Naval War College Review

Volume 53
Number 3 *Summer*

Article 4

2000

Boon or Threat?

Robert R. Tomes

Boon or Threat?

The Information Revolution and U.S. National Security

Robert R. Tomes

SIXTEEN MEN AND WOMEN GRADUATED from the National Defense University in June of 1995 to become the nation's first accredited joint "infowar" officers—the first graduates of the National Defense University's newly created School of Information Warfare and Strategy.[1] Other events over the last five years suggest that information warfare (IW) has become a central component of the U.S. national security milieu.

The Joint Staff's new IW directorate has published a number of books and manuals on establishing information-warfare doctrine. Regional commanders develop IW campaign plans spanning diverse contingencies, mapping the information architectures of states in their respective areas of responsibility. "Flexible deterrence options," which provide escalation options during the initial stages of a conflict, now include a range of offensive and defensive information operations. A National Infrastructure Protection Center exists to safeguard the entire U.S. information infrastructure, including power grids and systems for financial transactions.

On the defensive side of IW, Deputy Secretary of Defense John Hamre wrote in November 1998 that "the challenge of information assurance is akin to war, and we are approaching it that way by designating a Joint Task Force Commander for Computer Network Defense to organize our efforts."[2] Only a year earlier Hamre had warned the Senate Subcommittee on Technology, Terrorism, and Government Information that "there will be an electronic attack sometime in our future. . . . [W]hen it comes, our ability to withstand it will depend in large amount on steps we take now and in years ahead."[3]

Naval War College Review, Summer 2000, Vol. LIII, No. 3

About the same time, then–Director of Central Intelligence John Deutch, ranking long-term threats to American national security, placed information warfare third, behind only the proliferation of weapons of mass destruction and nuclear, chemical, or biological terrorism.[4]

On the offensive side, U.S. doctrine states that "offensive computer network attacks will become an intrinsic part of U.S. warfighting doctrine, and even could be used in peacetime operations."[5] William Church, publisher of an information operations newsletter, has remarked on the new infowar doctrine, "It is now official. Each country must build offensive-defensive information operations capabilities or be left unprotected."[6]

Considering both offensive and defensive information warfare, former Deputy Chief of Staff of the Army Claudia Kennedy concluded that information has the potential to be "the most destabilizing factor in the world today."[7]

As these and other statements suggest, the "information revolution" has come to dominate national security planning as much as it has come to dominate economic and social life. This revolution, building on and subsuming previous post–World War II "revolutions" (electronic, microelectronic, computer, communications, digital), represents more than cumulative technological advances. It is a new process of wealth creation; it has stimulated new ways to organize and manage tasks within society; it has changed the way organizations manage people and processes; it has provided the means to exploit and integrate specialization; and it has institutionalized the spatial-temporal changes commonly referred to as "post-modernity."

Robert Tomes is a doctoral student studying international relations and national security at the University of Maryland, College Park. Employed by Booz·Allen & Hamilton's National Security Team, he is a consultant with the National Imagery and Mapping Agency Initiatives Group. Previously, he was employed by ANSER (a not-for-profit research institute) in the Strategy and Policy Directorate of the Joint Staff, was a research consultant at the World Bank, and was Anna Sobol Levy Fellow of Middle East Studies at the Hebrew University of Jerusalem. He served for nine years in the U.S. Army and Navy reserves. Mr. Tomes thanks Rhonda Armstrong for comments and suggestions.

Is the information revolution a boon or a threat to U.S. national security? It is, of course, both. Several aspects of the information revolution, however, suggest an optimistic assessment for the United States. Understanding the effects of the information revolution on national security requires understanding the social, political, economic, and philosophical aspects of the information age. Accordingly, this article provides background on the information revolution and introduces information-age national security issues—which are often lost or obscured in writings about the current revolution in military affairs. Specifically, it gives an overview of the information revolution and develops definitions that now inform discussions of IW. It is particularly important that we grasp information-age concepts that can expand the way we think about information and the organization of society, especially processes for creating wealth. Whether we succeed in building a conceptual bridge from information-age dynamics to national-security imperatives depends on how well we understand the extent to which we have become an information society.

What is the information revolution? How does it affect national security? As we shall see, much of the information revolution touches on nonmilitary aspects of society, which means that it affects more than the military component of national security. Indeed, it may be that the greatest existential threat from IW to national security is not to military assets but to the civilian information infrastructure.

A number of innovations, inventions, and trends—beginning in World War II—culminated in the introduction of IBM's personal computer in 1981. Subsequently there occurred a digital revolution, as well as a determined global race for commercial space systems and—of central importance—a decline in the cost of computing power and of storing information.[8] According to one estimate, "The cost of storing a single digital unit of data in a memory chip fell from one-tenth of a cent in 1976 to one-thousandth of a cent in 1986, and it will keep dropping by about 35 percent per annum."[9] Indeed, digital technology, fiber optics, and satellite communications have combined to quicken the pace of microelectronic, telecommunications, and computing innovations that had begun decades earlier. It was

the accumulation, then, of decades of separate technological developments that established the information revolution.

Beginnings

The world entered the computing age in 1943, when the British built ten "Colossus" machines to help break the German Enigma code. Three years later, the Electronic Numerical Integrator and Calculator (ENIAC) was activated in Pennsylvania. A computer revolution was under way.

A seemingly unrelated event occurred soon after. In 1947, scientists at Bell Laboratories discovered the transistor effect: a small piece of wire with germanium contacts could be fashioned to produce an amplifying effect.[10] Within ten years numerous types of transistors were being produced, and still more were being researched. The first silicon-wafer transistor, created in 1959, gave birth to a microelectronics revolution. What made it a revolution? Prices for the "brains" of microelectronics products dropped by a third every year, while their sophistication doubled at the same rate.[11] A new era in the computer revolution started to take shape with the coining of a new term, "artificial intelligence." The quest for intelligent, thinking machines that are able to learn continues today.

Along the way, the computer and microelectronics revolutions converged, due in part to advances in digital technology: personal computers, small enough to fit on a desk, began to appear. Soon they appeared on yet more desks, as prices declined and society began to depend on them to add value to all manner of work and thought processes. In time we began to *expect* to see a PC on every desktop.

But the harbingers of the information revolution were not limited to these developments. Alongside the computer and microelectronic revolutions there occurred a telecommunications revolution. It originated with Alexander Graham Bell's 1876 invention of the telephone; a hundred years later, the world was using over half a billion of them. The digital revolution collided with analog telecommunications in the late 1970s; immediately, existing analog systems became antiquated and clumsy, and were replaced with digital ones—faster, cheaper, more efficient, and able to carry more information. These systems also carry different *kinds* of information: telecommunications and data processing could move over the same system. Soon

faxes, modems, and networking were integral parts of Western civilization.

Spatial and temporal distance no longer determined our communication parameters. Fiber optics, invented in the 1960s, reduced limitations on transmission size, and deregulation of the telecommunications industry in the 1980s opened the door to competition (producing the breakup of AT&T in 1984). By 1990, companies were moving ahead with plans to provide telephone cable and computer data service over the same lines. If one adds satellite communication and notes that all of these technologies rely on semiconductors and microchips, one begins to grasp the basic technological components of the information revolution.

The Revolution Takes Form, and IW Is Conceived

A software revolution, as distinct from the computer revolution, was foreshadowed in 1969, when IBM decided to market hardware and software separately rather than "package" them; the revolution itself began in the 1980s, with the explosion in personal computing.[12] Systems software and applications programs expanded with it. An entire industry emerged. Soon the fastest-growing employment sectors were computer programming and network management. Concurrent with the software revolution was a revolution in storage techniques and peripheral devices, including digital read-write hardware.

The various revolutions fed on one another. Better hardware meant more sophisticated software; new software created demand for faster processors; faster processors meant faster external devices and telecomputing; faster systems demanded quicker links between them—and on and on. By the late 1980s, the revolution was globalized. By 1990, "over 14,000 Internet databases [were] being used by over 30 million people in over 90 nations."[13]

An unprecedented amount of information is now carried over international networks, at unprecedented speed, among billions of people—this is the basic result of the combination of modern communications technologies (which transmit information) and the capabilities of modern computer processing. Add to that satellite television, VCRs, newsgroups, and scores of other information-based systems. Consider the computation power placed in the hands of billions of people, coupled with the power to manage and use

unprecedented amounts of information. Ponder the number of devices that now use semiconductors and microchips, the latter essentially micro-information managers. The totality of all these, existing at the intersection of the revolutions we have mentioned, characterizes the basic technological infrastructure of the information revolution.

But information technology is not the only aspect of the information revolution, as a number of theorists of the information age have pointed out. The futurists Alvin and Heidi Toffler are perhaps the

> *It is useless to pretend that the proliferation of these [information] technologies will not provide capabilities that can do serious harm. It is useless to pretend that military-based command and control warfare capabilities will not be developed, and it is useless to pretend that cyberwar technologies could not be turned to netwar applications.*
>
> —*Roger Hanseman*

most frequently cited observers of the information revolution. They were also among the first to call for an infowar occupational specialty in the U.S. military. For the Tofflers, revolutionary changes in warfare are preceded by changes in the process of wealth creation: "Starting with the very invention of agriculture, every revolution in the system for creating wealth triggered a corresponding revolution in the system for making war."[14] Their "wave" theory identifies three revolutionary changes in wealth creation, each of which stimulated a revolution in warfare. The first and second waves, the agricultural and industrial revolutions, are behind us. The third is going on now.

Like the industrial revolution, the third wave is more than the proliferation of a new kind of technology. The industrial revolution involved specialization, division of labor, and massive manufacturing complexes—all of which were mirrored in the military and in the defense industry. "As 'first wave' wars were fought for land and 'second wave' wars were fought for control over productive capacity, the emerging 'third wave' of wars will be fought for control of knowledge. And, since 'combat form' in any society follows the 'wealth creation form' of that society, wars of the future will be increasingly 'information wars.'"[15]

Information is the key to the third wave: "Knowledge, in short, is now the central resource of destructivity, just as it is the central resource of productivity."[16] First-wave (agricultural) and second-wave (industrial) societies still exist. There are also mixed societies, making the transition from one to the other; the defining aspects of third-wave nations—information technologies—are changing how this transition occurs in mixed societies. Because the United States does not anticipate armed conflict from a third-wave society in the near future (there are not many of them), potential aggressors at the state level are likely to be transition states with armed forces still organized to fight second-wave wars.

Off the battlefield, however, because aspects of the information revolution are guiding wave transition, nontraditional third-wave attacks can come from anywhere. One nightmare scenario for infowar defense planners involves attacks with no military purpose, assaults that are terrorist or ideological in nature. Because we value information and information systems, these are likely to be targeted and attacked.

Assessing the Revolution

Today, wealth depends on information, which is traded, sold, leveraged, and banked. Wealth is built by adding value to raw materials—by combining material, know-how, manufacturing processes, and marketing. In the information age, a whole sector of the economy is built solely around people who process and trade information. The single most important physical method of adding value in today's economy is to integrate, in an innovative way, a microprocessor into a product or production line to make it more efficient or effective. This "value adding" depends on knowledge; it depends on information or technology that stores, manages, or provides information. For example, because they use information and knowledge-based control systems (that is, expert systems), "modern steel plants use far less labor and energy, and even less raw material, to produce a given amount of steel than did plants of a generation ago."[17]

Also changing is how we organize for wealth creation. Organizations and management structures "are changing rapidly," becoming flatter, smarter, and more efficient.[18] Hierarchical organizations with middle managers, created during the industrial era to manage

information flow, are no longer efficient. Inventory control, accounting, marketing, research and design—all of which depend on computers and software—are being reengineered.

The Internet has also changed the economy. Millions of Americans work at home. Smaller "cottage industry" factories and home busi-

---

The electromagnetic spectrum will be our "Achilles' heel" if we do not pay sufficient attention to protecting our use of the spectrum and at the same time recognize that we must take away the enemy's ability to see us and to control his forces.

—General Jimmy Ross

---

nesses—much easier to adapt and upgrade than larger factories—are competing on the world market by becoming more efficient through applied technology. Desktop publishing and information-based employment, software engineering, accounting, editing, business-process reengineering—all these functions are now done over the Internet.

The information revolution has also changed international economics and has changed the very structure of the world economy.[19] An integrated European market would be impossible without information technology. Indeed, computers and telecommunications have blurred lines between local and international economies. Walter Wriston, former chairman of Citicorp, has observed that "the convergence of computers and telecommunications has created a new international monetary system and even a monetary standard by which the value of currencies is determined not by the arcane manipulations of central banks, whose total reserves are now dwarfed by a single day's trading on the world currency markets, but by myriad facts that are now instantaneously available."[20] Technology transfer, technological spillover effects, managing externalities created by the fungibility of know-how, electronic capital movements—these are now central issues in international business.

In *Turbulence in World Politics*, James Rosenau summarizes changes to global politics associated with the information age: "The advent of instantaneous communications and information . . . have so greatly collapsed the time in which organizations and movements can be mobilized that the competence of citizens feeds on itself, in the sense that they can virtually 'see' their skills and orientations being

culminated into larger aggregates that have consequences for the course of events."[21] Rosenau sees the information revolution (specifically the microelectronic revolution) as the primary cause of "turbulence" in international relations. He argues that technology engendered a globalized civil society:

> Technology has expanded the capacity to generate and manipulate information and knowledge even more [than] the ability to produce material goods, leading to a situation in which the service industries have come to replace the manufacturing industries as the current edge of societal life. It is technology, too, that has so greatly diminished geographic and social distances through the jet-powered airliner, the computer, the orbiting satellite, and the many other innovations that now move [more] people across space and time than ever before. It is technology that has profoundly altered the scale on which human affairs takes place, allowing people to do more things in less time and with wider repercussions than could have been imagined in earlier eras. It is technology, in short, that has fostered an interdependence of local, national, and international communities that is far greater than any previously experienced.[22]

In *The New Renaissance: Computers and the Next Level of Civilization,* Douglas S. Robertson surveys the impact of the information revolution on all aspects of life.[23] Even the way society approaches science has been altered. Previously, science hinged on theories and experiments. Now a third modality—simulation—has become a recognized route to scientific knowledge. Education, the theory of mathematics, and medicine have all been transformed. Challenging new issues confront society. In the case of medicine, the mapping of the human genome and of DNA has opened new frontiers. Synthetic drugs, cloning, and revolutionary treatments for previously fatal illnesses have become possible only with information technology. Medical ethics must address cloning humans; soon genetic engineering will be possible, as will DNA testing on fetuses to assess predisposition to disease. Other aspects of life dominated by technology include social services, emergency-response services, banking, education, athletics, entertainment, energy, and transportation.

In sum, the entire socioeconomic infrastructure of civilization in the United States is permeated with information technology.

Arguably, information technology has become part of the interstitial tissue of American life. For sociologists this was to be expected: the evolution of American society, more than most, has always been techno-centric. For example, Martin Gannon, a professor of international management and behavior, argues that "the United States has historically been 'short' on labor and 'long' on raw materials. To use their abundant raw materials, Americans had to substitute machinery and equipment for unskilled labor. Influenced by the success of their highly mechanized industry in the late 1800s, Americans were shrewdly induced to use the power of machines and technology. To Americans, technology was empirically proven to stimulate growth and success, and their dependence on machines grew heavier."[24]

Colin S. Gray offers a slightly different argument, that "the American fascination with technology . . . resulted from conquering the wilderness. The relative absence of societal support on the frontier bred a pragmatism that translated into an engineering, problem-solving approach—an approach that at times has dismissed conditions as merely problems. American society responded sensibly to its shortage of labor, particularly highly skilled labor, by embracing machines and taking the lead in producing machine tools. The American preference for the use of machines in war lies rooted in the sparse people-to-space ratio of frontier America, and in the acute shortage of skilled artisans that lasted well into the nineteenth century."[25]

The fact that America has led—some would say pulled—the world into the information age becomes an important consideration in how and why U.S. national security thinking has become focused on protecting information infrastructure.

A New View of Information

At the most basic level, the information revolution involves a shift in how we think about information on the ontological level. John Arquilla and David Ronfeldt provide one framework for conceptualizing this shift: "Three general views of 'information' appear in discussions about the information revolution and its implications. Each view approaches the concept differently; each harbors a different perspective of what is important. Two views are widespread: The first considers information in terms of the inherent *message*, the second in

terms of the *medium* of production, storage, transmission, and reception. The emerging third view transcends the former two; it speculates that information may be a *physical property*—as physical as mass and energy, and inherent in all matter."[26]

The information-as-message view sees information as a message or signal that is carried from a sender to a receiver. The second view, information as medium, incorporates the system of transmission and reception. It developed during the 1940s and 1950s, when a cybernetic, or feedback, approach to systems engineering expanded our concept of information to include the organization or structure associated with a message's content. In this sense, a book in itself—not just the cognitive import of its printed words—is information. The third view further expands the idea of information—it is about much more than message and medium (or content and conduit). "Its main thesis," according to one author, "is that 'information' is not merely a product of the human mind—a mental concept to help us understand the world we inhabit—rather, information is a [physical] property of the universe, as real as are matter and energy."[27] The third model is hard to grasp, but it does comport with information-warfare operations, which target and attack information—with information—as directly as does a "dumb" bomb dropped on a radio transmitter site. This third view of information is critical for understanding the proliferation of IW issues in discussions of U.S. national security.

We have reviewed the technical and socioeconomic aspects of the information revolution. However, the heart of information technology, perhaps the central factor in the convergence over the last fifty years of the numerous revolutions we have mentioned, is the microchip.

What is a microchip? Understanding the microchip is vital to understanding how information is now considered both a weapon and a target. A microchip, smaller than a pea, can contain as many as a million circuits. Circuits consist of layers upon layers on silicon, a substance reduced from its oxide, common beach sand. Each layer has a certain design that allows it to store a message—at its simplest, an open-closed dichotomy. Millions of these messages operating together represent a new form of language processing.

So the microchip both *contains* information and *is* information. Therefore, to defeat the microchip—paralyze it or otherwise keep it

from functioning—we have a number of options. We can cut off the microchip physically from the system it is embedded in, turn off its power, freeze its circuits, garble its internal connections, scramble its internal language, or change the grammatical properties of its "speech" to other chips (making its output indecipherable). Other possibilities exist, but this truncated list makes the point. Now consider that virtually every modern machine, computer, weapon system, vehicle, timekeeping device, sensor, radar, power grid, point of access to personal information, and engine is controlled or regulated by a microchip. Each of these systems and devices is vulnerable if that chip, its internal functioning, its communication capability, or its connection to other chips or systems is either destroyed or paralyzed.

Imagine a computer program downloaded from the World Wide Web as information; now call that program a virus, and envision trying to erase it using another computer program. Now imagine five hundred hackers all trying to insert viruses into national and local computer systems. Again, imagine an electromagnetic pulse aimed at your computer; the target is not so much your computer as the organization of the data within it and the functioning of its microchips. Once we conceive of information as an existential "thing" as much as a metaphysical or mental construct, it is much easier to understand the security implications of the information age. It is no longer necessary to bomb an airplane factory to keep a nation from producing combat aircraft—only to paralyze the chips in the systems that make, test, or operate aircraft. This can be done with another chip, or with information stored and communicated through information technology.

From Information Revolution to IW: Aggregation and Situational Awareness

In an article entitled "An Information-Based Revolution in Military Affairs," Norman C. Davis argues that "the Information Revolution is based primarily on significant technological advances that have increased our ability to collect vast quantities of precise data; to convert that data into intelligible information by removing extraneous 'noise'; to rapidly and accurately transmit this large quantity of information; to convert this information through responsive, flexible

processing to near-complete situation awareness; and, at the limit [of this awareness], to allow accurate predictions of the implications of decisions that may be made or actions that may be taken."[28] What Davis describes is an order-of-magnitude change in the way we collect, aggregate, analyze, store, retrieve, and benefit from information.

Situational awareness, a topic central to the information warfare component of the revolution in military affairs, is an extension of a biological organism's inherent proprioceptive *and* contextual-associative functions. Human proprioception is defined as "awareness of posture, movement, and changes in equilibrium and the knowledge of position, weight, and resistance of objects in relation to the body."[29] This awareness is drawn from unconscious inputs (which are processed into conscious awareness) from the peripheral nervous system; loss of those inputs isolates the brain from critical information about what is going on within the body and about the body's position in the world.

The contextual-associative functions of an organism are based on input from all sensory neurons and on how this input is used.[30] Humans can suffer paralysis and loss of sensation even without injury to these neurons or awareness processes. Without them, we are helpless. Nor can we ask for help. At the extreme (for instance, under the influence of drugs inducing deep sleep and impairing memory), we would not even know that we were in trouble.

Situational awareness is a function of the aggregation and clarity of information. Advances in information technology have increased our ability to aggregate information and refine it so as to achieve greater clarity, improving and clarifying our situational awareness. This means we can act more decisively and with more precision than ever before to affect our environment. Fund managers and magnetic-resonance-imagery analysts use information technology to extend their ability to sense their respective "worlds." The former applies risk assessments and other tools to make predictions about currency or stock performance; the latter uses advanced software and analysis techniques to evaluate the functioning of the body's organs.

Essentially, the information revolution has created systems, some would say networks, that extend the natural processes that support situational awareness. This is *virtual reality:* the creation of situational

awareness outside of the physical, tangible reality of the represented system. It can also be the re-creation of the system, in order to identify and understand its constituent properties—we call this *virtual simulation.*

What about military applications? In their *Multisensor Data Fusion,* Edward Waltz and James Llinas offer examples of functional architectures for creating "situation assessments," which depend on the ability to fuse, synergistically, multiple sensors, which may in turn collect data from more than one spectrum (such as electro-optical and infrared). "It is clear in fusion problems involving multiple targets in military scenarios, in which single platforms or events often associate with more than one possible intended hostile activity, that combinational aspects of the problem can grow quite rapidly. This situation leads to complex problem-solving logic, to requirements for fast computers, and especially to difficult database management problems[,] . . . aspects of real-world systems architectures that the fusion system designer has to realize are the constraints and interfaces provided by the surrounding system elements."[31]

Perhaps this is the essence of what Davis is describing: it is not only the single sensing system itself that has emerged from the information revolution but an entire new way of, a "metasystem" for, sensing, acting, and achieving. But if we are truly to achieve, the systems involved must all be advanced enough to do their shares of the work—an airborne early-warning AWACS plane is useless unless something can be done with the targeting information it provides. All of the microchips in the metasystem must be considered infrastructure "nodes." As such, they can all be located and attacked. Because they can be attacked, they must be defended.

When infowarriors speak of achieving "dominant maneuver" or "dominant battlespace knowledge," they are really talking about their situational awareness in relationship to enemy forces and terrain. One implication for national security is creating options for defense positioning at the strategic level. Another is creating a capability for nonnuclear strategic attacks—using advanced weapons to achieve a mass-destruction effect by knowing where and when to strike. Take away leaders' situational awareness concerning their entire armed forces, disaster-relief agencies, and financial systems, and we begin to induce strategic paralysis, in the same way that we might induce sleep.

A further factor in situational awareness is the ability to measure and manage information. Claude Shannon, an early analyst of the information revolution, recognized that "the fundamental unit of information measurement is the quantity of information needed to decide between two alternatives."[32] Indeed, the information revolution is partly an explosion in our ability to measure information.

Sophisticated systems with heuristic, interactive forecasting software allow users to measure and manage more information about the battlefield than could be stored in a large university library, meaning that they help commanders develop, and choose between, possible courses of action. The primary concern for national security, therefore, is to make sure that one's own situational awareness, one's own ability to measure and manage information, is not degraded.

Four additional aspects of data fusion and situational awareness are relevant to the information revolution and IW. First, different signals within spectra (various electromagnetic waves, levels of thermal radiation) can be fused into a single uniform output that is more useful than individual signals. The result is better sensory information with which to answer the question, "Is there anything out there?" The second aspect is fusion of different spectra, which provides answers to the question, "What are the characteristics of what is out there?" A third factor is "tracker correspondence," which provides insight into the location and movement of sensed objects. Finally, advances in situational awareness facilitate the transformation of information into actionable knowledge by enabling decision makers to assess the intent of the objects.

OODA: A Grand Theory of IW

John Boyd, a fighter pilot during the Korean War, developed the first and probably most frequently cited theory of control and of what we would now call situational awareness. His revelation came from comparing the performance of Soviet-made MiG-15 fighters in air-to-air combat with U.S. F-86 Sabres. Although the Soviet plane was arguably more advanced than the F-86, the latter's hydraulic controls proved to be the decisive factor: they provided "the ability to shift more rapidly from one maneuver to another during aerial dogfights. Just when the MiG pilot began reacting to the initial Sabre

movement, a rapid change in direction would render the enemy response inappropriate to the new tactical situation."[33]

In the late 1970s, examining aerial combat data, Boyd began developing a theory of combat. Originally an essay and later a five-part briefing to senior defense and military leaders, Boyd's "A Discourse on Winning and Losing" presented "a cognitive process that [he] insists is crucial to prevailing in a highly unpredictable and competitive world. It is a form of mental agility. . . . [H]e contends that one can depict all rational human behavior—individual or organizational—as a continual cycling through four distinct tasks: observation, orientation, decision, and action."[34] This is the most famous part of his theory: the "OODA loop."

The theory is simple but powerful. Consider two boxers. Each continuously cycles through his OODA loop. If they do so at the same speed and are otherwise evenly matched, it is difficult to predict who will win. Now give one the ability to cycle through his loop twice as fast; he can act faster than the other boxer can decide what to do next. He will win, even if the other boxer is stronger. If his OODA cycle is truly twice as fast, he can complete a loop in the time between the moment the other boxer starts to throw a punch and when the blow lands—or would have landed. In other words, the boxer with a more accurate and timely OODA loop can compress his decision cycle within an adversary's. In this way he exploits information superiority to achieve decision superiority.

True information-era situational awareness improves one's ability to cycle through OODA loops. Information technology also increases the efficiency of all of the steps in the loop, with the result that actions can be more decisive and effectual than at any other time in human history. The ability to measure and manage information (and thus decide among options) at unprecedented rates—with predictive understanding of the enemy's possibilities—translates into an advance in battlespace awareness and sensor-to-shooter capabilities that is nothing less than revolutionary.

Major General Kenneth Minihan, Air Force Assistant Chief of Staff for Intelligence, envisions how information warfare can be used to affect an OODA loop: "As we compare friendly and adversary OODA loops, it becomes a deadly game of compression and expansion. We will use information warfare to expand the adversary's and compress

our own action loops. If you can't think, can't hear, and can't see—and I can—you will lose every time."[35]

The Information Revolution: Boon or Threat?

The "boon or threat" issue can be addressed in a variety of ways—all under the assumption that the information revolution is not reversible, that the real question is whether the U.S. experience with the information revolution warrants optimism or pessimism. For three major reasons, among others, the information revolution is likely to be a boon to U.S. national security—though for each boon, for each positive, there is a threat, a negative, that must be accounted for.

First, it is important to consider, in assessing the boon-versus-threat question, the magnitude of the information revolution and the fact that the United States would not be in the economic or political position it occupies today had it never occurred. The nation's ascent to superpower status during the industrial era was, in no small part, due to its ability to outproduce its adversaries—both quantitatively and qualitatively. America's continued economic leadership in the world now depends on its performance in the information sectors.

The Importance of Being First. In many respects the severity of any information threat to U.S. national security is defined by what the United States has done to prepare for attacks that it has conceptualized. As the first nation to create an information warfare doctrine and the first to institutionalize information warfare within its national security infrastructure, the United States is positioned to meet future threats—provided it maintains its lead in information technology.

The threat here is the trap of linear thinking. Being first to go somewhere does not mean one has found the only or best route; *non*linear thinking is one of the trademarks of warfare in the information age. Consider the development and use of tanks: the Germans did not "get there" first, but they were surely the best in 1939. Avoiding this threat to national security requires the cultivation of innovative thinkers and the institutionalization of redundant, dissimilar defenses. Such defenses are currently not common, because

software standardization has tended to give all related systems similar vulnerabilities.

The Cultural Legacy. A cultural attribute commonly ascribed to Americans is technological know-how. The military aspects of the information revolution are being developed primarily in American research laboratories and corporations. Whatever technological "curves" opponents manage to throw, the United States is likely to find them only minor setbacks. It is unlikely that any country will develop before 2015 or 2020 an information warfare capability sufficient to cause serious harm to the United States. It is also unlikely that any armed force will be able to match U.S. warfighting capability with conventional forces. The threat here is another common cultural legacy ascribed to Americans, arrogance. Remember what the ancient Greek poets and playwrights taught us about hubris.

Knowing What Must Be Defended. The United States has already conducted a national survey of its critical infrastructure and has begun to prepare its defense. The report of the President's Commission on Critical Infrastructure Protection, published in October 1987, "was the first of its kind, an initial look at how America would have to defend itself in the infosphere that would evolve in the early part of the twenty-first century."[36] This means the United States has already mapped the information nodes that are critical to national security.

Not every level of daily life has been researched, but we do have an understanding of which nodes and systems are vital for the operations of such national systems as disaster response, emergency rescue teams, important national communication systems, banking and financial systems, transportation and power infrastructure, and water supplies. On the other hand, security specialists have learned a hard lesson: a determined and patient enemy can get to, and kill, anyone. Just because we have mapped critical infrastructure does not mean that we are invulnerable.

Beyond Reports. Some steps have already been taken based on the commission's findings. As noted, a National Infrastructure Protection Center has been created as an interagency body reporting to the National Security Council. Its staff includes representatives from the Department of Defense (including the Joint Staff), the Federal

Bureau of Investigation, the State Department, the Treasury Department, the Defense Threat Reduction Agency, the intelligence community, and national laboratories. In addition to monitoring, it has a law enforcement role—its staff can gather evidence and make arrests. Still, every organization has inherent weaknesses; one of these can be its people. Recent espionage cases argue against thinking that national secrets cannot be bought or compromised by ideologues. Most of the critical penetrations of banking systems have been accomplished using inside information.

Intelligence. Because the United States has an early start on understanding information technology-based warfare, it has been the first to attune intelligence agencies and security managers to the threat. No system or defense architecture is perfect, but knowing the realm of the possible is the first step toward developing the people and resources necessary. In addition, steps have been taken to coordinate infowar defense with other countries. Several specific cases have already demonstrated an ability of countries to work on information-era problems in the same fashion that they now collaborate against terrorism and drug trafficking. The downside is obvious: intelligence organizations have been known to fail.

Understanding First Steps—Because You Made Them. Another reason for optimism is our understanding of the steps leading up to the information revolution—we are the nation that took them first. Countries that did not keep up are decades behind in the technical and conceptual aspects of information warfare. All the non-Nato militaries (except perhaps Israel, although Martin van Creveld disagrees) are still equipped, trained, and organized to fight a World War II–era tank battle.[37] Such battles are linear, with stable fronts and identifiable rear areas. The United States no longer looks at the battlefield in such a way. Current doctrine, which has learned from the Gulf War, and current weapons, some of which are already a generation ahead of the most advanced used against Iraq, envision simultaneous attacks throughout the depth of a theater. No other country is likely to have this capability—which requires training, organization, advanced logistical skills, leadership, and intelligence capabilities in addition to weapon systems.

The problem is that nations opposed to the United States may turn to chemical or biological attacks to "level" the battlefield. "Asymmetric threats" have been recognized as a major concern for U.S. national security, especially where American resolve is sensitive to U.S. casualties. One of the aspects of the information revolution needing more attention is the emotive power of media to stimulate the public concerning overseas calamities. The United States was in Somalia in part because of the popular outcry over what was reported on television. A strong moral conviction running through the cultural fabric of America is that the weak and impoverished must be championed, a conviction that leads to a will to help. This will is quickly reduced when Americans die.

Notes

1. Roger G. Hanseman, "The Realities and Legalities of Information Warfare," *Air Force Law Review*, vol. 42, 1997, p. 180.

2. David Ruppe, "Hamre: Information Defense 'Akin to War,'" *Defense Week*, 9 November 1998, p. 16. Ruppe is quoting from Hamre's "Information Assurance and the New Security Epoch," in the November 1998 issue of the U.S. Information Agency's *Electronic Journal*.

3. Hamre quoted in James Adams, *The Next World War* (New York: Simon and Schuster, 1998), p. 187.

4. Ibid., p. 179.

5. George I. Seffers, "Joint Chiefs Inaugurate Information Combat Era," *Defense News*, 9–15 November 1998, p. 1.

6. Ibid.

7. Claudia Kennedy, *The Age of Revolutions*, Letort Paper no. 3 (Carlisle, Penna.: U.S. Army War College, 1998), p. 2.

8. Tom Forester, *High-Tech Society: The Story of the Information Technology Revolution* (Cambridge, Mass.: MIT Press, 1987), p. 1.

9. Ibid., p. 2.

10. Ibid., p. 19.

11. Ibid., p. 27.

12. Ibid., p. 146.

13. George J. Stein, "Information War—Cyberwar—Netwar," in *Battlefield of the Future: 21st Century Warfare Issues*, ed. Barry R. Schneider and Lawrence E. Grinter, Air War College Studies in National Security no. 3 (Maxwell Air Force Base [hereafter AFB], Ala.: Air Univ. Press, 1998), p. 156.

14. Alvin Toffler and Heidi Toffler, *War and Anti-War: Survival at the Dawn of the 21st Century* (Boston: Little, Brown, 1993), p. 37.

15. Stein, p. 154.

16. Toffler and Toffler, p. 71.

17. Ibid., p. 23.

18. Ibid., p. 15.

19. Susan Strange, "States, Firms and Diplomacy," in *International Political Economy: Perspectives on Global Power and Wealth*, ed. Jeffrey A. Frieden and David A. Lake (New York: St. Martin's, 1995), pp. 62–3.

20. Walter B. Wriston, *The Twilight of Sovereignty: How the Information Revolution Is Transforming Our World* (New York: Scribner's, 1992), p. 59.

21. James N. Rosenau, *Turbulence in World Politics* (Princeton, N.J.: Princeton Univ. Press, 1990), p. 15.

22. Ibid., pp. 16–7.

23. Douglas S. Robertson, *The New Renaissance: Computers and the Next Level of Civilization* (New York: Oxford Univ. Press, 1998).

24. Martin Gannon, *Understanding Global Cultures* (Thousand Oaks, Calif.: Sage, 1994), p. 190.

25. Colin S. Gray, "Strategy in the Nuclear Age: The United States, 1945–1991," in *The Making of Strategy: Rulers, States, and War*, ed. Williamson Murray, MacGregor Knox, and Alvin Bernstein (New York: Cambridge Univ. Press, 1995), p. 190.

26. John Arquilla and David Ronfeldt, "Information, Power and Grand Strategy: In Athena's Camp—Section I," in *In Athena's Camp: Preparing for Conflict in the Information Age* (Santa Monica, Calif.: RAND, 1997), pp. 144–5.

27. Quoted in ibid., pp. 148–9.

28. Norman C. Davis, "An Information-Based Revolution in Military Affairs," in Arquilla and Ronfeldt, p. 83.

29. *Taber's Cyclopedic Medical Dictionary* (Philadelphia: F. A. Davis, 1984).

30. For more on brain architecture, see John E. Dowling, *Creating Mind: How the Brain Works* (New York: Norton, 1998).

31. Edward Waltz and James Llinas, *Multisensor Data Fusion* (Boston: Artech House, 1990), p. 28.

32. Robertson, p. 18.

33. David S. Fadok, "John Boyd and John Warden: Airpower's Quest for Strategic Paralysis," in *The Paths of Heaven: The Evolution of Airpower Theory*, ed. Philip S. Meilinger (Maxwell AFB, Ala.: Air Univ. Press), p. 363.

34. Ibid., pp. 363–4.

35. James W. McLendon, "Information Warfare: Impacts and Concerns," in Schneider and Grinter, eds., p. 190.

36. Adams, p. 183.

37. Martin van Creveld, *The Sword and the Olive: A Critical History of the Israeli Defense Forces* (New York: Public Affairs, 1998).