onto the framework to characterize DOTMLPF changes needed to enhance tactical influence operations.[vi] Looking to the future, the chapter explores the potential role of Web 2.0 technology to enhance emerging influence operations.

In chapter 16, "I-Power: The Information Revolution and Stability Operations," Franklin D. Kramer, Larry K. Wentz, and Stuart H. Starr explore how information and information communications technology (I/ICT) can significantly increase the likelihood of success in SSTR operations. The chapter identifies a five-part strategy for the effective application of I/ICT: ensure that the U.S. Government gives high priority to a joint civil-military activity; require the military to make I/ICT part of the planning and execution of the SSTR operation; preplan and establish I/ICT partnerships with regular participants in SSTR operations; focus the intervention on the host nation; and harness key ICT capabilities to support the strategy.

In chapter 17, "Facilitating Stability Operations with Cyberpower," Gerard J. Christman complements the preceding chapter by identifying and discussing many of the institutional and policy activities that have recently been undertaken (for example, the promulgation of DOD Directive 3000.05, identifying SSTR operations as a core mission for DOD). However, there is still a need for developing follow-on instructions to the Services. Furthermore, additional effort is needed to foster trust and improve collaboration and information-sharing between the Government and other participants in SSTR operations (such as nongovernmental and international organizations).

Cyberpower: Strategic Problems

In part V, three chapters deal with ways in which changes in cyberspace can empower criminals, terrorists, and nation-states. In chapter 18, "Cyber Crime," Clay Wilson identifies and discusses the characteristics of and trends in cyber crime. The chapter concludes with a summary of policy issues to be considered to reduce cyber crime: seeking new ways and incentives for private industry and government to cooperate for reporting cyber crime and increasing cyber security; creating new agreements to encourage more international cooperation among law enforcement agencies to improve accuracy for attribution of cyber crimes and for pursuing malicious actors across national borders; and developing more accurate methods for measuring the effects of cyber crime.

In chapter 19, "Cyber Terrorism: Menace or Myth?" Irving Lachow analyzes the terrorist use of cyberspace. He notes that terrorists have gravitated toward the use of cyberspace because of the low cost of entry, the opportunity to achieve sanctuary, and its value in supporting a wide variety of key functions (recruiting, raising funds, propagandizing, educating and training, and planning of operations). However, Lachow maintains that terrorists are more likely to employ kinetic means, in the near term, to support terrorist operations.

In chapter 20, "Nation-state Cyber Strategies: Examples from China and Russia," Timothy L. Thomas discusses alternative nation-state perspectives on the use of cyberspace. In the case of China, the author examines the evolution of its cyber philosophy and how peacetime activities may be part of a cyber preemptive strategy (such as ongoing espionage activities). Based on an assessment of open source documents, he hypothesizes that China may intend to use electrons as they once used forces: packets of electrons might be used to fulfill the stratagem, "kill with a borrowed sword." As a result, Chinese strategy relies on preparation and mobilization to ensure that a cyber operation could be conducted suddenly, to gain the initiative by "striking the enemy's information center of gravity and weakening the combat efficiency of his information systems and cyberized weapons." Similarly, the author examines the terminology and strategic thought used in Russia to create a picture of Russia's potential cyber strategy. Russian theorists speak of "reflexive control" and seek to locate the weak link in the system and exploit it. Thomas affirms that Russia is replete with technical cybertalent, making it a potentially challenging cyberpower opponent.

Institutional Factors

In part VI, four chapters address the host of institutional issues that confront the cyber decisionmaker. First, in the area of governance, the contentious issues of governance of the Internet and the U.S. Government's role in that process are examined. Second, in the area of legal issues, selected elements of international law have been analyzed. These include the issue of attack assessment in cyberspace and the selection of suitable responses. Third, an assessment has been made of the performance and effectiveness of the actions of the Department of Homeland Security in the defense of critical infrastructures in the Nation. Finally, it is important to consider cyber issues from a whole-of-government perspective. This requires a viewpoint that considers the Presidential perspective.

In chapter 21, "Internet Governance," Harold Kwalwasser says that the mechanism for governance of the Internet is exceedingly complex (that is, there is considerable overlap among the functions and activities of the participating organizations). To assess the performance of the existing governance process, he introduces eight criteria: open, democratic, transparent, dynamic, adaptable, accountable, efficient, and effective. When evaluated against these criteria, the Internet governance process is assessed to have performed remarkably well to date. However, because of pressures from other nation-states, the U.S. Government needs to develop a viable strategy for achieving "Internet influence."

Chapter 22, "International Law and Information Operations," by Thomas C. Wingfield, describes appropriate frameworks and employs them to analyze the legal issues associated with two classes of problems: *jus ad bellum* (the lawful resort to force) and *jus in bello* (the use of force in wartime). In the area of *jus ad bellum*, the key question faced by cyber operators is, “When does an information operation (or group of operations) rise to the level of a ‘use of force’ under international law?” To address that question, the author introduces and applies the Schmitt framework (a multi-attribute utility approach to the factors of severity, immediacy, directness, invasiveness, measurability, presumptive legitimacy, and responsibility). In addressing the subject of *jus in bello*, Wingfield focuses on the key issue: “Once at war in cyberspace, what rules apply?” To address this question, he introduces and discusses four areas: discrimination, necessity, proportionality, and ruses of war and perfidy.

Chapter 23, “Cyberpower and Critical Infrastructure Protection: A Critical Assessment of Federal Efforts,” was written by John A. McCarthy with the assistance of Chris Burrow, Maeve Dion, and Olivia Pacheco. The chapter makes the major observation that the cyber infrastructure has become vital to the national defense infrastructure, the U.S. Government, and the global economy. However, the authors caution that there is the potential for a catastrophic cyber incident. They conclude that the best way forward is for the Government to serve as an organizational model, develop and test emergency procedures, and bring its expertise to the private sector to be leveraged. In order to play those roles, the Government will need to provide clear policy direction, develop operational guidance that includes roles and responsibilities, and shift its research and development priorities and its distribution of resources to the task of managing catastrophic issues.

Chapter 24, “Cyberpower from the Presidential Perspective,” by Leon Fuerth, addresses the cyber organizational issue from a “whole of government” perspective. The author notes that the organization problem is a complex, poorly structured issue that is in the class of “wicked problems.” In his assessment, he considers the possibility of a Cyber Policy Council at the White House level that might be analogous to the Council of Economic Advisors.

Potential next Steps

Although this cyber effort has been very broad in its scope, it should be regarded as an initial foundation for further work. Several areas will require additional research and deliberation. First, many of the trends associated with cyberspace are highly nonlinear (for example, global growth of the Internet and cellular technology; participation in social network systems). There is a need to perform in-depth technology assessments to anticipate when those trends begin to stabilize. Second, in the area of cyberpower, the book takes only the first steps in addressing the military and informational levers of power. Further research is needed, including about how changes in cyberspace are affecting the political, diplomatic, and economic levers of power. Third, in the area of cyber strategy, steps should be taken to assess how changes in cyberspace are affecting the empowerment of individuals, corporations, nongovernmental organizations, and international organizations. Fourth, in the area of institutional factors, it is important to explore the balance between civil liberties and national security. Overall, there is a need to develop and assemble analytic methods, tools, and data to help perform the assessments needed by senior decisionmakers to formulate sound cyber policies. Specifically, the community must develop and apply risk assessment methods to support the identification of key vulnerabilities and to identify preparatory steps to mitigate those vulnerabilities.

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

[ii] Recently, the Chairman of the Joint Chiefs of Staff has recommended that the term *cyberspace* be defined as a "global domain within the information environment consisting of the interdependent network of information infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers."

[iii] As noted above, emphasis was placed on the military and informational levers.

[iv] 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).

[v] Daniel Gonzales et al., "Network-centric Operations Case Study: The Stryker Brigade Combat Team" (Santa Monica, CA: RAND/National Defense Research Institute, 2005).

[vi] Ralph Baker, "The Decisive Weapon: A Brigade Combat Team Commander's Perspective on Information Operations," *Military Review* (May-June 2006).