The Risks of a Networked Military

by Richard J. Harknett and the JCISS Study Group

Lost in the welter of daily crises—Serbian atrocities, Chinese espionage, North Korean nuclear programs, and Iraqi intransigence—is the big story about American defense policy.[1] Away from the headlines, as the United States designs a security policy for the twenty-first century, two basic facts of long-term consequence have emerged. The first is that present and foreseeable defense budgets are simply not large enough simultaneously to support the current tempo of military operations worldwide, the high level of training and readiness that makes American skill at warfare second to none, and the modernization of the current arsenal. The second fact is less widely recognized, but just as certain, and it has important implications for how we deal with the first. Notions of an information technology–driven "revolution in military affairs" (IT-RMA) are now deeply embedded in American defense planning. But despite their intuitive attractiveness, these ideas are dangerously misguided.

American national security planners, informed by an influential group of academics and retired military officers, are pushing a dramatically new vision of conflict in the twenty-first century. These visionaries argue that the combination of advances in information computer processing, microelectronics, surveillance, and precision weapons technologies will permit a fundamentally new way of war. After reviewing the challenges for ensuring national security in the next century, the blue-ribbon National Defense Panel, for example, endorsed an aggressive transformation of the American military. The IT-RMA, it concluded, permits and demands a new force structure that "radically alter[s] the way in which we project power," reducing reliance on

[1] This article is a multi-authored product of the Joint Center for International and Security Studies. The article's co-authors include Stephen Biddle, Jan Breemer, Daniel Deudney, Peter Feaver, Benjamin Frankel, Emily O. Goldman, Chaim Kaufmann, William C. Martel, and Edward Rhodes.

Richard J. Harknett is associate professor of political science at the University of Cincinnati. The **JCISS Study Group** was organized by the Joint Center for International and Security Studies, a collaboration between the University of California, Davis, and the Naval Postgraduate School, and was directed by Emily O. Goldman and Jan Breemer.

industrial-age military forces such as heavy ground units and aircraft carrier battle groups.[2] The Clinton administration's 1998 *National Security Strategy for a New Century* also calls for such a transformation.[3] IT-RMA proponents argue that the United States cannot act like the early-twentieth-century army that boasted the world's finest horse cavalry while armored tanks rumbled in the distance. The United States now has the world's finest tanks, they argue, but the hum of computers in the background is deafening.

Advocates recognize that such a new force structure will require a very different allocation of service roles and missions among the army, navy, and air force. If it can accomplish this, however, enthusiasts predict that the IT-RMA can rocket the United States into a permanent position of unchallenged leadership in world politics. Moreover, as pressures grow to maximize the utility of every dollar spent on defense, the IT-RMA presents itself as the solution that will preserve U.S. leadership without straining the pocketbook or risking (too many) lives—a radical technological and organizational leap that could solve the defense budget and modernization problems in one fell swoop.

But should the United States, today's leading military power, pursue a revolution that challenges the basis of the very system it currently dominates? The promise of the IT-RMA is offset by significant potential difficulties that do not seem easy to overcome. Before altering U.S. military power to take advantage of what Joseph Nye and William Owens have called "America's information edge," policymakers need to examine the end state carefully.[4]

We conclude that the end state is a major and unnecessary gamble. Given the military preeminence that the United States would be exchanging for an IT-RMA, the burden of proof rests on the advocates of radical change to show that the gamble is worth the risks. Close inspection of the IT-RMA case reveals a series of ad hoc assumptions about perfect training, perfect coordination, and perfect innovation. Its advocates, furthermore, have yet to address the possibility of unanticipated side effects and new vulnerabilities.

A far more prudent approach than revolution is a "go-slow" approach to defense planning for the twenty-first century that emphasizes the preservation of near-term readiness while exploring the opportunities of an evolutionary transition. Incremental military adaptation has served this country well over the last generation, and before the United States abandons it for a leap into the unknown, policymakers should have a better idea of where they are going to land. Despite budgetary pressures to do otherwise, the United

[2] National Defense Panel Final Report, "Transforming Defense: National Security in the 21st Century" (www.dtic.mil/ndp), p. 33.

[3] *National Security Strategy for a New Century* (October 1998) (www.whitehouse.gov/WH/EOP/NSC/html/documents/nssrpref.html).

[4] Joseph Nye and William Owens, "America's Information Edge," *Foreign Affairs*, Mar./Apr. 1996, pp. 20–36.

States should not commit itself fully to a drastic shift until the new concepts, weapons, and organizations have demonstrated, through extensive experimentation, that their vaunted effectiveness can meet real security challenges. Absent further evidence, the prudent course is to skip the revolution and stick with evolutionary innovation.

The Revolutionary Argument

Technological advances in the ability to process, organize, and disseminate information are defining America's vision of the approaching millennium. In the most popular view, evolving information capabilities form the basis for fundamental changes in social and economic practices, organizational structures, and military affairs. The digitization of information processing is expected to cause a fundamental shift in the way societies pursue wealth and power, and leaders across the political spectrum have touted their unbounded optimism for the revolution. According to President Clinton,

> the invention of the steam engine two centuries ago and the harnessing of electricity ushered in an industrial revolution. . . . [T]oday, the invention of the integrated circuit and computer and the harnessing of light for communications have made possible the creation of the global Internet and an electronic revolution that will once again transform our lives . . . [as we] enter the new millennium ready to reap the benefits of the emerging electronic age of commerce.[5]

Former Speaker Newt Gingrich talks just as enthusiastically about how the "lessons of the information age" should guide policy decisions.

The U.S. defense community has picked up on these presumed lessons and connected them to centuries-old military maxims about the value of information. The military theorist currently in vogue is the ancient Chinese writer Sun Tzu, whose philosophy of war is captured in the admonition: "Know the enemy and know yourself; in a hundred battles you will never be in peril." In defense circles, information revolution enthusiasts hold out the possibility of knowing the disposition and movement of both opposing forces and one's own to a degree to which Sun Tzu could not even have dreamed. The goal is to replace Clausewitz's "fog of war" with total transparency across the battlespace of air, land, sea, and space.[6]

According to these IT-RMA proponents, the integration of information technologies will provide the United States with major military advantages. The combat value of fighting forces will be multiplied through information superiority—the payoff of a "system of systems" that connects remote sen-

[5] Office of the Press Secretary, Text of the President's Message to Internet Users, July 1, 1997 (www.pub.whitehouse.gov/uri-res/12r?urn:pdi//oma.eop.gov.us/1997/7/1/4.text.1).

[6] Sun Tzu, *The Art of War*, ed. James Clavell (New York: Delta, 1988); Carl von Clausewitz, *On War*, ed. Michael Howard and Peter Paret (Princeton, N.J.: Princeton University Press, 1984).

sors, soldiers in the field, commanders, and weapon platforms, thereby allowing the military to locate, target, engage, assess, and reengage with speed and efficiency. Total battlespace transparency will allow the United States to close out enemy options and overwhelm an opponent's capacity to take decisive actions in combat. The technologies that will underpin this military power are promised to require fewer weapons and deployed troops, and, very importantly, to jeopardize the lives of fewer American soldiers.

This image of the future is best captured in the Defense Department's *Joint Vision 2010*, which, according to General John Shalikashvili, then-chairman of the Joint Chiefs of Staff, lays out a blueprint for military doctrine and force structure in the next century. The document's core premise is that emerging technology will grant U.S. forces "information superiority," enabling them to prevail in anything from major war to low-intensity conflict to peacekeeping and humanitarian operations.[7]

Dominance across the spectrum of conflict is precisely what the United States needs, information enthusiasts argue, in part because the end of the Cold War has not ushered in an era of order and stability. On the contrary, regional rogues such as Saddam Hussein threaten vital American interests; international crime syndicates eat away at the internal fabric of American society; terrorists imperil American lives at home and abroad; and civil wars and ethnic conflicts cause mass migrations of refugees, threatening the stability of key allies and trading partners.

According to IT-RMA enthusiasts, new information-based methods and organizations will produce a flexible military able to adapt to any contingency in an uncertain world. This is not the military of the Persian Gulf War, but a fully networked, omniscient fighting force with global reach and a full spectrum of responses. Drawn from lessons of corporate restructuring around information technology, a networked military will function by way of organizational and command structures radically different from those that typify the traditional, hierarchical armed forces. According to IT-RMA proponents, since information content and connectivity have the potential to shape economic, political, and military realities in the next century, the United States should exploit the comparative technological advantage that it now enjoys and further develop the processes, norms, and organizations to maintain its predominance. However, three broad objections to this perspective must be raised. First, efforts to promote an IT-RMA will create significant vulnerabilities that do not currently exist. Secondly, an IT-RMA is unlikely to provide useful responses to the threats that will probably pose the greatest challenges to the United States. Finally, it risks triggering a backlash against U.S. foreign policy, even among allies.

[7] Joint Chiefs of Staff, *Joint Vision 2010* (1996) (www.dtic.mil/doctrine/jv2010/jvpub.htm).

The Revolution Creates New Weaknesses

Enthusiastic supporters of an IT-RMA argue that restructuring forces to take advantage of information technology can significantly reduce the uncertainty inherent in military operations and the inefficiencies common to large organizational action. Networked information systems will provide, according to this view, a shared sense of fluid military situations among all levels of command. Troops will know clearly where they are in relation to friendly and enemy soldiers and will have detailed information concerning the behavior and dispositions of enemy forces. Armed with such data, troops and commanders should be able to discern the probability that enemy soldiers can achieve their objectives or prevent the U.S. forces from achieving their own. Information superiority is expected to leave the enemy paralyzed and easy prey for coordinated, low-cost surgical strikes. Shared battlespace awareness will purportedly enhance efficiency by giving every actor access to all the best information the U.S. side possesses. If an entire military force, from the most junior foot soldier to the commander-in-chief, shares a common understanding of the whereabouts of enemy and friendly forces, mistakes such as "friendly fire" casualties or unintended collateral damage can be averted and military power brought to bear with precision.

For this shared sense of battlespace to be maintained during combat, of course, access to information will have to be relatively easy and comprehensive. Individuals must be able to connect to the information network in a variety of ways, and redundant access points must be available. What many of its advocates fail to acknowledge is that the changes the IT-RMA requires create the risks of a loss of information security, a reduction in force resilience, and significant management and organizational problems.

The Access/Security Tradeoff. If shared battlespace awareness can provide a critical, perhaps even decisive advantage, opponents will find that the data infrastructure and the data themselves make exceedingly valuable targets. The incentive to "eavesdrop" on, contaminate, or disrupt the information flow of the American military will be enormous. In the Persian Gulf conflict, Iraqi leaders did not fully appreciate the significance of highly advanced surveillance planes or networked computer communications, but it would be imprudent to expect that the next opponent will make the same mistake. Each access point into the system of systems will be a potential Achilles' heel in need of protection.

It is here that the tension between easy access and robust security creates a dilemma. Because networks are supposed to have a seamless quality—once in the network, one can see almost everything—an adversary who has gained access will be able to steal, change, or destroy critical information freely and swiftly. By contrast, within a traditional hierarchical organization, an opponent that impersonates an infantry soldier would have great difficulty discovering essential information simply because his rank

would restrict access. The very nature of non-hierarchical information systems means that penetration of one point of defense could provide access to enormous amounts of information or even unleash havoc throughout the information system. The opportunity to exploit the seamless quality of networked communication is amplified by the requirement that direct access be relatively easy. The problem is straightforward: it is easier to protect access to the filing cabinet if ten people have one key each than if a thousand people have five keys each.

One solution to this access/security problem is to recompartmentalize information so that the access of the private differs from that of the general. But this reintroduces hierarchy into information processing, essentially unnetworking the network and forgoing the benefits of seamless sharing of information. Another solution might be to keep a seamless network, but with fewer access points and restrictions for certain individuals or ranks, but again this would undermine shared awareness. A third response would be to maintain comprehensive access and seamless networking, but erect a very active and robust defense. IT-RMA proponents assume that reliable defense against enemy exploitation of information system vulnerabilities is possible. They may be correct, given the potential for encryption, passwords, and layers of firewalls to foil an opponent's attacks on an information system. The problem, however, lies not in developing effective countermeasures, but in the seamless incorporation of those countermeasures during combat. Can we expect that, in response to an assumed enemy penetration, an effective defensive software patch can be introduced in such a way that all friendly forces are able to update their access procedures quickly and maintain connections while the intruder is forced out of the system? For comparison, just consider the compatibility problems created when a new version of a word-processing program is introduced into a small office group.

A broadly accessible network would be vulnerable to a single individual's attack.

The issue is not whether it is possible to defend information operations, but whether it can be done without undermining the whole point of the network. Opponents need not gain ascendancy over the information system in order to frustrate the system's owner. All they have to do is persist long enough and force the creation of so many firewalls that the system no longer functions as designed. Recent navy wargames produced this result. In its efforts to protect the network, the American side effectively un-networked the network by recompartmentalizing access—that is, it did the enemy's job! Every step toward protecting information is a step away from shared awareness. Finding the correct mix of security and access will be a daunting task.

Individual empowerment and the leveling of hierarchy also raise the possibility of conscious misuse. The access/security dilemma involves keeping unauthorized persons out of the network, but a more serious problem

occurs when someone who is authorized to be in the system "goes south." Since it is much easier to move through an information system in a networked organization than it is in a hierarchical one, the potential for individuals to cause harm increases markedly. Ideological dissenters or simply disgruntled employees may seek to crash the system, leave time bombs that can be activated in the future, corrupt information, or engage in internal conspiracy, theft, or espionage.

Traitors and malcontents have always existed in militaries, but until now the problem has been manageable because, with few exceptions, the amount of damage an individual could inflict without great effort was marginal. Enemies within may have been able to pass along some narrow intelligence, scuttle a few weapons, or persuade a few others not to carry out their duty. Moreover, the greater the effort to do harm, the more likely a traitor would be caught by authorities. The empowerment associated with network organization dynamics changes this balance. Actions of individuals can have a ripple effect throughout the organization and occur at much greater speed. Consider what the likes of the Oklahoma City bombing perpetrators or the white supremacist group at Fort Bragg could do in the future with easy access to comrades in a million-person military. The number of malcontents and misfits is likely to remain small, but a single individual with access to critical nodes might be able to bring an entire system down. Individual empowerment means that lone rogues in the armed forces would not even need to recruit collaborators, dramatically reducing their risk of getting caught. Deterring such action becomes difficult if not impossible. As the former director of the National Security Agency, Lieutenant General Kenneth Minihan, has noted, "Unstructured attacks are occurring against our networks every day, but unfortunately, most are not even detected." When they are, he said, "we rarely know who the attacker was."[8] Imagine what the few spies that have inflicted serious damage, such as Jonathan Pollard, John Walker, Aldrich Ames, and Ronald Pelton, might have accomplished with wider and easier access.

Future opponents are unlikely to miss this opportunity. The National Defense Panel notes that adversaries will try asymmetric strategies to exploit American vulnerabilities and we must assume that all weaknesses cannot be completely eliminated. A recent Center for Strategic and International Studies report cites Pentagon experts who conclude that "well-coordinated attacks by fewer than 30 computer virtuosos . . . with a budget of less than $10 million, could bring the United States to its knees."[9] If even relatively small efforts can

[8] Quoted in Anthony Kimery, "When the Night Comes Crashing," *Military Information Technology*, vol. 3, issue 1 (1999), p. 12.

[9] *Cybercrime . . . Cyberterrorism . . . Cyberwarfare . . . : Averting an Electronic Waterloo*, Report of the CSIS Global Organized Crime Project (Washington, D.C.: Center for Strategic and International Studies, 1999), p. xiii.

have such sweeping effects, then increasing the Pentagon's dependence on the very systems such strategies target could be a dangerous gamble.

The Loss of Resilience. IT-RMA is often touted as a force multiplier. In fact, it will have to be, considering the reductions in force structure that will be needed to pay for the new technology. The result will be a smaller military that depends on high volumes of quality information merely to survive, much less succeed. If the information turns out to be unavailable, corrupted, insufficient, or misinterpreted, then the much smaller IT-RMA force structure could be in big trouble. Today's massive forces provide an insurance policy against unforeseen setbacks. If the breaks go against American forces, they currently are large and diverse enough to recover. Thus, if an opponent checks the U.S. deep-strike air force with unexpected electronic countermeasures, he can still be defeated in close combat; if the enemy stops the Marines with mines and obstacles on the beaches, he can still be pummeled from the air; if the enemy resorts to guerrilla tactics, U.S. infantry can pursue him. On the other hand, a force radically restructured to exploit new information technology by definition puts more of its eggs in the deep-strike basket. If the enemy's tactics outflank technology, an IT-RMA military may lack the size and diversity to compensate. To take a single example, the initial plan for intervention in Kosovo, for political reasons, involved air operations only. Force restructuring could mean that in the future other options may be unavailable or prohibitively costly. Today's forces are resilient. A radically restructured IT-RMA force would be much less so.

A less risky alternative could allow the United States to incorporate RMA information assets within the current force structure, which may well make the force more robust. However, maintaining two distinct organizational forms, one hierarchical and one networked, might prove problematic. In addition, this could not be done without major budget increases. Much of the IT-RMA's political appeal rests on its claim to square the circle of growing commitments and shrinking budgets by letting the United States do more with less. If all it offers is to do more with more, there may be few takers on Capitol Hill.

Organizational Problems. The problems of access/security and resilience are tied to a third problem that goes to the heart of the change being planned. The true revolution in military affairs is not only about weapons and doctrine, but about radical organizational change. Of all modern social institutions, the military has come closest to the ideal form of a bureaucratic hierarchy, in which information is tied to function, and function to rank. The responsibilities of a general require a different amount and type of information than do the duties of the private. Each possesses the information needed to perform his or her job and not much more.

The transformation of the military into a networked organization fundamentally alters the relationship between information and function. *Joint Vision 2010* states that "new technologies will allow increased capability at

lower echelons to control more lethal forces . . . thus leveraging the skills and initiative of individuals."[10] The document envisions empowered individuals exercising "maneuver, planning, and coordination . . . which were normally exercised by more senior commanders in the past." In the Persian Gulf War, for example, majors in Riyadh with secure fax machines and friends on Washington staffs could get information to which only generals had access in past wars. The scrambler phone shifted control of the flow of information to lower echelons of command than ever before, and this trend is likely to accelerate.

There are, however, troubling costs associated with extending this empowerment fully. In a non-hierarchical structure based on equal access to information, the notion of "higher" authority becomes problematic. This creates two mirror-image concerns. The first is intense micromanagement, that is, the potential for central authorities—civilian as well as military—to make every decision. If an American president, who is ultimately accountable, after all, has complete awareness of a military situation, it may be difficult to pass up the chance to take control himself. The network might thus function as a "hyper-hierarchy," wherein top leaders reach down to orchestrate action at the lowest levels. Perhaps, given full knowledge of the battlespace, such intervention by the centralized command might not have the deleterious effects that have been associated with past examples of micromanagement, such as Lyndon Johnson's selecting bombing targets in Vietnam or Jimmy Carter's intervention in Desert One. Yet, even with more information, the prospect of a president's making tactical decisions between Rose Garden ceremonies is not necessarily desirable. Among other consequences, such a ratcheting up of control would deny junior officers meaningful authority and responsibility and be certain to lead to morale problems. In the long run, it may give way to a mindset that is not conducive to effective leadership. In the U.S. Navy, for example, where there are currently only 1.6 ships for every admiral, the potential for hyper-hierarchy may create a serious challenge for command structures and rules.

The leveling of traditional hierarchical structure also creates the converse danger of macromanagement: the temptation of actors in the field to make decisions that should be made by higher authorities. Giving the troops a "god's-eye view" through direct access to satellites and other remote sensors may encourage them to act independently. Instead of more information leading to greater coordination, a breakdown of discipline could result. Will soldiers who are fully informed that they are outnumbered, surrounded, and without hope of timely support hold their positions? Even for courageous and well-trained troops, there is a difference between being ordered to hold a position when the risk is great but ambiguous, and doing so in the full

[10] *Joint Vision 2010*, p. 15.

knowledge that it is suicide. Complete knowledge may demoralize rather than embolden the troops. To be sure, the dire truth might be withheld, but then troops might interpret an information blackout as proof of their impending doom. In sum, empowering troops with better information could produce enormous, perhaps unattainable, challenges to discipline.

Pressures for micro- and macromanagement grow out of the different interests of actors within the network. The problem, simply stated, is that having the same information does not necessarily lead actors to reach the same conclusion about how to respond. A president will view information through political-strategic lenses; the field commander, through operational lenses; and soldiers, through tactical and personal lenses. Flattened, highly networked command structures, however, do not in and of themselves privilege particular lenses or viewpoints. Without a perfect integration of political-military goals throughout the network, without a fusion of perspectives and views, and without the development of new command rule sets that clearly determine who makes decisions, the potential for different actors with the same information to make conflicting choices will surely exist. Advocates of full battlespace awareness assume that shared information will translate into (indeed, will equate with) a convergence of interests and perspectives, but common sense and experience suggest that this is not so.

The redesigning of military institutions to take advantage of the information revolution will also create sweeping cultural and practical problems for the military services, problems that need to be addressed carefully. One of the objectives of military training is to create a military ethos, a particular view of the world. The creation of this unique social institution has been possible, among other reasons, because of its members' physical isolation on military bases, although students of civil-military relations differ on the optimal degree of separation during peacetime. A networked military that allows greater individual initiative will have to contend with closer connections between the military and civilian worlds even as the gap in understanding between these worlds widens.

This interconnection may boost morale, but could also erode it, particularly during combat. Once deployment is made and hostilities are in progress, a barrage of e-mail from concerned friends and relatives who are getting critical reports on an operation from local news broadcasters (who have their own satellite feed from the operation) can, at the very least, distract soldiers in the field. Add to that the home front's arsenal of fax machines, cell phones (a problem with which the Israeli military has had to contend), and e-mail pagers, and the traditional divide between the military and home front—a divide upon which a system of discipline rests—becomes blurred. The professional military will begin to take on the feel of a virtual militia, for which the conduct of military operations competes with concerns and responsibilities at home and on the job: when the crops are ready, the pitchfork replaces the gun. The main advantage of a professional structure is depend-

ability, but a professional military electronically connected to home may behave quite "unprofessionally" in combat.

Of course, total isolation during combat is not necessary. During the Second World War, mail call and movies were important, controlled distractions. The problem with networked integration is that commanders will have a hard time controlling the flow between the home front and the battlefront. The problem will intensify if the gap between civilian society and military institutions, as measured in values, attitudes, and life experiences, continues to grow. Civilians and the military may simultaneously have tighter communication links and increasingly disparate world views. Civilians, who increasingly know nothing about combat, will have the ability to tag along and chat with the troops, hardly a beneficial situation when American forces face prolonged combat conditions.

The military must also be concerned about the flow of information back to the home front. Stateside family and friends can cause problems, even unintentionally, by the way they use information gleaned from the deployed troops. An example of this concerns the rescue of air force captain Scott F. O'Grady, who was shot down in Bosnia in 1995. The rescue pilot e-mailed his pilot buddies describing the rescue in vivid detail, including sensitive information on American operational methods. Someone forwarded the message to another friend, who forwarded it again, and within hours a conversation that would have been a harmless diversion at the officers' club bar twenty years ago became a globe-circling security violation.

The negative aspects of individual empowerment can be eliminated by increasing the level of professionalism of the individual soldier, but this too is problematical. Even if we grant that 99.9 percent of military personnel are above distraction, that leaves a thousand weak links in a million-member organization. To this must be added the further complications created as the Defense Department increasingly contracts with civilian technicians to install, maintain, update, and repair complex technical systems. Civilian electronic engineers and software developers cannot be expected to have the same discipline demanded of the fighting forces, and the integration of people who may not carry what Eliot Cohen calls the "warrior's ethos" could increase the risk of internal conspiracy, theft, and espionage.[11] The flow of e-mail traffic out of national weapons laboratories, which was highlighted in the recent charges of Chinese espionage at Los Alamos, indicates a different cultural perspective on information between the scientific community and the military, even among that portion of the scientific community that is dealing with critical national security data.

All the offsetting costs listed so far will be exacerbated by the deployment of American forces as part of a coalition effort. An alliance-wide

[11] Eliot Cohen, "A Revolution in Warfare," *Foreign Affairs*, Mar./Apr. 1996, pp. 37–54.

information network will have even more potential access points in need of defense and a membership that by definition involves different cultural values and national interests, and different levels of training and equipment are also likely to impair access and hinder the development of a shared awareness. Already, one of the greatest concerns among NATO allies is common interface standards and interoperability with U.S. military technology. The United States' NATO allies simply cannot afford to keep up. If allies' access is limited for security reasons, it will reduce the ability to work together effectively. Burden-sharing resentments may also emerge if in future joint actions the United States contributes the advanced technology while its allies, with their more traditional and relatively larger fighting forces, are left to provide the troops whose lives are at risk.

The Wrong Response to Security Threats

Given the potential for so many new vulnerabilities, the transformation of the military is clearly fraught with risks. Perhaps, if the security challenges of the future required radically new responses, these risks would be acceptable. However, in light of the current U.S. position as unchallenged superpower, caution and restraint seem far more prudent. A revolutionary transformation in the security infrastructure cannot be justified until it is demonstrated that information superiority solves real problems and permits U.S. armed forces to accomplish real-world missions better. Upon closer examination, however, it appears that the IT-RMA would leave the military ill equipped to counteract the dangers most likely to threaten U.S. security.

Information technology may contribute the most added value in the case of major theater wars, but those are precisely the threats that today's U.S. forces are most clearly able to handle. Current U.S. military superiority is overwhelming and is unlikely to be challenged soon, and American defense spending is roughly equal to that of the next ten top defense-spending countries combined (most of which are U.S. allies), plus such rogue states as North Korea, Libya, and Cuba. Success in the Persian Gulf War reveals that the United States can integrate information technologies and exploit them to great effect without the radical organizational and operational changes called for in the IT-RMA vision. Enthusiasts warn that because the IT-RMA is embedded in, indeed led by, the communications revolution in the commercial world, peer competitors can emerge quickly. But it is rather improbable that another state could rise as a threat more quickly than the United States could adapt to face it. This is not a call for standing still, but for slower, value-added defense planning. If the most important national security threat can already be handled with the means at hand, why revolutionize—particularly when the change might come at the cost of declining preparedness for that threat?

Some argue that an information-enabled military will deal more effectively with low-intensity conflicts. If correct, this would truly be important since the most likely threats facing the U.S. military will involve instability among or the collapse of weak states. A critical problem, however, is that these scenarios will likely involve urban settings and opponents who are indistinguishable from the civilian population. As in Kosovo, the proximity between military targets and civilians may prevent planes from dropping their bombs or lead to the accidental killing of civilians. Opposing forces could rely on widely available low-tech means to communicate, defend themselves, and inflict damage. Or they could adopt the Serbian tactics of hiding forces in churches and schools. Organizational structure may be so simple or horizontal that isolation of leaders could be irrelevant. Alternatively, the adversary may have the sophistication to understand and exploit American technological and political vulnerabilities.

In any of these scenarios, there is no technological panacea. The fact that the United States could easily monitor the movement of Serbian forces in and out of Kosovo was only marginally helpful in dealing with the root causes of the crisis. Dominant battlespace awareness will do little to alter the centuries-old animosities and political struggles that give rise to such ethnic conflicts. In these cases, it is "boots on the ground" or the gunboat conspicuously offshore, and not information superiority, that restores short-term order and negates the military capacity of adversaries. NATO keeps the peace in Bosnia by means of soldiers on street corners backed by tanks and aircraft, not by radically transformed organizational structures and concepts. Indeed, if an embrace of the IT-RMA results in reductions in force levels, it may have the unintended consequence of reducing America's ability to deal with the low-intensity conflicts that seem likely to dominate in the foreseeable future.

The IT-RMA would leave the military ill prepared for the most likely threats.

In addition to improving U.S. capabilities to undertake major theater wars and low-intensity conflicts, enthusiasts argue that American sensors and communication systems can enhance such monitoring operations as arms control verification, scientific and environmental studies, refugee tracking, and everything collectively known as "military operations other than war." It is true that peace operations can be aided by more effective information collection, analysis, and dissemination. Additionally, intelligence-gathering capabilities for combatting terrorism and international crime will surely benefit from the greater use of information technologies. But none of that requires a radical restructuring of military forces. Indeed, doing so along the lines suggested by IT-RMA proponents may prove counterproductive because of the aforementioned vulnerabilities such an organization creates. It is hard to imagine a terrorist group taking on a combat brigade, but easy to imagine it taking down a computer network.

A final argument offered in support of the IT-RMA is that thinking of war and peace in traditional military terms simply misses the point about an information edge. Alvin and Heidi Toffler, William Owens, and Joseph Nye have contended that command of the information environment may be used to prevent genocide and ethnic clashes before they start, thus obviating the need to send troops to intervene. The United States, for example, could suppress inflammatory radio messages, denying nationalist leaders the ability to incite their populations. In the case of Rwanda, Nye and Owens wrote in *Foreign Affairs*, the United States could have "exposed the true actions and goals of those who sought to hijack the government and incite genocide, which might have contained or averted the killing."[12]

While propaganda can be effective, advocating the IT-RMA as an antidote to global instability mistakes content for context. The mindset necessary to grab a machete and hack another human being to death does not emerge overnight in response to a voice on the radio, but from much deeper fears and calculations. Indeed, information that contradicts an individual's preexisting conceptual mindset is itself likely to be rejected as propaganda rather than accepted as truth. American computers, satellites, and info-warriors will not stop Christian southern Sudanese and Arab Muslim northern Sudanese from hating and killing each other. An information-driven U.S. military will be no more effective in dealing with these problems than traditional militaries—but it will be smaller, more expensive, and more thinly stretched.

The Balance of Power Still Matters

A final reason for caution in approaching the IT-RMA is the international reaction it is likely to generate. In the late 1980s it was popular to observe that American power was in decline. One of the stronger objections to this school of thought was offered by Nye, who argued that the unique appeal of American democracy and free-market economics could translate into "soft power," that is, the ability to achieve foreign policy goals through attraction rather than coercion.[13] He concluded that the growth in American soft power could offset declines in military and economic predominance. In their 1996 *Foreign Affairs* article, Nye and Owens moved one step further, arguing that with an intelligent strategy America could actually increase its overall power relative to the rest of the world. They called on the United States to "adjust its defense and foreign policy strategy to reflect its growing comparative advantage in information resources."[14] Implicit in this strategy is their notion that other nations will view American power as benign or, failing

[12] Nye and Owens, "America's Information Edge," p. 33.
[13] Joseph Nye, *Bound to Lead: The Changing Nature of American Power* (New York: Basic Books, 1990).
[14] Nye and Owens, "America's Information Edge," p. 23.

that, as incontestable. According to Nye and Owens, the "United States can use its information resources to engage China, Russia, and other powerful states in security dialogues to prevent them from becoming hostile. At the same time, its information edge can help prevent states like Iran and Iraq, already hostile, from becoming powerful."[15]

But as suggested earlier, clarity of information does not guarantee a convergence of interests. Information advantages may enhance the U.S. ability to shape relationships, but they do not alter basic interests. Recent protests in response to the American-led NATO strikes against Serbia suggest that people disagree even about the need to resist so repugnant a policy as ethnic cleansing. Some countries may ultimately trust the United States to wield its strength benignly, but the history of international politics suggests that few states will be willing to accept uncritically and passively such preponderance of power. Some states, including friends and allies, may coalesce to try to offset an American hegemon.

Enthusiasts of the information revolution claim that, in a break with past patterns of international politics, American hegemony will not prompt a countervailing balance of power. The Tofflers talk about "the end of equilibrium (not history)." As they argue in the book *War and Anti-War*, numerous "theories about the global system tended to assume that it is equilibrial, that it has self-correcting elements in it. . . . The entire theory of balance of power presupposed . . . restoring equilibrium. . . . Yet none of these assumptions apply today." They warn that "the promise of the twenty-first century will swiftly evaporate if we continue using intellectual weapons of yesterday."[16] Yet, just as information does not equate to shared goals within a single organization, there is little evidence that information suspends or transforms the interests of states. Even when certain goals can be agreed upon, reasonable state leaders may disagree on how to achieve them. France and the United States agreed that international law against war crimes should be upheld, and they shared information as to the whereabouts of war criminals in Bosnia. This did not lead, however, to agreement on how to proceed, and better information would not have transcended their disagreements. Nye and Owens write that "the information advantage can strengthen the intellectual link between U.S. foreign policy and military power."[17] However, given other nations' fears of U.S. domination, a revolutionary technological leap could easily be viewed in, say, China or Russia as evidence of open-ended U.S. ambitions and clearly at odds with a political grand strategy of benign engagement. Allies' acquiescence in an American hegemony will

[15] Ibid., p. 22.

[16] Alvin and Heidi Toffler, *War and Anti-War: Survival at the Dawn of the 21st Century* (Boston: Little, Brown and Co., 1993), pp. 249–50.

[17] Nye and Owens, "America's Information Edge," p. 20.

last only as long as the United States can reassure them of the complementarity of American interests and their own.

A Revolution Today Is Premature

Although the benefit of a restructured American military is marginal for many missions, carries significant off-setting costs, and might encourage balancing by adversaries and unease among friends, defense planners are moving forward with the IT-RMA. The Joint Chiefs of Staff has produced a *Concept for Future Joint Operations* that requires fundamental organizational and operational change.[18] Political leaders in both parties accept the argument that incrementalism is "dangerous thinking," and the National Defense Panel calls for "aggressive transformation." Why does the revolutionary consensus continue to grow? The obvious (and cynical) reasons are threat inflation throughout the defense and policy-making communities, traditional service rivalries, and the attendant bureaucratic politics. But one could just as well expect that those quarters would favor existing institutional arrangements and practices rather than the shifting of resources—and power—to new programs and services. Nor does the attraction of technological revolution derive from the short-term perspective from which American politics tends to suffer. On the contrary, the current push for a radical change in military planning and force structure is remarkable because it is coming at the *expense* of parochial service interests and *despite* the short-term preoccupations of most leaders.

There are in fact five reasons why defense planners want a revolution. The first is that analysts have tended to misinterpret the Gulf War as a victory of technology. Although U.S. technology was unquestionably impressive in that conflict, the victory was the result of a fortuitous mix of superior American might and generalship with a good dose of Iraqi incompetence. The readiness level of American troops, created through rigorous and superior training, was especially critical. The second and third reasons for support of an IT-RMA are that the pursuit of innovation has become institutionalized, combined with a generally positive societal view of technological progress. These two factors reinforce each other. The Defense Advanced Research Projects Agency (DARPA) alone has a budget that exceeds the individual defense spending of all but the top twenty-two countries in the world, and its sole purpose is to innovate. Such bureaucratic players' vision of the future resonates in a larger political environment and culture that accepts all "progress" as good. Consider the difference between industrial America's emphasis on cars of the latest model-year and the current information-age cycle in which hardware and software are declared obsolete within months of

[18] Joint Staff, *Concept for Future Joint Operations* (www.dtic.mil/doctrine/jv2010/concept.htm).

hitting the stores. In the defense community as in America at large, to move slowly is not to move at all. The fourth reason is that information technology has become the most common means by which to gauge both competence and success. Here, too, the IT-RMA argument parallels social norms. In the 1950s Americans measured themselves in terms of their automobiles' horsepower; now the standards are gigabytes and RAM. Finally, and perhaps most significantly, support for revolutionary change in the military has unmistakable political appeal. If leaders worry about remaining engaged in world affairs but do not have sufficient domestic political support to cover the financial and human costs of such a commitment, they are likely to be open to a solution that promises them engagement with less sacrifice.

None of these appeals, however, address the costs and concerns detailed here. The information-age enthusiasts insist that the United States should overturn a system it already dominates and push to radically expand America's advantage. This is both unnecessary and dangerous. The United States has reached a pinnacle of world power without exhausting itself, and dire predictions of decline have proven groundless. Relative to most developed countries, the U.S. economy continues to show resilience and its military remains without peer. The United States is not only ahead, but it is well positioned, provided that readiness is maintained, to respond quickly to any threat that might arise.

The normal process of evolutionary adaptation is perfectly adequate to the times, and is a safer and wiser response to new technology. The kind of incremental change that has characterized U.S. defense planning for more than a generation is a better—if less exciting—bet than radical transformation. The revolution can wait.