STRATEGY RESEARCH PROJECT

KNOWLEDGE STRATEGIES: BALANCING ENDS, WAYS, AND MEANS IN THE INFORMATION AGE

BY

LIEUTENANT COLONEL WILLIAM R. FAST
United States Army

USAWC CLASS OF 1996

U.S. ARMY WAR COLLEGE, CARLISLE BARRACKS, PA 17013-5050

USAWC STRATEGY RESEARCH PROJECT

KNOWLEDGE STRATEGIES: BALANCING ENDS, WAYS, AND MEANS IN THE INFORMATION AGE

by

Lieutenant Colonel William R. Fast

United States Army

Colonel William J. Doll

Project Advisor

U.S. Army War College

Carlisle Barracks, Pennsylvania 17013

ABSTRACT

AUTHOR: William R. Fast (LTC), USA

TITLE: Knowledge Strategies: Balancing Ends, Ways, and Means in the Information Age

FORMAT: Strategy Research Project

DATE: 15 April 1996 PAGES: 27 CLASSIFICATION: Unclassified

Information age technologies are changing values and national interests, both of which drive the formulation of national security strategy. The *strategy equals ends plus ways plus means* paradigm must change. Information age knowledge strategy seeks the *ends* of cooperative and dynamic competition, uses the *ways* of network node control and organizational adaptation, and requires the resource *means* of valued information enhanced by experience in exploiting that information. A successful information age security strategy requires that we balance the *ends, ways, and means* of knowledge strategies. Whether we use the political, economic, military, or informational elements of national power, we serve our strategic ends best when we cooperate to shape robust information networks that promote dynamic competition and enhance mutual performance both in the public and private sectors. Further, we must control network nodes and communications links and secure our information resources. The security and integrity of our cyberspace must be considered an important, if not vital national interest.

Introduction

As we enter a new technological age, devising the proper national security strategy can have a profound effect on the outcome of war. There is no better example than the French approach after World War I. During the interwar period from 1919 to 1939, France formulated a weak and vulnerable strategy of forward defense, driven by her obsession with the methodical battle technique perfected at the end of World War I. On 10 May 1940, the world watched with horror as Germany, with far fewer resources, successfully invaded the Low Countries and Northern France. Germany had made the right strategic choices; her blitzkrieg concept of warfighting took full advantage of the mechanization of warfare.[1] While France was mired in an older strategy, Germany was energized by emerging technology to develop a bold offensive strategy.

Today, man's ways of making war are changing again because of new information age technologies. What can we do today to avoid repeating the French debacle? In War and Anti-War, Alvin and Heidi Toffler argue that we need to formulate a capstone concept of knowledge strategy to effectively take advantage of these information age technologies.[2] In other words, we need to understand the *ends, ways, and means* of information age strategy.

Change introduced by the information age is arguably greater than that which faced the post-World War I nations.[3] Moreover, knowledge strategy encompasses more than the military element of power. Knowledge strategy must also address the political and economic aspects of power, which become even more useful in the information age. Further, the extent to which we allow our organizational structures and social patterns to change will determine the success of knowledge strategy.

This paper describes the effects of information age technologies on our values and national interests, both of which drive the formulation of security strategy. It also explains how the *ends, ways, and means* paradigm of strategy must adapt to the emergence of information age warfare.[4] Finally, this analysis postulates a framework for formulating knowledge strategies.[5] To

begin, we must understand how the information age is changing our values and interests.

Changing Values and National Interests

Values. The information age brings a new level of personalization to our world that changes the value of consumer products and services. When ordering a new car, computer, or even new suit of clothes, we can customize the item to our needs, desires, and even our own physical measurements. While our personal buying habits have always characterized us as individuals, now the vendor can easily capture our unique preferences on bits of digital information. The value added to a product customized to personal preference is the value of knowledge. No longer do we have to accept the statistical norm.[6] We have come to expect and receive personalized products and services. We value personalization. Now the information-based market can tap this added value.

Americans also value their rights as individuals. The information age promotes and enhances these rights by empowering the individual. Unlike television and radio, information age digital communications allow on-demand programming -- we simply have to ask explicitly for what we want and when we want it. With a computer terminal and telephone modem, an individual can trade shares any time of the day on any of the world's major stock exchanges. Telecommunications and virtual reality technologies make it possible for doctors at the Mayo Clinic to perform surgery on patients in any part of the world. In sum, the information age empowers individuals with access, mobility, and the ability to effect change anywhere, instantaneously. This is what makes the information age so different from the past.[7]

The value that we place on personalization and individual rights affects our world view and our expectations of nation-states. Single-issue politics forces our government to act on problems that are important to a few but often secondary to the majority. For example, the narrow interests of lobbyists

have a disproportionate impact on legislation passed by the U.S. Congress. Knowledge workers, arguably better informed in their narrow fields of endeavor than government regulators, increasingly resent and even oppose government intervention.[8] They use the words *privatize*, *liberalize*, and *deregulate* when advocating the rules for applying information age technologies to businesses.[9] We must be careful not to politically disenfranchise these knowledge workers and their virtual communities.[10]

Spurred by information age technologies, our highly personalized social and political processes have become interconnected and nonlinear, making it difficult to distinguish cause from effect and effect from cause. We have created more nodes of power and influence. Our cyber-future will feature direct participation by the individual as opposed to group representation.[11] As a result, the relevance of authority and sovereignty have diminished.[12] This is not bad. In 1787, James Madison said: "To give information to people is the most certain and the most legitimate engine of government."[13] Yet harnessing the power of that engine is the challenge of knowledge strategy. How do we define national interests and objectives, the *ends* of strategy, in the information age?

National Interests. As its value increases within our global economy, information is fast becoming a strategic national asset. Natural resources (minerals, oil, etc.), long the strength of a growing industrial economy, are becoming less important. This is because information-based economies place more importance on intellectual capital and intellectual labor than on material capital and physical labor.[14] In addition, the computers that manipulate this information are potential first-strike targets. Most of our $6 trillion domestic economy depends upon our 125 million computers tied together by land- and satellite-based communications.[15] Protecting this infrastructure must now be considered as a primary security objective.

We have already witnessed the growth of national economic partnerships. An example is the partnership of American Airlines, MCI, and Citibank. Travel on American Airlines, phone calls on MCI, and charges on Citibank's credit

card now earn free American Airlines trips for the user.[16] Through networking, the information age will allow more international economic alliances as well. The paradox is that networked economic alliances decrease the sovereignty of the nation-state. When the exchange of value occurs by electronic transmission rather than the transfer of products, trade policies become less important than the location of the network nodes.[17] Governments that take the lead in understanding and building networks will gain enormous comparative advantages.[18] Thus, pursuit of economic well-being and prosperity take on new prominence in the information age.

Similarly, the information age elevates the importance of political interests over security interests. Information age technologies can seriously erode totalitarian regimes. The political change in Central and Eastern Europe from 1989 to 1991 was not the aftermath of war, but the result of peaceful movements for individual rights, democracy, and better economic conditions.[19] Encouraging the nations and peoples of the world to value human rights and democratic principles becomes easier with the Internet and direct broadcast television. In addition, political alliances become easier to maintain as common understanding replaces chaotic misunderstanding. The Clinton administration has understood this shift. One objective of Clinton's National Security Strategy is the enlargement of the community of democratic states committed to free markets and respect for human rights.[20] Clearly, information age technologies are tools of preventive diplomacy; they can help promote democracy and human rights in those states where we have the greatest concerns for stability and security.

Thus, the information age has changed the nature of our economic and political interests and impacted on our national security interests. During the Cold War, concerns for power balance drove our economic policies and diplomatic relations. It was a zero-sum game. Trade sanctions, embargoes, and prohibitions on exporting critical wartime technologies severely distorted our economic policies. At times, we supported nations despite their politics or stand on human rights so long as they didn't embrace communism. Unlike the

Cold War era, political and economic interdependency in the information age requires cooperation and the open exchange of knowledge.[21] We now play in a non-zero-sum game where win-win outcomes are not only expected but are required for democracies and information-based economies to flourish.

More than 2,300 years ago, the ancient Chinese strategist Sun Tzu appreciated values, interests, and the rational comparison of power. Before launching a military campaign, he said that the temple council should compare unity on the homefront and the morale of the army with that of the enemy. He also understood the inevitable economic burdens that war laid upon the people.[22] So it is today. Understanding shifts in our values, interests, and in the relative importance of the elements of power helps us understand why the *ends, ways, and means* paradigm of national security strategy must change in the information age.

Changing the Ends, Ways, and Means Model of Strategy

The *ends, ways, and means* paradigm posits that *strategy* equals *ends* plus *ways* plus *means*. *Ends* are expressed as national objectives drawn from national values and interests. *Ways* are courses of action to achieve *ends*. *Means* are the resources (manpower, materiel, money, forces, logistics, etc.) required to support each course of action. Unless *ends, ways, and means* are compatible and in balance, the strategy will be at risk. And the greater the imbalance, the greater the risk.[23] The information age changes all three elements of the strategy equation.

Ends. In the information age, national objectives (*ends*), other than the protection of the national information infrastructure, are not easily identifiable. Clearly, the emergence of global economic networks delink national corporations from national markets and turn them multinational. For example, profits from the sale of a new Boeing 777 aircraft find their way into countries worldwide. Boeing is a broker in the global economic network, buying materials and components worldwide, basing its acquisitions on price,

availability, quality and any other number of factors. In effect, Boeing attempts to optimize its entire operation globally. As it does so, it pays little attention to national allegiance. In such an environment, governmental influence over Boeing's purchases becomes problematic. Then the implications of a power struggle between government and industry are very real.[24]

Economic security and prosperity in the information age are functions of a kind of equality between nations and firms. The more firms act internationally, as in the Boeing example, the less they can be held to national accountability. Walter Wriston asserts that "Capital will go where it is wanted and stay where it is well treated."[25] Multinational firms play one nation-state against the other as they seek the greatest profit.[26] Now trade agreements among sovereign nations are really inadequate when they don't include the concerns of global business organizations.[27] The North American Free Trade Agreement and the European Union are recent attempts of nations to achieve competitive equality with the growing multinational economic networks. Yet, in a global information age economy, it will be futile for sovereign states to attempt to cut off and control even part of the world market.[28]

The organizing principles for the analysis of power have changed. Multinational firms anticipate events and react quickly in global markets. But governments, whose policies are geographically bound, react more slowly.[29] Power in the information age depends more on the ability to influence access and interconnection than on the capacity to enforce borders. It follows that the *ends* of our national security strategy will depend less on confrontation with opponents and more on cooperation and trust among competitors.[30] Moreover, total agreement on objectives within a globally linked network is virtually impossible.

If national economic objectives can't be achieved due to the emergent global and networked nature of markets, why not ignore global markets completely? Well, ignoring the networked global markets is risky business, if not impossible, for either a nation-state or a business concern. Each year since 1965, the U.S. commercial sector has invested more of its dollars in

research and development than has the Department of Defense (DoD).[31] If our military services are to preserve their technological superiority over potential foes, they must have access to these commercial products. Similarly, individual businesses can afford neither the enormous costs nor bear the high risks of remaining on the leading edge of all information age technologies. Yet they can't afford to miss a breakthrough that could create new product lines. When businesses share intellectual capital (knowledge) through participation in global markets, they avoid isolation from new technologies.[32]

Obviously, the *ends* of our strategy equation have become unclear, since it may be difficult to achieve all desired national objectives in the globally networked information age. At best, a sovereign nation might effectively pursue its interests only as it paradoxically subordinates those interests to the common interests of all networked partners.[33]

Ways. It is not difficult to show how the *ways* of security strategy change with the information age. For example, information age weapons are equalizers. They help small nations against large nations and favor the weak over the strong. Examples include Stinger missiles used by the Mujahedin against the Russians and computer viruses designed to invade individual weapon systems or an entire defense computer network.[34] However, the real problem lies in the fact that today's breakthrough technologies in electronics, computer systems, software, and telecommunications come from the commercial marketplace and are available to anyone in the world. Furthermore, foes may use these technologies to their advantage without even resorting to military applications.

In broadest terms, information warfare is not new. It encompasses any hostile activity directed against our knowledge and belief systems.[35] Cyberwar, the newest subset of information warfare, needs no battlefield -- it is fought in cyberspace. Cyberspace includes information itself, the communication nets that move it, and the computers that make it useful.[36] Cyberspace can be influenced and at times dominated by anyone possessing

inexpensive computers linked into existing global communication nets. The enemy may exploit global business organizations that produce cyber technology and determine the patterns of change.[37] He may attempt to propagate waves of data big enough to crash the network by overloading network switches.[38] Cyberwar operations can blind us electronically and may change the definition of what is a hostile attack and what determines defeat.[39]

Under the microscope of world opinion formed by means of pervasive communication satellites, open warfare is no longer an option for sovereign nations to pursue their national interests.[40] Cable News Network coverage can rapidly trigger a negative international response, as we have seen during the recent wars in Somalia and Bosnia. However, the information age offers a more subtle approach -- waging a quiet war in cyberspace where digital fingerprints are hard, if not impossible, to trace.[41] When information warfare enters and uses public cyberspace, collateral damage may be significant. Banking, finance, telecommunications, trade, travel, energy, and cultural systems are vulnerable.[42] Misinformation and disinformation campaigns are easily mounted and hard to defend against. Moreover, an adequate defense depends upon gathering, analyzing, and distributing intelligence to a flexible, networked interagency team.[43]

So, the information age introduces at least three new concepts in the *ways* of strategy. First, information age weapons are equalizers and can negate the military principle of mass. Second, cyberwar needs no battlefield and therefore no specially trained military organization -- even civilians may participate. Finally, the initial offensive strike in a quiet cyberwar would be hard to detect and to defend against. It is also impossible to limit the cyberwar battlespace to purely military networks.

Another way of assessing the changes in the *ways* of strategy is to compare World War I and II warfare to information age warfare. Whereas the world wars used attrition (WW I) and maneuver (WW II), information age war emphasizes control. Whereas the world wars attempted to exhaust (WW I) and annihilate (WW II), cyberwar seeks to paralyze. And whereas the tools of the

world wars were firepower weapons (WW I) and mechanization (WW II) produced in mass, the tools of information war are limited numbers of inexpensive computers linked via global communication systems.[44]

Means. Knowledge as a resource is not included in the current resource paradigm of manpower, materiel, money, forces, and logistics.[45] Knowledge, the "ammunition" of information war, is inexhaustible. Once produced (at a cost), knowledge can be used repeatedly -- it will not disappear. In fact, it only increases! Digital knowledge can be copied and never missed. It can be given away but still kept. Digital knowledge can be distributed instantly. It is non-linear; it defies the theory of economy of scale.[46] Knowledge is the key element of wealth in the information age. Compared with industrial age manufacturing, information-based industries can produce more with fewer resources, less energy, and less labor. Production runs of *one* are possible and even economical with intellectual capital (knowledge) encoded in software and used by smart machines.[47] The result is an explosion of personalized products and services.[48] Moreover, knowledge to inform people, coded as digital bits, can be turned into audio, video, or even graphics -- it is "mediumless."[49] Manpower, materiel, and forces, on the other hand, possess *none* of these characteristics.

Knowledge as a resource is often cheaper than materiel. It uses limited manpower or forces and may require little or no logistics. Thus the information age opens the doors to the resource poor. Knowledge diffuses and redistributes power to the weaker actors. It redraws boundaries and time and space horizons. It enables organizations to open up.[50] When it comes to balancing *means* with *ends* and *ways*, knowledge as a resource offers an economical solution.

In sum, it is difficult to apply the *ends, ways, and means* paradigm of strategy to information age security. Unlike traditional *means*, knowledge is relatively cheap and easy to balance with *ends* and *ways*. Unlike conventional *ways*, cyberwar defies the military principle of mass. And its primary objectives are control and paralysis. Unlike the clearly articulated *ends* of

Cold War security strategies, national objectives in a globally networked information age are more difficult to define and thus to achieve. Clearly, we need a new framework for formulating information age knowledge strategies.

A Framework for Formulating Knowledge Strategies

We can formulate knowledge strategies only with an understanding of the strategic environment of the information age. We can characterize this environment through three central concepts: cooperative and dynamic competition, the wisdom pyramid, and the productivity paradox. Also important is an understanding of how the bureaucracies of the industrial age might transform into the cyberocracies of the information age. Finally, we must review the importance of information dominance in cyberwar. This background and understanding will enable us to develop a formula for knowledge strategy.

Strategic Environment. In Being Digital, Nicholas Negroponte proclaims with optimism that "the control bits of that digital future are more than ever before in the hands of the young."[51] This is a profound statement when you consider the relatively advanced age of those who are currently responsible for formulating knowledge strategies! Fortunately, commercial knowledge industries are at the forefront in formulating knowledge strategies; they can enlighten us on the characteristics of the strategic information age environment.

The movement of portions of the silicon chip industry from Northern California to Bangalore, India, is an example of the environment knowledge industries create. Historically, innovative entrepreneurs in the Silicon Valley in California have made our computer chips. Now it seems that much of this chip design and engineering has moved to Bangalore. The reason: Bangalore engineers work for $500 per month, compared with $15,000 per month for an engineer in the Silicon Valley. Further, it is no coincidence that Bangalore is also the center of the Indian atomic energy industry. As American firms pour money for computer chips into Bangalore, one must ask what

this investment is doing for India's nuclear weapons program? Clearly, the ability of our government (or the government of India) to control such economic activity at the national level is in steady decline as the entrepreneurial net draws the entire world more closely together.[52]

In a global information economy, the growth rates of individual countries should converge over time. As in the silicon chip example, India gains the newest, most innovative computer chips while U.S. firms absorb all the costs and risks.[53] Moreover, such alliances could create new free markets. Cybernations consisting of many like-minded virtual companies with cyber-economies could emerge. Cultures that have vanished from the real world may yet be reborn in cyberspace. A network superpower may emerge.[54] Thus, the strategic environment of the information age equalizes competitors while creating a potential for international instability.

Cooperative and Dynamic Competition. Another lesson of the silicon chip industry is that knowledge industries today seek cooperative competition, a framework that simultaneously enhances mutual performance but shapes the form of their competition. The United States could also pursue a strategy of cooperative competition in building global information age networks that would allow her to pursue her national objectives in concert with other nations. Most important, cooperative competition would allow us to shape the competition by controlling the protocols of these information networks.[55]

We can become a strategic network broker, balancing competition and cooperation with other nations by controlling access to and participation in these networks. As the strategic broker, we would have the upper hand in formulating the rules for competition. Yet the fact that we cooperate with the nations of the world promises them benefits such as converging growth rates. All nations could compete for the location of high value economic activities. Within the U.S., cooperative competition would promote a healthy domestic environment of technological and organizational innovation. Government policy would not stifle but encourage and support industry to reach out and tap knowledge banks throughout the world. In the information age, an

alternate strategy of isolation supported by policies to shelter domestic industry (as experienced in the industrial age) could have disastrous consequences.[56]

Beyond cooperative competition, we also need *dynamic competition*: competition that allows new technologies to compete against and replace older technologies. In earlier times, dynamic competition gave us the automobile while the world was still looking for stronger horses (termed *static competition*). In the 1980s, dynamic competition transformed the computer industry from mainframes to mini and personal computers. It gave the U.S. world dominance in telecommunications, mircroelectronics, computer networking, and software applications. Significantly, American business and technological leadership created these vast new markets, not government oversight or policy making.[57] Through dynamic competition, we can further shape our competition and reap the greatest possible benefits from our information age economy.

Wisdom Pyramid. While the information age equalizes competitors, the wisdom pyramid mitigates against instability. Visualize a pyramid with the base composed of *raw data*. Add the next layer and call it *information* that rises like cream to the top of the data. On top of information, lay down another layer called *experience*. Finally, cap the pyramid with *wisdom*. Each person is a product of his or her own experience. Information, filtered up through that experience, creates wisdom at the top of the pyramid.[58] So it is with nation-states. The data and information others gain through information age networks has real value only as it filters through real experience. More important, corporate knowledge embedded in teams -- like NASA's team that put man on the moon -- is knowledge that none of the individual team members knows alone.[59] Embedded knowledge is hard, if not impossible, to steal. Thus our experience and social networks that develop and use information technologies are precious commodities. We can identify them as our strategic center of gravity in the information age environment.

Productivity Paradox. Another precept of the information age is that useful applications of knowledge require adaptive organizations and processes.

The productivity paradox says that, initially, organizations will insert new information technologies into existing organizational structures. These technologies will simply improve the speed and increase the efficiency of current processes. However, to take full advantage of the technology, organizations need to change their processes and adapt their structures.[60] In this way, we tailor our knowledge to specific applications and capture the value of exchanged information.[61]

Information age military forces, evolving in their use of cyberspace, will follow the same path -- first accommodating information technologies by incorporation, and next by reinventing their processes and adapting their organizational structures.[62] We see technological incorporation in the Army's effort to digitize the battlefield. The objective today is to add "applique" computers to combat vehicles to improve situational awareness. Yet true leveraging of computers depends less on improving situational awareness in every combat vehicle and more on how the entire combat force reconfigures itself to exploit the knowledge gained through the added technology. Such reinventing exploits the exponential power of information networks.

Success in future wars will require armed forces with open, adaptable organizations that can react more quickly to changes than can the competition.[63] These organizations must easily reconfigure to fill specific needs, saving time and money in the process. Such open organizations are not wedded to any one operating system; they can rapidly incorporate new information age technology. Ultimately, they must be adaptable to the knowledge they use.

Cyberocracy. The differences between a bureaucracy of the 20th century and a cyberocracy of the information age highlight the importance of organizational adaptation. Whereas bureaucracy forces and often limits information flow through defined channels connecting discrete points, cyberocracy broadcasts large volumes of information among many interested parties. Whereas bureaucracy emphasizes the hard quantitative skills of programming and budgeting (like DoD's Planning, Programming, Budgeting and

Execution System), cyberocracy emphasizes soft skills such as policy management and understanding culture and public opinion. Whereas bureaucracy observes traditional boundaries between public and private sectors, cyberocracy breaks across these boundaries and allows for mixing of public and private interests. Bureaucracies must transform into cyberocracies if the new techniques of the information age are to take hold.[64]

A cyberocracy should have greater capability than a bureaucracy for dealing with the complex issues of an interconnected world. Yet to transform our organizations we must break the paradigm that establishes "big budgets" and "big staffs" as the basis of bureaucratic power. We must demonstrate the value of "big information" as the source of power in a cyberocracy.[65]

Information Dominance. In Infotrends, Jessica Keyes notes that "Most organizations suffer from a proliferation of data that is either redundant or underutilized. These same organizations suffer from not recognizing the true value of their data."[66] Once the value of data is understood, knowledge derived from that data can be used offensively to increase an edge or defensively to reduce an edge held by an opponent.[67] The ability to recognize the value of data and use this data to derive knowledge is the first step toward information dominance.

Information dominance is achieved by transforming knowledge into capability. It is the ability to identify the vulnerabilities and centers of gravity of an enemy, or even a competitor or customer. It is the capability to reshape organizations and revise strategies based upon a systematic analysis of the opponent.[68] For example, Federal Express (FedEx) won unchallenged leadership in global express delivery services when it realized "that information about the package is just as important as the package itself."[69] Understanding that the customer cares about where his or her package is at anytime, FedEx transformed its knowledge of bar coding, hand held computers, and global telecommunications into the capability to provide near real-time location information on every package in their possession.[70]

Knowledge-based alliances that share resources and save costs can also

propel technology to new heights while preserving competition. For example, IBM and Apple Computer agreed in 1991 to share knowledge to create a new computer operating system based upon object-oriented technology and desktop multimedia software. Such a venture was too costly for just one company to undertake.[71] Recognizing strategic uses of information technology and leveraging intellectual capital, as in the cases of FedEx, IBM, and Apple Computer is truly in the realm of strategic art. However, as we found with the productivity paradox, such success comes through process and structural changes within the organization.[72]

At the national strategic level, we should build flexible organizations (cyberocracies) around information and intelligence processing, rather than around traditional functions and bureaucratic departments.[73] National information dominance is achieved through the fusion of all networks (similar to the fusion of human, signals, electronic, and other kinds of intelligence into *all source* intelligence). Offensively, national information networks can change the minds of our adversaries if they are synchronized to carry specific but coordinated messages.[74] Defensively, a national information security strategy is required for the protection of our key information systems, to include their nodes, communications links, and data. The effort exceeds the responsibilities of the joint military services; critical information and networks belonging to all federal agencies, the private sector, and even our allies must as well be protected.

A Formula for Knowledge Strategy. To this point, we have identified several facets of the strategic information age environment and cybercratic institutions that shape knowledge strategies. Before redefining the strategy paradigm, we must recall two additional characteristics of network theory: First, value is added only at nodes; second, the strength of networks comes from their redundancy, or multiple pathways between any two points.

Consider our nation's interstate highway network and how it has enabled our economy to grow. Many businesses and industries locate close to city beltways (nodes) and bring great wealth to these areas. Moreover, when

adverse weather or construction blocks one route, usually a near-by route can handle the traffic. Similarly, governments that take the lead in shaping information networks and in locating nodes within their borders stand to reap enormous comparative advantage.[75] Because of multiple nodes and pathways, networks have no center of gravity and must be defeated in detail.[76] Moreover, bureaucracies might be defeated by networks (cyberocracies), so it may take networks to counter other networks. "The future may belong to whoever masters the network form."[77]

With some modification to the meaning of the additive terms, knowledge strategy fits the *strategy equals ends plus ways plus means* equation. It follows from the discussions above that knowledge strategy (KS) seeks the *ends* of cooperative and dynamic competition (C/DC), uses the *ways* of node control and organizational adaptation (NC & OA), and requires the resource *means* of valued information (VI) enhanced by experience (E). Symbolically, the strategy equation changes to this:

Knowledge Strategy =	Cooperative/Dynamic Competition	+ Node Control & Org. Adaptation	+ Information Dominance
KS =	(C/DC)	+ (NC & OA)	+ (VI x E)
Strategy =	*Ends*	+ *Ways*	+ *Means*

Cooperative and dynamic competition permits us to pursue our national security objectives in concert with other nations while shaping the competition. Control of network nodes adds value to information, strengthening information dominance and denying dominance by others. Organizational adaptation overcomes the productivity paradox and ensures that we exploit information networks to their fullest potential. Finally, knowledge strategies require information dominance that comes from the value of information enhanced by experience.

Knowledge strategies incur a degree of risk unless we balance all elements of the equation. Unbalanced conditions can result if cooperative and dynamic competition are not the stated objectives of the strategy, if we don't control the network nodes, if productivity suffers because the organization hasn't truly adapted to the technologies, or if the value of information is

high but the experience to exploit this information is low.

Knowledge strategies focus on the important role of a strategic broker in crafting the rules of information networks and in locating the nodes. They shape a strategic environment that promises technological and organizational innovation both in the public and private sectors. Moreover, knowledge strategies promote cooperative and dynamic competition that enhance mutual performance while shaping the form of competition.[78]

Conclusion

The information age has shifted the focus of our values and national interests. Empowered by information age technologies, we have come to value individual preference in products and services and direct participation in the democratic process. Similarly, the pursuit of economic well-being and the promotion of democratic values takes on added importance in contrast to our traditional security interests. Information is fast becoming a strategic national asset. Thus, the security and integrity of our cyberspace must now be considered an important, if not vital, national interest that we cannot afford to compromise.

A successful information age security strategy requires that we balance the *ends, ways,* and *means* of knowledge strategies. Whether we use the political, economic, military, or informational elements of national power, we serve our strategic *ends* best when we cooperate to shape robust information networks that promote dynamic competition and enhance mutual performance. Ironically, global information networks, built to bring peace and prosperity to the world, will be among the first attacked in a cyberwar. Denying access to these networks in hopes of preempting attack is totally counterproductive: it accomplishes the adversary's mission for him! Therefore, before an enemy attempts to fire the first hostile bits across our networks, we must control network nodes and communications links and secure our information resources.

Successful knowledge strategies require the mastery of information

networks. Information networks operate on the win-win philosophy: one wins only if all win. The more our national interests reflect those of the networks, the better chance we have of achieving them. Thus, we must be the primary architects of networks and seek to broker network operations. At times, we must be willing to subordinate our national objectives to the greater objectives of the networked nations and multinational firms with whom we interact. We must be willing to share knowledge resources and enter into knowledge-based alliances that allow us to leverage information age technologies. Our government can empower information age enterprise and encourage innovation by easing access to global networks. In relations with other nations, we should trade economic network integration for democratic and human rights reform. A more stable and safer world is one whose players share similar values and interests and who depend upon each other in a globally networked market economy.

We must realize that our strategic center of gravity is shifting to encompass our experience and the virtual communities we establish to exploit the information environment. We must care for our knowledge workers and educate the youth of our nation who will take their place. We can't exploit the information age without them. The "hub of all power and movement" in the information age will be our dominant knowledge.[79] Only through non traditional open organizations with decentralized power structures can we truly achieve this dominance. We must create cooperative cyberocracies organized around the knowledge workers and processes that can best exploit all available information networks. Thus the *ways* of a knowledge strategy must break down the boundaries between government bureaucracies and the private sector. Most important, the extent of organizational adaptation -- and how much it ultimately transforms the rules of information age networks and cyberwar -- will determine whether we are using information age technologies to our fullest advantage.

Finally, to resource information age strategies, we must recognize that knowledge is a very economical *means* that can stretch and positively leverage

our nation's wealth. Declining defense budgets have been -- and will continue to be -- the primary engines transforming the U.S. military and driving information age technologies into the hands of our armed forces. However, just as our armed forces engage in a revolution in military affairs, so must other government agencies and the private sector engage in revolutions in political, economic, and informational affairs. Big bureaucracies with big operating budgets must downsize and leverage the power of information. We must share knowledge resources within the federal government and between the public and private sectors, even as they are transforming to adapt to the information age. We must invest only in those information age technologies and intellectual capital that will generate the most significant returns in information dominance.

Again, we should recall that France's disappointment in World War II was not that she was surprised, but that she made the *wrong* strategic security choices.[80] France knew that war with Germany was coming. So she prepared for that war. However, she failed to understand the significance of the new mechanized age. Germany understood the strategic importance of mechanization and overwhelmed France with the blitzkrieg.

So it is with the United States today. The dawning information age gives us an opportunity to make strategic choices. We must not simply continue the security strategies of the past. Rather, we must seek to understand the strategic importance of knowledge and discover the rules of cyberspace and cyberwar. Understanding how to balance the *ends*, *ways*, and *means* of knowledge strategies is the first step in making the *right* strategic choices for the emerging information age.

ENDNOTES

[1]Robert A. Doughty, The Seeds of Disaster: The Development of French Army Doctrine 1919-1939 (Hamden, CT: Archon Book, 1985), 190; Gordan R. Sullivan and Anthony M. Coroalles, Seeing the Elephant: Leading America's Army into the Twenty-First Century (Hollis, NH: Puritan, 1995), 20.

[2]Alvin Toffler and Heidi Toffler, War and Anti-War: Survival at the Dawn of the 21st Century (Boston: Little, Brown & Co., 1993), 141.

[3]Sullivan and Coroalles, 21.

[4]Arthur F. Lykke, Jr., ed., Military Strategy: Theory and Application (Carlisle, PA: U.S. Army War College, 1993), 3.

[5]Richard A. Chilcoat, Strategic Art: The New Discipline for 21st Century Leaders (Carlisle, PA: U.S. Army War College, 1995), 4.

[6]Nicholas P. Negroponte, Being Digital (New York: Knopf, 1995), 155 and 164.

[7]Ibid., 166, 169 and 231.

[8]Walter B. Wriston, The Twilight of Sovereignty: How the Information Revolution is Transforming Our World (New York: Scribner's, 1992), 38.

[9]Richardo Petrella, "Information Society - Future Prospects" (British Computer Society and UNISYS Annual Lecture, 4 Nov 94); available from http://www.bcs.org.uk/unisys.html; Internet; accessed 14 Apr 96.

[10]Joe Costello, "Electronic Polity" (Quantum Polis, 17 Feb 95); available from http://www.cts.com/browse/joec/qpolis/local.html; Internet; accessed 14 Apr 96.

[11]Joe Costello, "The Organic Information Age" (Quantum Polis, 21 Jun 94); available from http://www.cts.com/browse/joec/qpolis/oia.html; Internet; accessed 14 Apr 96.

[12]Donald N. Michael, "Too Much of a Good Thing? Dilemmas of an Information Society," Vital Speeches of the Day L, no. 2 (1 Nov 83): 54.

[13]John P. Foley, ed., The Jeffersonian Cyclopedia (New York: Funk and Wagnels, 1900), 277.

[14]Wriston, 6.

[15]Winn Schwartau, Information Warfare: Chaos on the Electronic Superhighway (New York: Thunder's Mouth Press, 1994), 12-13.

[16]Jessica Keyes, Infotrends: The Competitive Use of Information (New York: McGraw-Hill, 1993), 200.

[17]James R. Golden, Economics and National Strategy in the Information Age: Global Networks, Technology Policy, and Cooperative Competition (Westport, CT: Praeger, 1994), 16-17.

[18]David F. Ronfeldt, Cyberocracy, Cyberspace, and Cyberology: Political Effects of the Information Revolution (Santa Monica, CA: RAND, 1991), 77-78.

[19]Sir Leon Brittan, "EU Pursues Global Answers: International Economic Instability is New Threat," Defense News 10, no. 48 (4 Dec 95): 27.

[20]The White House, A National Security Strategy of Engagement and Enlargement (Washington: February 1995), 22.

[21]Golden, 7.

[22]Sun Tzu, The Art of War, trans. Samuel B. Griffith (New York: Oxford University Press, 1971), 39-40 and 63-71.

[23]Lykke, 3-5.

[24]Jorge Reina Schement and Terry Curtis, Tendencies and Tensions of the Information Age (New Brunswick, NJ: Transaction, 1995), 63.

[25]Wriston, 61.

[26]Joe Costello, "In Defense of Progress(ives)" (Quantum Polis, 19 Dec 94); available from http://www.cts.com/browse/joec/qpolis/prog.html; Internet; accessed 14 Apr 96.

[27]Schement, 64.

[28]Wriston, 37.

[29]Jerome Glenn, "Japan: Cultural Power of the Future," The Nikkei Weekly (7 Dec 92).

[30]Golden, 16-17.

[31]Paul G. Kaminski, "Investing in Tomorrow's Technology Today," Defense Issues 10, no. 46 (1995): 2.

[32]Golden, 16.

[33]Michael, 41; Wriston, 37.

[34]Wriston, 15.

[35]Richard Szafranski, "A Theory of Information War: Preparing for 2020" (n.d.); available from http://www.cdsar.af.mil/apj/szfran.html; Internet; accessed 14 Apr 96.

[36]G.A. (Jay) Keyworth II, "Telecommunications: More Computing than Communications" (The Progress & Freedom Foundation, 31 Jan 95); available from http://www.pff.org/pff/Telecommunications.html; Internet; accessed 14 Apr 96.

[37]Golden, xiv.

[38]Ian D. Pearson, The Future of Social Technology, 60 min. (Atlanta: World Future Society, 1995), audiocassette and vu-graphs, 19.

[39]John Arquilla and David Ronfeldt, "Cyber War Is Coming!," Comparative Strategy 12 (April-June 1993): 157; available from http://www.stl.nps.navy.mil/c4i/cyberwar.html; Internet; accessed 14 Apr 96.

[40]Wriston, 13-14.

[41]Martin C. Libicki, The Mesh and the Net: Speculations on Armed Conflict in a Time of Free Silicon (Washington: National Defense University, 1994), 26.

[42]Szafranski, 5.

[43]Thomas X. Hammes, "The Evolution of War: The Fourth Generation," Marine Corps Gazette 78, no. 9 (September 1994): 44.

[44]John Arquilla, "The Strategic Implications of Information Dominance," Strategic Review 22 (Summer 1994): 26.

[45]Lykke, 4.

[46]Jerome Glenn and John Peterson, Information Warfare, Cyber Warfare, Perception Warfare and their Prevention, 60 min. (Atlanta: World Future Society, 1995), audiocassette.

[47]Jerry Harris and Carl Davidson, "The Cybernetic Revolution and the Crisis of Capitalism" (The Chicago Third Wave Study Group, 18 Jul 94); available from http://www.bradley.edu/las/soc/syl/391/papers/cyb_revo.html; Internet; accessed 14 Apr 96.

[48]Alvin Toffler and Heidi Toffler, Creating a New Civilization: The Politics of the Third Wave (Atlanta: Turner, 1995), 37.

[49]Negroponte, 72.

[50]Arquilla and Ronfeldt, 142.

[51]Negroponte, 231.

[52]Charles William Maynes, "The World in the Year 2000: Prospects for Order or Disorder," The Nature of the Post-Cold War World (Carlisle, PA: U.S. Army War College, 1993), 21-22; Harris, 8; Pearson, 50.

[53]Golden, 13.

[54]Pearson, 43; Glenn.

[55]Golden, 4.

[56]Ibid., xv.

[57]Esther Dyson et al., "Cyberspace and the American Dream: A Magna Carta for the Knowledge Age" (The Progress & Freedom Foundation, release 1.2, 22 Aug 94); available from http://www.pff.org/pff/position.html; Internet; accessed 14 Apr 96.

[58]Wriston, 176.

[59]Seev Neumann, Strategic Information Systems: Competition Through Information Technologies (New York: Macmillan, 1994), 109.

[60]Ronfeldt, 9-10.

[61]Golden, xiv.

[62]Libicki, 3.

[63]John J. Patrick, Reflections on the Revolution in Military Affairs (Washington: Techmatics, 1994), 8-9.

[64]Ronfeldt, 21.

[65]Ibid.

[66]Keyes, 150.

[67]Ibid., 188-189.

[68]Arquilla, 29.

[69]Fred Smith, founder of FedEx, quoted in Keyes, 194.

[70]Ibid., 192-197

[71]Neumann, 107-108.

[72]Keyes, 198-199.

[73]Stuart Johnson and Martin Libicki, eds., Dominant Battlespace Awareness (book on-line)(Washington: NDU Press, 1995), 30; available from http://198.80.36.91/ndu/inss/books/dbk/dbk1.html; Internet, accessed 14 Apr 96.

[74]Hammes, 44.

[75]Ronfeldt, 77-78.

[76]Libicki, 33.

[77]Arquilla and Ronfeldt, 155.

[78]Golden, xv and 4.

[79]Clausewitz defines *center of gravity* as "the hub of all power and movement"; see Carl von Clausewitz, On War, ed. and trans. Michael Howard and Peter Paret (Princeton, NJ: Princeton University Press, 1976), 595.

[80]Doughty, 190.

BIBLIOGRAPHY

Arquilla, John and David Ronfeldt. "Cyber War Is Coming!" Comparative Strategy 12 (April-June 1993): 141-165. Available from http://www.stl.nps.navy.mil/c4i/cyberwar.html; Internet; accessed 14 Apr 96.

Arquilla, John. "The Strategic Implications of Information Dominance." Strategic Review 22 (Summer 1994): 24-30.

Brittan, Sir Leon. "EU Pursues Global Answers: International Economic Instability is New Threat." Defense News 10, no. 48 (4 Dec 95): 27.

Chilcoat, Richard A. Strategic Art: The New Discipline for 21st Century Leaders. Carlisle, PA: U.S. Army War College, 1995.

Clausewitz, Carl von. On War. Translated and edited by Michael Howard and Peter Paret. Princeton, NJ: Princeton University Press, 1976.

Costello, Joe. "In Defense of Progress(ives)." Quantum Polis, 19 Dec 94. Available from http://www.cts.com/browse/joec/qpolis/prog.html; Internet; accessed 14 Apr 96.

_____. "Electronic Polity." Quantum Polis, 17 Feb 95. Available from http://www.cts.com/browse/joec/qpolis/local.html; Internet; accessed 14 Apr 96.

_____. "The Organic Information Age." Quantum Polis, 21 Jun 94. Available from http://www.cts.com/browse/joec/qpolis/oia.html; Internet; accessed 14 Apr 96.

Doughty, Robert A. The Seeds of Disaster: The Development of French Army Doctrine 1919-1939. Hamden, CT: Archon Book, 1985.

Dyson, Esther, George Gilder, George Keyworth, and Alvin Toffler. "Cyberspace and the American Dream: A Magna Carta for the Knowledge Age." The Progress & Freedom Foundation, release 1.2, 22 Aug 94. Available from http://www.pff.org/pff/position.html; Internet; accessed 14 Apr 96.

Foley, John P., ed. The Jeffersonian Cyclopedia. New York: Funk and Wagnels, 1900.

Glenn, Jerome and John Peterson. Information Warfare, Cyber Warfare, Perception Warfare and their Prevention. 60 min. Atlanta: World Future Society, 1995. Audiocassette.

Glenn, Jerome C. "Japan: Cultural Power of the Future." The Nikkei Weekly (7 Dec 92).

Golden, James R. Economics and National Strategy in the Information Age: Global Networks, Technology Policy, and Cooperative Competition. Westport, CT: Praeger, 1994.

Hammes, Thomas X. "The Evolution of War: The Fourth Generation." Marine Corps Gazette 78, no. 9 (September 1994): 35-44.

Harris, Jerry and Carl Davidson. "The Cybernetic Revolution and the Crisis of Capitalism." The Chicago Third Wave Study Group, 18 Jul 94. Available from http://www.bradley.edu/las/soc/syl/391/papers/cyb_revo.html; Internet; accessed 14 Apr 96.

Johnson, Stuart and Martin Libicki, eds. Dominant Battlespace Awareness. Book on-line. Washington: NDU Press, 1995. Available from http://198.80.36.91/ndu/inss/books/dbk/dbk1.html; Internet; accessed 16 Apr 96.

Kaminski, Paul G. "Investing in Tomorrow's Technology Today." Defense Issues 10, no. 46 (1995): 1-17.

Keyes, Jessica. Infotrends: The Competitive Use of Information. New York: McGraw-Hill, 1993.

Keyworth, G.A. (Jay) II. "Telecommunications: More Computing than Communications." The Progress & Freedom Foundation, 31 Jan 95. Available from http://www.pff.org/pff/Telecommunications.html; Internet; accessed 14 Apr 96.

Libicki, Martin C. The Mesh and the Net: Speculations on Armed Conflict in a Time of Free Silicon. Washington: National Defense University, 1994.

Lykke, Arthur F., Jr., ed. Military Strategy: Theory and Application. Carlisle, PA: U.S. Army War College, 1993.

Maynes, Charles William. "The World in the Year 2000: Prospects for Order or Disorder." The Nature of the Post-Cold War World. Carlisle, PA: U.S. Army War College, 1993.

Michael, Donald N. "Too Much of a Good Thing? Dilemmas of an Information Society." Vital Speeches of the Day L, no. 2 (1 Nov 83): 38-42.

Negroponte, Nicholas P. Being Digital. New York: Knopf, 1995.

Neumann, Seev. Strategic Information Systems: Competition Through Information Technologies. New York: Macmillan, 1994.

Patrick, John J. Reflections on the Revolution in Military Affairs. Washington: Techmatics, 1994.

Pearson, Ian D. The Future of Social Technology. 60 min. Atlanta: World Future Society, 1995. Audiocassette.

Petrella, Richardo. "Information Society - Future Prospects." British Computer Society and UNISYS Annual Lecture, 4 Nov 95. Available from http://www.bcs.org.uk/unisys.html; Internet; accessed 14 Apr 96.

Ronfeldt, David F. Cyberocracy, Cyberspace, and Cyberology: Political Effects of the Information Revolution. Santa Monica, CA: RAND, 1991.

Schement, Jorge Reina and Terry Curtis. Tendencies and Tensions of the Information Age. New Brunswick, NJ: Transaction, 1995.

Schwartau, Winn. Information Warfare: Chaos on the Electronic Superhighway. New York: Thunder's Mouth Press, 1994.

Sullivan, Gordan R. and Anthony M. Coroalles. Seeing the Elephant: Leading America's Army into the Twenty-First Century. Hollis, NH: Puritan, 1995.

Sun Tzu. The Art of War. Translated by Samuel B. Griffith. New York: Oxford University Press, 1971.

Szafranski, Richard. "A Theory of Information War: Preparing for 2020." n.d. Available from http://www.cdsar.af.mil/apj/szfran.html; Internet; accessed 14 Apr 96.

Toffler, Alvin and Heidi Toffler. Creating a New Civilization: The Politics of the Third Wave. Atlanta: Turner, 1995.

_____. War and Anti-War: Survival at the Dawn of the 21st Century. Boston: Little, Brown & Co., 1993.

The White House. A National Security Strategy of Engagement and Enlargement. Washington: February 1995.

Wriston, Walter B. The Twilight of Sovereignty: How the Information Revolution is Transforming Our World. New York: Scribner's, 1992.