Doomed to Fail: America's Blind Faith in Military Technology

JOHN A. GENTRY

The US Department of Defense has pinned the military capacity of the nation on hopes that as yet unproven technology will generate significant operational advantages. In the glow of the apparent effectiveness of "precision" munitions during Operation Desert Storm in 1991, the department adopted strategies that promise success through creation of massive technologically-oriented support structures that would make smaller field forces much more effective. The Joint Staff in 1996 promulgated *Joint Vision 2010*, which listed high-tech capabilities it hoped to acquire.[1] In 2000 the Joint Staff released a modified version called *Joint Vision 2020* (*JV 2020*).[2] Neither document provides much insight about how such an end-state can be achieved.[3] Nevertheless, the department believes that a revolution in military affairs (RMA) will dramatically, if miraculously, improve its capabilities, primarily through achievement of information superiority, which it defines as "the capability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same."[4]

Operational inadequacies, technical limitations, and fundamental institutional problems indicate that these dreams are doomed to fail, however. The United States may be creating what historians will one day call the Maginot Line of the 21st century. The 2001 Quadrennial Defense Review and the early conduct of the global war on terrorism do not indicate a change in this aspect of US defense policy.

The *JV 2020* concept has four fundamental problems. Each is a potentially fatal flaw. Together, they virtually assure a financially inefficient force and disappointing field results. Against a competent enemy, the deficiencies may be catastrophic:

- *Narrow applicability*. Despite paying lip service to a spectrum of missions, *JV 2020* addresses only a small portion of US military activities. Desert Storm-like operations are in the small part of the spectrum particularly amenable to the RMA—medium-intensity conventional conflict against weak opponents.
- *Vulnerable infrastructure*. *JV 2020* relies on information technology (IT) and other infrastructures that are incompatible and unreliable. The infrastructures regularly fail in peacetime for many reasons. They offer abundant opportunities for enemy attack.
- *Easy countermeasures*. Even where the US has technical advantages, effective countermeasures usually exist. In some cases these degrade US capabilities directly. In other instances, adversaries operate in politico-military arenas beyond the scope of US military capabilities, rendering the technology irrelevant.
- *Institutional impediments*. The US military cannot implement what it wants to do even if funds and technology were available. The most daunting reasons are internal and institutional—and highly resistant to change.

Promises, Promises

JV 2020 promises operational effectiveness derived from a complex set of hardware, software, and procedural systems. In the ideal world of *JV 2020,* intelligence, surveillance, and reconnaissance (ISR) systems like imagery satellites would gather data that troops need to "see" areas of operations. Computers would convert the data into visual displays of the battle space that provide a common operational picture. Because US forces would get more data more quickly than enemies, they would have information superiority. Possession of data would generate good command and field operator decisions, and decision superiority. Communications networks would instantly transmit information and orders to troops, who would promptly convert them into effective action. Precision munitions would rain on targets. Victory would be assured. The story has fairy-tale appeal.

In the vision, US forces will be tied to interactive, or collaborative, networks that work continuously. Such network-centric warfare means that the United States must maintain constant control of the land, sea, air, and space through which US forces and communications travel and keep thousands of IT systems functioning in unison. This is an enormous requirement never before at-

Lieutenant Colonel John A. Gentry, USAR Ret., is an analyst with the Center for Integrated Intelligence Systems, the MITRE Corporation. He served with the 1st Special Forces Group in East Asia, with the 352d Civil Affairs Command in Bosnia, and in a variety of intelligence assignments. He is the author of a book on the Central Intelligence Agency titled *Lost Promise* (University Press of America, 1993) and several articles on military affairs.

tempted by any military organization. The United States does not do it well in peacetime. There is no good reason to think the US military can achieve it while fighting a competent enemy.

Technology is to help provide four basic capabilities of *JV 2020*, narrowly military in scope, which are to provide full-spectrum dominance through achievement of information superiority:

- *Dominant maneuver.* US forces are to be able to move faster than enemies. This concept refers, effectively, to battlefield movement of conventional combat forces against similar forces.[5] However, it is not very helpful against guerrilla adversaries because they are hard to find and/or identify. It is largely irrelevant to humanitarian relief and peacekeeping operations because rapid movement usually is not important in the sense of outmaneuvering an enemy.
- *Precision engagement.* US forces are to be able to hit targets accurately from far away. But against a weak opponent in 1999, much of American airpower, cruise missiles, and hundreds of allied aircraft inflicted little damage on the Yugoslav military; after-action reports indicate significant operational and technical deficiencies.[6] In late 2001 and early 2002, errant US munitions killed allied troops and many Afghan civilians, and twice struck well-marked Kabul facilities of the International Committee of the Red Cross.
- *Focused logistics.* The business processes part of *JV 2020*, this goal aims to assure that troops have the gear they need. The United States is deficient in many logistical areas, however. Perhaps the most important inadequacies are the sea- and airlift needed to carry the massive quantities of supplies that US forces like to have.[7]
- *Full-dimensional protection.* A reflection of the US military's preoccupation with its own safety, this goal seeks to assure that enemies cannot successfully attack US forces. While full protection is impossible, the military nevertheless wants sensor/computer/weapon complexes that defend against attacks. Operational architectures generally envision these capabilities surrounding fixed camps. Thus, the US Army occupies a fortress at Camp Bondsteel in Kosovo—hampering its operational effectiveness—while the US Air Force retreated after the June 1996 Khobar Towers bombing to an airbase deep in the Saudi desert.[8]

Why This Approach?

Why has DOD adopted such a limited approach? The lessons of Desert Storm that provoked *JV 2020* came from an extraordinary conflict. An inept, demoralized Iraqi army let its enemies assemble forces unmolested for six months, then allowed them to attack on their schedule. The geographical and atmospheric conditions of Kuwait and Iraq—generally good weather and largely flat, barren terrain—were well suited to use of precision munitions. Iraq ceded control of the air, then placed much of its armor and other key assets in fixed locations that were easy to find and hit. The result was similarly unusual—clear victory with few allied casualties. No wonder the generals want to fight this war again! The abnormality of Desert Storm should be apparent to even beginning students of military history and strategy.

The technology envisioned in *JV 2020* cannot enhance the performance of troops in most US military operations because it focuses predominantly on gathering and processing information about the weapons, equipment, and tactics of conventional military forces—friendly and enemy. Technology contributes virtually nothing, however, to complex civil-military operations—like recent ones in Haiti, Somalia, Bosnia, and Kosovo in which the US military has not performed particularly well.[9]

Technology has little applicability to political and many military situations for elementary reasons. Sensors track physical things and activities that have electromagnetic and other signatures. Sensors cannot identify human motives, measure human emotions, quantify the coherence of human organizations, or assess the importance of the data they gather; they can provide limited amounts of relevant data to people for analysis *if* they are so targeted. This is a big "if," because US intelligence is heavily focused on supporting commanders who are mainly concerned with force protection and their specific military missions. Technology-based "analyst tools" have been marginally helpful and show little promise of soon becoming more than data manipulators. Moreover, DOD devotes few resources to, and places less emphasis on, building the political sophistication its people need to use information well.[10]

Fragile and Vulnerable Infrastructure

DOD's IT infrastructure is expensive, limited in capabilities, subject to chronic technical and operator-induced failures, and vulnerable to attack. The department recognizes many of the specific problems, but has not systematically assessed the costs and limitations in conjunction with expected advantages. The issues are numerous:

- DOD is working to protect critical systems through its Critical Infrastructure Protection and Information Assurance programs, but single points of failure and vulnerabilities to enemy attack and industrial accidents remain.
- DOD relies on its multibillion-dollar Global Positioning Satellite (GPS) network to provide locations for forces and guidance for most precision munitions. But GPS signals are weak and easily jammed. The Russian company Aviaconversia offers a four-watt GPS jammer commercially for less than $4,000.[11] Some observers believe that jammers effective over ten-mile radiuses can be built for $400 from parts available at retail electronics stores.[12] US forces are poorly equipped even to identify the existence of jamming.[13]
- Some 95 percent of US military communications travel over commercial telecommunications networks, including satellite systems, which are subject to interdiction. To reduce vulnerabilities in space, a presidential commission chaired by Donald Rumsfeld (before he became the Bush Administration's

“The United States may be creating what historians will one day call the Maginot Line of the 21st century.”

Secretary of Defense) advocated substantial, but unspecified, new expenditures on space activities.[14] Later, Secretary of Defense Rumsfeld called for initiatives that would militarize space for the first time, with unforeseeable but probably negative political and military consequences; such initiatives seem unlikely to assure the security of US reconnaissance and communications systems.[15]

- The DOD IT infrastructure, including its intelligence infrastructure, regularly fails during normal operations without help from enemies. A particularly serious failure virtually shut down the headquarters of the National Security Agency (NSA) at Fort Meade, Maryland, for over three days starting in the evening of 24 January 2000.[16] The outage left the United States virtually deaf for what is, in the intelligence business, a long time. NSA Director Lieutenant General Michael V. Hayden was so concerned at the time that he ordered NSA people to keep the failure secret.[17] Said Stephen B. Tate, chief of NSA’s Strategic Directions Team, “Our information technology infrastructure is a critical part of our mission and it needs some repair. . . . It is a burning platform and we’ve got to fix it.”[18]

- DOD extensively uses commercial off-the-shelf software. This practice, while having many advantages, also provides potential attackers access during peacetime to key parts of DOD’s networks—giving them time to develop attack strategies and to plant malicious software for activation later.

- Hackers and US “red teams” trying to identify vulnerabilities have attacked the infrastructure with ease. DOD reported 22,144 attacks on its unclassified systems in 1999, and in late 2000 indicated that the rate of attacks was up about ten percent over the previous year.[19] In March 1998, DOD detected a group of hackers who eventually attacked hundreds of US government networks; despite mounting an extensive operation code-named Moonlight Maze, investigators three years later had learned little of the attackers and had failed to stop the attacks.[20] Carnegie Mellon University’s Computer Emergency Response Center estimates that only about ten percent of attacks are detected. In Joint Staff exercises Eligible Receiver in 1997 and Zenith Star in 1999, NSA personnel successfully entered a variety of DOD networks and US civilian networks controlling electric power grids and 911 emergency response networks.[21] Michael Vatis, former chief of the National Infrastructure Protection Center, says the threat of cyber attack is growing daily and that there is no known way of protecting against some types of attack.[22]

- “Secure” networks are vulnerable. NSA personnel have identified theoretical vulnerabilities of the Secret Internet Protocol Router Network (SIPRNet) that carries much of the military’s command and control communications via the Global Command and Control System, as well as other sensitive information.[23] The creation of large networks increases both vulnerability and the potential damage an incompetent soldier, malcontent, or enemy agent can cause. In August 2001, a retired US Air Force sergeant was arrested for allegedly selling to Libya documents he obtained from the top-secret Intelink website. In the world of network-centric operations, there is no better espionage or sabotage recruit than a system administrator for a key command and control or intelligence system. Recruitment of an employee is not necessary, however. The chronic lack of computer discipline that leads to periodic introduction of computer viruses into secure networks also gives enemies opportunities to use unwitting but careless Americans to place malicious software in key places.[24]

Easy and Effective Countermeasures

Potential US military opponents have doubtless noted the limitations of US capabilities, have countermeasures, and are planning other ways to overcome US strengths. Among the public comments and actions of potential adversaries:

- Chinese military strategists have written that attacks on space communications and computer networks, including civilian infrastructure, could be part of a successful attack strategy.[25]
- Information operations aimed at civilian decisionmakers—not their computers—can alter US military rules of engagement (ROE) and decisions to use force. Effective information operations against nonmilitary targets can render US military capabilities irrelevant—by preventing their deployment—or change US operational objectives or ROE to the advantage of those manipulating US perceptions. These include putative friends; Bosnian Muslims waged a sophisticated propaganda campaign that portrayed themselves as innocent victims of Serb aggression during the Bosnian civil war of 1992-95, gaining strategically important US support that continues. Israel has mastered this technique at substantial financial, political, and, since 11 September 2001, human cost to the United States.[26] The Yugoslav government targeted Western political decisionmaking during NATO’s war against Yugoslavia—and came close to winning the war by convincing Western societies to stop an allegedly illegal and ill-advised war. US Air Force Lieutenant General Michael Short, chief of NATO’s air campaign, complained publicly about the political directives that formed his ROE, suggesting that he did not understand the impact of information operations on his force.[27] NATO Commander General Wesley Clark, by contrast, understood these ramifications but could not do much about either NATO political guidance or the nations’ military responses to the guidance—including US responses.[28] Nongovernmental organizations (NGOs) used the internet to orchestrate the 1997 land mine treaty over US objections. Osama bin Laden and

his allies have extensively used information operations, aided by errant US air strikes, to portray the US war against the Taliban as a crusade against Islam. Meanwhile, DOD is fixated on a definition of information operations that focuses on computer network attacks.

- Use of unconventional methods and tactics do not expose US enemies to the mass of US military power. Many of these alternative approaches, including attack on the US military information infrastructure, are inexpensive by many definitions, including political cost. The Defense Department euphemistically calls some of these approaches "asymmetric threats."
- Ways of avoiding the sensors the United States uses to achieve "information superiority" are well known. The Soviet Union called this complex of techniques *maskirovka*. Orbits of US intelligence satellites are posted on the internet, making evasive measures relatively easy. "Deception and denial" techniques are in common use; associated with hills, forests, clouds, and rain, they regularly foiled US sensors over Yugoslavia in 1999. There are no immediate prospects for overcoming these facts of nature. Moreover, many aspects of unconventional warfare are not susceptible to monitoring by traditional sensors. Forces have but to disperse among civilians and have communications discipline in order to be all but invisible to sensors—as members of the Taliban have shown yet again. NSA has publicly lamented changes in the telecommunications industry—including the use of fiber-optic cables and encryption—that degrade its traditional capabilities.[29] Precision munitions cannot hit targets they cannot identify.

The combination of the easy evasion of sensors and cheap countermeasures makes war of attrition an attractive strategy for potential US enemies—at first blush an incongruous strategy for conflict against the world's military superpower and wealthiest country.[30] However, the United States has relatively few of the expensive precision weapons it likes, while America's dearth of collective patience and self-discipline is legendary. Combined with the imperatives of force protection, the ISR, financial, and sometimes political costs of even mundane US operations are high. This means that enemies can devise strategies to run US troops and intelligence processing capabilities ragged while protecting their own forces. Opponents can take deception actions that lead US forces to waste scarce precision munitions on low-value targets. Adversaries also can use information operations to bully the United States into policies and actions they want—like forcing Washington to order an unseemly, hasty withdrawal of 800 US Marines from an exercise in Jordan in June 2001 due to concerns about force protection. If they can kill a few GIs and plant doubts in the minds of US decisionmaking constituencies, even weak opponents—as defined in traditional military terms—reasonably can expect to defeat the United States. Yugoslavia nearly accomplished the feat in 1999.[31] Surely many states and groups are studying ways to exploit US politico-military vulnerabilities.

Institutional Impediments Cannot Be Overcome

Even if engineers achieve the technical goals of *JV 2020*, DOD has systemic institutional deficiencies that would prevent fielding of operationally effective technology. Military attitudes, doctrine, and inertia would prevent effective operation of even limited RMA-inspired technology.

The sheer size and organizational complexity of the DOD IT infrastructure make achievement and maintenance of interoperability and security a daunting task—without the complication of attacks. DOD has over 10,000 computer systems, of which its component agencies have designated about 2,300 as "mission-critical." DOD has some 1.5 million individual computers, most of which are networked; to keep abreast of changing technology, about a third are replaced each year. Software is upgraded regularly. Hundreds of organizations procure and operate the equipment. Even the massive effort to prepare the department for Year 2000 (Y2K) produced only crude DOD-wide lists of important IT assets.[32]

The lack of centralized accounting of DOD equipment means that there is not and, given current institutional arrangements, cannot be "enterprise" management of DOD's IT. While the loose confederation of fiefdoms with parochial interests works most of the time in the pluralistic society that is the Department of Defense, the physics of network communications is much less tolerant of incompatible technical designs and inconsistent execution. The fractured design and control of DOD's IT infrastructure creates opportunities for attackers.

● *Acquisition failings*. Despite unified acquisition procedures as outlined in DOD Directive 5000-series documents, other Defense efforts to achieve department-wide system interoperability, and homilies about the virtues of jointness, the services and Defense agencies refuse to obey the spirit and letter of sometimes long-standing policies and continue to buy systems for their use alone.[33] In late 2000, some $36 billion in planned acquisition reportedly would not be interoperable.[34] During the war against Yugoslavia, US forces used some 30 ISR systems that, according to the Defense Science Board, were only "integrated into a loose federation of collection capabilities."[35]

Program managers of key systems are not responsible for assuring interoperability with other systems. Indeed, they would be "out of their lanes" if they tried. While nominally the organizational chief information officers and agency heads have such responsibilities, in practice the acquisition of single systems occurs largely independently. This sometimes leads to what some DOD IT professionals call "drive-by fieldings"—surprise delivery of IT for which users are neither technically nor financially prepared.

For the same reasons, program managers and their agencies do not systematically address enterprise-wide consequences of their systems, including basic ones like the impact of their systems on the IT infrastructure and the impact on DOD's limited stock of IT professionals. Often they do not care whether there is adequate bandwidth to operate their systems; that is somebody else's problem.

"Even the United States cannot continue to build massive technological tails in support of deployed forces in the hope of ensuring only comfortable and safe missions."

They similarly do not assess how attackers could cripple their systems or have responsibility for the consequences of such attacks.

Compounding the consequences of a lack of interoperability are the minimal development and practice of continuity of operations plans. Program managers sometimes develop technical aids for users and operate help desks, but they have no responsibility for assuring the integration of their systems with others, or for users' operation of their systems. Operators of equipment, particularly unit commanders, are supposed to develop operational contingency plans—ways to assure that they can continue to perform key functions by alternative means. But preparations for Y2K found that many of these plans are incomplete, superficial, or unrehearsed.[36] To address this issue following the big NSA outage, then-Assistant Secretary of Defense Arthur Money directed drafting of new policy.[37] Given the time needed to develop and exercise such plans, DOD is far from able to overcome losses of key systems.

Elements of DOD and the US intelligence community recognize these deficiencies and have limited programs to address them. The Office of the Secretary of Defense is working on a Global Information Grid concept, for example, and the intelligence community management staff is working to improve system architectures and inter-agency cooperation. However, agency compliance remains voluntary and there is no prospect for coordinated efforts for the foreseeable future.

● *Erroneous notion of the value of data*. Explicit in DOD's definition of information superiority is a belief that the acquisition and transmission of information alone produce military power. This is not true.

Troops must acquire adequate background knowledge and understanding of their areas of responsibility before they deploy in order to be able to convert the incremental bits that their sensors and other intelligence sources give them into useful information. US troops rarely make such preparations. The military seldom performs even the second-best solutions of assigning functional experts to commanders' staffs. As a result, personnel unfamiliar with their operational surroundings chronically are overwhelmed with data and intelligence analyses because they cannot distinguish important messages from fluff. Worse, they sometimes are content to ignore the information and expert advice that are available to them.[38] Area experts, by contrast, often lament shortages of useful information because they understand the limitations of the reporting they receive and know what they need to understand local complexities. Awareness of local conditions is important even for warfighters in conventional operations. US troops deal with coalition partners, local politicians, and civilians who have agendas. They must understand the military consequences of the political aims and tactics of their enemies, and appreciate the diplomatic consequences of their own actions.

The information needs of military forces vary greatly according to their size, organization, training, doctrine, and objectives. Well-trained special operations forces, including terrorists, usually need little real-time communications because they typically decentralize control of operations. The 11 September hijackers evidently communicated little but were "superior" that day. By contrast, forces with large support tails may need volumes of communications. The US military uses huge PowerPoint briefings, with fancy graphics on each slide, to conduct basic command and control; it requires substantial IT and communications resources just to muddle along. Thus, the United States can have massive information superiority as measured by the volume of data collected and communicated, but be far less operationally effective than its enemies.

The creation of large sensor and communications capabilities requires US military dominance over large parts of world. The pursuit of dominance now is widely called American "hegemony" and is widely resented—by states like China and also by friends and allies. The quest for information superiority is consequently both exacerbating world tensions and increasing DOD's conviction that it needs such alleged superiority. It is a spiral that threatens to become increasingly expensive, both financially and politically, and may contribute to the outbreak of hostilities.[39]

● *Retention of IT professionals*. DOD's recruitment and retention of IT professionals have been so ineffective in recent years that a working group chaired by the Under Secretary of Defense for Personnel and Readiness is addressing the issue. There is no solution in sight. DOD cannot now conduct normal IT operations well, let alone surge to support a national emergency or reconstitute following attacks.

● *Culture*. Members of the US military, despite defeat in Somalia and marginal performances in the 1990s in Haiti and the Balkans, believe they constitute the best military in the world. While surely the United States can put munitions on any place on the planet through sheer mass of resources, there is no corresponding superiority of individual troops or units—and, more important, no superiority of operational result. There is no public evidence that the cruise missile attack on Khartoum, Sudan, in August 1998—a classic RMA operation—hit anything of significance; it certainly did not offset the associated diplomatic costs. Yet *JV 2020* is a virtual article of faith in DOD. The root cause is simple arrogance. The American military chronically believes itself to be a superior group possessing superior technology. A generation ago, many Americans thought they and their technology were superior to the peasants of Vietnam; the United States paid the price for this hubris and its other judgmental errors in the Vietnam War.

The National Security Agency is an intriguing test case of the struggle between a reformer and bureaucratic inertia. NSA director Hayden reportedly concluded that the root causes of NSA's major IT failure in early 2000 were managerial in nature; for example, NSA then had five largely autonomous directorates and 68 e-mail systems at Fort Meade alone.[40] Hayden attacked leadership problems by bringing in new senior managers, reorganizing, and developing new technology in a program called Trailblazer. In July 2001, NSA finalized its "Groundbreaker" program of outsourcing IT by awarding a $2 billion, ten-year contract to Computer Sciences Corporation. These efforts generated internal resistance; Hayden advisor James Adams estimates that 25 percent of NSA personnel support Hayden, another 25 percent oppose him, and the rest are fence-sitting.[41] Meanwhile, Secretary Rumsfeld in mid-2001 encountered military opposition to his review of national defense priorities and opined that, for the military, "change is hard."[42] Under the best of circumstances, even vigorous reform efforts will bear fruit slowly. Many agency heads are not even trying.

● *Excuse for "force protection."* The putative advantages of *JV 2020* provide the military with something it wants very much—a rationale for avoiding the messy business of combat and other operations that may result in casualties and require hard work. *JV 2020* offers technology-based justification for force protection policies that effectively place the protection of US troops over the accomplishment of the mission without admitting to laziness or cowardice. Engineers promise that troops can have the best of all worlds—safety, personal convenience, and easy victory.

Force protection imperatives have generated massive demands on the military's ISR and IT networks. Collection systems once devoted to strategic national information requirements now, to a large degree, provide tactical intelligence designed to assure that a limited number of troops remain protected. Thus, hypothetically, to support the flight of four aircraft over Iraq, the US Central Command might task the satellites of the National Reconnaissance Office to provide data to NSA and the National Imagery and Mapping Agency, which would rapidly process the data into signals and imagery intelligence that would show that Iraqi surface-to-air missile batteries still do not threaten pilots. Multiplied around the world, mundane tactical demands on expensive strategic assets extensively task the US intelligence community. The financial cost is enormous, but one can only speculate about the opportunity costs these short-term projects that produce perishable intelligence impose on the development of knowledge and understanding that the United States requires to identify genuine crises. It is no coincidence that the greatest admitted US failing in the early stages of its war against terrorism is a shortage of human intelligence—a resource that virtually by definition cannot be procured by technology.

● *Serving the combatant commanders*. The legal status of regional combatant commanders gives them significant operational independence in their areas of operation. This power encourages them to demand DOD-wide resources on a priority basis because, using the logic of Lake Woebegone, they all have missions of above average importance. The combatant commanders' powers preclude meaningful department-wide planning of the use of ISR assets and enable them to resist "enterprise" management of information and other assets. Moreover, their voracious and undisciplined appetites for information and IT—largely for force protection—are not constrained by the government's abilities to satisfy them. DOD has no systemic, rational way to adjudicate these and other conflicting demands.[43]

● *Lack of measures of effectiveness*. The Defense Department has no measures of effectiveness to help it assess how well current or planned technologies work in operational contexts—let alone whether they are worth their financial and opportunity costs. DOD is fundamentally ignorant about how the department's assets work together, and which result in meaningful contributions, because it has no functional cost accounting system. DOD has failed to comply with the Clinger-Cohen Act of January 1996, which mandates that federal agencies use fairly standard private sector techniques to measure the effectiveness of IT investments. In order to assess the cost-effectiveness of new programs, decisionmakers must understand the value and effectiveness of the existing assets the new IT will interface with or replace.

Were measures of effectiveness available—ones that include opportunity costs within DOD, the diplomatic costs of perceived US hegemony, and imputed costs of operational vulnerabilities across the range of operational scenarios—one might be able to calculate the cost-effectiveness of military technology. Without them, I hypothesize that in high-intensity combat, competent opponents will be able to disrupt US networks, causing massive command and control failures and very poor cost-effectiveness. Similarly, in a nuclear environment, electromagnetic pulses would wreak havoc on computers and networks that are not hardened. Conventional devices also can disrupt the electrical systems so critical to DOD. Such outages would create chaos because our personnel are not conditioned to operate, psychologically or doctrinally, without their electronic crutches.

In low-intensity combat and peacetime operations, the gadgets of RMA simply are unlikely to have much effect. This means that the huge opportunity costs of *JV 2020*—smaller forces with a reduced ability to recover from unexpected defeats or to accommodate unusually large demands for their services, a reduced intelligence targeting of political actors, doctrinal blinders, and others—will lead to modestly negative net contributions in most operations. Only in medium-intensity conventional conflict against weak opponents might US military technology be cost-effective.

“The deficiencies of* JV 2020 *are so overwhelming that DOD should abandon it.”

Even RMA successes create new categories of weaknesses and vulnerabilities. Enhanced connectivity already increases the generals’ ability to micromanage tactical operations from afar—a propensity they have demonstrated repeatedly with lesser communications capabilities—to the detriment of initiative, operational performance, and the morale and retention of junior officers. Technology also enables undisciplined “cruise missile diplomacy,” like the 1998 strikes on Khartoum and Afghanistan, that feel good for a time but accomplish little and have harmful long-term diplomatic costs. So much for “decision superiority.”

Can DOD Escape the Trap?

DOD has created a conundrum for itself. Its electronic system-based force structure is expensive, fragile, and vulnerable, but system architectures are not easy to change. Rapidly evolving technology and the independent decisions of members of the DOD confederacy assure that enterprise-wide interoperability will not occur soon. But because DOD envisions an interconnected “system of systems” and the services and Defense agencies generally are moving in that direction (though marching to the beat of different drummers), retrenching in just a few areas is not a workable option. Even a single major lapse in performance or a gap in communication between organizations that depend upon each other defeats the purpose of the overall concept. Therefore, a decision to move away from *JV 2020* would require a coordinated effort nearly as large as the one to create *JV 2020*. Key aspects of a redesign of DOD include equipment, doctrine, and training the force—core functions that cannot be changed quickly, easily, or inexpensively.

DOD’s basic problem is leadership. As a recent Center for Strategic and International Studies report on the US military concluded, while most individual problems and challenges are solvable, the systemic deficiency is leadership.[44] The most difficult problems include: the power of vested interests; narrow and parochial outlooks of IT specialists in charge of most IT development; infatuation with technology in general; the propensity of personnel in a “zero-defect” culture to accept even bad guidance; and the debilitating effects on military ethics resulting from the technologists’ promises of easy victories and comfortable lives. Secretary Rumsfeld’s program to “transform” DOD, while commendable in intent, barely addresses the fundamental institutional problems and pushes the department to use yet more gadgetry.[45]

Requirements for a New "Vision"

The deficiencies of *JV 2020* are so overwhelming that DOD should abandon it. Yet the fiasco of current policy is no reason for DOD to overreact and become Luddite. While *JV 2020* is fundamentally flawed, the evolving technologies that stimulated it are critical to the future of US military power. It is important to recognize them, to know how to use them, and to know how to defend against them. How, then, can DOD wisely adapt to a changing technological world in ways that foster national security and foreign policy objectives? The United States should:

- Most important, abandon the notion that military objectives may be won or made easy and costless through the use of technology. Improvements in technology can help US forces, but the quality of people and their institutions is more important than technology.[46]
- Abandon integrated networks that mandate collaboration except where they are *clearly* effective—perhaps for naval forces. Instead, create electronic systems that support tailored unit- or mission-specific needs. Use networks in support of operations, but eliminate total dependence upon them. By doing so, make organizations and individuals capable of independent actions consistent with collective plans.
- Alter doctrine and train forces to use information and IT as aids, not crutches. US military folklore places the American fighting man's ability to operate independently in support of the commander's intent as second-to-none. While the legend is not entirely supported by history, it is certainly a standard worth emphasizing.
- Use technology only when its benefits demonstrably exceed the sum of *all* its costs. Accomplishing this means that DOD would have to comply, finally, with the Clinger-Cohen Act. It may also mean accepting casualties rather than straining ISR systems in support of force protection to the point that the effectiveness of the department is degraded, US foreign policy interests are damaged, and the nation is endangered. Even the United States cannot continue to build massive technological tails in support of deployed forces in the hope of ensuring only comfortable and safe missions.
- Radically change recruiting, training, doctrine, and career management policies to improve the capacity of military personnel and organizations to use information. While there is sometimes information overload, the main problem is that many military users cannot distinguish critical information from junk data. DOD should work harder to improve the capabilities of its people—not just procure more mediocre software tools designed to do the thinking for them. This means creating and sustaining a more intellectually sophisticated military force and requiring that IT professionals produce products that are genuinely useful.
- Make the US military less vulnerable to attack.[47] This may mean using less RMA-inspired technology.

- Radically redesign the Department of Defense. There is no possibility of unified effort until there is fundamental change in the institutional structure of DOD. Congress must act first. Title 10 of the US Code, which gives the services authority for training and equipping their forces, should be radically reformed. The Goldwater-Nichols Act of 1986 should be revisited. The Secretary needs to gain much better control over the services and Defense agencies that nominally work for him. Finally, military and civilian leaders need to revitalize a culture that in many ways is dysfunctional.

These reforms are unlikely to occur in the absence of a significant US battlefield defeat. Organizations that agree on little within the Pentagon close ranks when collectively challenged. The military services have significant lobbying clout on Capitol Hill and powerful supporters in reserve and veterans organizations. Policymakers and the citizenry should continue to expect poor military performance and avoid—for a myriad of reasons—policies that run the risk of major war. The best we probably can hope for is a moderate conflict in which the inadequacies of *JV 2020* are obvious but the United States does not suffer disastrous defeat. Hundreds of lives and the associated diplomatic and domestic political ramifications of a defeat will probably be part of this awakening. We can but hope the cost will not be higher.

NOTES

The author gratefully acknowledges the assistance of Colonel Kenneth Allard, USA Ret., and Deborah Avant, who provided valuable comments on drafts. As with all *Parameters* articles, this article reflects the opinions of the author and does not necessarily represent the views of any agency of the US government or the author's employer, the MITRE Corporation.

[1] US Department of Defense, Chairman of the Joint Chiefs of Staff, *Joint Vision 2010* (Washington: Office of the Chairman, Joint Chiefs of Staff, 1996).

[2] US Department of Defense, Chairman of the Joint Chiefs of Staff, *Joint Vision 2020* (Washington: GPO, June 2000).

[3] Robert Tomes and Peter Dombrowski, "Arguments for a Renewed RMA Debate," *National Security Studies Quarterly*, 7 (Summer 2001), 109-22.

[4] US Department of Defense, *Joint Vision 2010*, p. 16.

[5] This attention is incongruous because the military brass has been willing for many years to give only low priority to key parts of "maneuver"—the sea and air lift needed to get forces transported in a timely fashion. It took six months of Operation Desert Shield (August 1990 to February 1991) before the United States was ready to liberate Kuwait. The US Army moved a very small force very slowly into Albania in early 1999 in preparation for a possible ground attack on Yugoslavia.

[6] See, for example, Daniel Goure and Jeffrey Lewis, "The Strained U.S. Military: Evidence From Operation Allied Force," *National Security Studies Quarterly*, 6 (Winter 2000), 21-42.

[7] The US Army plans to address this issue in part by creating new, medium-weight brigades, but there is no systemic DOD-wide program under way.

[8] R. Jeffrey Smith, "A G.I.'s Home Is His Fortress," *The Washington Post*, 7 November 1999, p. A11.

[9] While a judgment that the US military has not performed well is blasphemy in the Pentagon, it is backed by a large literature of analysis by capable US observers, NATO members, and, in narrow aspects such as the conduct of information operations during the war against Yugoslavia, DOD's own after-action reports.

[10] Rhetoric in this area is strong, however. See Henry H. Shelton, "Professional Education: The Key to Transformation," *Parameters*, 31 (Autumn 2001), 4-16.

[11] Office of the Undersecretary of Defense for Acquisition and Technology, *The Defense Science Board 1999 Summer Study Task Force on 21st Century Defense Technology Strategies*, Volume II, Supporting Reports (Washington: Office of the Undersecretary of Defense for Acquisition and Technology, March 2000), p. 115.

[12] Thomas K. Adams, "GPS Vulnerabilities," *Military Review*, 81 (March-April 2001), 10-16.

13. Office of the Undersecretary of Defense for Acquisition and Technology, *The Defense Science Board 1999 Summer Study Task Force on 21st Century Defense Technology Strategies*, p. 115.

14. Donald H. Rumsfeld, chairman, "Report of the Commission to Assess United States National Security Space Management and Organization," 11 January 2001, internet, http://www.defenselink.mil/pubs/space20010111.html, accessed 14 June 2002.

15. Michael Krepon, "Lost in Space," *Foreign Affairs*, 80 (May/June 2001), 2-8.

16. Vernon Loeb, "Test of Strength," *The Washington Post Magazine*, 29 July 2001, p. 9.

17. Ibid., p. 10.

18. James Bamford, *Body of Secrets* (New York: Doubleday, 2001), p. 574.

19. Arnaud de Borchgrave et al., *Cyber Threats and Information Security: Meeting the 21st Century Challenge* (Washington: Center for Strategic and International Studies, December 2000), p. 9. See also Carnegie Mellon University's website at http://www.cert.org/research/.

20. For a list of details, see James Adams, "Virtual Defense," *Foreign Affairs*, 80 (May/June 2001), 98-112. See also Vernon Loeb, "NSA Adviser Says Cyber-Assaults on Pentagon Persist With Few Clues," *The Washington Post*, 7 May 2001, p. A2.

21. James Adams, pp. 98-112.

22. Dan A. Vise, "Cyber-Crime Fighter Stays Vigilant," *The Washington Post*, 7 May 2001, p. A17.

23. Borchgrave et al., p. 48.

24. Obvious candidates are screen-saver programs and games, but surely there are many other possibilities.

25. Qiao Liang and Wang Xiangsui, *Unrestricted Warfare* (Beijing: People's Liberation Army Literature and Arts Publishing House, February 1999), trans. Foreign Broadcast Information Service.

26. Jerome Slater, "What Went Wrong? The Collapse of the Israeli-Palestinian Peace Process," *Political Science Quarterly*, 116 (Summer 2001), esp. 171-75.

27. Dana Priest, "Air Chief Faults Kosovo Strategy," *The Washington Post*, 22 October 1999, p. 14.

28. Wesley K. Clark, *Waging Modern War: Bosnia, Kosovo, and the Future of Combat* (New York: Public Affairs, 2001).

29. Bamford, pp. 460-64.

30. For another variant of the attrition strategy, see Richard K. Betts, "The Soft Underbelly of American Primacy: Tactical Advantages of Terrorism," *Political Science Quarterly*, 117 (Spring 2002), 26-33.

31. Clark. See also Richard K. Betts' review of Clark's book, "Compromised Command," *Foreign Affairs*, 80 (July/August 2001), 126-32.

32. John A. Gentry, "CINC Y2K Operational Evaluations: Purpose and Result," presented at the MILCOM 99 conference, Atlantic City, N.J., November 1999. Other conference papers describe the services' and DOD agencies' Y2K preparations.

33. Secretary Rumsfeld rescinded DODD 5000.1 and related instructions in September 2002, saying they do not foster efficiency, creativity, or innovation.

34. Lisa Troshinsky, "DoD Creates Interoperability Coordination Program," *Navy News & Undersea Technology*, 2 January 2001.

35. Office of the Undersecretary of Defense For Acquisition and Technology, *The Defense Science Board 1999 Summer Study Task Force on 21st Century Defense Technology Strategies*, p. 86.

36. Gentry, "CINC Y2K Operational Evaluations: Purpose and Result."

37. DOD Instruction 3020.39, "Integrated Continuity Planning for Defense Intelligence," 3 August 2001, internet, http://www.dtic.mil/whs/directives/corres/html/302039.htm, accessed 14 June 2002.

38. John A. Gentry, "Knowledge-based 'Warfare': Lessons From Bosnia," *American Intelligence Journal*, 18 (October 1998), 73-80.

39. For a discussion of the dangers of seeking superiority in space, see Michael Krepon, "Lost in Space," *Foreign Affairs*, 80 (May/June 2001), 2-8.

40. Loeb, "Test of Strength," p. 23.

41. Ibid., p. 24.

42. Thomas E. Ricks, "For Military, 'Change Is Hard,'" *The Washington Post*, 19 July 2001, p. A16.

43. For descriptions of part of this inter-command bureaucratic combat, see Clark, *Waging Modern War*, passim.

44. Joseph J. Collins, et al., *American Military Culture in the Twenty-first Century* (Washington: Center for Strategic and International Studies, February 2000).

45. Donald H. Rumsfeld, "Transforming the Military," *Foreign Affairs*, 81 (May-June 2002), 20-32.

46. US Army and Marine Corps doctrine reflects this, and many individual military personnel believe it. But adherents of airpower, in particular, and the department as a whole, believe that RMA is changing the fundamental nature of military conflict.

47. Steven Metz, "Strategic Asymmetry," *Military Review*, 81 (July-August 2001), 23-31.