

---

**INTRODUCTION**

*Zalmay Khalilzad and John White*

---

*As we approach the 21st Century, our foes have extended the fields of battle from physical space to cyberspace; from the world's vast bodies of water to the complex workings of our own human bodies. Rather than invading our beaches or launching bombers, these adversaries may attempt cyberattacks against our critical military systems and our economic base.*

—President William J. Clinton, May 22, 1998

*Computers are changing our lives faster than any other invention in our history. Our society is becoming increasingly dependent on information technologies, which are changing at an amazing rate. . . . We must ask whether we are becoming so dependent on communications links and electronic microprocessors that a determined adversary or terrorist could possibly shut down federal operations or damage the economy simply by attacking our computers.*

—Senator Fred Thompson, May 19, 1998

As these quotes imply, the United States and indeed the world is undergoing dramatic changes due in great part to the dramatic transformations brought about by new information technologies. The technical changes include advances in how information is collected, stored, processed, and communicated. While the speed with which these processes have taken place has increased manyfold, the costs for propagating and storing information have decreased dramatically. The implementation of these capabilities has vastly increased our communications and related functions, including large increases in international connectivity. More and more people and nations around the world are acquiring access to the Internet

and to space-based communications and reconnaissance capabilities.

These changes have been rapid, and more are on the way. Advanced information technologies will fundamentally alter how people and societies interact, in ways that cannot be predicted. Nations around the world are both adapting to and trying to shape the ongoing developments in information technologies. This interaction between advancing information technologies and society is one of the key phenomena of our era.

One facet of how the world adapts to changes in information technologies will be in the way that conflicts are conducted. If current trends hold, these changes could have a profound effect on our national security, in terms of the threats we face, the way we fight, and how we advance the national interests of the United States.

Of course, the role of information as a key factor in warfare is not new. Nonetheless, the changes in technology and the integration of those changes into weapons, concepts, and organization means that the role of information relative to more-conventional measures of military strength is likely to change in dramatic ways.

Changes in information technology have already affected the global balance of power. The collapse of the Soviet Union, which transformed the international system, was facilitated by these changes. (See Shane, 1994.) The Soviet style of communism and command economy failed in part because it was not compatible with the requirements of the information age. These changes in information technologies have helped strengthen free markets and democratic forces around the world. They have also promoted greater international interdependence, including increased international trade and investment. Some of the consequences of the changes under way are reflected in the weakening of government control over society and the shifting of power away from governments to nongovernmental organizations, small groups, and individuals. The recent consequences identified here may continue, but we do not know whether they will.

The ultimate effects of changes in information technologies on the future of the nation-state and on conflict are far from obvious. History does not offer clear precedents. Earlier changes in information

technology—such as the introduction of the printing press, telegraph, telephone, or wireless radio—produced direct and indirect effects that were at times in tension with each other. For example, the printing press initially was seen as a way to ease access to traditional and religious texts, but it soon became a way to spread new and revolutionary documents. (Dewar, 1998.) The changes predicted at the onset of these capabilities were very often wrong as society adapted to them in unexpected ways. There is another uncertainty that is also important and difficult to predict: Different political and cultural systems often use new technologies differently.

An assessment of the situation up to now indicates that, at the international level, the changes in information technologies have benefited the United States and reinforced its military preeminence. Not only did these changes help undermine the only global adversary to U.S. power, they have also aided the rejuvenation of the U.S. economy and strengthened the appeal of the U.S. system of market democracy around the world. The information age has allowed the United States to knit together the political, economic, and military sources of its national power. But such advantage may be transitory.

Militarily, as the Gulf War demonstrated, the United States is in a good position to exploit the advances in military technology, especially changes in information technology, due in great part to the high quality of its personnel and their training. The U.S. military has an unsurpassed ability to integrate complicated technical systems into preexisting forces. This military technological prowess is backed up by a solid civilian technological base. The United States has made large investments in its national information infrastructure and has a well-established market for computers, software, and Internet services. Most other nations depend on our systems and technology.

But there is another side to all of these profound changes. The United States may become increasingly vulnerable to disruption—perhaps catastrophically so—because of its heavy reliance on advanced information systems in both the civilian and military sectors.<sup>1</sup> The increased potential vulnerability to disruption—which

---

<sup>1</sup>Three recent General Accounting Office (GAO) reports document this type of vulnerability at the Department of Defense (DoD) and the Department of State and in the Air Traffic Control network: GAO (1996), GAO (1998b), and GAO (1998a), respectively.

some potentially hostile nations and nonstate actors recognize—is the negative side effect of an otherwise very positive development.

The same techniques that can be used to disrupt and manipulate civilian targets can be used for military purposes. Information attacks may be used to gather critical intelligence (for military or commercial purposes), to reduce military readiness, or to blunt or delay military operations. These developments could greatly complicate the U.S. capability to project power in a timely fashion. At times, such a delay could result in having to accept a *fait accompli* and putting at risk important national security interests. Disruption attacks also can degrade the combat effectiveness of U.S. forces that rely heavily on rapid communications and joint operations. (Bennett, Twomey, and Treverton, forthcoming.)

Adversaries are likely to rely on modern information operations, such as computer hacking or network attacks—in addition to traditional means, such as communication jamming and physical attacks—as an asymmetric strategy to compensate for their own weaknesses and for conventional U.S. military preeminence. They may value information attacks as a new type of guerrilla warfare against U.S. conventional weaponry—but one with a very long reach.

Propelled by numerous press reports of break-ins into DoD and other sensitive computer systems, threats to our information systems have become an important national issue. A recent presidential commission documented the widespread information vulnerability of various critical infrastructures, ranging from the financial system to the air traffic control system.<sup>2</sup> In response to these developments and to the report of the commission, President Clinton recently announced the goal of building “the capability to protect critical infrastructures from intentional acts by 2003.” (The White House, 1998, p. 1.<sup>3</sup>) The military threats have also been recognized. Two recent congressional commissions, the Commission on Roles and Missions of the Armed Forces and the National Defense Panel, have

---

<sup>2</sup>The eight infrastructures that the commission identified as both critical and vulnerable were information and communications, electrical power systems, gas and oil transportation and storage, banking and finance, transportation, water supply systems, emergency services, and government services. (PCCIP, 1997.)

<sup>3</sup>The President also appointed a national Coordinator for Security, Infrastructure Protection, and Counter-Terrorism.

enunciated these concerns. The DoD has been working to deal with these threats in numerous ways. The Joint Chiefs have recognized the vulnerability of the military to information attacks and have emphasized the need for “full dimensional protection.” (DoD, 1996.)

These changes will continue to affect our lives and our national security, both positively and negatively. Consequently, there is a strong need to increase our understanding of this revolution and its implications. The President’s decision and other actions taken by the U.S. government represent important first steps in defending the nation against information attack. Plans for achieving the objectives will have to be developed. This volume is intended to assist in the development of such plans, as well as to assist in understanding the potential opportunities for U.S. military forces and society that derive from information technology.

## **STRUCTURE OF THE BOOK**

Because emerging information technologies will affect all corners of our lives, their national security implications have many dimensions. This volume will reflect those wide-ranging implications. The book is divided into three parts: Part I analyzes the effects of information technology on society and the international system. Part II focuses on the United States and examines what new opportunities and vulnerabilities these new information technologies will present for the United States. Part III focuses on current issues and lessons that today’s U.S. decisionmakers need to understand if they are to function in the world to come.

### **Information Technology and Society**

Part I begins with the implications of information technologies at the highest level: their effects on society and the international system. The late Carl Builder believed that the most important national security implications of new information technology will come at the societal level. He argued that, while the American military is attempting to use new information technologies to improve what it currently does, societal changes mean that the military’s missions, indeed its very reason for existence, will change as society adapts to new technology.

David Gompert also foresees that the most important changes will come at the societal level, but he is much more sanguine about the outcome. For Gompert, information technology requires democracy and free markets to unleash its vast productive and military potential. Countries that choose not to embrace democracy and free markets will therefore lose power relative to open democracies. The world's great powers will therefore be, like the United States, open, free, and united in their opposition to any threats that may arise.

In contrast, John Arquilla, David Ronfeldt, and Michelle Zanini believe that these changes will shift the locus of power away from the nation-state altogether and toward nonstate actors whose nonhierarchical, networked form of organization will allow them to take best advantage of new information technologies. This shift in power from governments to nonstate actors means that the problems of terrorism, transnational criminal organizations, and insurgent groups will grow increasingly difficult to control. They suggest that the U.S. military and government organize themselves around networks to meet this growing threat.

### **U.S. Opportunities and Vulnerabilities**

Part II explores the many opportunities and vulnerabilities that new information technologies will create for the United States. First, Jeremy Shapiro offers a cautionary note by questioning the idea, often taken for granted, that information technology will revolutionize warfare. He suggests, instead, that the idea of an information-based revolution in warfare actually serves as an attempt to use technology to solve the perennial U.S. problem of lack of political will to accomplish foreign policy objectives.

In contrast, Ted Harshberger and David Ochmanek are quite convinced that new technologies offer a multitude of revolutionary military opportunities for U.S. forces. They describe how recent advances in surveillance, communications, and guidance technologies have allowed U.S. forces to approach Sun Tzu's "acme of skill." They predict that the ability of the U.S. military to use these technologies to achieve "information dominance" will enable the United States to maintain a vast military superiority for the foreseeable future.

Brian Nichiporuk elaborates on these ideas by demonstrating how the United States can use new information technologies and infor-

mation warfare to counter some prospective enemies' most appealing asymmetric strategies. He presents four concepts of operation for how the United States could, with little expenditure of blood or treasure, effectively preserve its power-projection capability and diminish the utility of enemy weapons of mass destruction.

Steve Hosmer continues this discussion by analyzing how the new technologies will allow the United States to conduct ever more-sophisticated psychological operations. While the United States will gain a substantial capability to influence enemy perceptions and to reduce U.S. casualties, Hosmer warns that the new technologies will also present opportunities for U.S. adversaries to achieve new psychological effects.

Roger Molander, Peter Wilson, and Robert Anderson expand on this discussion of the vulnerabilities that information technology may create for the United States. They analyze how U.S. adversaries might use the tools and techniques of new information systems to hold at risk key national strategic assets, including the financial system, the public switched network, and the transportation system. They call for a new decisionmaking framework to take into account the emerging challenge of "strategic information warfare" in national security and military policy.

Glenn Buchan then takes up the thread of vulnerability at the military operational level. He examines how an increasing military reliance on the systems described by Ochmanek, Harshberger, and Nichiporuk may create dependencies that could be exploited by clever enemies. He analyzes the dependence of Air Force operations on information and information systems and concludes that the risks are manageable but that the military needs to maintain sufficient skilled manpower to continue operating if new information systems fail.

### **Issues and Lessons for Decisionmakers**

Part III presents some issues and lessons for U.S. decisionmakers that emerge from the preceding chapters. First, Frank Fukuyama and Abe Shulsky draw on lessons from the corporate world about how to adapt organizational structures to new information technology and apply those lessons to military organization. They conclude

that, to take full advantage of information technology, the military will need to institutionalize an environment of constant learning, one that includes the freedom to fail without serious consequences. They also stress the need to redistribute skills and authority toward the bottom of the hierarchy and to give more autonomy to lower levels of the military. Finally, they cite the need to solve the debilitating yet seemingly intractable problem of streamlining the procurement system to allow the military to benefit from cutting-edge commercial technology.

Lynn Davis analyzes the role that arms control and nonproliferation regimes might play in managing some of the vulnerabilities mentioned in the preceding chapters. She concludes that it will be very difficult, and perhaps undesirable, to attempt to apply previous arms control and nonproliferation regimes to information technology. While variants of such responses may become necessary in the future, the greater need at present is to establish more effective means for multilateral cooperation to manage cross nationally the new threats posed by emerging information technology.

Zalmay Khalilzad discusses how the United States should undertake to defend itself from information attacks. He notes that, as with nuclear weapons, the United States is unlikely to be able to eliminate its vulnerability to information attacks completely. A successful national defense, therefore, will require strategies that also strive to deter adversaries from using information weapons and to prevent adversaries from developing the capability to produce or use such weapons.

Finally, Martin Libicki and Jeremy Shapiro assess the implications the changes in information technologies hold for the U.S. military, especially the U.S. Air Force.

## REFERENCES

- Bennett, Bruce, Christopher P. Twomey, and Gregory Treverton, *Future Warfare Scenarios and Asymmetric Threats*, Santa Monica, Calif.: RAND, MR-1025-OSD, forthcoming.
- Dewar, James A., "The Information Age and the Printing Press: Looking Backward to See Ahead," Santa Monica, Calif.: RAND, P-8014, 1998.

DoD—see U.S. Department of Defense.

GAO—see U.S. General Accounting Office.

PCCIP—see President’s Commission on Critical Infrastructure Protection.

President’s Commission on Critical Infrastructure Protection , *Critical Foundations: Protecting America’s Infrastructures*, October 1997.

Shane, Scott, *Dismantling Utopia: How Information Ended the Soviet Union*, Chicago: Ivan Dee, 1994.

U.S. Department of Defense, Joint Chiefs of Staff, *Joint Vision 2010*, Washington, D.C., 1996.

U.S. General Accounting Office, *Information Security: Computer Attacks at the Department of Defense Pose Increasing Risks*, Washington, D.C.GAO/AIMD-96-84, May 1996.

U.S. General Accounting Office, *Air Traffic Control: Weak Computer Security Practices Jeopardize Flight Safety*, Washington, D.C., GAO/AIMD-98-155, May 1998a.

U.S. General Accounting Office, *Computer Security: Pervasive, Serious Weaknesses Jeopardize State Department Operations*, Washington, D.C., GAO/AIMD-98-145, May 1998b.

The White House, Office of the Press Secretary, “Protecting America’s Critical Infrastructure,” Washington, D.C., PDD 63, May 22, 1998.