National Security in the Information Age

David C. Gompert

THE INFORMATION REVOLUTION HAS BEEN in full swing long enough to permit a broad assessment of its effects on U.S. national security. This burst in human ability, owing to rapid growth in the processing of data and sharing of knowledge, is proving beneficial in three ways. First, it is improving the international security environment by spreading the ideals of freedom, putting oppressive state power on the defensive or out of business, and helping long-poor societies modernize. Second, it is enhancing the power of the United States at the expense of nations opposed to its principles and interests, by increasing the strategic value of free markets, science, and technology. Third, it is altering warfare in a way that will enable the United States to protect its interests and international peace at an acceptable risk, despite the spread of weapons of mass destruction.

These promising trends should continue. In the long run, the international equities of the United States and other free-market democracies can be secured by the superior economic, technological, and military potential their openness provides in the information age. Put differently, because the information revolution has strengthened both the relationship between freedom and knowledge and that between knowledge and power, it links power to freedom. A rosy forecast? Perhaps—yet a plausible one, all the more likely to come true if pursued.

Of course, a bleak alternative hypothesis must also be examined. Have we not watched too many despots manipulate modern communications to write them off as easy prey instead of skillful predators of the information age? Will the information revolution not produce insecurity for the United States and other democracies, whose very openness creates paths for new dangers? Free economies and societies may already be vulnerable to electronic attacks on the communications networks and computer systems that enable them to function. Such new threats could come not only from rogue states seeking to outflank the military might of the United States, but also from sub- and transnational adversaries, emboldened by the fact that information technology lets them operate as elusive networks even as it erodes the power of governments. Finally, the rise of a new strategic challenger—China, perhaps—able to exploit off-the-shelf information technology cheaply and quickly for military purposes cannot be excluded.

This article finds that the contributions to security of the information revolution are profound, cumulative, and sustainable, and the dangers serious but manageable. It surveys both the contributions and the dangers and concludes with some thoughts on how to encourage the former and avert the latter.

Progress in World Politics

Information technology is enriching, integrating, and expanding the world's democratic core, promising improved security on much of the planet. It has played a role in the three great political developments of the late twentieth century: the metamorphosis of Japan and Germany, the demise of the Soviet Union, and the emergence of previously underdeveloped regions. In the old nomenclature, it has helped revitalize the First World, liberate the Second, and uplift the Third.

It took several decades following World War II for the economic dynamism at first concentrated in North America to yield sustainable prosperity in Western Europe and Northeast Asia. It then took a mere

decade—the 1980s—for economic freedom to get the upper hand and for modernization to ensue in Southeast Asia and Latin America. Within just a few years of the democratic revolutions of 1989, private enterprise overtook decrepit state sectors in Eastern Europe. Whereas massive policy interventions—the Marshall Plan, strong government, domestic market protection—were needed to nurture Western Europe and Northeast Asia, private investment and the accompanying transfer of technology are propelling the newly emerging economies. The enterprises of the democratic core, now competing globally, seek not only new markets but new locations where they can produce at lower cost. Where once they explored for raw materials to extract and process, global firms now find labor to train and employ. Capital, management know-how, and market distribution systems are spreading eastward and southward, ushered by the ideology of openness.

It is no coincidence that this accelerating globalization has run alongside the information revolution. Information systems permit distributed production—scale without geographic concentration—and global marketing: designed in the United States, chips fabricated in Japan, subsystems built in Taiwan, software written in India, the final product marketed in Europe. Information technology equips, rewards, and elevates "human capital" (that is, people) by expanding, using, and sharing the output of their minds. The 6–10 percent gross domestic product growth rates common among emerging markets reflect their citizens' newfound chance to add value, thanks to information technology. Behind the numbers lie the new skills, productivity, and hopes of a billion workers.

Investment in information infrastructure is both a cause and a consequence of modernization. Digital telecommunications networks are expanding rapidly, responding to the demands of business but also dramatically increasing personal access. Improved communications carry the spores of economic and political freedom, spores that grow into democratic movements and institutions. Just as the economies of emerging countries are altered by reform, investment, and participation in global industry, their politics are transformed by the information and ideas that their new infrastructure distributes. Countries cannot import crucial technical know-how without also receiving packets of smuggled democracy. Working on a computer-based production line is bound to increase both the interest and the ability of the employee to use essentially the same technology to expand his or her personal knowledge, potential, and freedom.

But did not the industrial revolution also produce notions of great political advancement, only to yield (owing to some of those notions!) history's most violent century? True; yet industrial-age technologies—metal-bending, machine-propelling, even atom-smashing—do not require the same degree of economic freedom that it takes to create and apply information technology. Indeed, industrial technology is conducive to concentrated state power, whereas information technology abhors it. Nor do the old technologies directly stimulate and improve the minds of those who use them, as information technology does. Information technology is altogether different, because it expands knowledge, which promotes freedom, which in turn aids the creation and use of information technology.

New research reveals strong causal links between the availability of information technology and demands for democracy;[1] it buttresses a belief as old as Western democracy: "To give information to the people is the most . . . legitimate engine of government."[2] Other recent empirical work confirms that the freeing-up of markets intensifies the urge for political freedom, because economic freedom whets the appetite of a growing middle class for the permanent right to challenge the policies and even the tenure of the ruling regime.[3] It appears as well that the current economic turmoil and disappointment in East Asia is not undermining adolescent democracy but rather opening it up and thus toughening it. Whatever the cause-and-effect relationship among marketization, democratization, and access to information, it suffices here to note that the three come in a package, of varying shapes and sequences from one country to the next.

By enabling citizens to learn what is happening outside as well as inside their country, information technology leaves illegitimate governments with just three options: reform, crackdown, and extinction. The shrewd and ruthless ones—Saddam, yes; Gorbachev, no—know that reform can lead to extinction, or at least

early retirement, so they crack down as needed to retain power. Consequently, we are left with a dwindling number of quite odious regimes, in Pyongyang, Baghdad, Belgrade, Tehran, Yangon, Lagos, Damascus, and Havana, all living on borrowed time. The self-isolation, oppression, and knowledge control they practice is grinding down their economies, even as their citizens inevitably learn about their thriving neighbors.

Nevertheless, the optimist must concede that the information revolution will not soon corner and banish every single dictator. But if access to knowledge and the technology that spreads it is not a mortal threat to authoritarian states, why are they so determined to suppress or monopolize it? Why does the Milosevi… regime oppose every alternative to state-controlled television? Why must information about the Internet stay underground in China? Why is the number of telephone lines per capita so much higher for democracies than for authoritarian states of comparable wealth? As the variety and sophistication of communications media increase, democracy becomes both more urgent and more feasible for peoples of any culture, faith, or stage of development.

Of course, some of the regimes who tremble at the political effects of the information revolution are friendly and important to American interests. Perhaps U.S. policy makers are learning the lesson—of the shah, Marcos, Mobutu, et al.—that ignoring the need for "friends" to reform will eventually imperil American security interests. The conservative, oil-producing Arab states remain a dilemma because of their economic importance and our fears of a militant Islamist alternative. But wisely managed, the information revolution creeping across the Arabian Peninsula can reform and thus legitimize, not radicalize, these important states.[4] Conversely, even friendly and favored autocrats can resist the information revolution only by becoming more autocratic.

How are these political changes affecting international security? For the most part, as the information revolution speeds the integration and expansion of the democratic core, it has a pacifying effect. In Eastern Europe and Southeast Asia, as before in Western Europe and Northeast Asia, economic reform, democratization, and open information are extinguishing instability and violence. These were four of the world's most dangerous regions during the industrial age; they seem at last to have exorcised the demons of ethnic and territorial conflict. Accountable government, the rule of law, and economic success make majorities and minorities alike less inclined to resort to violence. Democracies may not be angelic, but as a rule they do not go to war with one another, and they normally abide by norms of responsible international behavior that spring from the same basic values as does democracy itself.[5]

It is not surprising, therefore, that most recent conflicts (Afghanistan, Somalia, the Caucasus, Haiti, Kosovo, Bosnia, Central Africa, Kurdistan, Tajikistan) have occurred beyond the pale of the democratic core. We no longer worry about war between Germany and France, or Japan and Korea; perhaps we can soon stop worrying about war between Hungary and Romania, Argentina and Great Britain, and Russia and Poland. Finally, as the information revolution topples one after another of the remaining dictatorships, there will be fewer left to threaten their neighbors, dispatch terrorists, and stockpile nuclear, biological, and chemical weapons.

This is not to say that permanent peace will arrive as soon as Kim, Saddam, Milosevi…, and company depart. Knowledge-based human progress is uneven; ancient feuds persist; population growth is too high in the very regions that can least afford it. We have not seen the last state to collapse in Africa. Other regions outside but important to the core—the greater Middle East and the former Soviet Union—remain dangerous to themselves and to U.S. interests. The increasing availability of weapons of mass destruction and the means to deliver them could threaten international security, especially in these unstable regions. U.S. defense planning, as embodied in the recent Quadrennial Defense Review and the independent National Defense Panel review, is becoming less concerned with the number of rogue states—especially with North Korea teetering (and Iran flirting?)—and more concerned with how dangerous each of them might be.

Still, the trend line is promising for a growing area of the world. Except for oil and gas reserves (admittedly a large exception), the essential economic interests of the United States are concentrated in regions that are now peaceful and safe. The demands placed on U.S. forces are increasingly from contingencies short of war, typically in places and for reasons that are not vital. These demands will persist, and the immediate situations in Iraq and Korea will remain tense, but the danger of armed aggression against the global interests of the United States and the core, let alone against the core itself, is small and shrinking. Moreover, as what follows will suggest, the beneficial effects of the information revolution on U.S. military power and on the nature of warfare should prepare the United States well to respond to the changing international security environment.

To sum up, information technology spurs economic development by rewarding and enhancing human capital. It facilitates the globalization of production and marketing, fostering direct investment, new information infrastructure, and the integration of healthier nations into the core. As it extends economic and political freedom, the information revolution helps reduce internal and international conflict. Since the global security environment took a sudden turn for the better in 1989-1991, positive developments have been less spectacular. Setbacks have occurred and will occur again. But the vector is toward a less violent new century—thankfully, since this one was the most violent yet—owing in large part to the information revolution and its contribution to freedom and security.

The Information Revolution and National Power

The Cold War ended in an ironic failure of containment: that is, Soviet failure to contain the democratic core. The information revolution made the Soviet Union an economic, political, and even military loser. A brief look at that collapse illuminates how the essence of power has shifted as the industrial age has given way to the information age.

Information technology widened the gap between Western and Eastern economic performance that had already been evident before 1980. By the end, not only the United States but its protectees, Western Europe and Japan, dwarfed the Soviet Union in most of the measures that matter. The Soviet state did not just neglect and resist the information revolution; it was incapable of joining in it. Its futile, last-ditch attempt to import computer and communications technologies suggests that it fundamentally misunderstood them. Information technology especially rewards innovation and entrepreneurship (the proverbial two guys in the garage having, implementing, and marketing breakthrough ideas that the big organizations do not dream of), market agility, and scientific and intellectual freedom—hardly socialist strengths. As well, the information revolution amplified the "cost of empire" by spreading the truth about Afghanistan, the West, Solidarity, and communism itself. Unable, and under Gorbachev unwilling, to stifle the sharing of knowledge among its citizens, the Soviet empire and state crumbled much faster than anyone had imagined was possible. The information revolution delivered a swift coup de grâce to a system grown feeble late in the industrial age that bred it.

The information revolution even stripped the Soviet Union of its specialty, military power. Technology from commercial markets decided the great strategic race. Competition in computers, telecommunications, and chips among U.S. firms, and between them and Japan, propelled the revolution that bypassed the communist world. Information technology sprouted in the military's hothouse of the 1950s but bloomed outside it. In the 1980s, banks and manufacturing giants displaced the defense establishment as the most sophisticated and demanding users of data processing and networking. In the United States, the military was the dominant segment of the information technology market in 1975, with a 25 percent share; it now holds less than 3 percent of that market, owing to phenomenal growth in nonmilitary demand.[6] The civilian economy has furnished both the incentive and the profit revenues to develop the microelectronics, software, and networking technologies that determine the performance of contemporary military systems and forces.

Not embedded in a thriving civilian economy, the Soviet military was, of all things, too small to support

adequate research and development (R&D) on the vital technologies. Ironically, the military's dominance in information science and technology within the USSR contributed to its own undoing: what it dominated turned out to be a bogus industry in a phantom market. The growing microelectronic content of high-performance military systems in the United States compounded the Soviets' inability to keep pace. All that land, all those minerals, all those factories, all those engineers, even the vaunted Soviet education system could not make up for the lack of stimulus and funds for investment that markets for VCRs, PCs, and digital networks provide.

The failure of Soviet political, economic, and military power was only the most spectacular recent example of mind over muscle in world politics and warfare. (The outcome of the contest between South and North Korea also comes to mind.) Information technology has made traditional assets of power—territory, huge armies, heavy industry—less strategically relevant. Military systems, thus military power, now depend more on the freedom of commerce and science than on the strength of the state.

With its favorable climate for high-risk/high-value invention and unrestricted use, the United States enjoys a distinct edge in the information era. Openness, a hallmark of the American political economy, is the key to success in the information industry, and thus to national power. The United States is increasing its military superiority even as its forces shrink. Moreover, the countries in the next-best position to improve their military capabilities with information technology are not adversaries but America's Western European and Northeast Asian partners.

Actually, the gap in military technology is widening between the United States and these allies. Collectively, the Western Europeans have roughly as many men under arms (1.5 million) and spend two-thirds as much on defense ($160 billion) as the United States. But only a small fraction of their forces can operate effectively at a distance (where they are most likely to be needed). Consequently, the strategic contribution of our Nato allies is declining. While this is obviously not good, it does underscore the fact that America's success with information technology is enlarging its lead over friend and foe alike. The combination of the Pentagon's $30-plus-billion R&D budget and, more importantly, the nation's edge in information technology will keep the United States in a class of its own.

Information technology should also begin to yield major reductions in the cost of defense systems and infrastructure. Even allowing for gains in performance, the cost of advanced weapons systems has not fallen nearly as fast as has the cost of civilian systems of comparable complexity and microelectronic content. With military procurement reform—the process remains a problem—we are just beginning to see impressive per-weapon cost reductions.[7] Operational and structural efficiencies and savings that private firms have derived from the information revolution in the past decade are just beginning to infiltrate the defense establishment. The defense logistics system, for example, can slash inventories, warehouse space, and labor costs if and as it adopts practices and technology now commonplace in private industry.

Such opportunities are surface effects of much deeper forces that connect freedom and power in the information age. Success in creating and applying information technology depends on healthy markets and political openness. Adequate financial returns and confidence in unimpeded application, both key in this technology, are not to be found in closed states. Authoritarian states may not be incapable of utilizing information technology for military purposes, but they plainly are handicapped.[8] The United States is able to enjoy these benefits first and foremost, adding to its military advantages and unrivaled power. While other open societies have a similar potential, the United States alone is poised to pass through a military revolution.[9]

The Changing Nature of Warfare

Roughly stated, information technology can help those who master it to win large wars at long distances with

small forces. While recent official statements of U.S. defense strategy (the Quadrennial Defense Review and "Joint Vision 2010") are careful not to promise dramatic results, they point toward a future in which the U.S. lead in information technology will permit one-sided wars with low American casualties. In a more revolutionary version, tomorrow's battlefield could consist of enemy troops absorbing friendly fires, with friendly forces beyond the range of enemy fires. While technology allows this, the motivations for it are an aversion to casualties and also the lethality of the battlefield, especially as weapons of mass destruction (WMD) proliferate. If the United States had an affordable way of defeating a threat to, say, Persian Gulf oil supplies without placing a huge force and all its supplies in the target-sights of a WMD-armed enemy, it surely would.

The revolution's mortar and pestle are stand-off weapons and information dominance—that is, complete knowledge of what all enemy and friendly forces are doing. This lets small, light forces armed only for self-defense call in devastatingly accurate long-range fires. In theory, such forces could fight defensively or offensively.[10] Ubiquitous information technology permits precise and split-second intelligence, "fused" readings from multiple sensors, communications between battlefield units and distant weapon platforms, and coordination among alternative strike options (land, sea, and air-based). Since the size of the force needed on the battlefield is reduced, forces are more rapidly deployable virtually anywhere, and they depend less on vulnerable forward bases, choke points, and skittish local allies. Ideal conditions (surgical projection of power, enemies rendered defenseless, U.S. forces operating at will, casualties reduced on one side if not both) are no longer far-fetched.

So much has been written lately about the revolution in military affairs (RMA) that it is both impossible and unnecessary to reproduce that debate here, but the main misgivings deserve to be noted. First, as the actual uses of U.S. forces since the Persian Gulf War show, the new international environment is less likely to confront the United States with unambiguous circumstances, in which force can be used decisively, than with messier "smaller-scale contingencies" in which information dominance is of less value and stand-off strike is largely irrelevant.[11] Second, the sophisticated information systems on which the RMA is predicated could become vulnerable to information warfare (more on this later). Third, the threat of rogues and nonstate actors committing acts of terror, possibly with weapons of mass destruction, directly against American territory and citizens is more likely to be stimulated than preempted by the revolution in military affairs, since these adversaries will be left no other routes of attack. Fourth, the diffusion of information technology, aided by globalization, will permit potentially hostile states to acquire military capabilities pioneered at great cost by the United States; thus, some argue, the RMA might lead to a high-tech arms race that will leave U.S. interests less secure.[12]

Apart from questioning its *desirability*, skeptics have doubts about the RMA's *feasibility* in the foreseeable future, citing technical, institutional, and fiscal hurdles. Some say that too much attention is paid to technical feasibility and too little to doctrinal and organizational implications; others warn of technological risk. So which is it? The technologies are at hand. The sensors, communications, weapons, and integration needed require no qualitatively new level of wizardry. The biggest technical uncertainty is the affordability of the accurate stand-off weapons that will be needed in great quantity to make up for massive battlefield firepower; still, if the cost of these weapons follows the declining cost of much of their microelectronic content, as suggested earlier, they should be affordable in sufficient quantities.

A more serious impediment is the reluctance of a large, successful, and unthreatened institution like the U.S. Defense Department to transform itself. There is as well a reluctance in some quarters of the uniformed military to shift toward a stand-off warfighting strategy: the Army is concerned that substituting remote strike power for "boots on the ground" would leave the nation able to respond only in (rare?) situations that are ideal for that kind of war; the Air Force is as keen as ever to build new penetrating combat aircraft rather than rely mainly on stand-off weapons. Finally, Congress may be a roadblock; it has rejected the administration's

initial proposal to close more bases in order to pay for RMA modernization.[13]

In the RMA debate, every "pro" and every "con" can be rebutted and re-rebutted. In the end, however, three powerful points still stand. First, having the option to conduct warfare along the lines of the RMA can only be positive for U.S. power and credibility, provided it is not developed at the expense or neglect of other options for using force. Second, if there is a way to remove human beings from increasingly lethal battlefields without compromising national security, there is a political and moral responsibility to pursue it. Third, there is no reason to believe that the information revolution will bypass warfare as it alters most other human activity. If information technology is bound to change warfare, better for the United States to lead and affect that change than be compelled to react to its effects.

If some form of the RMA is coming, we had best consider its ramifications. Because fear of high U.S. casualties is the chief reason for public hesitation about going to war, the possibility of projecting force without endangering personnel adds to U.S. freedom of action and credibility, at least in those circumstances where this is a suitable option. In the continuing stand-off with Iraq over the UN's search for weapons of mass destruction, for instance, the American people have not had cold feet, largely because they assume a low-risk operation would do the job. With both its ability and will to use force increased or at least preserved by the RMA, the likelihood of the United States needing actually to use force should decline.

The prospect that the world's dominant military power can be confident not only of winning wars but of avoiding significant losses has major strategic and political implications for that power and for the international system. If one believes that the will and ability of the United States to wage war is, on the whole, good for international security—an argument far too subjective and complex to present here—this shift in the nature of combat must be viewed favorably. Granted, even some old friends of the United States, having had a glimpse of U.S. unilateralist diplomacy and legislation, are now raising questions (typically over brandy) about the drawbacks of American dominance. Objectively, however, there is little reason to worry that America's lead in the revolution in military affairs will cause it to be injudicious, let alone hegemonic or aggressive.[14]

Dangers from the Information Revolution

The upbeat assessment to this point does not exclude that hostile states will exploit the information revolution to the detriment of U.S. and international security. As noted, adversaries—whether rogue states, nonstates, or a superstate—could attack the economic and military information systems of the United States and its partners or use improved information-based conventional forces to threaten U.S. interests or defeat its military strategy.

Most rogue states are on the ropes, as explained above, because of the information revolution's "one-two-three punch" combination of globalization, democratization, and access to knowledge. Self-isolation and savagery may be enough to keep some going, but with depleted economic strength and little ability to marshal human talent. It will be extremely hard for an authoritarian regime, sitting atop a volcano of discontent and surrounded by enemies, to acquire, apply, and operate sophisticated, knowledge-based military technology and systems on a large scale. Although we should anticipate such adversaries causing specific problems, perhaps with improved surface-to-air and surface-to-surface missiles, the ability of the United States to render them defenseless will not be in doubt.[15]

Thus frustrated by insurmountable conventional military inferiority, rogue states are likely to turn to asymmetric strategies, for instance, weapons of mass destruction, terrorism, and information warfare (IW) attacks on the United States and its partners. Obviously, the use or threat of nuclear, biological, and chemical weapons is extremely risky, especially against a superpower. Rogues might therefore be tempted to try information warfare. If they do, they will find readily available the computer tools and talent they need to

target the nodes and links on which the U.S. economy and military increasingly depend.[16]

A recent series of war games involving attacks on U.S. "cyberspace" strongly suggests that this country's ability and resolve to defend its overseas interests are put at risk by the sorts of IW attacks that could be within the means of a number of unfriendly states within a few years. Coordinated attacks on the command and control of deploying U.S. forces, on its allies, and on the public telephone network could derail an otherwise "routine" projection of military power. The games also show that neither government nor industry is well prepared for this threat, technically, institutionally, or intellectually.[17]

Do not look for a single "silver electron" to defeat the multifaceted danger of information warfare. The efforts now under way by large corporate providers and users of information technology to increase data security will provide some, though by no means enough, protection of the nation as a whole. Threat of U.S. retaliation (electronic or kinetic), improvement in the security of networks and systems, strength to absorb minor attacks, and an ability to recover from major ones should all play a role in counter-IW strategy. Over the long run, because the integration of the world economy is globalizing many key networks, it will take an international consensus on protecting cyberspace to prevent our reliance on information technology from becoming a source of insecurity.

An aspect of the IW threat that makes prevention and response especially difficult is the multitude of potential attackers, from nations down to individuals. Nonstate actors, such as international crime rings, terrorist organizations, separatist groups, and cults, can acquire IW weapons or hire IW warriors. Compared to the acts of clumsy governments, their attacks could be hard to trace, punish, and deter. These are increasingly dispersed entities, interconnected by (what else?) information technology. Network communications could both increase the potency and hide the signature of nonstate actors who target nation-states, including the United States.

The information revolution is spawning a new form of basic human organization, the network, to accompany if not crowd out those of history: the tribe, the hierarchy, and the market.[18] Nongovernmental organizations and nebular communities of interest, ranging from saintly to diabolical, are growing in number and capability at the expense of governments, political parties, established religions, corporations, law enforcement, and the nation-state itself. As the report of the National Defense Panel stresses, these actors might become the main source of security in the twenty-first century.

Still, the nation-state surely has a few good years (or centuries) left and will remain the chief concern of U.S. national security for the next decade or two. Consequently, even if smallish, garden-variety rogue states cannot prevent or deter the United States from protecting its interests, perhaps an unfriendly super-state—one able to produce information technology and the advanced weapons that use it—could.

The countries with the greatest technical capacity to pose such a strategic challenge to the United States are the least likely to do so. Because of their ability to create and use information technology, the most capable candidates are the other democratic economic powers: Japan and the European Union. Both have the means to put this technology to greater military use than they have so far. Their lack of appetite for international power, however, is unlikely to change. The Japanese and Germans, in particular, have no interests that would tempt them to return to aggressiveness, which brought them complete destruction and an unforgettable lesson. They will not veer from their course of the last fifty years, when being democratic and a friend of the United States has paid off handsomely.

The only other plausible candidate, China, can realistically aspire to becoming a modern power, and it does. It has the necessities: scale, talent, access to capital, and a growing role in the world economy. In addition, moderating Chinese international ambitions via the U.S. strategy of "constructive engagement" will be difficult, because China's huge market gives it both political license and policy leverage, as it has shown in

defying foreign concerns about its behavior toward Taiwan and its own people. Unlike Japan and Europe, China could develop both the capability and intention to challenge the United States.

Current Chinese military capabilities are old and weak, particularly in power projection. But this is exactly what the People's Liberation Army has made its highest priority, with the ability to assault or at least intimidate Taiwan as its motivation. U.S. planners must assume that Chinese power-projection forces will be much improved within twenty years, giving China the ability to interfere with American power projection on the Chinese periphery. That will clearly make the defense of Taiwan more difficult, but would it make China a strategic challenger? Could China even leapfrog the United States by buying or copying information technology available in the global market?

Neither is likely. Some information technologies are becoming commodities, as are individual pieces of advanced military hardware, but modern military systems require sophisticated design, engineering, integration, management, and operation. China may be able to buy and even make many of the piece-parts; the RMA, however, is less about gadgets than about knowledge—no forte of a closed society. Moreover, success in generating and using information technology, in general, depends on a willingness (unproven in China's case) to abandon vertical control and distribute authority, within the nation and within each enterprise. So the road ahead for the Chinese in building information-age military power is a steep and difficult one, and they are unlikely to draw close to the United States along the way. As China heads up that road, it will—indeed, it must—become more ensnared in the world economy and more exposed to creeping political reform, if not democratic transformation. By the time China has become a global power—after, say, two decades—it may well also be a friendly and open one.[19]

A Net Assessment and Policy Directions

Goebbels, Stalin, and Milosevi… notwithstanding, knowledge shared is stronger than knowledge denied, distorted, or manipulated. The recent past shows that information technology, unlike the technologies of the industrial age, requires freedom and openness. We can now also begin to see that information technology is the key to power—"soft" economic and technological power, of course, but also "hard" military power.[20] It follows that the greater the economic and political freedom of a society, all else being equal, the greater its capacity to be an information-age power. The United States and the other leading democracies thus have an inherent advantage. If China proceeds with its transformation, it will acquire a major stake in international security as its power grows; alternatively, if China abandons reform and integration it will have trouble modernizing and especially harnessing information technology, thus sacrificing power. Rogue states will remain dangerous, especially as they get weapons of mass destruction, but the combination of the relentless pressures for change and the coming revolution in military affairs will keep them in check.

Running against these encouraging trends is the danger that reliance on information technology will become America's Achilles' heel. So far, it has not, but global economic integration and the RMA itself will increase that reliance; as nonstate rogues proliferate and the means to attack information systems and networks become widely available, the IW peril could grow. Still, the optimist could argue that the American "system"—economy, society, politics, institutions, military forces—is too resilient, resourceful, and stable to be seriously damaged by plausible IW attacks and that U.S. technological superiority will prevail. Openness is more an advantage than a handicap.

Admittedly, this net assessment of national security in the information age leans toward the sunny side, but it also recognizes pitfalls and uncertainties. The aim of policy, simply stated, should be to encourage the trends that increase security and discourage those that degrade it. In considering policy recommendations, a dose of humility about the U.S. government's power is in order. To credit Washington with information technology's contribution to national security is a bit like praising it for the fact that the nation is protected on two sides by oceans. Except by its noninvolvement, the government did not cause the information revolution, and it cannot

direct the revolution's future course. The information industry's current leaders want to be left alone by the government, and they have the First Amendment and market economic theory on their side. Moreover, the technical expertise of this revolution, unlike that of, say, nuclear power, is almost entirely, and necessarily, outside of government.

In this spirit, let us consider some thoughts about policy on three fronts: the diffusion of information technology, the pace and priorities of the RMA, and countering the IW threat.

Information Technology Transfer. The diffusion of information technology is a consequence of economic globalization, especially the building of modern telecommunications infrastructure and the spread of manufacturing, R&D, and other product and process know-how. The technologies of interest range from microelectronic devices to large-scale digital networks, and they include hardware and software. While some are specifically for military use, most are inherently dual use and intended mainly for civilian markets. Although the U.S. government can barely keep track of this diffusion, it has several policy interests: first, that adversaries not acquire militarily useful information technology; second, that the United States not lose control over information technologies on which it depends for important military uses; and third, that sharing this technology with allies enhance coalition military effectiveness without damaging U.S. commercial interests.

Because information technologies are dominated by private markets and enterprises, efforts by the government to restrict their transfer have foundered over the difficulty of stemming the flow and its own reluctance to forego profitable revenue from this largely nondefense trade. Nevertheless, the unstated presumption of policy, ingrained from decades of Cold War export control, is that technology transfer ought to be restricted when we are able and can afford to do so.

When it comes to information technology, we ought to set aside this presumption and ask whether in fact we want to, and need to, restrict the spread. Approaching the issue from this angle would reveal what is different about this technology. First, it fosters openness, economic reform, democratization, legitimacy, integration—and thus international security. For instance, we should want China to have a modern digital network, broadcast technologies, and host computers and terminals galore. Whatever risk is involved is more than offset by the effects of these technologies on China's eventual transformation, integration, outlook, and behavior.[21]

Second, the strategic and operational military advantages of the United States transcend hardware and software. The flair for innovation, application, and competition; the ability to design, integrate, and operate complex systems; and the lightness of government control are U.S. strengths that will not seep away through export licenses. The best proof of this is that most information technologies have been flowing freely in international markets for decades, yet the U.S. lead in them is actually growing. Diffusion of information technology does not necessarily weaken the source, absolutely or relative to the recipients. Indeed, the spread has benefited U.S. firms, strengthened the nation's economy, enriched the technology itself, and thus given the U.S. military a stronger base on which to modernize.

In sum, when the government has the means to intervene effectively to prevent a known adversary from acquiring a technology of known military benefit, it should of course do so. Nonetheless, as a general philosophy, we do not want or need to restrict the diffusion, even if we could.

Similarly, globalization is unlikely to leave the United States dependent on critical information technologies that some potential adversary controls to its disadvantage. Again, there will be exceptions. Still, the more widely diffused production becomes, the less the United States need worry that one or two countries can, much less will, deny access to some strategically important capability. Moreover, the countries most likely to produce devices or services deemed critical to the United States are either its current partners in the democratic core or are emerging states whose own future depends on integration into the core and good U.S.

ties. A transnational pool of information technology has formed and is expanding. Just as the United States cannot deny others access to the pool, it should have no concern about its own access being denied.

Finally, the diffusion of information technology to allies presents a dilemma, in that the United States is the market leader and its closest allies are its main commercial competitors. This dilemma is sharpened by the fact that the military technology of U.S. allies is slipping relatively, which may be good commercially but is bad for coalition military effectiveness and political cohesion. Although Japan, Korea, and Israel are interesting cases, the larger and immediate concern is Nato. If the United States wants to rebuild the Atlantic military coalition—with joint power projection replacing the Cold War mission of territorial defense—it has a stake in reversing the trend. It should therefore pursue such alliance priorities as C3I, [*] precision strike, missile defense, and streamlined logistics. Such cooperation would not jeopardize the U.S. technological lead. If the president's advisors are wondering what he should propose at the next Nato summit, they might consider an initiative to foster transatlantic defense technological cooperation: an "alliance RMA."

Military Transformation. The revolution in military affairs, as defined here, has yet to occur: Desert Storm was the equivalent of the Boston Tea Party. [**] Unless confronted by a formidable adversary—as was Great Britain at the beginning of this century and the United States after World War II—or by grave crisis or war, successful nations and institutions tend not to make radical change. Do not count on technological fascination, even if accompanied by enthusiastic journal articles, to bring about the RMA. The recent Quadrennial Defense Review satisfied few military affairs revolutionaries, reflecting to some degree the institutional hurdles but also the substantial investment cost of the RMA. With Congress balking at more base closures, the Defense Department does not wish to pay for more revolutionary modernization at the expense of readiness, force structure, or pay.

While it is easy, sitting in a think tank, to criticize these priorities, lament the lack of imagination, and indict vested interests, the RMA must in any case occur programatically and thus incrementally. In a more bottom-up than top-down fashion, small units will acquire more firepower through access to remote-strike weapons; the unit cost of those weapons will come down; intelligence will become more complete and timely; sensors will become more precise and integrated; command and control architectures and technologies will be renovated; doctrines, practices, and training—do not forget the human—will be honed. Such gradualism is not only realistic, it is prudent. As noted earlier, the fast lane has doctrinal, institutional, and technical potholes. Moreover, strategy and politics will have to adjust to a world in which the United States can wage large wars with small risks.

Proceeding without haste, the defense establishment can take several measures to help ensure progress. First, the vision should be sketched out, not only its technical parameters but its strategic purpose. Incremental steps in force structures, doctrine, and modernization need a beacon; this has only partly been provided by "Joint Vision 2010." Second, experiments ought to be performed: R&D, special units, and new systems that follow the beacon should be (and are being) supported and protected, not only from budget cutters but from the services' and unified commanders' own current priorities. The Defense Department has a decent record of incubating promising technologies; we shall now see if it can do the same for a fledgling revolution. Third, research on possible RMA countermeasures (technical and tactical) should be intensified. For example, could the electromagnetic pulse from a high-altitude nuclear blast disable sensors, networks, and weapons?

The forgotten factor in U.S. technological superiority is people. The success of the American all-volunteer force over the past two decades has been as extraordinary and important as the stream of technical innovations. With the information revolution, however, complacency in managing that asset would jeopardize the U.S. edge as surely as would neglecting research and development. The ability of the United States to recruit, train, retain, and motivate high-quality service personnel is already being seriously tested by the increased requirement for skilled "knowledge workers" and the fierce competition with industry for those people that the military needs.

Information Warfare. Because this is a new and open field, there is a danger of analysis outrunning reality. Only now is a conceptual framework being constructed.[22] Only now is the government getting organized. Enhancing the security of information systems has become a cottage industry; this is not the place, and this author is not the person, to offer new technical prescriptions. From a policy standpoint, however, several thoughts are worth mentioning.

The last thing the United States needs is an IW "czar." Within the government, a networked solution is needed, perhaps with, at most, a secretariat. No department should have total responsibility, yet clear responsibility must be assigned to and within existing line departments. The Defense Department's bailiwick should be to ensure that network services circuits essential for military operations are protected, by partitioning them from public traffic, at least upon alert. Others—the Treasury, Justice, and Commerce departments, the Central Intelligence Agency—should have responsibilities aligned with their functional roles.

The role of government as a whole should be to assure national security operations, protect public resources, and foster consciousness raising, information sharing, and standard setting. This could require inducements to win industry support for the security of sectors that are crucial to the nation. The know-how, money, and much of the incentive to guard against IW attacks reside with information technology providers, service providers, and users. Only a light touch from the government will work; with standards set and a modicum of coordination provided to industry, that light touch should suffice.

One indispensable role for the government is deterrence. If and as the IW threat becomes real, the United States should declare that an IW attack on the nation or its interests will be treated as a hostile act, that the attacker should be prepared for a response involving whatever means the United States might select. By no means should the United States adopt a tit-for-tat (IW-for-IW) strategy, since an attacker is likely to be far less dependent on information infrastructure and therefore could be unimpressed by an IW retaliatory threat.

The global interconnectedness of networks and the economic functions they support requires international collaboration in combating IW. The key members of the democratic core, Nato and Japan, should form an inner circle. The U.S. government should encourage the Europeans, East Asians, and Canadians to take the same steps it takes itself to improve security.[23] The idea of an international convention equating IW attacks with hostile acts is worth examining. Admittedly, this would be hard to define, harder still to negotiate, and would limit U.S. offensive IW options. Like the biological and chemical weapons conventions, it would not eliminate the danger from nonsignatory or cheating rogues, much less nonstate actors. Nonetheless, it would be consistent with the fact that the United States and the rest of the advanced democratic world have more to lose than to gain from rampant information warfare. It would also reinforce the declaratory policy, just suggested, that IW aggression would justify a deadly response.

A Final Observation

Admittedly, this is a restrained strategy to preserve the U.S. lead in information technology and to increase the payoff in national security. The role of government and of policy in the information revolution has been modest and, generally speaking, should remain so. Improvement in the international security environment has been mainly the result of market and technological forces and their salutary political effects. The advantages held by the United States are deeply rooted in its competitiveness, entrepreneurship, science, and openness—qualities that are not about to atrophy if the government fails to take charge. Indeed, state-led competition in information technology, whether for economic or strategic reasons, is not the right perspective for the United States. The positive effects of information technology on world politics and U.S. security come not from controlling it but from its free creation and use, its spread, and its harmony with basic American strengths, interests, and ideals.

Notes

1. Christopher R. Kedzie, "Communications and Democracy: Coincident Revolutions and the Emergent Dictator's Dilemma," RAND Graduate School, Ph.D. dissertation, RGSD 127, RAND Report No. MR-678.0-RC (Santa Monica, Calif.: RAND, 1996).

2. James Madison, 1787.

3. Samantha Fay Ravitch, "Marketization and Prosperity: Pathways to East Asian Democracy," RAND Graduate School, Ph.D. dissertation, RGSD 132 (Santa Monica, Calif.: RAND, 1996).

4. George S. Park, *Information Technologies in Saudi Arabia,* RAND Report MR-918.0 (Santa Monica, Calif.: RAND, 1997).

5. James Lee Ray, *Democracy and International Conflict: An Evaluation of the Democratic Peace Proposition* (Columbia: Univ. of South Carolina Press, 1995); and Francis Fukuyama, *The End of History and the Last Man* (New York: Free Press, 1992).

6. Institute for Defense Analysis, *Research Summary*, vol. 3, no. 2, 1996.

7. The cost of precision guided munitions, for example, has started to come down, even though reform of the Defense Department's acquisition process has just begun.

8. These ideas are examined in depth in National Defense University McNair Paper no. 59 by David C. Gompert, *Right Makes Might: Freedom and Power in the Information Age* (Washington, D.C.: NDU Press, 1998).

9. Joseph Nye and William Owens, "America's Information Edge," *Foreign Affairs*, March/April 1996.

10. Samuel B. Gardiner and Daniel Fox, *Understanding Revolutions in Military Affairs* (Santa Monica, Calif.: RAND, 1996).

11. Obviously, this capability will not be decisive in every imaginable conflict. For example, against large, dispersed infantry forces or in urban areas, it might not be effective at all. It is also unclear how much leverage the revolution will provide in operations short of war, such as peacekeeping and humanitarian operations, which will occur more frequently than wars. At the same time, information technology itself can help a great deal in these other situations, such as by improving intelligence, command and control, logistics, and confidence among the parties.

12. James Stavridis, "The Second Revolution," *Joint Force Quarterly*, Spring 1997, pp. 8–13.

13. The proposed fiscal 1998 defense budget contained a new Base Realignment Commission, which Congress did not authorize.

14. A recent Ditchley Conference on the U.S.-European "RMA gap" (report pending) revealed virtually no allied sensitivity on this point.

15. The WMD asymmetric threat is not addressed in this paper, because it is not based on information technology.

16. Roger Molander, Peter Wilson, David Mussington, and Richard Mesic, *Strategic Information Warfare Rising* (Santa Monica, Calif.: RAND, forthcoming in 1998; cited with the authors' permission).

17. R. Molander, A. Riddle, P. Wilson, "Strategic Information Warfare" (Report on "Day After . . . " games) (Santa Monica, Calif.: RAND, 1996).

18. John Arquilla and David F. Ronfeldt, eds., *In Athena's Camp: Preparing for Conflict in the Information Age* (Santa Monica, Calif.: RAND, 1997).

19. Gompert, *Right Makes Might.*

20. See Joseph Nye, *Bound to Lead: The Changing Nature of American Power* (New York: Basic Books,1990).

21. This does not mean that it is desirable or acceptable to provide the Chinese with the know-how to improve their ability to launch rockets, even for the purpose of placing communications satellites in orbit.

22. The best such framework, in the author's view, can be found in Molander et al., *Strategic Information Warfare Rising*.

23. R. Hundley, R. Anderson, et al., "Security in Cyberspace: Challenges for Society," Report of RAND-Ditchley conference (Santa Monica, Calif.: RAND, 1996).

*Command, control, communications, and intelligence.[Return]

**On 16 December 1773, American colonials disguised as Indians boarded British East India Company ships in Boston harbor and threw overboard 342 chests of tea to protest the tax, and the Company monopoly, on tea ("Boston Tea Party," *Britannica Online,* http://www.eb.com:180/cgi-bin/g?DocF=micro/80/14.html [5 May 1998]).[Return]

David C. Gompert is Vice President of the National Security Research Division and Director of the National Defense Research Institute at the RAND Corporation. From April 1997 to April 1998 he was on leave from RAND as a Distinguished Research Professor at the National Defense University at Fort McNair and Visiting Professor at the U.S. Naval Academy. From 1990 to 1993, Mr. Gompert served on the National Security Council staff as Special Assistant to the President and Senior Director for European and Eurasian Affairs. He has held a number of positions at the State Department, including Deputy to the Under Secretary for Political Affairs (1982-1983), Deputy Assistant Secretary for European Affairs (1981-1982), Deputy Assistant Secretary for Politico-Military Affairs (1977-1981), and Special Assistant to the Secretary of State (1973-1975). Mr. Gompert worked in the private sector from 1983 to 1990. At Unisys (1989-1990), he was President of the Systems Management Group and Vice President, Corporate Development. At AT&T (1983-1988), he was Vice President, Civil Agency Sales and Programs, and Director, International Market Planning. Mr. Gompert has an engineering degree from the U.S. Naval Academy and a master of public affairs degree from the Woodrow Wilson School at Princeton. [Return to top]