PUBLICATION

Strategic Knowledgecraft:
Operational Art for the
Twenty-First Century

Roc A. Myers
September 2000

Program on Information Resources Policy

Center for Information Policy Research

Harvard University

The Program on Information Resources Policy is jointly sponsored by Harvard University and the Center for Information Policy Research.

Roc A. Myers, Colonel (s), USAF, directs modernization and investment planning for the U.S. Air Force's Intercontinental Ballistic Missiles (ICBM) and national space launch capabilities. He has twenty-seven years' experience in space operations, systems acquisition management, command and control, communications, computers, and intelligence. This report was prepared while he was an Air Force National Defense Fellow with the Program in 1997–98.

ISBN 1-879716-64-X **P-00-4**

September 2000

PROGRAM ON INFORMATION RESOURCES POLICY

Harvard University **Center for Information Policy Research**

Affiliates

Anonymous Startup
AT&T Corp.
Australian Telecommunications Users Group
BellSouth Corp.
The Boeing Company
Booz-Allen & Hamilton, Inc.
Carvajal S.A. (Colombia)
Center for Excellence in Education
CIRCIT at RMIT (Australia)
Commission of the European Communities
Critical Path
CyberMedia Convergence Consulting
CyraCom International
DACOM (Korea)
ETRI (Korea)
eYak, Inc.
Fujitsu Research Institute (Japan)
GNB Technologies
Grupo Clarin (Argentina)
Hanaro Telecom Corp. (Korea)
Hearst Newspapers
High Acre Systems, Inc.
Hitachi Research Institute (Japan)
IBM Corp.
Intel Corp.
Korea Telecom
Lee Enterprises, Inc.
Lexis-Nexis
Eli Lilly and Co.
Lucent Technologies
John and Mary R. Markle Foundation
McCann North America
Microsoft Corp.
MITRE Corp.
Motorola, Inc.
National Security Research, Inc.
National Telephone Cooperative Assoc.
NEC Corp. (Japan)
NEST–Boston
Nippon Telegraph & Telephone Corp (Japan)
NMC/Northwestern University
Research Institute of Telecommunications and Economics (Japan)
Samara Associates
Siemens Corp.
SK Telecom Co. Ltd. (Korea)
Strategy Assistance Services
TRW, Inc.
United States Government:
- Department of Commerce
  - National Telecommunications and Information Administration
- Department of Defense
  - Defense Intelligence Agency
  - National Defense University
- Department of Health and Human Services
  - National Library of Medicine
- Department of the Treasury
  - Office of the Comptroller of the Currency
- Federal Communications Commission
- National Security Agency
- United States Postal Service

Upoc
Verizon

Acknowledgements

The author gratefully acknowledges the following people who reviewed and commented critically on the draft version of this report. Without their consideration, input, and encouragement, this study could not have been completed:

Stephen A. Beardslee
Alan D. Campen
Craig Cook
Fred R. Demech, Jr.
Walter P. Fairbanks
Thomas Fuhrman
Jacques S. Gansler
Seymour E. Goodman
Martha Maurer
Henry H. Shelton
Marilyn Z. Wellons

These reviewers and the Program's Affiliates, however, are not responsible for or necessarily in agreement with the views expressed here, nor should they be blamed for any errors of fact or interpretation.

A number of other people have made significant contributions to this work: Tom Armour, Albert Edmonds, Dan Kuehl, Dorothy Leonard, James Peak, Marshall Potter, and Greg Rattray. The research was cosponsored by the Institute for National Strategic Studies at the U.S. Air Force Academy.

I especially thank Sally Myers and Roc Myers II, for their understanding and encouragement.

The views, opinions, and conclusions expressed in this paper are those of the author and should not be construed as an official position of the Department of Defense or any other government agency or department.

Executive Summary

One of the most complex tasks of the U.S. national security community is creating the richest possible set of integrated military, economic, and diplomatic alternatives for convenient use by decisionmakers. This task is made even more difficult in the absence of effective doctrine, operational strategies, and tactics for the effective marshalling and mobilizing of its general collective knowledge (CK).

Since the late 1960s, the United States's national-security information strategy has been technology-driven. In these years, national security strategies were focussed on the wholesale creation, movement, and storage of information but not on investing significant resources to manage the national security community's CK and prepare it for retail consumption. Decision-makers are problem-driven. They prefer to have substantive information marshalled according to problems they are trying to solve or options they are developing and then mobilized for quick assimilation into their working knowledge. The unspoken assumption of a technology-driven strategy is that decisionmakers will somehow provide the resources to convert information into usable knowledge for decision and action. Thus, adequately marshalled information and mobilized knowledge have become largely a luxury reserved for only the most senior decisionmakers.

Events in the 1990s have emphasized that the ability to exploit the knowledge at one's immediate disposal quickly and confidently is critical at all levels of command. Agile, precise, global military operations envisioned for the next decades will be possible only through sustained, deliberate management of the national security community's working knowledge. Future decision cycles are unlikely to permit long times for mobilization and organization. Indeed, less and less time will be available to decisionmakers for evaluating and selecting appropriate courses of action. Demands, in turn, will compress the time available to staffs for locating and integrating increasing amounts of potentially relevant information and knowledge. Without well-developed knowledge-marshaling and -mobilization activities, the national security community will almost certainly be unable to generate agile CK or the capacity for shared problem-solving needed to realize the potential of the high-performance military forces envisioned for the twenty-first century.

This report proposes a doctrinal concept of strategic knowledge operations (SKO) and the operational concepts of collective knowledge and knowledge marshalling and mobilization. It attempts to set the stage for dialogue among joint, interdepartmental, interdisciplinary staff by identifying challenges that the leadership of the national security community may need to address if the United States is to develop knowledgecraft and collective knowledge management as a core competitive capability.

Contents

Illustrations

Figures

Tables

Preface

> *Absorbing a new discipline into the hierarchy of military activities is never done without at least some painful adjustment and accommodation; but the sudden growth in dependence upon the various high-technology instruments that enable commanders of today's forces to control them effectively has presented unique challenges in this regard. The reason, of course, is that these enabling tools and instruments cut so pervasively, not only across organizations, but into every kind of endeavor within.*
>
> Robert Herres[1]

During a military command-and-control exercise in 1996, a Director of Operations wished to "test drive" collaborative software available in the then fledgling Global Command and Control System (GCCS).[2] The operations staff was instructed to make maximum use of this software to solve problems during the exercise. As the local representative for GCCS, I was asked to host a meeting of representatives of the various operations staff to prepare for the exercise. Because the exercise was to have begun on the thirtieth day of a simulated crisis, I began by explaining that the software was essentially a blank slate that contained no information about what had, hypothetically, occurred in the first twenty-nine days—no operational analyses of events, no intelligence products, no maps, nothing to establish the context in which collaborative planning and problem solving could take place.

After clarifying the need for such a "contextual database," I asked who would prepare it. In response, the operations staff representatives pointed out that they were only users and had neither the time nor training for "that type of analysis." The computer and communications folks said they only installed and maintained hardware and software, that, in effect, they "delivered the mail" but did not create it. The various intelligence representatives pointed out that they only "did intelligence" and were not staffed to perform the operational analysis needed for such a database. So it was with all the representatives around the table. A quick survey of those present revealed that no one in the organization had yet experimented with the GCCS collaborative planning software nor developed any skill in or knowledge of its use. Several representatives even admitted they did not know with whom they were to collaborate or why. What became clear was that while it was everyone's job, it was also no one's.

---

[1]Robert T. Herres, Introduction, *Command and Control for War and Peace*, by Thomas P. Coakley (Washington, D.C.: National Defense University Press, 1992), xvi.

[2]GCCS is a Department of Defense (DOD) information system designed to support deliberate and crisis planning with the use of integrated analytic tools and data-transfer capabilities. See the Defense Information Systems Agency (DISA), [On-line]. URL: http://spider.osfl.disa.mil/new_home/about.html (Accessed May 11, 1998.)

In the end, the necessary information and knowledge were available, but the organization did not have the doctrine, cultural incentives, or tactical skills with which to marshal and mobilize them in time for these exercises.[3]

Although a relatively local event, the meeting had the makings of a metaphor for the general state of acquisition, management, and application of U.S. national security knowledge. As of the middle of the year 2000, no formal doctrine exists for the employment of general information systems as "weapon systems" or for the management of national security knowledge as a means to influence opponents.[4] Individuals, military units, and staff organizations are pretty much left on their own to figure out how to use information technology and to build and manage knowledge.

Nowhere is the knowledge management deficiency more apparent than in the military's development of new weapons systems. Throughout the life cycle of a new weapons system, one closely monitored process is the development of operational tactics for employing that system. Specialized weapons schools develop advanced curricula that take as a foundation extensive basic skills training. Graduates of these schools then return to field units where they, in turn, train others. Both individuals and units are recognized and rewarded for exploring weapons system capabilities and exploiting them to the fullest. Tactics and training are solidly grounded doctrine based on time-tested principles of warfare, and institutionalized activities insure that these are widely distributed and up to date. In stark contrast, knowledge management and information systems training consists largely of "buttonology," which is often taught by instructors not trained in warfare, intelligence operations, or diplomacy. Few individuals become highly proficient at exploiting information systems capabilities, and, as of this writing, no significant doctrinal linkages exist between knowledge management and the general principles of warfare.[5]

From 1985 to 1997, I studied this problem first-hand while involved in many activities, notably: development of Tactical Exploitation of National Capabilities (TENCAP)[6] technology and systems; deployment of the Defense Dissemination System to Operation Desert Shield/Desert Storm; development of Intelink; development and prototyping of the Global Broadcast System; and deployment of the GCCS. Four broad observations repeatedly came to the fore:

---

[3]Marshal: to assemble; arrange, and coordinate for a purpose; mobilize: to make mobile, capable of action.

[4]Limited exceptions can be cited, in intelligence, information warfare, and psychological operations (PSYOPS), but these exceptions apply only to relatively narrow, specialized activities within the national security community.

[5]This phenomenon is not new to the national security community nor unique to information technology. For example, aircraft, artillery, and tanks were first distributed among tactical army units where they were used only to enhance the effectiveness of infantry forces. Nearly thirty years passed before these technologies came into their own as weapons systems.

[6]An umbrella term for activities that promote the tactical application of intelligence and data from satellites and other advanced national reconnaissance activities.

- That throughout the national security community[7] there was no general agreement about the fundamental role of knowledge management as a tool of national power.
- That no formal doctrine existed about how general, national security knowledge and information should be managed and shared to achieve national purpose.
- That within this community there is a widespread belief that having information technology automatically confers knowledge, interoperability and collective action upon its users.
- That investment in tactics and knowledge-building activities to effectively employ the vast general knowledge and information resources available within national security community has been limited, at best.

The aim of U.S. national security information strategy appears to have been off-center. Because the national security community has been shooting for *knowledge* but aiming at *information*, development efforts may have been off the mark. By fixing its aim on information technology, it has neglected to develop a coherent vision that would underpin and promote the development and employment of knowledge assets, information systems tactics, and general *knowledgecraft*.[8]

This is not to say that the United States has not benefited from the national security community's emphasis on information and information technology—it has. But by concentrating investments on technology to improve the collection, duplication, storage, and dissemination of information, this community has upset the critical balance between its ability to collect and its ability to use information. The competitive advantage that, until the 1980s, the U.S. derived from information technology has been offset by major changes in the global competitive environment and a relatively weak ability to capitalize on information and manage knowledge.[9] This imbalance is especially great in the cases of technical intelligence, transactional data, and geospatial information, where the capacity of the United States to use information lags

---

[7]The term *national security community* is used throughout to mean government organizations that play a primary role in determining or achieving national security objectives (i.e., the DOD, the Department of State [DOS], the Department of Energy [DOE], the Executive Office of the President [EOP], the National Security Council, Congress, and the Central Intelligence Agency [CIA], among others) and their supporting contractors. From time to time, this community may also include nongovernmental and commercial activities. The acronym NSC, which is commonly stands for the National Security Council, is not used here to avoid confusion of that organization with the national security community.

[8]The word *craft* has a variety of uses; here it seems the best way to describe the skill and art involved in creating or building knowledge.

[9]Samuel P. Huntington, *The Clash of Civilizations and the Remaking of World Order* (New York: Touchstone, 1996), 81-86. James Beniger gives a detailed account of the benefits and impacts of technology in his book *The Control Revolution: Technological and Economic Origins of the Information Society* (Cambridge, Mass.: Harvard University Press, 1986).

significantly behind the capacity to produce it.[10] During the Persian Gulf war (August 1990–March 1991), for example, communications initially limited the availability of information, particularly intelligence, but after data and information "pipes" were opened into the theater of operations, the bottleneck shifted to sorting and organizing of volumes of information according to the problems to be solved. Seven years later, and in spite of order-of-magnitude increases in performance of information technologies, information overload remains a primary complaint of operations staffs.[11]

The present course will be difficult to change. The national security community has historically been a "community of communities," each functionally autonomous and with its own values, language, and authority to design and procure its own information systems. Budgetary and political pressures to use information technology to strengthen and preserve hard-won roles and missions were, and remain, enormous. The primary application of technology by each "subcommunity" has been to preserve existing ways of doing business and marginally to improve and promote its preferred means and methods.[12]

How can the United States refocus national strategies and balance investments to produce a sustainable advantage over competitors, even possibly a formidable edge that would justify the expense of collecting, processing, storing, moving, and protecting its vast accumulation of information? Knowledge management will need to become explicit. Comprehensive discussion of how to manage knowledge resources, however, is only now emerging, mainly in business and in academic research,[13] and dialogue on how to create usable working knowledge[14] and gain a competitive strategic advantage from vast national security information resources is embryonic.

To go beyond the mere acquisition of information and make knowledge management an explicit part of U.S. national security policies and strategy; the United States national security community would need to accomplish three main tasks:

- Develop joint military and interagency doctrine that clearly articulates and expands understanding of the nature and role of knowledge in international competition and the

---

[10]For example, the Defense Intelligence Agency (DIA) estimates that only 10 percent of all the imagery intelligence collected is ever analyzed. Interview by the author with David Lee (Headquarters, DIA, Feb. 3, 1998).

[11]This view is based on the author's experience in 1989–97 with deployment and operations of the Defense Dissemination System (DDS-III) and the GCCS.

[12]An extrapolation of C. Kenneth Allard's observation, "paving over the existing cow paths," about technology and warfare. See Allard's "Information Warfare: The Burden of History and the Risk of Hubris," in *The Information Revolution and National Security: Dimensions and Directions* (Washington, D.C.: Center for Strategic and International Studies [CSIS], 1996), 234.

[13]Although researchers and educators such as Davis, Leonard-Barton, Nonaka, and Oettinger have been pursuing this question since as early as the 1960s, most publications and studies on knowledge-management publications and have appeared since the early 1990s.

[14]Davenport and Prusak coin this term in title of their book on knowledge management, *Working Knowledge*.

specific strategic ends that knowledge activities can support. Then, incorporate that doctrine into professional training and education.

- Create common tactical knowledgecraft, which includes identifying and initiating activities to build and sustain a dynamic, relevant, collective knowledge.
- Create within all levels of the national security community an environment that promotes and rewards effective management, sharing, and collective exploitation of knowledge to achieve national purposes.

This report is devoted to expanding dialogue on these three tasks. **Chapter One** discusses the importance of discriminating between knowledge and information, while **Chapter Two** outlines the growing requirement for knowledge management and looks at current information strategy, in particular, the pitfalls of concentrating exclusively on information and technology in the competitive environment of the twenty-first century. In **Chapter Three**, on strategic knowledge operations (SKO), a doctrinal basis is proposed for the role of knowledge in the context of national power. This chapter focusses on ends and means; defines the role of SKO in managing collective knowledge (CK), and introduces the concept of collective knowledge activities (CKA) as a critical part of SKO. **Chapters Four** and **Five** further expand on the ideas of CK and CKA as models for developing operational strategies and tactics for implementing knowledge management. **Chapter Six** offers suggestions for blazing the way ahead.

Chapter One

Introduction

All around us, information is moving faster and becoming cheaper to acquire, and the benefits are manifest. That said, the proliferation of data is also a serious challenge, requiring new measures of human discipline and skepticism. We must not confuse the thrill of acquiring or distributing information quickly with the more daunting task of converting it into knowledge and wisdom. Regardless of how advanced our computers become, we should never use them as a substitute for our own basic cognitive skills of awareness, perception, reasoning, and judgement.

David S. Benehume[1]

The essence of international competition and competitive activities is knowledge management. Nations, like individuals and businesses, compete on the basis of their ability to create and use knowledge, which makes knowledge management as important as the management of other national resources. Some knowledge and expertise are needed simply to survive or to achieve parity with the competition, but certain critical capabilities can distinguish a nation from among others. One of these is the ability of its security apparatus to provide decisionmakers with a rich selection of diverse, innovative, valid responses to competitive pressures across the spectrum of conflict, from waging peace to waging war, and to do so rapidly. This ability is contingent on how well the government and its agents manage and appropriately apply the nation's collective knowledge.[2]

Why make knowledge management explicit? Why discriminate between knowledge, information, and data? All are produced and maintained by different processes (see **Table 1-1)**. All are important both to making time-sensitive decisions and to distinguishing between knowledge that is readily available to decisionmakers and information that requires processing and resources to prepare it for use. Second, knowledge costs; learning costs.[3] The costs are a major source of the value of knowledge and of the overall cost of day-to-day national security operations (see **Figure 1-1**).[4] People must assimilate information into their minds before they can

---

[1]David S. Benehume, Technorealism, MEME 4.02, [On-line]. URL: http:/memex.org/meme4-02.html (Accessed March 11, 1998.), 3.

[2]Here collective knowledge represents the totality of the knowledge a nation can marshal and mobilize to create an advantage over competitors. See Chapter Three.

[3]A compelling illustration of these costs is the hundreds of thousands of staff hours and the millions of dollars the DOD alone spends every year to compose, present, and understand slide presentations.

[4]Thomas H. Davenport and Lawrence Prusak, who reach the same conclusion from a slightly different tack, point out that "one of the reasons we find knowledge valuable is that it is close and closer than data or information to action."

Table 1-1

Working Definitions of Wisdom, Knowledge, Information, and Data

- *Data* consist of measurements or observations of the environment. They are discrete and static. Each datum is a "snapshot in time."
- *Information*, which is composed of data, describes the environment. Even if information consists of only a single datum, it is always the result of correlation, inference, and interpretation. Like data, information is static. It must be recorded in some form of memory, or it reverts to the component data.
- *Knowledge* is a representation or model of the environment. Knowledge is created and exists only in the mind, and it changes continually. It is synthesized from information, context, and the decisionmaker's judgment. It contains much less information than the environment it represents and permits a working perception of that environment in the absence of perfect information. When recorded, knowledge reverts to a static state as information. Because no two persons have identical contexts, when knowledge passes from one person to another, it is always transformed—it becomes new knowledge.
- *Wisdom* is the human ability to select relevant information and apply knowledge to human affairs through decision or action. Wisdom implies sound judgment and the consideration of risks. Wisdom derives from creating and using knowledge.

use it to decide or to act. The process can be as simple as comprehending a single fact or as complicated as determining the domestic implications of an economic crisis in a region on the other side of the world. There is always a learning cost in time, money, and physical resources, a cost proportional to the timeliness and complexity of the knowledge required.[5] Learning is so intuitive and natural a part of human activity that it may well be taken for granted and its costs overlooked, excluding the costs of formal education and training.[6] Last, a common practice in the U.S. national security community has been to refer to all steps of knowledge development generally as "information management." This practice, however, obscures the relative costs and value of the products of each step, and confusion about what data, information, and knowledge mean and has resulted in enormous expenditures on technology that rarely delivers what was

---

See Davenport and Prusack, *Working Knowledge: How Organizations Manage What They Know* (Boston: Harvard Business School Press, 1998), 6.

[5]Learning cost, as used here, includes the rediscovery of relevant information and data beyond initial discovery or collection. Depending on the way information may be organized, and the number of people who need it, rediscovery cost may significantly inflate the learning cost.

[6]DOD 8000-series acquisition directives, some of the most comprehensive information policies in the national security community, are fuzzy about the role of knowledge in decisionmaking. In one directive knowledge and data are defined as types of information, although knowledge is noticeably absent from Policy subparagraph 4.1.2, which states, "Data and information shall be corporate assets structured to enable full integration and interoperability across DOD activities." See U.S. DOD Directive 8000.1, Subject: Defense Information Management Program (ASD(C3I), Oct. 27, 1992, 11, 2.

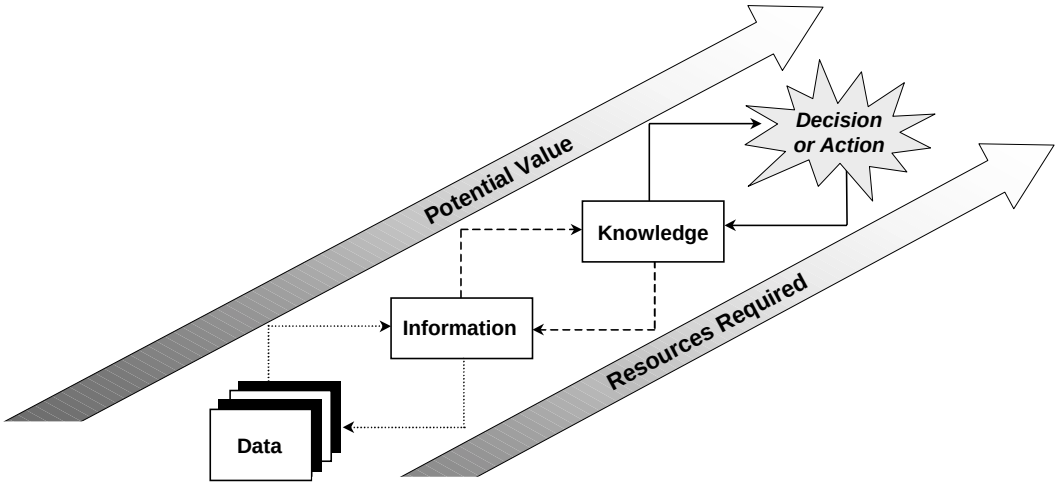

Figure 1-1

Relationship of Data, Information, and Knowledge

expected.[7] Insufficiently specific terminology produces unclear communication and leads to ineffective command and control. Imagine the state of national security were only the general terms “weapons,” “diplomacy,” and “intelligence” used for all products and phases of national security operations.

The definitions given in **Table 1-1** provide means to developing clearer insight into the processes that produce knowledge, information, and data as well as the fiscal and operational arguments for explicitly managing collective national security knowledge. They anchor the doctrinal, strategic, and tactical concepts proposed here.

[7]Thomas H. Davenport and Lawrence Prusack, *Working Knowledge: How Organizations Manage What They Know* (Boston: Harvard Business School Press, 1998), 1.

Chapter Two

The Need for Knowledgecraft in the Twenty-First Century

What we must remember is that this new information technology is only the pipeline and storage system for knowledge exchange. It does not create knowledge and cannot guarantee or even promote knowledge

Thomas H. Davenport and Laurence Prusak[1]

Information is an explicit component of national security strategies in the 1990s.[2] The main objectives of these strategies are to deny competitors access to information, collect intelligence, improve the accuracy of weapons targeting, and maintain for the United States freedom of access to its own information. The overarching approach to executing these strategies has been the development and deployment of advanced information technologies.

Why, then, in spite of the United States's strength in information technology, has this technology-driven approach not met expectations of national security planners and developers[3] nor, as Barry Watts has pointed out,[4] substantially reduced the friction of competitive decisionmaking? First, the objectives of this approach are fundamentally flawed. Merely possessing technology and access to information does not guarantee decisionmakers a significant competitive advantage. Second, changes in the global competitive environment are eroding many of the advantages of owning information technology. Last, the effectiveness of traditional processes of command and control is declining, in spite of efforts to bolster these processes with modern information technologies.

2.1 Technology-Driven Strategy, Problem-Driven Decisionmakers

An unintended consequence of information- and technology-driven strategies is the current general emphasis on the production, storage, and movement of information; the results—a

---

[1]Thomas H. Davenport and Laurence Prusak,, *Working Knowledge: How Organizations Manage What They Know* (Boston: Harvard Business School Press, 1998),18.

[2]See, for example, William J. Clinton, *A National Security Strategy for a New Century* (Washington, D.C.: The White House, 1997), 14; Office of the Chairman, Joint Chiefs of Staff, *Joint Vision 2010* (Washington, D.C.: Chairman, Joint Chiefs of Staff, Pentagon, [1996]), 13, 16; William S. Cohen, *Report of the Quadrennial Defense Review* (Washington, D.C.: Dept. of Defense, May 1997), 14-17; The Joint Chiefs of Staff, *C^4 for the Warrior* (Washington, D.C.: The Pentagon, January 1998), 2-21.

[3]For example, preliminary estimates of on-line collateral intelligence use are well below expected rates, on the basis of the number of registered users. Interview by the author with James P. Peak, Director, Intelink Management Office, May 26, 1998.

[4]Barry D. Watts, *Clausewitzian Friction and Future War* (Washington, D.C.: Institute for National Strategic Studies [INSS], National Defense University [NDU], McNair Paper 52, 1996), 119-120, 122-123.

preoccupation with (empty) formats and processes as well as relatively primitive substance compared with the requirements of decisionmakers. The physical characteristics of information are incidental: It is inedible, offers no direct protection, and probably cannot be traded in a way that would contribute significantly to national security.

Decisionmakers are primarily problem-driven; they generally prefer substantive information marshalled and mobilized according to particular problems or options. Decisionmakers cannot realize the potential of information until they assimilate information as knowledge. A weak and tacit assumption of the technology-driven approach is that decisionmakers will provide the resources to cull and concentrate weak information substance from many sources to attain knowledge usable for decisions and actions. In the context of modern global competition, this is like sending boxes of powder, casing, and bullets to soldiers and assuming they have the time and wherewithal to assemble their ammunition reliably while performing their primary warfighting duties.

An unintended consequence if technology-driven information strategies is the tendency to organize information for "wholesale" consumption, yet problem-driven users usually want information culled, sorted, and packaged for "retail" consumption. For example, in a foreign political crisis that might require emergency evacuation of personnel, planners need competitive knowledge of the crisis in order to develop courses of action and make valid recommendations to decisionmakers. Planners need all types of information bundled to create a picture of the environment of the crisis situation, such as diplomatic constraints, status of transportation assets, possible threats, port and airfield information, medical status of evacuees, available communications, weather forecasts, among others. Unfortunately, national security information traditionally is bundled according to the following:

- the organization that provides the information (e.g., Defense Intelligence Agency, Department of State, Defense Information Systems Agency, regional unified command, among others);
- the type of data from which the information was interpreted (e.g., imagery intelligence or signals intelligence, for example); and
- the type of analysis that produced the information (e.g., geopolitical, economic, historical, for example).

If planners are not knowledgeable about potential information-producing organizations and their processes, they can spend more time wandering through the warehouses searching for useable information than dealing with the crisis.[5]

[5]An alternative often used is to train local liaisons from each information provider to perform "information shopping," which reduces the burden on planners but increases both staff size of decisionmakers and overhead costs.

2.2 In the Future, the Competitive Advantage Will Belong not to Those Who Have Technology But to Those Who Use It Best

The global conditions that made a technology-centered strategy viable are, as of mid-2000, in flux, and, clearly, three trends are weakening that strategy: broadening of the spectrum of competition, diffusion of information technology, and global dispersion of resources.

The growth of Asian economies beginning in the early 1980s expanded global competition. The loss of U.S.–Soviet bipolar competition, once a stabilizing factor, has increased global interdependence. Multinational activity now envelops international issues; leaving stand-alone military, economic, or political actions little probability of achieving most foreign policy objectives. Competing in this environment requires a toolkit filled with innovative and integrated responses for each situation, especially with widely varying capabilities among competitors. Competitors may seek asymmetric measures, such as the use of weapons of mass destruction (WMD), terrorism, political-cultural or technical means to counter perceived U.S. strengths, in particular military strength.[6]

Influencing competitors in ways that deter or mitigate asymmetric countermeasures requires both collective and distributed problem solving abilities, which themselves require systems both for continual sensing and feedback and the capacity to adjust the mix and intensity of actions as often as necessary. Filling and maintaining the United States's foreign policy toolkit with appropriate responses requires the national security community to collect and interpret vast quantities of data and to help decisionmakers at all levels rapidly assimilate information. Even after desired effects are achieved, unintended secondary effects may occur, which may not show up for years and which require long-term follow-up and analysis. Modern U.S. political, economic, and military strategies are therefore highly knowledge-dependent, and control structures, intelligence techniques, weapon applications, and sanction concepts envisioned by 2025 will be even more dependent.[7]

Although much of the strength of a technology- and information-centered strategy has derived from an almost total domination of advanced information technology industries by the West and its Asian allies, that dominance is waning as the twentieth century draws to a close. Technologies, particularly information technologies, are being disseminated globally. Kenneth Allard noted that the "information revolution may be remembered [mainly] for equalizing power between have and have-not countries."[8] In the late 1990s, much unclassified government and

---

[6]Clinton, 12.

[7]Gary Clyde Hufbauer and Elizabeth Winston, of the Institute for International Economics, provide insight into the knowledge needed to employ economic sanctions as "smart weapons" in "Smarter Sanctions: Updating the Economic Weapon," *National Strategy Review* **7**, 2 (1997), [On-line]. URL: http://www4.interaccess.com/strategy/v7n2ft1.htm (Accessed Jan. 10, 1997.)

[8]Allard, 233.

technical information and ideas are available to anyone with Internet access.[9] In the future, a competitive advantage will accrue not to those who have information or technology but to those who use them best. The United States can to some degree slow the dispersion of technology, but in an increasingly interconnected world, largely created by the West, regulating the diffusion of technological information has become difficult and is made more so by economic pressure on technology-producing nations to export products to sustain their industries' growth.[10]

The importance of finding new ways to acquire and apply knowledge will only grow in the twenty-first century, while control over other sources of national power—i.e., territory, population, economic product, manufacturing output, and "military manpower"—will increasingly be dispersed among competitors. According to Samuel P. Huntington:

> The West's control of these resources peaked in the 1920s and has since been declining irregularly but significantly. In the 2020s, a hundred years after that peak, the West will probably control about 24 percent of the world's territory (down from a peak of 49 percent), 10 percent of the total world population (down from 48 percent) and perhaps 15–20 percent of the socially mobilized populations, about 30 percent of the world's economic product (down from a peak of probably 70 percent), perhaps 25 percent of manufacturing output (down from a peak of 84 percent), and less than 10 percent of global military manpower (down from 45 percent).[11]

The efforts of other nations to reduce the U.S. hegemony more and more limit the United States's ability to use its national power resources (listed in the previous paragraph) internationally. In strengthening collective management through organizations such as the United Nations, other nations can reduce the possibility of U.S. unilateral options and thereby themselves gain advantage.[12]

---

[9]Two examples are the National Technical Information Service (NTIS) and Govbot. NTIS, operated by the U.S. Department of Commerce, at URL: http://www.ntis.gov , lists more than three million titles in technical information, available to the world at reasonable prices. The Govbot database, operated under contract by the Center for Intelligent Information Retrieval (CIIR), at URL: http://ciir.cs.umass.edu/ciirdemo/Govbot, provides links to more than 60,000 federal government and military Web sites.

[10]Samuel P. Huntington, *The Clash of Civilizations and the Remaking of World Order* (New York: Touchstone, 1996), 87-88. Alan M. Webber refers to this effect as "the self-canceling technological advantage"; see Webber, "What's So New About the New Economy?" *Harvard Business Review* (January–February 1993), 27.

[11]Huntington, 90-91.

[12]See Richard F. Staar, *Russia's National Security Concept*, in *Perspective* **8**, 3 (January–February 1998), 5-6; Chandler Rosenberger, "Moscow's Multipolar Mission," *Perspective* **8**, 2 (November–December 1997), 4-6.

2.3 The Declining Effectiveness of Traditional Command and Control

Although the strength and agility with which to apply tools of national power are increasingly attained through management of knowledge,[13] U.S. national security bureaucracies continue to function as their predecessors did, using information technology in support of decisionmaking, as was true a century ago, primarily to automate manual processes.[14]

Advances in military information operations since the early 1970s have led to such gains in precision and speed of military operations that the amount of information processing required to use modern, high-performance military forces to the full threatens to overwhelm the resources of traditional command-and-control organizations and systems. Several trends have led to this point:

- precision weaponry and advances in intelligence, surveillance, and reconnaissance;
- advances in information technology, global media, and increasing computer literacy;
- expeditionary strategies, rapid response requirements, decentralized execution;
- increased costs and decreased risk tolerance; and
- joint and coalition military operations and diplomacy.

By most indications, these trends will continue, and pressure on command-and-control structures will increase.

According to James Beniger, the "control crisis" is not the result of revolution:

> microprocessing and computing technology, contrary to currently fashionable opinion, do not represent a new force only recently unleashed on an unprepared society but merely the most recent installment in the continuing development of the Control Revolution. This explains why so many of the components of computer control have been anticipated, both by visionaries like Charles Babbage and by practical innovators like Daniel McCallum,[15] since the first signs of the control crisis in the early nineteenth century.[16]

---

[13]Pierre Lévy uses "collective intelligence," but in the realm of national security operations the meaning of "intelligence" is narrower. See Lévy, *Collective Intelligence: Mankind's Emerging World in Cyberspace*, trans. Robert Bononno (New York: Plenum Trade, 1997), 1-2.

[14]I am indebted to James Beniger for this insight; see Beniger, *The Control Revolution: Technological and Economic Origins of the Information Society* (Cambridge, Mass.: Harvard University Press, 1986), 390-433.

[15]McCallum, superintendent of the Erie Railroad in the 1850s, was one of the first to appreciate and document the breakdown of control that results when a system exceeds its span of control.

[16]Beniger, 435.

Command-and-control and bureaucratic structures are firmly rooted in nineteenth-century technology,[17] which worked well so long as commanders and staffs had time to organize and assimilate information. The expansion of militaries in the past two hundred years has posed a fundamental problem: how to command and control forces beyond one's sight. That problem was compounded in the twentieth century by increased use of aircraft, indirect-fire and directed-fire weapons, and increasing speed of combat units and increasing distances between them, all of which will only increase in the twenty-first century. A commander can no longer see at one glance either the enemy or the forces commanded.[18]

In the past, the response to the growing volume and complexity of information was to create ever larger command staffs equipped with more and more information technology. In the 1970s, military information operations focussed on automating separate weapons and support functions; the 1980s saw a significant effort to improve communications and link automated functions to form joint, integrated, and automated processes; and in the 1990s, improvements in microprocessors and digital communications accelerated automation of command-and-control operations. The underlying control structures and methodology, however, remained the same.[19] Through thirty years of development, the mobility, autonomy, and accuracy of conventional weapons increased steadily, while the overall autonomy of the forces employing the weapons changed little.[20]

In the late 1990s, the complexity of high-performance military forces puts them beyond the control of either individuals or hierarchical management systems. The increasing occurrence of combat in urban areas requires highly mobilized knowledge about the inhabitants, that is, the occupants of buildings and local infrastructure. The popular asymmetric countermeasure of locating military targets near sensitive civilian facilities stresses the ability of traditional staffs to create timely, effective targeting solutions. Twenty-first century weapons like the Airborne Laser anti theater ballistic missile system, and space based laser systems will engage fleeting targets at the speed of light. They will require scrupulous marshalling and continual monitoring of all knowledge and information affecting the rules of engagement. Finally, just as the United States came to understand that the economy is essentially collectively controlled and therefore beyond long term manipulation by individuals, so it is coming to see that predicting the effects of force,

---

[17]Beniger, 433-435. Lévy notes that it was through the creation of writing society entered the stage of command and control evolution. Written language increased the efficiency of communication and accommodated the organization of human beings into groups much larger than speech alone would have allowed. The price, however, was the division of workers into administrators and specialists in information processing, on the one hand, and, on the other, administered individuals and users of information. See Lévy, xxviii.

[18]George and Meredith Friedman, *The Future of War: Power, Technology, and American World Dominance in the 21st Century* (New York: Crown Publishers, Inc., 1996), 37.

[19]There have been changes within tactical units, notably structures based on "control by negation," but, in general, strategic and operational command and control have remained hierarchical.

[20]Allard, 234.

sanctions, or aid designed to change behavior is not possible in a large, complex system.[21] "There always appear to be second-, third-, and fourth-order implications that were never part of the original plan."[22]

2.3.1 Toward Collective Capabilities

Beginning in the 1960s, analysts, diplomats, and military personnel found it increasingly difficult to inherit the "traditions of the trade," that is, to exercise an enduring professional identity within one's particular functional stovepipe. Technologies changed rapidly, and learning how to regulate and reorganize one's activity continuously, on the basis of comparison and communication with members of other disciplines, grew urgent and gradually created the "perception of computing and communications as bundled inextricably into computing-and-communications processes, *compunications* processes for short."[23] The evolution of "compunications" completely altered traditional knowledge and information pathways by interconnecting computers and storage systems via satellites, telephone lines, and digital transmission networks, greatly expanding the potential for elements of knowledge to be connected regardless of their organizational or disciplinary affiliation or location.[24]

By the late 1980s and early 1990s, initiatives such as C^4I (command, control, communications, computers, and intelligence) for the Warrior, Intelink, and TENCAP were exploring ways to make information more widely available. Data and information previously transmitted through decisionmaking hierarchies began to flow through digital networks directly to end users, often uncorrelated and with little or no preprocessing or analysis. This direct flow of information assumed that individuals had considerable skill in subjective decisionmaking and collective problem solving. Omnidirectional communication—up, down, and across disciplines—stripped away anonymity. No longer was it sufficient to identify oneself as a nameless member of a military service, technical specialty, or community. Now one's personal identity and judgement were implicated in professional life. It is precisely this form of knowledge mobilization, highly

---

[21]According to Robert E. Lucas's hypothesis of rational expectations, individual actions and government policy to stabilize or change the economy have no effect and can even make matters worse; see his *Rational Expectations and Econometric Practice* (Minneapolis: University of Minnesota Press, 1981). See also John L. Peterson, "Information Warfare: The Future," in *Cyberwar: Security, Strategy, and Conflict in the Information Age*, edited by Alan D. Campen, Douglas H. Dearth, and R. Thomas Gooden (Fairfax, Va.: AFCEA International Press, 1997), 174-175.

[22]Peterson, 174-175.

[23]"Once upon a time people perceived computing and communications processes as distinctly independent from one another." See Anthony G. Oettinger, "The Abundant and Versatile Digital Way," in *Mastering the Changing Information World*, edited by Martin L. Ernst (Norwood, N.J.: Ablex Pub. Corp., 1993), 85. See also Anthony G. Oettinger, Ithiel De Sola Pool, Alain C. Enthoven, and David Packard, "Compunications in the National Decisionmaking Process," in *Computers, Communications, and the Public Interest*, edited by Martin M. Greenberger (Baltimore, Md.: The Johns Hopkins Press, 1971), 74.

[24]Lévy, xx.

individual as well as cooperative, that the traditional bureaucratic system was incapable of generating and often tried to prevent.[25]

As the United States increasingly relies on integrated application of its national tools of power, the technology- and information-focussed decisionmaking bureaucracy meets greater difficulty in generating the quantity and quality of innovative responses required. Because integrated application of economic, political, cultural, and military power is increasingly a collective, cumulative effort whose results must be taught and diffused, it also requires improved methods of distributing and assimilating information. The difficulty is that bureaucratic command-and-control hierarchies and hierarchical network technologies that can only partially mobilize and coordinate information and knowledge are ingrained in the culture and values of the U.S. business and national security communities and thus are slow to change.[26] For this reason, the development of new ways of thinking and negotiating engendered by the growth of genuine collective action becomes particularly urgent.[27]

2.4 The Need for Knowledgecraft

Every problem or crisis of national security tests the United States's collective knowledge and its ability to share that knowledge. With luck, in a crisis the government can quickly locate people with relevant knowledge and information and can spend its limited time assembling teams, assessing the substance of the information, and developing solutions. As is often the case, however, precious time is wasted fussing with formats and processes, putting information into the context of the particular problem, finding out who knows what, and settling for the first solution to appear.[28] How can the U.S. national security community spend less time figuring out what it knows and dedicate more time to applying its knowledge?

Ideally, decisionmakers and their staffs would be able to find all the knowledge and sources of information relevant to their inquiry preprocessed, categorized, catalogued, indexed, and presented in a convenient way that facilitates quick assimilation, yet an effective knowledge-sharing and reuse capability potent enough to supply a competitive edge requires explicitly stated

---

[25]Ibid., 3.

[26]Dorothy Leonard-Barton, in *Wellsprings of Knowledge* (Boston: Harvard Business School Press, 1995), discusses the challenges involved in modifying and "re-operationalizing" organizational and cultural values; see 24-27, 50-57.

[27]Lévy, xxiv-xxv.

[28]A casual examination of government information networks reveals that very little information or knowledge ordinarily is organized across the national security community. This condition forces users to jump inefficiently from source to source searching for possible nuggets of information or expertise to help solve their problems. Knowledge at each source tends to be organized in the jargon of the activity that created it, further complicating the user's task. See William M. Arkin, *The U.S. Military Online: A Directory for Internet Access to the Department of Defense* (Washington, D.C.: Brassey's, 1997), xii.

and accepted concepts of how national security knowledge is organized, used, and shared as well as a high level of trust in the national security community's ability to work collectively.

Sharing knowledge and developing trust are effective when individuals and organizations are united by shared doctrine, common operational strategies, and standard tactics.[29] Common doctrine and shared tactics can define the vocabulary for the exchange of queries and assertions about knowledge.[30] Commercial knowledge management services find that a common vocabulary is effective when developed from the viewpoint and context of those using the information and knowledge, rather than those supplying it.[31] This finding implies that those who develop and use national security knowledge have a responsibility to develop and disseminate knowledge management doctrine and tactics—not those who develop the technology.

Although joint warfighting doctrine contains some limited, common information management vocabulary, among national security organizations formal knowledge management doctrine does not exist.[32] The lack of general doctrine and operational employment concepts for knowledge management may well be a major reason for the paucity of rigorous operational requirements to guide developers and investment. Fortunately, an extensive body of well-developed doctrine exists to guide the application of economic, diplomatic, and military forms of national power. In **Chapter Three** these preexisting doctrinal models are used to propose a foundation for the development of knowledge management doctrine. **Chapters Four** and **Five** follow up with suggested operational concepts for thinking about and designing strategic knowledge operations.

---

[29]Davenport and Prusak (98-99) point out that shared vocabulary may be the most important benefit of all.

[30]*Ontology* is a term frequently used by researchers in knowledge management and artificial intelligence (AI) for such a common concept. Borrowed from the branch of philosophy of that name, which deals with the nature and relations of being, ontology is used here inn a limited sense to mean "how we think about what we know.". Ontological commitments are agreements to use the shared vocabulary in a coherent and consistent manner. For an extensive and detailed definition, see Tom R. Gruber, *What Is Ontology?* [On-line]. URL: http://www-ksl.stanford.edu/kst/what-is-an-ontology.html (Accessed March 18, 1998.) Also, Tom R. Gruber, *Knowledge Sharing Papers*, [On-line]. URL: http://www-ksl.stanford.edu/kst/what-is-an-ontology.html (Accessed March 18, 1998.)

[31]Interview by the author with Srinija Srinivasan, Chief Ontologist, Yahoo! Inc., March 11, 1998; interview by the author with Mark Kraatz, Manager, Corporate Web Systems, Open Text, Inc., March 27, 1998.

[32]A limited effort toward a common vocabulary has concentrated on data standardization within the DOD. See the DOD, *Data Standardization Procedures (Draft)* (Washington, D.C.: Office of the Assistant Secretary of Defense, Command, Control, Communications, and Intelligence, DOD 8320.1-M-1, November 1996).

Chapter Three

Strategic Knowledge Operations

If you know the enemy and yourself, you need not fear the result of a hundred battles.

Sun Tzu[1]

Think first, fight afterwards—the soldier's art.

Robert Browning[2]

Reality is messy.

John L. Peterson[3]

3.1 The Nature of Strategic Knowledge Operations (SKO)

All nations engage in knowledge building, to a greater or lesser extent, but creating, sustaining, and using competitive knowledge requires a broad and intuitive understanding of the role of information and knowledge in global competition and of the means by which they are applied. This understanding needs to be ingrained in the culture and values of the national security community and needs to form the foundation for joint and interdepartmental operations among all national security activities.[4]

3.1.1 SKO Defined

SKO are the broad activities whereby nations manage their affairs.[5] Every nation seeks the knowledge that will permit it to secure cooperation, promote its interests, and, when necessary,

---

[1]Sun Tzu, *The Art of War*, edited by James Clavell and trans. Lionel Giles (New York: Delacorte Press, 1986), 16.

[2]Robert Browning, "Childe Roland to the Dark Tower Came," *Poems of Robert Browning* (Boston: Houghton Mifflin, 1956), 162-168, 165, l. 89.

[3]John L. Peterson, "Information Warfare: The Future," in *Cyberwar: Security, Strategy, and Conflict in the Information Age*, edited by Alan D. Campen, Douglas H. Dearth, and R. Thomas Gooden (Fairfax, Va.: Armed Forces Communications and Electronics Association (AFCEA) International Press, 1997), 175.

[4]The 1989 version of Fleet Marine Field Manual 1 (FMFM 1) provides a model of readability without technical jargon that is used here as a framework for this chapters and Chapter Four. Although many of the sources cited in these chapters, including FMFM 1, focus on only one type of international competition—war—where appropriate, conclusions or statements from those sources are extrapolated and applied to international competition in general.

[5]Nation as used here includes both state and nonstate actors. It primarily signifies a political body, a people united under independent government or common leadership without regard for their origins, and, secondarily, denotes institutional ties, a community of economic and cultural interests.

impose its will on competitors. Each nation's environment consists of the complex combination of natural, human-made social and political conditions and events that affect its growth, development, and survival. The ultimate use of a nation's knowledge is to shape its environment, through innovation, decision, and action.

The objective of SKO is the execution of national strategies. That objective is achieved by monitoring environmental conditions, discovering viable responses to observed conditions, and recommending appropriate instruments of national power as well as facilitating their controlled application.

- With respect to political power, SKO are the means by which a nation secures the cooperation of partners and reconciliation with competitors through negotiation, treaties, and agreements.
- With respect to military power specifically, SKO are the means by which the United States orchestrates the application (or threat) of violence, enforcement, or aid. They enable the government to select appropriate combinations of military forces, insure that these forces make effective transitions to a place and time of the leadership's choosing, and focus their actions to compel competitors toward reconciliation.[6]
- With respect to economic power, SKO are the means by which the United States achieves national objectives through the selection and application (or threat) of economic incentives and deterrents.
- With respect to cultural power specifically, SKO are the means by which the United States advances its national interests through selective dissemination and encouragement of its culture. Domestically, SKO recognize and reward cultural values that enhance national competitiveness and discourage behavior that threatens national security.
- With respect to collective knowledge (CK), SKO are the means by which a nation develops, marshals, and mobilizes its CK. Successful execution of national strategy depends on a nation's capability for using its CK to interpret conditions correctly and respond appropriately through other instruments of national power. CK capability is most critical when a nation has no significant or other resource advantage over its competitors.

All nations desire self-determination and prosperity. To this end, they cooperate and compete with others for security and resources. As nations compete in peace, crisis, or war, they seek ways to influence rivals by applying, sharing, or withholding knowledge.

[6]Although the characteristics of war, its potential for violence and the directness of casualties, merit consideration, war remains part of the spectrum of international competition and is not isolated in some clearly defined space and time. It has both epilogue and prologue.

3.1.2 Complexity

SKO, thus outlined, appear simple. Knowledge, however, is a state of mind. It is created in the mind by a complex synthesis of context, information, and judgment,[7] so that, by its nature, it is transient, subjective, imperfect. Complexities may appear even in what otherwise seem simple situations. The complexity of SKO is a primary source of what Clausewitz called friction, "the force that makes the apparently easy difficult."[8]

SKO are nonlinear, which means that outcomes can neither be predicted nor easily understood by adding together the potential results of separate actions any of which may lead to unintended consequences.[9] The knowledge in the mind of a decisionmaker is rarely equal to the sum of its parts nor easily recognizable as a combination of those parts. This characteristic is at once a source of strength and weakness. Countless historical examples exist in which carefully developed and applied knowledge enabled leaders and nations to prevail against equal or more powerful rivals—and countless examples of where poorly prepared, ignored, or missing knowledge resulted in catastrophe.[10]

Understanding the limitations of imagination is important. Linearity is excellent for systems designed to behave predictably but offers only a narrow window on most natural and social systems. Narrowness puts blinders on the perception of reality and offers a weakness for an opponent to exploit. Understanding individual and collective limitations can minimize the extent and duration of surprise and help the nation to be more successfully adaptive amid changing

---

[7]Lévy, 14.

[8]Carl von Clausewitz, *On War*, ed. and trans. Michael Howard and Peter Paret (Princeton, N.J.: Princeton University Press, 1976), 121.

[9]As a result, even simple systems often display complex, nonlinear relationships. When dealing with a nonlinear system, especially one that is complex, it is not sufficient to analyze its parts or aspects and then combine those analyses in an attempt to describe the entire system. This approach alone does not offer a way to understand the behavior of the entire system. The French mathematician Poincaré demonstrated more than a hundred years ago the effects of nonlinearity in simple systems by showing that the motion of as few as three bodies (the sun, the moon, and the earth) defies exact solution. The German physicist Werner Heisenberg, founder of quantum mechanics and famous for his uncertainty principle, showed that determining the position and momentum of a simple subatomic particle (such as the electron) with arbitrarily high accuracy is impossible. The effect of this principle was to convert the laws of physics into statement about relative, rather than absolute, certainties. The American computer scientist Walter Brooks described software as more complicated than other artifacts constructed by human beings. The number of possible states for software combined with unintended reactions among its parts and with hardware all make finding potential sources of error improbable. When grappling with the desire to model global "compunication" networks of hundreds of thousands of nodes, these anecdotes provide a useful caution.

[10]The most frequently cited cases are the Japanese attack on Pearl Harbor in 1941 and the Bay of Pigs incident in 1961.

circumstances. Thinking constructively about nonlinearity may lead to the ability to design more robust systems when needed.[11]

In practice, on one hand knowledge operations are difficult because of the complexity of both the environment the nation seeks to shape and the opponents the nation wants to influence. The nation's competitors, it is important to keep in mind, are not inanimate objects but nations and organizations with independent forces of will. Opponents seek to resist the will of the United States and to impose their own on it. Allies and partners seek to bend the efforts of the United States toward achieving their own goals. On the other hand, complexity may be self-begotten by such predicaments as unclear goals, incorrect or unavailable information, inflexible or complex task organizational structures, or uncooperative organizational relationships.

Although striving to minimize needless complexity is important, what is more important is to embrace complexity as a fact of life and operate effectively within it. The means to mitigate complexity is human will. Members of the national security community must recognize complexity of knowledge development, persevere to understand it, and resist the temptation of artificial simplicity and the resultant blind spots in knowledge.[12]

3.1.3 The Certainty of Uncertainty[13]

A main source of friction in planning, decisionmaking, and action is the uncertainty of knowledge.[14] The nature of knowledge makes absolute certainty impossible. Even though uncertainty may be reduced by refining accuracy and resolving unknowns, it remains true that the context constantly changes and that the elimination of uncertainty is never possible.

Uncertainty invariably involves an estimation and acceptance of risk. Risk, inherent in life, is involved in every aspect of competition. It implies the possibility of potential gain, and, ordinarily, the greater the potential gain the greater the risks involved. Further, risk is equally common to action and inaction. Competing in an ever-changing world entails a willingness to accept reasonable risk, but it also entails a clear understanding that accepting risk means striking

---

[11]Alan D. Beyerchan, "Clausewitz, Nonlinearly, and the Importance of Imagery" in *Complexity, Global Politics and National Security* (Washington, D.C.: NDU Press, 1997), 168.

[12]"Although it is tempting to look for simple answers to complex problems and deal with uncertainties by pretending they don't exist, knowing more usually leads to better decisions than knowing less, even if 'less' seems clearer and more definite. Certainty and clarity often come at the price of ignoring essential factors. Being both certain and wrong is a common occurrence" (Thomas H. Davenport and Laurence Prusak, *Working Knowledge: How Organizations Manage What They Know* [Boston: Harvard Business School Press, 1998], 9).

[13]This heading is taken from the subtitle of Anthony G. Oettinger's *Whence and Whither Intelligence, Command, and Control? The Certainty of Uncertainty* (Cambridge, Mass.: Harvard University Program on Information Resources Policy, P-90-1, February 1990).

[14]Barry D. Watts, *Clausewitzian Friction and Future War* (Washington, D.C.: NDU Press, INSS, McNair Paper No. 52, 1996), 120.

a balance between waiting to learn more and more about a situation and acting in time to do something about the situation. The ability to maintain this balance implies a high standard of subjective judgment among all decisionmakers involved and a prudent unwillingness to gamble on the success of a single, highly improbable event.

Risk involves the ungovernable element of chance, a universal component of competition and a constant source of complication. Chance is a turn of events that cannot reasonably be predicted and over which none of the competitors has control. Chance favors the competitor best prepared to assess opportunities in a situation quickly, devise viable alternative responses, and deal with the situation accordingly.[15]

3.1.4 Cultural and Human Factors

Decisionmakers use three attributes to evaluate information: confidence, significance, and accuracy. Confidence in the information determines how to use it to weigh risk. Without confidence in information or its source, a decisionmaker will not include that information when developing knowledge, no matter how significant or accurate it may be.[16] Decisionmakers determine the significance of information by its relevance and timeliness. The decisionmaker considers accuracy last. Accuracy of information is important for calculating risks and probabilities, but without confidence and significance, accuracy means nothing.

The effectiveness of SKO is affected by the ability of decisionmakers to access knowledge and assimilate information. A critical factor in planning and executing decisive competitive actions, particularly military actions, is the robust ability to exploit quickly and confidently the knowledge at one's immediate disposal. People will choose to use the information at hand, rather than deal with the effort and uncertainty involved in trying to discover a better source.[17] Information and knowledge not easily accessible to decisionmakers or planners are irrelevant, especially when decisionmakers have limited supporting staff.

---

[15]In his analysis of Scharnhorst and Clausewitz, Watts points out that "The positive aspects of the solution to the play of chance in war deserve special emphasis"; ibid., 24-25. This statement is expanded here to include all competition.

[16]Davenport and Prusak, 100-101. "Knowledge is the most sought after remedy for uncertainty"; ibid., 25. See also, Amos Kovacs, "Using Intelligence," *Intelligence and National Security* **12**, 4 (1997), 146-148.

[17]According to Davenport and Prusak, "Studies have shown that managers get two-thirds of their information and knowledge from face-to-face meetings or phone conversations. Only one-third comes from documents" (12). See also Thomas H. Davenport, "Saving IT's Soul: Human-Centered Information Management," *Harvard Business Review* (March–April 1994), 121.

3.1.5 Adaptiveness

Effective SKO are integrated and adaptive.[18] The United States largely relies on governmental and government-sponsored organizations to respond appropriately on its behalf.[19] To do so in changing environmental conditions, organizations tend to orient themselves so that they are receptive to innovation and knowledge networks.[20] Changes in SKO are driven by both internal and external competitive pressures on these organizations.[21]

The demand for knowledge follows networks of "knowers," not technical architectures or the management hierarchy. People with useful knowledge sit at all levels of organizations.[22] Architectures and reporting structures either adapt to change, at some point becoming significantly different from their original incarnations, or fail to adapt and disappear. SKO benefit from hierarchies and architectures that are able to shift on the basis of who knows what and how helpful they are.

Knowledge that cannot be focussed on a problem is useless, and inaccessible information is irrelevant. Without confidence in or access to knowledge, competitive organizations will create or cultivate their own knowledge-building activities.[23]

3.1.6 Blind Spots and Rigidity

Blind spots and rigidities are principal sources of weakness and vulnerability. Blind spots are holes or errors in knowledge stemming from several sources: failure to assimilate information, failure to analyze context correctly, and poor judgement. In extreme cases, blind spots can be so significant that they can cause strategic paralysis. Rigidities create blind spots; they inhibit the flow of knowledge and make decisions and actions unintentionally predictable. Rigidities derive from the activities that once produced success. They are created whenever people overvalue particular ways of carrying out activities, particular disciplinary approaches, particular ways of

---

[18]"Complex systems adjust and adapt to their conditions in very sophisticated and surprising ways, even though component parts are often driven by a set of very simple principles. It should be obvious: There is no central controller who dictates how families, economies, governments, educational systems, and Pentagons work" (Petersen, 174-175).

[19]Gregory B. Stock and John H Campbell, "Human Society as an Emerging Global Superorganism: A Biological Perspective," in *Evolution, Order, and Complexity*, edited by Elias L. Khalil and Kenneth E. Boulding (New York: Routledge, Routledge Frontiers on Political Economy, 1996) 187-188.

[20]Lévy, 2.

[21]Stock and Campbell, 192-193.

[22]Davenport and Prusak, 50.

[23]Behavioral pathologies such as knowledge hoarding and the not-invented-here syndrome obstruct the flow of knowledge. Organizational pathologies, such as knowledge and information monopolies and artificial scarcity because of hoarding or excessive security are the primary cause of inaccessibility. See Davenport and Prusak, 44.

operating or communicating, or favorite technologies. In the best case, leaders make every effort to identify blind spots and rigidities and eliminate them.[24]

Opponents will look for blind spots in an effort to seize opportunities to surprise and shock—that is, to force the United States into premature or delayed transition or to diffuse its focus. Opponents may also compensate for their own disadvantages by striving to affect the political, cultural, economic, or military context to change the nature of the competition.[25] By discovering and dealing with blind spots and rigidities, the national security community can reduce their value to competitors and minimize the extent and duration of surprise.

3.1.7 The Evolution of SKO

Although the basic human drive to control the environment by acquiring and applying knowledge, skills, and technology[26] remains constant and predictable, means and methods are always evolving. The functions and objectives of SKO are therefore timeless, and only circumstances and technology change. Change may be gradual, or it may be extreme. Gradual change is often the result of technical innovation, such as the invention of the printing press, the transistor, or space flight. Extreme change in the nature of SKO may result from events that upset the equilibrium of control systems, for example, the fatal Western Railroad passenger train wreck in 1841, the attack by the Japanese on Pearl Harbor in 1941, or the stock market crash on “Black Monday” in October 1987.[27]

SKO are characterized by the interaction of cultural and technological forces. Technological forces, such as hardware, software, and physical processes, while complex, are generally easily observed, measured, and understood. The combination of advancing technology and innovation in knowledge-building activities is a major catalyst of change in SKO. As the technology improves, so must the skills in employing it, both to maximize the competitive capabilities of the United States and to counterbalance the strength of its competitors. Cultural characteristics, such as national resolve, national or individual conscience, morale and leadership, are more intangible

---

[24]Dorothy Leonard-Barton, *Wellsprings of Knowledge* (Boston: Harvard Business School Press, 1995), 51-55.

[25]Iraq pursued such a strategy during the Gulf War in 1990–91, when it tried, with some success, to drive a cultural wedge between the Islamic and Western countries if the U.S.-led coalition.

[26]James Beniger, *The Control Revolution: Technological and Economic Origins of the Information Society* (Cambridge, Mass.: Harvard University Press, 1986) 434.

[27]Public outcry about the fatal train wreck pushed the Western Railroad to pioneer changes in bureaucracy, programming, information processing, and communications that were afterward adopted by government, military, and industry; see Beniger, 224. The attack on Pearl Harbor forced the U.S. Navy to become skilled at improvising doctrine, information processing, and control functions; see Roger Beaumont, *War, Chaos, and History* (Westport, Conn.: Praeger, 1994), 35. The U.S. stock market crash in 1987 led to an overhaul of computerized trading practices and to the institution of “circuit breakers” to halt automated trading when the market falls very quickly; see Will Morton, “Can It Happen Again,?” in Black Monday—A Look Back at the 1987 Crash, CNN Financial Network, [On-line]. URL: http://cnnfn.com/markets/crashagain (Accessed April 10, 1998.)

and, for that reason, difficult to grasp, impossible to quantify, and slow to change. Both nations and individuals may often be blind to cultural forces, because both exist within the culture. Yet cultural forces exert a greater influence on the nature and outcome of competition that does technology. None of this, however, lessens the importance of technology, which offers the only means to exert influence beyond the reach of arms or the sound of the human voice.

3.1.8 The Art and Science of SKO

SKO are some of the most complex of a nation's endeavors, with characteristics drawn from both art and science. Aspects of SKO, particularly those dealing with the physics, processes, methods, and formats for the collection, movement, storage, and display of information, fall principally into the realm of science and technology. But these are (some) parts of SKO, and to list them is not to describe the whole. Human frailties, cultural factors, physical and cognitive limits, subjective judgments, and other such intangibles contribute to the whole. The science of SKO stops short of the need for knowledge, the wisdom to apply it creatively, the impact of moral forces, and the influence of serendipity. The conduct of SKO ultimately is therefore an art, a subjective human activity of creativity and intuition, and a potential source of great strength or weakness.

3.2 Theory of SKO

In spite of the complexity of competition, two concepts are of such significance and universality that they can be advanced as principles: transition and focus.[28]

Transition is the adaptation, preparation, movement, and arrangement of resources (people, knowledge, technology, funds) to enable the execution of selected national responses at decisive times and places. Many integrated responses generally are necessary to achieve a desirable condition or objective.

Focus is the controlled use of resources both to execute responses and then to monitor the environment and modify or modulate further responses until desirable conditions have been achieved. A need to focus assets at a decisive place and time may require a strict economy and an acceptance of risk elsewhere and at other times. Effective focus requires great collective awareness of primary objectives.

The principles of transition and focus embody the fundamental tenets of surprise, security, marshalling, mobilization, timing and tempo, unity of effort, and simplicity.

Effective SKO enable the nation to do the following:

---

[28]Clausewitz used the terms speed and concentration to represent only physical aspects (*On War*, 617). *Transition* suggests a change in state, style, or form as well as place, while *focu*s implies sharpness, clarity, centeredness, and concentration.

- Focus appropriate resources at the time and place of its own choosing;
- Shape the environment to influence competitors' transitions and reduce competitors' influence on its own transitions; and
- Monitor and sustain desired influence or conditions once these have been achieved.
- Success in such efforts is contingent on the quality of integration among supporting national security activities and on the nation's effectiveness in mobilizing its CK.

The art of SKO thus lies, first, in unified, collective recognition of the need for and, then, in orchestrating the appropriate physical, psychological, social, cultural, economic, military, and political transitions to create the necessary preconditions for focussing national power.

3.2.1 The Nature of Knowledge

For a better understanding of the development, management, and application of knowledge to national security decisionmaking and operations, it is useful to classify knowledge into individual, shared, and CK. Each type has its characteristic strengths and weaknesses, as well as different inherent strategies and resources for acquiring, maintaining, and applying it.

Individual knowledge is the knowledge developed and internalized by a single person over time. If effective, it allows one to form a usefully complete perceptual model of the environment. Individual knowledge is like a moveable window on the environment. One cannot keep all one's knowledge in view all the time.

Individual knowledge may be intuitive. Sometimes one has so thoroughly learned the steps that they take place automatically and without conscious thought and therefore at great speed. Intuition has been likened to "compressed expertise," a phrase that vividly suggests how knowledge works and what it can do.[29] In some cases, an individual's heuristic judgement about a complex problem is so highly calibrated that it can serve as "rule of thumb." Experienced intelligence analysts, operations officers, technicians, and negotiators, for example, often have this type of tacit knowledge.[30]

Tacit knowledge is nearly impossible to capture in a conventional document or database. Such accrued knowledge may be so embedded in one's behavior that its rules may be impossible to separate from how one acts.[31] Some knowledge simply cannot be represented outside the

---

[29]Davenport and Prusak, 10-11.

[30]During the Gulf War in early 1990, I observed an impressive display of tacit knowledge. A veteran Australian intelligence analyst regularly presorted dozens of tiny images on a light (viewing) table, stepped back, squinted, then selected one or two of them. When his teammates examined them under a microscope, the images invariably contained just the items or area they were seeking.

[31]The difficulty lies mainly in that the rules depend on the context in which the knowledge is invoked. Technology to some extent allows the identification and recording of past context, but none has yet been devised that can sense or interpret context as changes unfold. See Davenport and Prusak, 70-71.

human mind. Because such knowledge is extremely difficult to record adequately as shared information for the benefit of others, tracking and mapping it are important. Apprenticeship and mentoring remain the best ways to capture it.

Shared knowledge is created when individuals have both a common context and common information. If the common context consists of the background and understanding of operational goals and strategies and the common information is the intent of leadership, then shared knowledge can greatly facilitate decentralized execution of national security activities. This is especially important in shared problem solving, where shared knowledge enables implicit communication—the ability to communicate through mutual understanding.[32] Using key, well-understood concepts and knowledge of others' practices, or even anticipating one another's thoughts—is a faster, more effective way to communicate than through detailed, explicit instructions.

A common strategic and tactical understanding of how information and knowledge are acquired and shared can make knowledge-building activities more effective. Implicit communication is enabled by familiarity and trust, which are based on a shared philosophy and shared values and experience. A large proportion of shared knowledge, however, can also result in limited options and "groupthink,"[33] the antidote to which is a cultural practice of shared problem solving, using people from diverse disciplines.

Collective knowledge (CK) is the totality of the knowledge the nation can marshal and mobilize to create an advantage over competitors.[34] It is distributed knowledge—distributed among the individuals of the national security community and related communities worldwide. No single person or even group can master all knowledge and skills or know where all the information simultaneously required to manage the nation's affairs is located. CK is also a form of metaknowledge,[35] because it includes "what the nation knows about what it knows."[36]

---

[32]Shared knowledge and implicit communication are especially important at the tactical level of operations, when teams in combat or in highly sensitive diplomatic situations may be unable to communicate freely.

[33]For a description of the "groupthink" syndrome, see Irving Janis, *Groupthink: Psychological Studies of Policy Decisions and Fiascos* (Boston: Houghton Mifflin, 1972), 174, 196.

[34]The term *collective knowledge* used here is similar in many respects to Lévy's "collective intelligence" (see Lévy, 13-19), and I am indebted to him for parts of my concept of collective knowledge. His concept of collective intelligence, however, contains universal and utopian aspects not included here in the concept of collective knowledge. In addition, the narrowing within the U.S. national security community of the term intelligence to mean "foreign intelligence" limits its usefulness.

[35]Here metaknowledge means "knowledge about knowledge," including such ontological aspects as the role, applications, sources, and acquisition of knowledge.

[36]According to Lew Platt, chief operating officer (COO) of Hewlett–Packard (HP), speaking about knowledge, "If HP knew what HP knows, we would be three times as profitable." See Davenport and Prusack, xii.

A nation's CK is its working knowledge, its knowledge at hand, its actionable knowledge. A nation's decisionmakers draw the majority of its courses of action from its CK. Activities that develop, enrich, and mobilize CK are therefore among the most important parts of SKO.

CK is essential to effective SKO. A nation with well-developed collective knowledge can respond to conditions with a richer set of valid alternatives; greater flexibility; and a greater probability of achieving its goals. A nation's ability to tap its collective knowledge and skills can be its greatest source of competitive advantage.

3.2.3 Knowledge Enables National Power

The execution of SKO does not rest solely with the national government, through its military or its civil organs, because SKO comprise the widest range of military, governmental, and civilian capabilities that enable national-level exploitation and application of knowledge and information assets. At this level SKO integrates economic, military, diplomatic, cultural, technological, and other forms of knowledge to provide leadership with the fullest range of alternatives to use in attaining national strategic objectives.[37]

3.2.2 The Nation's Nervous System

The proportions of forms of national power devoted to influencing a competitor or attacking enemy sources of power are contingent on a nation's ability to assess the competitive environment and monitor operational situations. SKO may be thought of as the nation's nervous system, continually assessing environmental situations by providing, coordinating, and controlling four functions necessary for survival: sensing, communication, interpretation, and response (see **Figure 3-1**).[38] Each function is critical, but none is more important than the others. Although it is possible to conceive of simple scenarios that employ these functions sequentially, in general all of them operate simultaneously in a complex interaction. SKO are critical to

---

[37]The idea in this paragraph was originally articulated under the theme of national information power by Dan Kuehl. See Kuehl, "Defining Information Power," *Strategic Forum*, 115 (June 1997).

[38]The metaphor of a nation's strategic nervous system is adapted from an analogy in Stock and Campbell (185-188): because nations and their organizations are made up of human beings and therefore tend to behave organically, this model has been especially appropriate and has served as a basic strategy for survival and competition over thousands of years. There is a strong resemblance between this model and the tactical command and control models of John R. Boyd and Joel S. Lawson. For a side-by-side-description and comparison of both Boyd's and Lawson's models, see C. Kenneth Allard, *Command, Control, and the Common Defense*, rev. ed. (Washington, D.C.: NDU Press, 1996), 153—157. Boyd's contributions to command-and-control theory can be found largely in unpublished papers and briefings. Allard's presentation of Boyd's theories are based on personal copies of Boyd's work and extensive interviews and discussion with him from 1982 to 1996 (Allard, 321). For a discussion of Lawson's model, see Joel S. Lawson, Jr., "State Variables of a C^2 System," in *Selected Analytical Concepts in Command and Control*, edited by John Whang et al. (New York: Gordon and Breach, 1982), 61-84.

providing relatively stable conditions, even in the face of a continually changing national security environment.[39]

- **Sensing.** The United States has many types of sensors, both human and automated agents, including spy satellites, weather stations, journalists, diplomatic missions, intelligence agencies, economic and market analysts, military services, law enforcement, and security systems. They generate a flood of data about the nation's external and internal environment. Watching, recording, and interpreting, they are the nation's means of observing the environment and orienting itself within it. Human beings, as well as

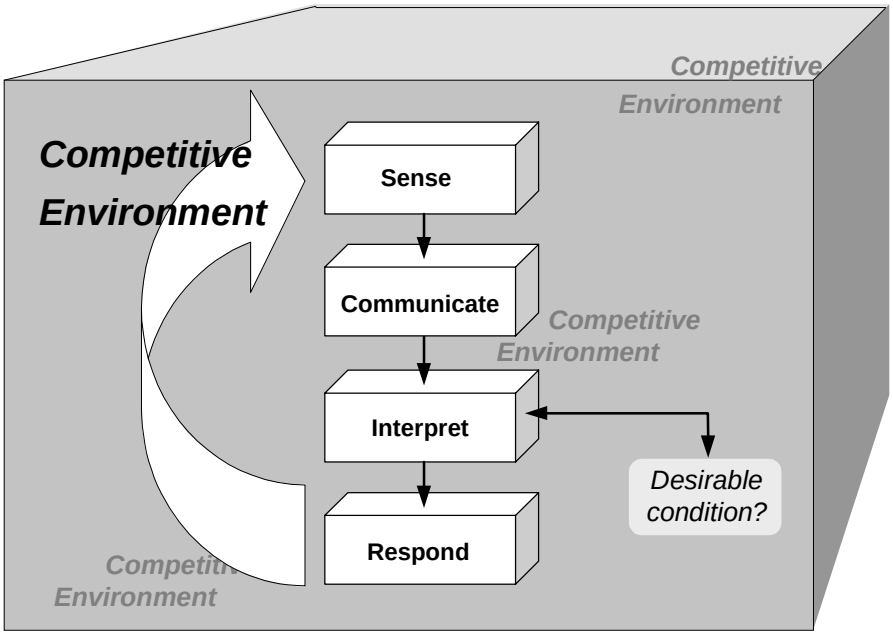

Figure 3-1

Model of SKO as the "Nation's Nervous System"

technology, play an important role in sensing. Only a complex and diversified sensing system can faithfully render a complex environment.[40] Relying on a single, uncontradicted data source can offer an illusion of omniscience, but because those data may be flawed in unrecognized ways, they may lead to nonadaptive action and disproportionate or mismatched responses.[41]

---

[39]In 1929, the American physiologist Walter Cannon coined the term *homeostasis* to describe the ability to maintain a dynamic state of balance, not a static state. See Elaine N. Marieb, *Human Anatomy and Physiology* (Reading, Mass.: Benjamin-Cummings Pub. Co., 1989), 12.

[40]Karl Weick, *Sense-Making in Organizations* (Thousand Oaks, Calif.: Sage Publications, 1995), 34-35.

[41]Karl Weick, "Cosmos vs. Chaos: Sense and Nonsense in Electronic Contexts," *Organizational Dynamics* (Autumn 1985), 57.

- **Communicating.** This function includes not only communication of data and information but also transportation of people and material assets. The nation communicates immense amounts of data and information through the global infrastructure of telecommunications, computers, libraries, broadcast media, and direct conversations. Communication implies storing, protecting, and presenting data and information, as well as sending and receiving them. Some of the data and information eventually reaches human minds, where through a complex process it becomes knowledge or is fed directly to preselected automated processes, especially in cases where reaction times are limited. Often the most effective way to use or communicate knowledge is to relocate people so they can talk face to face or work on a problem "hands-on."

- **Interpreting.** This function incorporates the complex, subjective processes of creating usable knowledge.[42] An initial interpretation assigns meaning to data, thereby creating primitive information. Sensory data and information stream constantly through the nation. Some may, in turn, be interpreted with other data or information to create new, more substantive information. This cycle can be repeated many times until the information has been learned by a decisionmaker, interpreted once more, incorporated into the decisionmaker's knowledge, and ultimately become part of the nation's collective knowledge. "Knowledge can also move down the value chain, returning to information and data" (see **Figure 3-2**).[43] Every decisionmaker decides what to do on the basis of many intricate factors, including risks, gains, goals, and guidance. Success in one sphere of activity may be adversely affected by failure or unexpected consequences in another. Effective SKO detect interrelated events and help the decisionmaker see the "bigger picture."

- **Responding.** The United States responds to competitive pressure by selecting and executing alternatives on the basis of its diplomatic, economic, military, and cultural strengths. Its selections are heavily influenced by time limits, the depth of its collective knowledge, and the effectiveness of its SKO. As a nation, the United States cannot respond so quickly as individuals or small groups but needs to rely on its components, focussed by collective knowledge, to respond appropriately on its behalf. If the nation's knowledge-building activities are well integrated, the nation will behave as "purposefully" as individual members.[44]

---

[42]Decisionmakers may judge or guess whether information or knowledge is usable, but it is not possible to determine usefulness prior to the outcome of a decisionmaking use of the information or knowledge. By implication, part of the function of interpreting includes post-facto analysis of decisions and of the usefulness of the knowledge and information used, even though determining which of the items of information considered were actually used to make a decision or take an action may be difficult. See Kovacs, "Using Intelligence," 146-148.

[43]Davenport and Prusak, 7.

[44]My paraphrase here of Stock and Campbell's description (186-187) of national response is meant to indicate clearly the underlying mechanism that permits a nation to exhibit purposeful behavior.

The functions of nervous system operate in two modes, surveillance and decision.[45] The different knowledge required for each mode guides how SKO use resources and the forms of the activities that employ those resources.

In surveillance mode, SKO scan the environment synoptically, building knowledge of the "big picture" of possible vulnerabilities or opportunities while also watching for possible crises or surprises or items of specific interest. In decision mode, SKO focus on acquiring and mobilizing specific knowledge critical to developing and selecting responses. Although operating in both modes simultaneously is to be preferred, the complexity of the international environment and

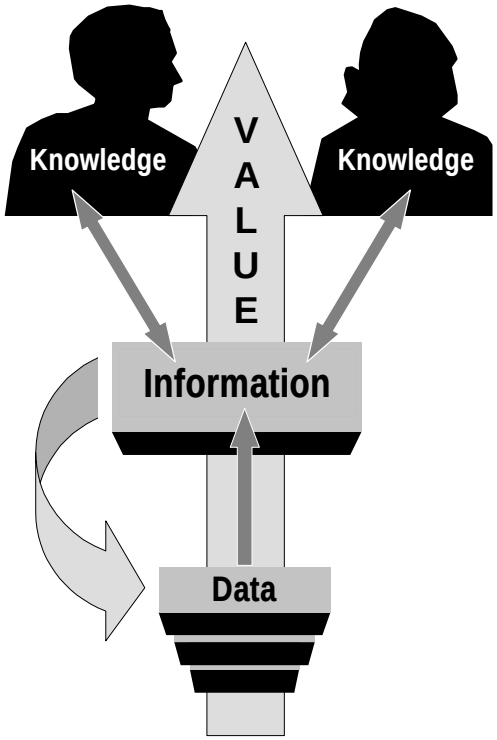

Figure 3-2

The Value Chain

Limitations on resources often require SKO to switch constantly between them. Leadership needs to consider carefully the risks associated with staying in one mode too long.

---

[45]Martha S. Feldman and James G. March use these modes in reference to information collection, but here these behaviors are extrapolated to primary motivators behind all knowledge-seeking activities, of which information collection is just one. See Feldman and March, "Information in Organizations as Signal and Symbol," *Administrative Science Quarterly* **26** (1981), 171-86. Amos Kovacs makes a similar extrapolation regarding military and political decisions; see Kovacs, "Using Intelligence," 151-152.

SKO tasks are performed by the combined capabilities of the military, economic, political and cultural components of national power, but some broad capabilities, such as intelligence collection and communications, may belong to more than one form of national power. Each combination of capabilities contains three types: core, enabling and supplemental.[46]

Core Capabilities. Core capabilities (see **Table 3-1**) constitute a competitive advantage for the nation. They have been built up over time, cannot be easily imitated, and are not easily disabled by competitors. They are distinct from both supplemental and enabling capabilities, neither of which is sufficiently superior to those of competitors to offer a sustainable advantage.

Table 3-1

Examples of Core Capabilities

- Global Force Projection
- Worldwide, all weather, technical intelligence collection
- Highly developed Collective Knowledge
- Strategic partnerships and coalitions
- Access to space and unimpeded on-orbit operations
- Economic and cultural influence

Enabling Capabilities. These capabilities, although necessary, are not in themselves sufficient to give the nation a competitive edge (see **Table 3-2**). Excellent communications and information operations are increasingly the ante for entering international competition and do not in themselves assure superiority. Nations cannot compete in global politics without being able to negotiate and analyze on a par with competitors. Such capabilities may be core if they embody proprietary knowledge (that is, not available from public sources) and if superior to those of rivals. Even excellent information warfare operations are not likely to constitute a permanent core technological capability because the knowledge content (including automated equipment) needed to optimize them is increasingly available to all competitors.

Supplemental capabilities, for example, skilled use of commercial information technology or collection of open-source intelligence, add value to core capabilities but can be imitated or bought.

[46]For a definition and development of the concept of competitive capabilities, see Leonard-Barton, 4-28.

Table 3-2

Examples of Enabling Capabilities

- Strategic transportation and lift
- Highly trained military forces, intelligence analysts, and foreign service
- Broad diplomatic presence
- Information technology and infrastructure
- Reliable air, space, maritime, and surface lines of communication

3.3 Summary

SKO are the means a nation uses to monitor the competitive environment, devise, select, and direct its responses, and measure its success. A nation's SKO allow it to interpret the intent of competitors and determine its own. They are how a nation recognizes opportunities as well as the critical vulnerabilities and opportunities of opponents and itself.

SKO help to coordinate and protect competitive capabilities while in transition and to control the focussing of those capabilities to create a competitive advantage. They protect the flow of information, build and sustain knowledge, and, if necessary, may prevent or inhibit the knowledge-building activities of competitors.

SKO respond to complexity in complex ways. The environment is inherently complex, and its future cannot be shaped with precision. Effective SKO generate many viable options, so that when the time to take action arrives the United States is not restricted to predictable or limited alternatives. In the next chapter, a new operational concept is proposed, collective knowledge (CK), as the key to effective implementation of SKO as described here. CK is the indivisible entity, based on objectives, threats, and opportunities, that SKO strives to manage and make available to decisionmakers. Highly developed CK, guided by tested doctrine and tactics, can become a core competitive capability.

Chapter Four

Collective Knowledge

No one knows everything; everyone knows something.

Pierre Lévy[1]

Collective knowledge (CK) is the relevant portion of a nation's total knowledge that can be effectively marshalled and mobilized to create a competitive advantage. Nations that attain, sustain, and apply CK are strategically agile and less vulnerable to exploitation. They are better able than rivals to preempt, mitigate, or respond to crises, thereby reducing the extent and duration of strategic surprise.[2] Summarizing his theory of war, Clausewitz wrote, "Knowledge must become a capability,"[3] a dictum that may be applied at any point on the spectrum of competition from peace to war. The nation that responds to challenges with the greatest number of valid courses of action has an advantage that cannot easily be disabled, copied, or purchased by competitors. Clausewitz used the word "knowledge," rather than information, and took care to point out that knowledge is more than information or data, that it has a quality of "readiness" not attributed to information, thus suggesting that maintaining ready knowledge is a continuing process.[4]

It is difficult to overstate the importance of CK in executing strategic knowledge operations. A nation interprets the environment with its CK, its responses are formed from its CK, and the range of acceptable, desirable conditions is heavily biased by its CK. It is therefore in a nation's best interest to map, understand, sustain, and expand its CK.

4.1 Understanding CK

CK is difficult to define in detail because it is dynamic. CK can be described by listing examples of its many manifestations (i.e., a military operations plan, a collaborative report from a distributed network of intelligence analysts, a common operational situation display, a radio news broadcast, or customized Internet navigation databases), but even an exhaustive list offers only an incomplete picture and cannot provide insight into how CK affects the quality of decision-making

---

[1]Pierre Lévy, *Collective Intelligence: Mankind's Emerging World in Cyberspace*, trans. Robert Bononno (New York: Plenum Trade, 1997), 14.

[2]This is the strategic variation of the tactical planning phrase "turning inside the opponent's decision cycle." See C. Kenneth Allard, *Command, Control and the Common Defense*, rev. ed. (Washington, D.C.: NDU Press, 1996), 153.

[3]Carl von Clausewitz, *On War*, edited and translated by Michael Howard and Peter Paret (Princeton, N.J.: Princeton University Press, 1976), 147.

[4]Ibid., 146-147.

or contributes to desired effects. CK is best understood through its role in decision-making, its characteristics, and its nature.

4.1.1 The Role of CK

The role of CK in decisionmaking can be illustrated by imagining national security knowledge as a pyramid[5] consisting of four layers, each layer representing a different and important part of the spectrum of national security knowledge (see **Figure 4-1**). The relative thickness of the layers will vary according to a nation's ability to create, manage, and exploit its knowledge. The two topmost layers represent all the nation knows or has known. The two bottommost layers represent all that the nation does not know. The following discussion of each layer clarifies the conception of the nature of knowledge and suggests methods to measure how well a nation—in particular, the U.S. national security community—manages knowledge.[6]

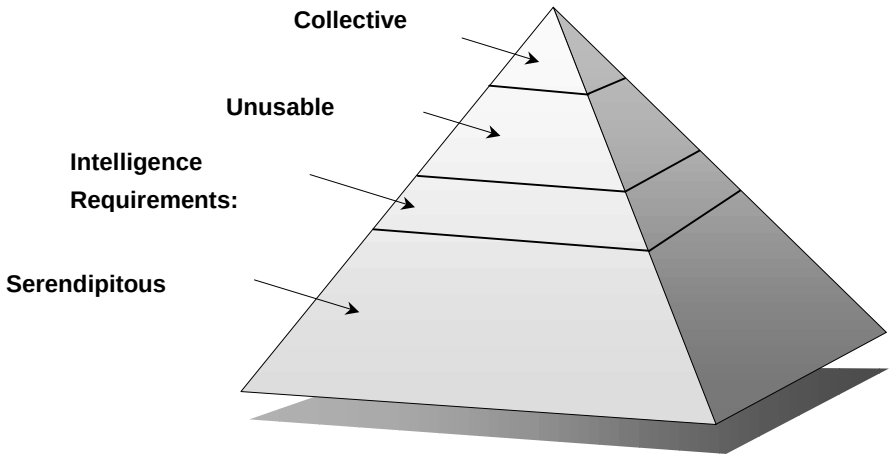

Figure 4-1
The Spectrum of Knowledge

Known-Knowns. The topmost layer of the pyramid represents CK—knowledge from all sources that a nation and its organizations may readily apply to problem-solving or decision-making. Known-knowns represent knowledge and information that have been marshalled and mobilized for the appropriate decisionmakers. Known-knowns do not include knowledge, information or skills a nation may be aware of but unable to use. This layer includes meta-

[5]This model borrows from one developed by Anthony G. Oettinger; see Oettinger, "Building Blocks and Bursting Bundles," in *Mastering the Changing Information World*, edited by Martin L. Ernst (Norwood, N.J.: Ablex Pub. Corp., 1993), 63.

[6]The model may, however, be applied to an analysis of the management practices of any organization.

knowledge—an awareness of the relevant knowledge or information others may bring to a problem, and a collective understanding of how it is organized and where to find it (i.e., knowledge maps). In essence, CK includes what a nation knows about what it knows.

Unknown-Knowns. The next layer down represents the nation's potential but unusable knowledge, that is, available knowledge the nation is not aware of, information resources it is not able to assimilate, or expertise it is not able to apply. The most frequent cause of unknown-knowns is inadequate marshalling and mobilizing of information[7]; much hidden information and knowledge may sometimes be exposed by disciplined and creative indexing, cataloguing, classification, and mapping of information and expertise. Unknown-knowns also result from tacit knowledge (e.g., because of knowledge hoarding or inadequate knowledge mapping), failure to analyze and derive knowledge from relationships among known-knowns, failure to interpret data, or lack of well-defined doctrine and tactics (see section **2.2.2**).[8] Unknown-knowns may be hidden in plain sight by logical, cultural, or emotional blind spots and are potential sources of competitive disadvantage. Unusable national security knowledge is almost always expensive; maintaining it costs something, and it returns no measurable benefit or competitive advantage to the nation.

Known-Unknowns. Known-unknowns include knowledge, skills, or information decisionmakers know they need but do not have. Nations traditionally dedicate most of their resources for intelligence collection and analysis to resolve known-unknowns, because these are factors essential to evaluating risk and carry great weight in decisionmaking. Taken out of the context of other knowledge, the desire to resolve known-unknowns may paralyze decision-making.[9] Once resolved, known-unknowns must be adequately marshalled and mobilized to incorporate them into the nation's CK, or they quickly become unusable unknown-knowns.

Unknown-Unknowns. "Unk-unks" make up the bottommost and largest layer of the knowledge pyramid. They consist of knowledge of which, for a variety of reasons, decision-makers remain completely unaware. They are most often discovered through creative insight and serendipity. Critical unk-unks are portions of knowledge hidden by logical, cultural, or emotional blind spots, especially when they are among an opponent's known-knowns.

---

[7]See Thomas H. Davenport and Laurence Prusack, *Working Knowledge: How Organizations Manage What They Know* (Boston: Harvard Business School Press, 1998), 7. Davenport and Prusack call this "de-knowledging" and claim its primary cause is too much volume, compared with the resources and capabilities of marshalling and mobilizing activities.

[8]Unknown-knowns that require analysis to resolve generally require human-aided analysis and effort.

[9]In the jargon of the U.S. national security community, "analysis paralysis."

4.1.2 Three Characteristics of CK

The breadth, depth, and responsiveness of a nation's CK directly determine the effectiveness of national responses. These three characteristics interact, and imbalances among them can impair responses. Balanced CK can help a nation detect and recognize symptoms of problems before crises emerge as well as conditions its knowledge activities to prepare for them.

Breadth means that knowledge-building activities are marshalling and disseminating the "big picture" and that collective national security knowledge is well mapped and integrated across all operations helping the United States to respond purposefully (see section **3.2.3**) by being aware of what the nation does and does not know, quickly locating tacit knowledge, and assembling multidisciplinary problem-solving teams. Without breadth, awareness can narrow, and the nation will not readily detect growing threats or unexpected consequences of its actions. Breadth of CK can be measured by the richness of the knowledge interchange among activities and the quantity, quality, and novelty of the national responses generated.

Depth means that the nation has sufficient organizational and individual expertise to develop, select, and apply specific responses without spending valuable time "getting up to speed" on a problem. Without depth, a nation may have difficulty making timely decisions. Depth can be measured by the speed and ease with which expertise can be located or detailed information made accessible.

Responsiveness means the speed with which CK can switch between synoptic and focussed views of the environment. How quickly can the nation bring various knowledge assets to bear on a specific problem? Without responsive CK, a nation will be subject to paralysis in decisionmaking or to circumvention by competitors. Although the responsiveness of CK can be measured only after the fact, it is the result of the day-to-day quality and readiness of CK building activities.

4.1.3 The Nature of CK

CK is mobile knowledge. In the competitive national security environment, institutional awareness is necessarily everyone's business, not that of only a few specialists.[10] Someone outside may know something useful. The complexity of national security problems, the proliferation of technical specialties relevant to those problems, and the global distribution of the national security community all require that the problem-solving activities involved in creating, integrating, and controlling national responses be able to share knowledge across departmental, organizational, disciplinary, geographic, and cultural boundaries.[11] Knowledge that cannot be mobilized and assimilated by the appropriate decision makers has no value—an unknown-known.

---

[10]Ibid., 8.

[11]Dorothy Leonard-Barton, *Wellsprings of Knowledge* (Boston, Mass: Harvard Business School Press, 1995), 61.

CK is inseparable from shared problem-solving, which is the means by which CK is applied. Both involve wiring together the brains of the appropriate people, so that sharing, reasoning, and collaborating become almost instinctive and part of everyday work. Effective and efficient shared problem-solving requires effective marshalling and mobilizing of information, according to timing and substance needs of the problem-solving team.[12]

CK is networked knowledge in that it is enabled by some form of networking technology, whether language, print, bureaucratic hierarchy, broadcast media, "yellow pages" telephone listing, business cards, or digital communications network. Past a certain quantitative threshold, effective, real-time coordination of knowledge requires high-speed "compunications"[13] technology.[14] CK is universally distributed throughout the national security community. Depth, breadth, responsiveness, as well as access to it are all affected by technology and by how technology is used.

CK is the operational level of knowledge that links strategic and tactical or field levels of knowledge by common doctrine and tactics . It is the use of knowledge of the tactical or field context to inform decisions at the strategic level about how, when, where, and in what conditions to respond. It informs the tactical level with shared knowledge of strategic goals and objectives to permit decentralized execution.

4.2 Making CK a Core Capability

Once the role and potential of CK are acknowledged, then, to exploit it as a valuable source of national power better, CK needs to be an explicitly developed and managed capability (see section **1.5**). Two factors critical to successful development of CK are shared vision and common processes. Decisionmakers and information producers must share a vision of CK that encompasses an understanding of its role, characteristics, and nature and of the ends CK will be employed to achieve. Common processes are the accepted and understood CK activities (CKA)

---

[12]Here substance is used to mean a subjective combination of meaning, completeness (for the purpose of decisionmaking), and value to a decisionmaker. It can be primitive (i.e., raw, uninterpreted data) or prototypical (i.e., potentially usable, but insufficient in quantity or timeliness), requiring effort and resources to become usable. Or it can be rich (i.e., well interpreted, correlated, documented, and complete) or definitive (i.e., exactly what the decisionmaker needed to know when it was needed and easily assimilated). Setting substance apart from format and process makes it plain how discretionary the ties are between the different kinds of formats and processes. Geographic and location information substance are not inexorably tied to cloth, despite the derivation of *map* from the Latin for *napkin cloth*, on which early maps were drawn. See Anthony G. Oettinger, "Building Blocks and Bursting Bundles," in *Mastering the Changing Information World*, edited by Martin L. Ernst (Norwood, N.J.: Ablex Pub. Corp., 1993), 23-25.

[13]See Anthony G. Oettinger, "The Abundant and Versatile Digital Way," in *Mastering the Changing Information World*, 85.

[14]Lévy, 14-15.

and their people and associated procedures and systems, which support effective assimilation of information and make knowledge, skills, and experience generally available.[15]

4.2.1 Shared Vision of CK

Efforts to promote, organize, and disseminate the CK of civilizations, governments, and commerce go back more than four thousand years, to the creation of the earliest libraries (Sumer, Akkad, Elba [Syria]). The drive to increase the efficiency and effectiveness of sharing and applying knowledge, now as in the past, pushes the development of new technologies. The possibilities for new knowledge capture, tracking and distribution, and the requirements and corresponding activities that would enable them have historically been recognized well after (sometimes generations) new technologies became widely available. For example, the invention of writing neither brought an immediate end to traditional oral dissemination of knowledge nor instantly spawned libraries. The extent of lag time between the introduction of new technologies and their application to CK management is principally governed by the spread and general acceptance of a shared vision of their possibilities within a culture or community. The rate at which a shared vision spreads depends largely on perceived benefits, penalties, and other cultural factors.[16] The central importance of leaders' understanding and encouragement of a shared vision of CK determines whether leaders will foster or inhibit the unimpeded flow of CK.[17]

4.2.2 CK Activities (CKA)

A nation's CK is its ready knowledge. CKA are a subset of SKO whereby a nation acquires and manages its collective competitive knowledge and creates operational strategies, tactics, and requirements that enhance its ability to apply it readily in the determination and pursuit of national objectives.

The primary function of CKA is to marshal and mobilize information, data, and sources of knowledge for retail consumption by individual decisionmakers. Secondarily, CKA help decision-makers learn and assimilate information accurately and quickly. (For detailed examples of CKA, see **Chapter Five**.)

In knowledge-intensive activities, such as those of the U.S. national security community, CKA may exist formally or informally.[18] Two widely known examples are (1) formal compilation and distribution by the DOD of a daily "Early Bird" news summary and (2) the informal practice

---

[15]These activities are often described as "knowledge management." See Knowledge Management, in the World Wide Web Virtual Library, edited by Yogesh Malhotra, [On-line]. URL: http://www.brint.com/km (Accessed June 16, 1998.)

[16]I am indebted to Richard Dawkins and Douglas R. Hoftsadter for this insight.

[17]Leonard–Barton, 30.

[18]Davenport and Prusack, 25.

of U.S. government organizations of hiring consultants and civil service personnel as a "corporate memory," to preserve and distribute organizational knowledge, to compensate for the loss of knowledge that results from frequent rotation of military and foreign service personnel, periodic turnovers of political appointees, and the lack of any collectively developed knowledge-mapping or -tracking activities.[19] The main shortcoming of informal CKA is that they tend to create organizationally focussed repositories of unknown-knowns of little benefit to the nation's CK.

Although CKA always, to some extent, exist, their most effective forms are culturally and functionally explicit, such as encouraging and rewarding multidisciplinary development of new CKA and shared problem-solving capabilities[20]; interdepartmental working environments in which people from different functions and levels collaborate on and resolve issues[21]; and specifically committing funding, people, and technology to acquiring, mapping, and managing knowledge for rapid application to national security problems. The culture that encourages and fosters explicit CKA manages its knowledge resources better and develops more mechanisms for generating and exchanging insights.[22]

4.3 Art and Science of CKA

Although CKA are developed through many technological and scientific activities, their management ultimately remains an art, a subjective balancing act. CK constantly needs to be enhanced and coordinated to remain relevant to the needs of decisionmakers. A strategic balance can be maintained only by continually observing and orienting the nation within the competitive environment and making appropriate corrections to CK. Leaders of CKA, expert negotiators, policymakers, intelligence collectors, and skilled pilots have in common that they maintain balance by frequent small adjustments, rather than infrequent large ones.

CKA are not "how-to" checklists or assembly lines mass-producing "know-how." CKA have no meaning separate from the people conducting them, because these people bring to the CKA their own idiosyncratic abilities, histories, and personalities. Dorothy Leonard–Barton sounded a warning of the dangers of managing knowledge-building activities as a sterile process.[23] U.S. national security leaders and policymakers need to monitor CKA policies actively for signs of imbalance—for example, between efficiency and effectiveness, for excessive

---

[19]This practice is so widespread that many contract consultants advertise it as a service. See William H. Starbuck, "Learning in Knowledge-Intensive Firms, in *Knowledge in Organizations*, edited by Laurence Prusack (Boston: Butterworth–Heinemann, 1997), 156-157.

[20]See Iain Somervill and John E. Mroz, "New Competencies for a New World," in *The Organization and the Future*, edited by Frances Hesslebein, Marshall Goldsmith, and Richard Beckhard (New York: Josey–Bass, 1997), 71; and Leonard-Barton, 73-84.

[21]Somervill and Mroz, 1.

[22]Davenport and Prusak, xii.

[23]Leonard–Barton, 8.

concentration of resources in one area of knowledge to the detriment of others, for unproductive activities that do not lead to usable capabilities, and for vulnerability or opportunity. They need also to watch CKA for pathologies that create blind spots and rigidities in the nation's CK, as in the following examples: "overshooting the target—that is, succumbing to the simplistic notion that more of a good thing is always better"[24]; the inability to devise new tools or methods, that is, using new technology to pave old paths; or screening out external knowledge.[25] Such judgments are highly subjective and demand that leaders and policymakers maintain balanced perspectives and an awareness of their organization's CKA and of the state of the nation's CK.

4.4 Summary

CKA are the art and science of enlarging, sustaining, and coordinating the United States's collective national security knowledge. CKA include protecting, mobilizing, marshalling, and mapping information and knowledge for collective use and shared problem-solving.

Their primary objective to provide decisionmakers with the richest possible set of validated options for responding to competitive pressures. This objective can be achieved through the dissemination and clarification of strategic goals and vision, by aiding the flow and transfer of knowledge, promoting and enabling shared problem-solving, and acquiring and maintaining relevant competitive knowledge within the national security community.[26]

The goal common to all CKA is to provide timely access to moderately organized, broadly classified, cross-discipline competitive knowledge for a majority of the national security community.

A nation with well-developed CK can respond to conditions with a rich set of valid alternatives; great flexibility; and great probability of achieving its goals. A nation's ability to tap its CK and skills can be its greatest source of competitive advantage.

All of which, however, is more easily said than done. Few national security CKA exist and those that do remain narrowly focussed on specific types of knowledge and information. As of 1999, no operational activities, such as those described in **Chapter Five**, exist for marshalling and mobilizing the national security community's general knowledge.

---

[24]Ibid., 32.

[25]Ibid., 38-40.

[26]See Somervill and Mroz, 73-74; see also Davenport and Prusack, 144, 161.

Chapter Five

Mobilizing and Marshalling Collective Knowledge

If you know what's going on with technology, you, the user, ultimately control it. If you don't, it controls you.

Mark R. Stokes[1]

"It is important to start digesting information and creating knowledge before crisis occurs; by the time the crisis hits it may be too late to respond."[2] As noted at the start of **Chapter Four**, by the time a crisis does hit, the nation has developed responses from its collective knowledge (CK). Thus, the quality and variety of its responses depend directly on the quality of day-to-day information and knowledge marshalling and mobilizing activities.

In the parlance of current business-oriented texts, information and knowledge marshalling and mobilization fall under the general rubric of knowledge management.[3] Although the tools and techniques that support the effective use of information resources and make skills and experience generally available apply to all competitive activities, national security operations are a different type of competitive activity from business. National security operations are extremely knowledge-intensive, and timelines, the effects of decisions, ends, and means all are different enough that it is useful to use terms different from business terms[4] to reflect accurately the way knowledge flows in national security processes. Naming CKA by such terms as "marshalling" and "mobilization," which parallel and emphasize the military, crisis-management, and consensus-building aspects of international competition, de-emphasizes format and process and

---

[1]Mark R. Stokes, "The Case of the Missing Tags: The State of Internet Search Engines and Directories," *OnTheInternet* **4**, 3 (May-June 1998), 19.

[2]Thomas H. Davenport and Laurence Prusak, *Working Knowledge: How Organizations Manage What They Know* (Boston: Harvard Business School Press, 1998), 65.

[3]The terms "marshalling" and "mobilization" are intended here to represent two major activities of knowledge management in U.S. national security decisionmaking. Although others may describe and classify basic knowledge-building activities differently, "knowledge management" has been accepted as an umbrella term. See. for example, The World Wide Web Virtual Library on Knowledge Management, edited by Yogesh Malhotra, [On-line]. URL: http://www.brint.com/km (Accessed June 16, 1998; Davenport and Prusak, *Working Knowledge: How Organizations Manage What They Know*; and Dorothy Leonard-Barton, *Wellsprings of Knowledge* (Boston: Harvard Business School Press, 1995). Other terms used frequently are "knowledge networking" and "competitive knowledge development." See Kirk W. M. Tyson, *Competition in the 21st Century* (Delray Beach, Fla.: St. Lucie Press, 1997); and Iain Somervill and John E. Mroz, "New Competencies for a New World," in *The Organization and the Future*, edited by Frances Hesslebein, Marshall Goldsmith, and Richard Beckhard (New York: Josey-Bass, 1997).

[4]Which is not to imply that business knowledge-management terminology does not to apply to many business functions that support and sustain national security operations.

focusses those activities instead on substance and context. Classifying in this way may also clarify where to establish CKA and how to allocate resources.

Fortunately, several powerful knowledge-management techniques are available that are well suited to developing marshalling and mobilizing activities, with few, if any, technological challenges associated with them. Resource allocation and cultural biases against knowledge-sharing are the main barriers to implementing those techniques widely. A sustained focus and direction from leadership are needed to establish these knowledge-sharing activities and to make them effective. The balance of this chapter discusses some commercially successful knowledge-marshalling and -mobilizing activities that the national security community could emulate or purchase and put into operation almost immediately.[5]

5.1 Mobilizing Information and Knowledge

When people create knowledge, they organize it in their minds in accord with how they envision applying it. Making knowledge and information ready for use requires organizing it with consideration for how people expect to use it. Such organization is known as context-based processing.[6] Context-based access to information (i.e., potential knowledge) is especially critical, because time spent locating and accessing information subtracts from the time available for assimilating it as knowledge.

Context-based processing is not a new concept in national security operations but is well known to military planners, particularly in transportation, the development of marshalling areas, and the mobilization of reserve forces. Whenever possible, planners try to “combat load” military equipment and personnel, in “last in, first out” order so that they can unload in the order in which they are expected to be used and so be effective as soon after debarking as possible. The flow of forces into an area of engagement is ordinarily planned to coincide with the way the forces are expected to be employed on arrival. Sustainment activities are planned on the basis of rates of expected use. In the commercial world, department stores and supermarkets use highly refined context-based processing techniques to design store layouts, product presentations, and shelving practices in order to conform to ways they consider customers are attracted to products. U.S. commercial retail enterprises have so accustomed people to this kind of presentation of items that Americans now automatically assume all products and services are organized by context, but the commercial practice has not been generally adapted to national security information, especially

---

[5]The Intelink Management Office (IMO) has implemented prototypes of some of these activities to support intelligence community operations within days and weeks.

[6]Context-based processing is also called vocabulary-based processing (see Cyril Brookes, Vocabularies for Knowledge Management, [On-line]. URL: http://www.grapevine.com/wirtings/km/vocab.htm [Accessed March 4, 1998]); but many prefer the term “context,” because it refers to the “decision context” of the information user. Interview by the author with Srinija Srinivasan, chief ontologist, Yahoo! Inc., March 11, 1998.

the vast and ever growing amount of information provided through networked databases and Internet technologies.

Imagine arriving at a local supermarket or department store and finding, to your great irritation, that the store's shelf stock has been rearranged not by type of product or use or brand name but by manufacturer and production process and for ease of delivery of products. Looking closely, you find that produce is mixed in with house-cleaning items, poultry with automotive supplies, and some cookies are next to facial tissue while others are next to canned vegetables! Locating your favorite brand of barbecue sauce or motor oil requires you to search aisles at random, because you cannot recall the names of companies that manufacture and distribute these items. In frustration, you select one of the following less than perfect responses:

- You ask store personnel to find the product you want (which reduces the possibility of comparison shopping for more suitable ones); or
- You search until you find a suitable substitute (satisfice)[7]; or
- You leave the store without the product you wanted (and imagine the nature of the problem had you been shopping for more than one item).

This scenario may sound ludicrous, but quickly "surfing" any government network will verify that most national security information is currently (1998) organized in this way.[8]

Searching (even with computerized search technology) is by itself an inadequate strategy. Equipping knowledge-seekers only with search tools is like asking them to find buried treasure in landfill without a map—and often they will not even know what the treasure is until they see it. The same problem arises with sources of information and knowledge. Unless users have a map, they may dig many virtual holes and sort through much irrelevant junk before they find the treasure, if, indeed, they find it all. Locating, identifying, and editing material stored on networks is nearly impossible to do efficiently unless the material has been usefully categorized and

---

[7]"Satisficing" is the most frequently chosen alternative. If you cannot find what you want, then one way to proceed is surrender the idea of finding the best product, set lower expectations for various goals, which, if attained, would be "good enough," and seek a solution that will at least meet these expectations. See E. S. Quade, *Analysis for Public Decisions* (New York: North-Holland, 1984), 92-95. For further reading on satisficing behavior, see H. A. Simon, *Admini-strative Behavior* (New York: Macmillan, 1961).

[8]Compare any commercial context-based information services—Yahoo!™ (URL: http://www.yahoo.com), AOLFind™ (URL: http://www.aol.com), Livelink Pinstripe™ (URL: http://pinstripe.opentext.com), among others on the World Wide Web—to the search capabilities available on government intranetworks, such as the Nonclassified Internet Protocol Router Network (NIPRNet), the Secret Internet Protocol Router Network (SIPRNet), or the Joint Worldwide Intelligence Communications System (JWICS). Information is generally organized by the name of the distributing organization, intelligence discipline and subdiscipline, and type of product, etc. Users seeking information about a particular crisis or activity must "shop each" organization's site and then correlate and fuse the information across discipline and products. Examples of "state-of-the-art" activities optimized for finding unclassified government information include the Defense Technical Information Center (DTIC) (URL: http://www.dtic.mil) and Govbot (URL: http://ciir.cs.umass.edu/ciirdemo/Govbot), although neither site presents context-processed information.

preprocessed, and often it is necessary to categorize a large and evolving collection of documents that exists in many databases.

Classification based on context has proved an effective tactic for dealing with many sources of knowledge and large volumes of information.[9] Services based on context are extremely popular among users; these so-called portal sites organized by predicted user context are among the highest trafficked sites on the Internet.[10] Yahoo!, Inc., pioneered this approach with a service designed for a large population with general interests.[11] The challenge is to apply context-based processing to national security information networks, and two pioneering government knowledge-building activities have been working to do so. Intelink has been steadily adding context-based preprocessing to its "Wher'zit" search service and has been developing experimental regional intelligence "supermarkets" for groups of intelligence users. The U.S. Transportation Command's (USTRANSCOM) Global Transportation Network (GTN), which tracks movements of cargo and personnel via government transportation assets and uses predefined queries based on common user context to help customers learn the status of shipments and transportation availability. Unfortunately, the charters and resources of Intelink and GTN limit them to intelligence information and transportation information respectively, and these services are not integrated. A family of knowledge-building activities such as Intelink and GTN, however, optimized for accessing military, diplomatic, cultural, and intelligence information and integrated under a "Yahoo!" or "Wher'zit" for national security information would offer great potential for building CK and improving human-to-system and human-to-human interoperability. For example, governmentwide context-based processing could serve as a means of disseminating and infusing a common ontology throughout the national security workforce and could encourage implied communications among all users by helping to standardize vocabulary about knowledge and information sharing.[12] Such a service would be especially powerful on networks that support military planning, crisis response, and command-and-control activities.[13] Planning and operations staffs would spend more time learning than searching. The ability to browse quickly through all types of information related to a question or to track down experts would promote more

---

[9]This concept underlies the telephone directory "yellow pages."

[10]RelevantKnowledge, "RelevantKnowledge First to Release Top Twenty-Five Web Site Lists for the Month of January," press release (1-12-98), [On-line]. URL: http://www.relevantknowledge.com/Press/release.html (Accessed March 17, 1998.) 1-2 . "RelevantKnowledge Releases February's Top 25 Properties and Web Sites by Unique Visitors, press release (3-9-98), [On-line]. URL: http://www.relevantknowledge.com/Press/release.html (Accessed March 17, 1998), 2-4.

[11]See URL: http://www.yahoo.com

[12]Cyril Brookes, Vocabularies for Knowledge Management, [On-line]. URL: http://www.grapevine.com/wirtings/km/vocab.htm (Accessed March 4, 1998), 2.

[13]Companies such as RelevantKnowledge, Inc., and Open Text, Inc., "slice" information for specific user communities. New software and hardware technologies designed for the Internet make this service very cost effective.

innovative and diverse responses to situations, not to mention increasing the probability of recognizing important situations earlier than is now possible.

Although information and knowledge mobilizing activities can prepare information to become knowledge quickly and prepare knowledge for action, they do not necessarily reveal hidden insights about data or information nor reduce the amount or cost of unusable knowledge. The tasks of acquisition, development, and maintenance of CK are the focus of activities to marshal information and knowledge.

5.2 Marshalling Knowledge and Information

The objective of the United States's knowledge and information marshalling activities is a broad, balanced CK to support national security decisionmaking and action. This objective can be achieved by maintaining and increasing the nation's known-knowns through the reduction of unknown-knowns, resolution of known-unknowns, and the discovery of unknown-unknowns by cultivation of serendipity (see sections **2.2.1** and **4.2.6**). Knowledge, and potential knowledge, may be derived from a multitude of people and sources inside and outside the national security community, but the challenge is to develop and implement efficient marshalling activities and tactics that maximize usable knowledge and information and keep track of where they are located.

With the exception of the DOD's Information Analysis Centers (IAC),[14] most national security knowledge and information marshalling activities have historically been restricted both to defined intelligence requirements and to database searches. Databases generally are "stand-alone" and not correlated with other sources of related information. No widely available interagency "yellow pages" of individual or organizational expertise exists. Consequently, the potential of the information remains unrealized and not incorporated into the nation's CK.

One key information marshalling activity is "data mining,"[15] which focusses primarily on legacy data and information, with the ultimate goal of uncovering hidden relationships among elements of data and information that may produce potential competitive knowledge. A secondary focus of data mining is to discover forgotten information or to mark unusable data for modification or disposal.

---

[14]Managed by the DTIC and the military Services, the IACs are formal organizations chartered by the DOD to locate, analyze, and use scientific and technical information; staffed by scientists, engineers, and technical-area information specialists, they establish and maintain comprehensive knowledge bases. See DOD, "Information Analysis Center (IAC) Help U Better (HUB) Page, [On-line]. URL: http://www.dtic.mil/iac/#home (Accessed June 16, 1998.)

[15]For further information on data mining and for links to other Web sites on this subject, see "data mining—PC Webopaedia Definition and Links,", [On-line]. URL: http://www.pcwebopaedia.com/data_mining.htm (Accessed June 16, 1998.)

The results of data mining include the following[16]:

- Associations, when one event can be correlated with another (competitors buying computers also buy a specific type of software a certain percentage of the time);
- Sequences, when one event leads to another, later event (a certain competitor significantly increases purchases of paper products directly before or after intensive planning activities); and
- Classification, the recognition of patterns that results in a new organization of data (for example, profiles of competitors' purchasing practices).

Data mining software can initially screen the data according to rules laid out by data analysts. The software alerts or reports to the analysts when it finds problems or possible useful relationships. Data mining is used on information networks to screen out network operations data in order to increase customer support and balance resource. Data mining is most useful when diverse but related data from several sources are compared and analyzed by experts from both information-producing and information-using activities. For example, by using data mining techniques to sample and track how its members use information and then correlating this information with world events, the national security community may overcome some of the problems associated with predicting information requirements, learn which ways of bundling information are most effective (i.e., refining context processing), and gain insight into how to balance and apportion resources to different knowledge-building activities. Data mining is more than just panning for nuggets; one of its main benefits is insight gained from doing it. It can show the United States as others see it and reveal to the United States its own blind spots or biases.

Another critical activity for marshalling knowledge is mapping tacit knowledge. In general, members of the national security community, especially military and foreign service personnel, move often, to new posts within that community or leave government service or move to academe, and they take their expertise with them. They often arrive at the new posts without expert knowledge of the subject-matter associated with the new positions. Further, organizations reorganize frequently, but people rarely change their core area of expertise. Keeping a "yellow pages" database of where all this expertise is located is essential to the timely mobilization of knowledge.

5.3 No Free Lunch

There is no free lunch in knowledge-building activities. The assumption that someone else is mobilizing and marshalling information and knowledge allows people to ignore the costs of these critical activities. The potential inefficiency and confusion caused by relying on individuals to develop their own operational strategies and tactics may be more costly than the effort to

[16]See "What Is…Data Mining" [a definition], [On-line]. URL: http://whatis.com/datanini.htm (Accessed June 16, 1998.)

develop, train, and maintain standard ones formally. Because these services are neither cheap nor, at this point in the development of technology, completely automated, expecting some organization altruistically to set aside a portion of its resources to provide collective mobilizing and marshalling services to the entire national security community is unreasonable. At one extreme, Yahoo!, Inc., has estimated that it employs about 386 full-time staff,[17] plus contracted services and partnering agreements, to maintain automated software agents, market services, and to form teams of subject-matter experts to think about the best ways to preprocess, organize, and index information for use by the general public. At the opposite extreme, Open Text Corp.'s Livelink/Pinstripe™ service employs about five full-time technical staff to update and maintain its automated, business-specific databases.[18] Surveys of Intelink and DTIC indicate that the cost of services customized for national security operations would fall somewhere between these extremes.

[17]The exact number of Yahoo ontologists, "web surfers," and technical staff remains a closely held trade secret, but the company is known to employ about 386 marketing, administrative, and technical staff. Interview by the author with Dana Young, Public Affairs, Yahoo!, Inc., March 4, 1998.

[18]Open Text Corporation basically offers only a mobilizing service. Its cost strategy is to take as much advantage of existing documents and evaluation processes as possible. It performs all the mobilizing activities according to a "slicing" scheme based on existing the North American Industry Classification System (NAICS) business categories and relies on other companies, such as *Fortune* magazine and *Forbes* magazine for quality control and marshalling. Interview by the author with Mark Kraatz, manager, Corporate Web Systems, Open Text, Inc., March 27, 1998.

Chapter Six

What's Next?

Finding good players is easy, getting them to play together is the hard part.

Casey Stengel[1]

6.1 Challenges

Given the potential advantages, there may be several reasons why the U.S. national security community has not yet developed context-based information and knowledge management as a core capability:

1. U.S. technocentric strategies have not explicitly focussed on marshalling and mobilizing operational and strategic knowledge.

2. The U.S. national security community has not developed and internalized a doctrine or tactics for knowledge management (KM) operations.

3. Within the budgetary and political arenas, such knowledge and information marshalling and mobilizing activities have neither a home nor designated advocates.

4. No explicit joint or interdepartmental infrastructure exists to nurture KM activities.

5. Despite the efforts of the U.S. national security community to improve the information flow among organizations, within its organizational cultures the bias toward the notion that "knowledge is power" has yet to be overcome.

Formal knowledge management and the deliberate development of SKO doctrine and CKA pose challenges to traditional beliefs about centralized control, interagency collaboration, military staff operations, and strategies for technical development.

6.1.1 The Main Challenge: Changing Culture

According to James Peak, the Director of the Intelink Management Center, the main challenge in developing activities for marshalling knowledge and information and promoting collaborative problem-solving is to nurture and coevolve cultural values along with the technology.[2] Values and beliefs are integral to how people think, and as of early 1998, much of

---

[1]Attributed to Stengel by Howard Millman, "The Pros and Perils of Mining Intellectual," *Infoworld* **19**, 46 (Nov. 17, 1997), 128.

[2]See James Peak, "Gutenberg, I Feel Your Pain," *View From the Summit* **1**, 21 (July 13, 1997) (Intelink), [On-line]. URL: http://www.imo.ic.gov.summit/view_13jul97.html (Accessed May 26, 1997.) Also see by Peak, "Short-Circuit in the Crystal," *View From the Summit* **2**, 14 (May 24, 1998) (Intelink), [On-line]. URL: http://www.imo.ic.gov.summit/view_24may98.html (Accessed May 26, 1997.)

the thinking on information and knowledge operations still looked suspiciously familiar—that is, new variations on old cultural themes. That is not surprising, given that the national security community suffers from "value confusion,"[3] which is to say that over time, people and organizations have come to prize the ways in which they accomplish their mission as much as the mission itself, as the following examples suggest:

- particular means (diplomacy, air power, maritime power);
- functional activities (intelligence, operations, communications, logistics, administration);
- specific disciplinary approaches (imagery intelligence, signals intelligence, open-source intelligence); or
- preferred technologies (personal computers, mainframe computers, "no computers," satellites, aircraft).

These values are entrenched in the culture of the national security community, incorporated into the skills and knowledge of its people, embedded in managerial systems, and implemented in physical systems, and they tend to preordain how knowledge and information flow through the community. For example, in the 1990s, much of the organizational and command-and-control structure preferred by the national security community reflects the era of industrial work (pre-1960), when many tasks were physical and information was communicated mainly through the "chain of command." Physical tasks were easily divided into specialties, which led to management by function or specialty, which in turn led to the establishment of rewards and promotions based on functional career paths and to the preservation and consequently the rigidity of the structures that produced success. It should come as no surprise, then, that the vast majority of national security organizations and their budgetary and planning systems are all structured hierarchically along functional departments.

Formal knowledge-management, the development of joint, unified, and interdepartmental SKO doctrine and CKA challenge many such traditional beliefs and will be slow to be implemented—and without significant cultural change are liable not to be implemented at all. To be effective, CK, and communitywide activities for marshalling and mobilizing knowledge will require collaborative, cross-specialty teams, with common training so that specialties may blur. Planning and acquisition authority for CKA will need to be integrated within these teams as well. For example, the success of CKA will heavily depend on the teams' ability to acquire, implement, and retire, both rapidly and on a communitywide basis, commercial sources of information and knowledge as well as commercial marshalling and mobilizing services in which the technological and functional generations turn over every six weeks to six months. That stands in sharp contrast to the typical U.S. government acquisition program cycle of one to three years, or more.

---

[3]Dorothy Leonard–Barton describes this as confusion between "Big Values" and "little values"; see Leonard–Barton, *Wellsprings of Knowledge* (Boston: Harvard Business School Press, 1995), 51-53.

6.1.2 Avoiding Hubris and Hyperbole

In the rush to cash in on knowledge management, many businesses are willing to sell the national security community technology solutions to its knowledge-management problems, but these solutions are complex and therefore difficult to implement and need to be specifically tuned to the collective goals of the community. Rather than install-and-ignore solutions, these demand constant monitoring and tuning—the better the tuning, the more pronounced the advantage. And they can be expensive, especially compared to alternatives on the market. Purchasing such a solution makes no sense if the advantage or service it offers can be obtained elsewhere and particularly if, like many technology solutions, it will go unused if it threatens community values or does not help members get their jobs done.[4]

Collective and distributed problem-solving and rapid development of innovative, integrated solutions are capabilities that cannot be created by a massive worldwide installation of Lotus Notes™ software and Internet technology.[5] The U.S. national security community needs to resist both techno-hype and the bureaucracies that can spring up in government around such popular notions as "total quality management" or "business process reengineering"; it needs to avoid cheerleading and the rush for immediate results; it needs quietly to set about building collaborative teams to define, experiment, and develop CKA and then to let the results speak for themselves. The concepts of SKO and CKA are not grand designs that will finally connect, once and for all, every aspect of information and knowledge operations. Rather, they are transitional frameworks, to get the national security community "from here to there," and other uses of the nation's knowledge resources will prove more effective as that community lives, grows, and changes.[6]

6.1.3 Cultivating Serendipity

Serendipity, according to the dictionary, is "the faculty of making fortunate and unexpected discoveries." In a competitive global environment, the U.S. national security community needs to find ways to use its information technology to focus the creative energy of experts from government and nongovernmental and business organizations and to seek ways to bring them together, not only to solve problems but also to find new ways to marshal and mobilize information and to use its collective knowledge. That is, the community needs to learn how to promote serendipity.[7]

---

[4]Bill Ginchereau and Julie Dunn, "Knowledge Equals Power," *Infoworld* **19**, 46 (Nov. 17, 1997), 117.

[5]Wanda, Orlikowski, "Learning From Notes: Organizational Issues in Groupware Implementation," in *Knowledge Management Tools*, ed. Rudy L. Ruggles III (Butterworth-Heinemann, 1996), 231-246.

[6]See James Peak, "Ionian Enchantment of the Web," *View from the Summit* **2**,7 (1998) (Intelink), [On-line]. URL: http://www.imo.ic.gov.summit/view_05apr98.html (Accessed April 29, 1998.)

[7]In Elizabeth Jamison Hodges' retelling of *The Three Princes of Serendip* (New York: Atheneum, 1966), the dying king of Serendip sends his sons on a quest to save their country. In their travels, the sons discover, both by accident and

Modern cognitive research reinforces the notion that serendipity is the primary source of innovative thinking. Discoveries generally are made not by one person thinking alone but by groups of people from different disciplines; most discoveries are collaborative, involving many participants with various backgrounds. "[S]erendipity depends very little on blind luck or grand strokes of genius and much more on solid logic, a talent for apt comparison, and minds so steeped in various disciplines that they can recognize an unexpected clue for what it is worth."[8]

Recognizing this phenomenon, leaders and decisionmakers usually surround themselves with good staffs. The most successful of them contend that a staff and teams with widely varying backgrounds can produce a greater quantity and better quality of new and different solutions and alternatives.[9] Cognitive research, again, supports this contention and has indicated the advantages of "distributed reasoning," in which people with varying backgrounds put their heads together to solve a problem.[10] As the national security community has learned repeatedly, the advantage of group reasoning fades when the members have similar backgrounds; progress is no faster than were such individuals working alone.[11]

6.1.4 A Different Approach to Information Technology

As suggested earlier (section **6.1.1**), information technology has, for the most part, been used to automate familiar functions, processes, and tasks, and this pattern will not easily be changed. The technology that national security organizations choose to use not only helps to condition tactics, strategy, organization, logistics, intelligence, command, control, and communications but also the mental framework used to think about competition and national security. This framework, in turn, influences choices of which technologies to develop.[12]

---

through wisdom, that which they were not seeking and, in doing so, solve many problems, and complete their quest. Each prince possess a different special knowledge (e.g., military, political, artistic), and their accomplishments are possible only because their depth of knowledge allows them to recognize unexpected opportunities and understand how to use their knowledge collectively.

[8]Rick Weiss concisely summarized the research in this area. See Weiss, "In Recognizing Surprise: Researchers Go from A to B to Discovery," *The Washington Post*, Jan. 26, 1998, A-3.

[9]Leonard-Barton, 73-84.

[10]Kevin Dunbar, "How Scientists Really Think and Reason: Scientific Reasoning in Real-World Laboratories," *Mechanisms of Insight* (Cambridge, Mass.: Massachusetts Institute of Technology [MIT] Press, 1995), 365-395.

[11]Michael R. Gordon and Bernard E. Trainor relate an illuminating case from Operation Desert Shield. Although the Jedi Knights, an elite group whose nickname recollects the warriors of the *Star Wars* film trilogy, were selected from various Army specialties to plan the ground war, they were still a highly homogenous group: "The Jedis were supposed to be the best and brightest of the Army, but they had essentially come back with the same thing Schwarzkopf had sketched out a month and a half before." See Gordon and Trainor, *The Generals' War* (Boston: Little, Brown, 1995), 128-129.

[12]Martin van Creveld makes this critical point, here paraphrased, about computers and technology in war, but it is applicable also to all forms of international competition. See van Creveld, *Technology and War* (New York: The Free Press, 1989), 246.

Although designers need time to become familiar with a technology, the serendipity that allows teams to see new applications—ones that never before existed—issues from strategically encouraging cross-fertilization among a variety of disciplines and rewarding "out-of-the-box" thinking by individuals.

The national security community's leadership needs to focus on knowledge management as a core capability and to emphasize that information technology is only one of many ways in which to achieve it. As the demand for knowledge-management technologies and techniques grows in the public sector, so will new options such as information marshalling services, training and educational techniques, nontextual communications, and nonlinear narrative, as well as advanced context-processing techniques.

The national security community is arguably one of the greatest collections of information and knowledge "niche markets" gathered under one umbrella. A positive benefit of the past emphasis on information technology is that now information and knowledge-based products can be, in nearly real time, tailored quite close to users' needs. This kind of service, however, would require substantial rethinking of how that community marshals information, in particular intelligence.[13]

6.1.5 A Revolution in Thinking

Much of what has been written about a "revolution in military affairs" (RMA) focusses on technology. Many advocates of an RMA argue that technology products and services emerging from the "information revolution" can overcome the problems of information and knowledge flow associated with command and control of high-performance military forces. If one believes, with Clausewitz, that in military activity moral and material forces are inseparable, then a technocentric strategy for an RMA would appear only to preserve and refine traditional means and preferred methods means of warfare.[14] In an ideal world, a knowledge-management system would monitor a decisionmaker, listen to and interpret questions, and retrieve, organize, and deliver whatever a decisionmaker needs to know; but systems are not yet so intelligent. Although they can, for example, search and query structured data and information sources (e.g., databases and documents), systems cannot yet recognize the significant content of an image, analyze a decisionmaker's context, or create knowledge. These are still human skills. The United States cannot yet trade human minds for technology. If a revolution occurs, it will most likely be

---

[13]For example, Amos Kovacs has pointed out that present (1990s) methods for collecting and using imagery intelligence make it possible to supply either highly aggregated, synoptic, and somewhat delayed information to a great many customers or very detailed, customized, timely information to only a few, but not to supply detailed customized, timely information to many. See Kovacs, "Using Intelligence," *Intelligence and National Security* **12**, 4 (1997), 155.

[14]C. Kenneth Allard, "Information Warfare: The Burden of History and the Risk of Hubris," in *The Information Revolution and National Security: Dimensions and Directions*, edited by Stuart J. D. Schwartzstein (Washington, D.C.: CISS, 1996), 234.

sparked by changes in thinking about the nature, character, complexity, and probable evolution of international competition.

6.1.6 Balancing Policy

A balanced approach is best when forming policies that affect the establishment and growth of SKO. Two of the balances urgently needed are presented here, although more, doubtless, will become evident as the national security community becomes more adept at identifying and creating knowledge-building activities.

The balance between technologically driven collection and processing of information and problem-driven building of knowledge. As early as 1986, Clarence McKnight recognized that

> If you look at the genesis of C^3 [command, control, and communications] networks, they deal with sensors, correlation, analysis, decision making and posturing of either military or diplomatic forces, all of which constitute a feedback loop that comes back and forth, but is primarily centered around that human intelligence in the center and the experience of that decision making node—be it the President and his advisors, or the Chairman [JCS] and his advisors, or the duty officer and his people on the floor. You've got to design your systems so as to take into consideration the experience of those people who are in the system; yet this is one thing we forget, and we put in last.[15]

Balance between roles and missions and unified action. Maintaining a balance between the need for functionally aligned organizations to provide training, analysis, research and development, and resource management of information systems according to function and the need for joint, interagency, interdepartmental knowledge marshalling and mobilizing activities is critical.

If the departments and agencies of the national security community did not exist, they would need to be invented. Like most "real worlds," the world of national security is too big to treat as an undifferentiated whole.[16] Breaking it up into specialties—military Services, intelligence agencies, diplomatic services—is essential, even if the boundaries are somewhat arbitrary. McCubbin Owens emphasized the necessity for this type of strategic organizational diversity to provide a hedge against uncertainty, to make competitors' problems tougher, and, as

---

[15]Clarence E. McKnight, Jr., "C^3I Systems at the Joint Level," in *Seminar on Intelligence, Command, and Control, Guest Presentations, 1986* (Cambridge, Mass.: Harvard University Program on Information Resources Policy, I-87-1, February 1987), 1–30.

[16]See Anthony G. Oettinger, *Whence and Whither Intelligence, Command and Control? The Certainty of Uncertainty* (Cambridge, Mass.: Harvard University Program on Information Resources Policy, P-90-1, February 1990), 16.

internal competition will, to strengthen the national security community.[17] The strongest reason for encouraging strategic diversity derives from the saying that a rut is just a grave with the ends kicked out. A diversity of ideas and knowledge produced by specialization is critical to effectively shared problem-solving, deep CK, serendipity, and generally to keeping SKO out of a rut. As discussed in section **3.2.1**, high levels of shared knowledge and cultural homogeneity tend to limit options and produce the same old solutions.

However (as noted in section **6.1.1**), the hierarchical structure and functional divisions of national security organizations are ingrained. Given the cultures, history, and legislative origins of these organizations, assuming they might all cease to act out self-interest unless there were strong policy incentives to do so is unwise. Although the growing crisis of control presents a big incentive for national security organizations to lay aside bureaucratic "food fighting" and instead cooperatively build a true joint, interagency, interdepartmental knowledge management and control system, there is still a need for strong policy and for budgetary and legislative incentives to guide and reconcile the profusion of strategic plans and maintain balance.

6.2 Two New Frontiers for Leadership

While conducting the research for this report, the author collected more than ten strategic plans as well as many supporting documents, all of which describe pieces of the information operation "elephant"; but what remains unclear is whether, once these documents are put together, there really is an elephant somewhere in there. Management of the nation's competitive knowledge is too important either to be left to coalesce eventually through gradual consensus or to be slapped together in response to a train wreck. The national security community's leadership needs to explore aggressively the unknown territory of CKA by sending in multidisciplinary teams of trailblazers and creating incentives and awards for the pioneers who will follow.

The national security community will need to establish an integrated joint and interagency and commercial oversight body with authority to assemble and task collaborative teams to do the following:

- Initiate and sustain, in cooperation with academia and commerce, an interagency/interdisciplinary dialogue on CKA;
- Draft an explicit national strategy for mobilizing and marshalling vast quantities of national security knowledge and information;
- Identify and promote current knowledge-building activities, and recommend and prioritize new CKA for implementation;
- Identify and recommend solutions for overcoming cultural barriers to SKO and CKA; and

[17]McCubbin Thomas Owens, "Use and Abuse of Jointness," a presentation made at the National Security Seminar Series, Massachusetts Institute of Technology, Feb. 4, 1998. Quoted by permission.

- Determine ways to include appropriate nongovernmental and noncommercial organizations (NGOs and NCOs) in SKO and CKA.

It will need to explore new or expanded roles for existing activities. Given the real constraints on national security budgets, leaders will need to be exceptionally creative in finding the resources, especially personnel, to support formal activities mobilizing and marshalling knowledge information. Even if some activities were commercial services, they would still require operational, security, and planning oversight. Several possibilities bear exploring:

- Within constitutional and legislative constraints, consider expanding the charter of the intelligence community beyond traditional collection of only foreign intelligence. Consider redefining intelligence to include information from all sources.
- Use Combat Support Agencies (CSA), such as DISA and DTIC, or create a supporting Unified Command as potential candidates for expanding and operating knowledge-mobilizing activities.
- Consider the possibilities offered by Federally Funded R&D Contractors (FFRDCs) for providing analytical capabilities to catalog tacit knowledge, develop common ontology, and to experiment with prototypical strategies for presenting information.
- Consider the National Guard and Reserves as possible resources for marshalling and mobilizing knowledge, especially given that in civilian life many members are employed in knowledge- and information-technology activities; this option might also increase coordination and enhance shared problem-solving.

6.3 Is the U.S. National Security Community Ready?

According to Machiavelli:

> [I]t ought to be remembered that there is nothing more difficult to take in hand, more perilous to conduct, or more uncertain in its success, than to take the lead in the introduction of a new order of things. Because the innovator has for enemies all those who have done well under the old conditions, and lukewarm defenders in those who may do well under the new. This coolness arises partly from fear of the opponents, who have the laws on their side, and partly from the incredulity of men, who do not readily believe in new things until they have had a long experience of them.[18]

Various programs and planning initiatives already under way indicate growing recognition of the role of knowledge and shared problem solving in national security decisionmaking. Although many of these efforts still tend to be oriented toward only a single function (i.e.,

---

[18]Niccolò Machiavelli, *The Prince*, Chapter Six, "Concerning New Principalities Which Are Acquired by One's Own Arms and Ability," [On-line]. URL: http://www.sas.upenn.edu/~pgrose/mach/chpt6.htm (Accessed May 5, 1998.)

intelligence, transportation, logistics, etc.), on the whole they demonstrate increasing willingness to entertain collective and shared solutions to managing knowledge.

The vision of the 1999–2003 Intelligence Community Information Systems Strategic Plan emphasizes the need of decisionmakers "reliably and securely [to] provide the knowledge needed to make decisions and to take actions, wherever they may be."[19] Although the emphasis of the plan is technical, Goal 1 is to "identify and provide information systems services based on customer needs."[20] Three important objectives are to accomplish the following:

- "Use advanced information technology to enrich the knowledge environment of the customer and to meet evolving customer requirements";
- "[E]nrich the knowledge environment of the customer"; and
- "[M]onitor, measure, and evaluate mission benefits and customer satisfaction."[21]

Other parts of the plan directly address improved marshalling and mobilizing of information through development and implementation of data and information enrichment practices, in particular, tagging data and information products with more bibliographic, contextual, and security information to enhance their substance and interpretive capacity.

Through the Intelink initiative, the Intelligence Systems Secretariat (ISS) of the Community Management Staff (CMS) has for some time been working toward creating collective management of intelligence information. Intelink services are working toward improving access to intelligence community information on-line on classified networks, and Intelink has been essential to breaking down barriers between intelligence customers and the intelligence community and within the community itself.[22]

Two leading initiatives working to mobilize and make effective use of collective knowledge are the Project Genoa of the Defense Advanced Research Project Agency (DARPA) and Joint Intelligence Virtual Architecture (JIVA) of DIA[23] (see section **5.3**). Both initiatives are concentrating on developing activities, knowledge-based methodologies, cognitive tools, and

---

[19]Office of the Director, Intelligence Systems Secretariat (ISS), Community Management Staff (CMS), *Intelligence Community Information Systems Strategic Plan: Enabling a More Agile Intelligence Enterprise: FY 1999–2003* (Washington, D.C.: ISS CMS, November 1997), 1.

[20]Ibid., viii.

[21]Ibid.

[22]Comparisons made by the author in April and May of 1998 showed that Intelink, while a relatively new activity, compared favorably to many commercial knowledge and information mobilizing services, and was experimenting with context-based information processing capabilities similar to those used by top commercial leaders Yahoo!™, Excite™, Infoseek™, and Lycos™.

[23]Project Genoa, [On-line]. URL: http://genoa.wwwhome.com/briefing (Accessed Jan. 15, 1998); JIVA Program Office, *Focus on Intelligence a Strategic Plan*: *Joint Intelligence Virtual Architecture Strategic Plan* (Washington, D.C.: DIA, February 1997), 10.

automated capabilities for marshalling and mobilizing information from all sources; both emphasize the importance of collaborative and shared problem-solving. Project Genoa is focussed on crisis management operations, while JIVA is concerned mainly with intelligence support for military operations. Both are concerned with first-time "discovery costs" of newly created knowledge and with potential sources of the human expertise necessary to staff marshalling and mobilizing activities that cannot be automated.[24]

The military transportation community, under the auspices of USTRANSCOM, has been working to develop collective knowledge and management activities to support transportation capabilities. Its Global Transportation Network (GTN) initiative has developed extensive transportation information marshalling and mobilizing capabilities. Its Joint Mobility Control Group (JMCG) initiative is developing completely integrated collaborative planning and coordination for the DOD's transportation services. USTRANSCOM's LOGBOOK initiative has developed context-based knowledge-management tools designed for command-and-control center activities and used for collectively managing knowledge and information associated with transportation planning and operations. As of early 1997, the LOGBOOK software was being integrated into the Global Command and Control System to make the software available throughout the national security community.

The strongest indicator that it is time for creating capabilities for managing CK is the growing awareness in industry and academia of the importance of managing knowledge. Thomas H. Davenport and Lawrence Prusak,[25] Dorothy Leonard–Barton,[26] and Ikujiro Nonaka and Hirotaka Takeuchi ,[27] among others, have found interest in their writing and their concepts of knowledge management has been increasing. Educational institutions the Harvard Business School and the School of Public Policy at Georgia Institute of Technology (Georgia Tech) offer courses in the management of knowledge assets. Major information technology consulting companies and software houses are marketing knowledge management expertise and software, and many major corporations, frustrated by inadequate returns on information investments, have created senior executive positions with titles such as "chief of knowledge officer" to oversee and develop knowledge-management activities.[28] According to Howard Millman, large companies are realizing the cost of knowledge and employing specialists, called "subject matter experts,"

---

[24]Interviews by the author with David Lee and Lt. Commander Dan Driscoll, USN, for JIVA, DIA, Feb. 3, 1998; and James Kelley, for Project Genoa, Syntech Corp., Feb. 4, 1998.

[25]Thomas H. Davenport and Laurence Prusak, *Working Knowledge: How Organizations Manage What They Know* (Boston: Harvard Business School Press, 1998).

[26]Leonard–Barton, *Wellsprings of Knowledge*.

[27]Ikurjiro Nonaka and Hirotaka Takeuchi, *The Knowledge Creating Company* (New York: Oxford University Press, 1995).

[28]See WWW Virtual Library on Knowledge Management, edited by Yogesh Malhotra, [On-line]. URL: http://www.brint.com/km/ (Accessed June 16, 1998); see also Andersen Consulting, *Thought Leadership—Managing Intellectual Assets*, [On-line]. URL: http://www.ac.com:80/services/cstar/cstr_thought4.html (Accessed June 17, 1998).

"domain experts," or "competitive-intelligence professionals," to relieve decisionmakers and operational activities of the burden of mobilizing and marshaling information and knowledge.[29]

6.4 Knowledge Management Must Be Explicit

Dialogue on infrastructure and on defensive, offensive, and foreign intelligence components of its information operations has been extensive, internally and in public. Comprehensive discussion, however, of how to manage knowledge resources is only now emerging, mainly in business and in academic research,[30] and dialogue on how to create usable working knowledge[31] and gain a competitive strategic advantage from vast national security information resources is embryonic. To make SKO both a core competency and an explicit part of U.S. national security policies and strategy; the United States would need to establish a sustained, interagency, interdisciplinary dialogue to articulate doctrine clearly and expand the understanding of the nature and role of knowledge in international competition and the specific strategic ends that knowledge activities can support.

---

[29]Millman, 128.

[30]Although researchers and educators such as Davis, Leonard-Barton, Nonaka, and Oettinger have been pursuing this question since as early as the 1960s, most publications and studies on knowledge-management publications and have appeared since the early 1990s.

[31]Davenport and Prusak coined this term in title of their book on knowledge management, *Working Knowledge*.

Acronyms

AFCEA	Armed Forces Communications and Electronics Association
AI	artificial intelligence
C^3	command, control, and communications
C^4I	command, control, communications, computers, and intelligence
CIA	Central Intelligence Agency
CIIR	Center for Intelligent Information Retrieval
CK	collective knowledge
CKA	collective knowledge activities
CMS	Community Management Staff
COO	chief operating officer
CSA	Combat Support Agencies
CSIS	Center for Strategic and International Studies
DARPA	Defense Advanced Research Project Agency
DDS	Defense Dissemination System
DIA	Defense Intelligence Agency
DISA	Defense Information Systems Agency
DOD	Department of Defense
DOE	Department of Energy
DOS	Department of State
DTIC	Defense Technical Information Center
EOP	Executive Office of the President
FFRDCs	Federally Funded Research and Development Contractors
FMFM	Fleet Marine Field Manual
GCCS	Global Command and Control System
GTN	Global Transportation Network
IAC	Information Analysis Center
IMO	Intelink Management Office
INSS	Institute for National Strategic Studies
ISS	Intelligence Systems Secretariat
JMCG	Joint Mobility Control Group
JCS	Joint Chiefs of Staff
JIVA	Joint Intelligence Virtual Architecture
JWICS	Joint Worldwide Intelligence Communications System

NAICS	North American Industry Classification System
NCO	noncommercial organization
NDU	National Defense University
NGO	nongovernmental organization
NIPRNet	Nonclassified Internet Protocol Router Network
NTIS	National Technical Information Service
PSYOPS	psychological operations
RMA	revolution in military affairs
SIPRNet	Secret Internet Protocol Router Network
SKO	strategic knowledge operations
TENCAP	Tactical Exploitation of National Capabilities
USTRANSCOM	U.S. Transportation Command

PPMYERS

ISBN 1-879716-64-X