Stanford University

CISAC

Center for International Security and Arms Control

The Center for International Security and Arms Control, part of Stanford University's Institute for International Studies, is a multidisciplinary community dedicated to research and training in the field of international security. The Center brings together scholars, policymakers, scientists, area specialists, members of the business community, and other experts to examine a wide range of international security issues. CISAC publishes its own series of working papers and reports on its work and also sponsors a series, *Studies in International Security and Arms Control*, through Stanford University Press.

Center for International Security and Arms Control
Stanford University
320 Galvez Street
Stanford, California 94305-6165

(415) 723-9625

http://www-leland.stanford.edu/group/CISAC/

The Information Technologies and Defense: A Demand-Pull Assessment

S. E. Goodman

Center for International Security and Arms Control
Stanford University

February 1996

The Center for International Security and Arms Control, part of Stanford University's Institute for International Studies, brings together faculty members from several scholarly disciplines with senior specialists from around the world and pre- and postdoctoral fellows for research projects, seminars, conferences, and international scholarly exchange. The Center publishes its own series of reports and papers on its work and also sponsors a series, *Studies in International Security and Arms Control*, through Stanford University Press.

The Center is grateful to the Carnegie Corporation of New York for support of this project as part of the Center's Science Program. The Department of Management Information Systems at the University of Arizona also contributed support. The opinions expressed here are those of the author and do not represent positions of the Center, its supporters, or Stanford University.

Center for International Security and Arms Control
320 Galvez Street
Stanford, California 94305-6165
(415) 723-9625
Douglas Peckler, Editorial Associate

Printed in the United States of America

ISBN 0-935371-41-9

Abstract

During World War II and the first few years of the Cold War, military demand essentially pulled digital computing out from nonexistence. The information technologies (IT) have since been used for a comprehensive make-over of the U.S. defense establishment.

This essay considers the demand-pull and technology-push drivers of the use of IT in the U.S. military. Demand-pull factors stem from foreign threats and other tasking that arises from U.S. foreign policy initiatives, such as peacekeeping missions. Technology-push factors stem from IT-related means and opportunities created in response to demands other than foreign threats or missions, for example, from commercial markets. Since the initial heavy demand-pull weighting of the 1940s, the imbalance has shifted to the technology-push side. This shift has accelerated since the early 1980s. The reasons include revolutionary changes in technology, and foreign threats and missions. This study addresses the following questions related to this shift and the ensuing weakness of demand-pull factors:

Did these technologies have much of a role in "winning" the military-technological confrontation with the U.S.S.R.? How did American and Soviet IT demand-pull and technology-push environments differ and compete?

The end of the Cold War removed the U.S.S.R. as a global military superpower. What continues to drive the extensive infusion of IT into the U.S. defense community? Is some combination of foreign threats directly and convincingly behind the pervasive use of IT?

The U.S. government seems driven toward IT for military and intelligence capabilities to deal with a wide assortment of conflicts and other missions. How much of this assortment has been amenable to IT-based solutions so far? What constrains their use? The United States went through the Cold War with enormous IT advantages over every other country. Has the accelerated global diffusion of information technologies in the post-Cold War period augmented or eroded these advantages, and increased or decreased vulnerabilities?

To what extent do the IT-induced civil "information revolutions" feed technology-push or demand-pull into a prospective revolution in military affairs (RMA)? If the United States has a civil information society and economy, then where are they located, who threatens them, and who will defend them?

The United States seems intent on pursuing an IT-based RMA, but nobody else is following suit to anywhere near the same extent. How or why might this RMA be accomplished without comparable military competition? Is there a compelling, demand-pull basis for a sweeping, near-term RMA with a 12-digit price tag?

Author

Seymour E. Goodman is Professor of Management Information Systems and Policy at the University of Arizona. He studies the international dimensions of the information technologies and related public policy issues. He was an undergraduate at Columbia University and obtained his Ph.D. from the California Institute of Technology. Professor Goodman has been a CISAC Science Fellow since 1994.

Acknowledgments

Many people were helpful during the course of this study. Much of their assistance took the form of commenting on drafts, or providing insights or leads into various uses of the information technologies for defense. These people include Alan Brown, Vaughn Cable, Chris Demchak, Valry Fetrow of the U.S. Naval Institute staff, Richard Gronet, Barry Horton, Martin Libicki, Shawn McKinley of the AFCEA staff, Robert Melford, Richard O'Neill, Thomas Rona, Lauren Rusk, Wayne Thornton, Mark Zimmermann, and scores of serving military officers and civilian scientists and engineers in DoD and each of the armed services. The collegial setting within CISAC provided an abundant local supply of knowledgeable readers and discussants, notably including David Bernstein, Cameron Binkley, Jonathan Epstein, Diane Goodman, Lawrence Greenberg, Melanie Greenberg, John Harvey, David Hoffman, Allan Krass, Michael May, and Kevin Soo Hoo. Diane Goodman also provided technical and administrative help. Given the wide scope of this study, clearly, not all these people necessarily agree with each of the views expressed herein.

This study was supported by the Carnegie Corporation of New York, the Center for International Security and Arms Control at Stanford University, and the Department of Management Information Systems at the University of Arizona. Their support does not necessarily imply endorsement of the views this report expresses.

The Information Technologies and Defense: A Demand-Pull Assessment

S. E. Goodman

1. Remaking Defense

Since the beginning of the modern digital computing era during World War II, the information technologies (IT) have been used for a technology-based make-over of the U.S. defense establishment. These technologies are now more noticeable by their absence than their presence in the development cycles and the use of almost all U.S. military and intelligence systems. IT is seen as enabling or enhancing functionality in so many ways that its applications have become central to defining U.S. defense and intelligence elements, structure, processes, and capabilities. However, such dependence also incurs new mismatches and vulnerabilities.

For our purposes, the primary information technology is digital computing. A strong trend in technology and applications is the fusion of computing and telecommunications; in this report *IT* refers to both.[1] The essential added value of IT is the transmission, storage, and transformation of data and information in more ways, at finer levels of granularity, faster, more cheaply, in greater volumes, and more autonomously than has ever before been possible. Thus what IT brings to defense is the ability to communicate more completely, and the capability to provide unprecedented, distributed, automated, sensory and logical functions and control.[2] Much of this requires less human participation than did the military machinery of the industrial era.[3]

The potential of this added value, and the experiences acquired so far, have been such that some people think it is now possible and necessary to rebuild America's strategic deterrent by shifting from nuclear to smart, that is, computerized, conventional weapons.[4] IT is central to the futures envisioned by both the traditional "big platform" advocates, who favor such weapons as tanks, aircraft carriers, and bombers, and more radical thinkers, who envision, for example, a battlefield covered with many small, smart, sensors under an integrated management information system targeting long range brilliant weapons that find and destroy their targets with high probability. Hence, IT is at the core of all views of what has been called "the main argument now roiling the Pentagon ... whether the way wars are fought will change fundamentally."[5]

Be it with big platforms carrying literally tons of IT or with little robotic ants, or with anything in between, the U.S. Department of Defense (DoD) seems determined to pursue a "military-technological revolution" (MTR) or "revolution in military affairs" (RMA).[6, 7] An

MTR is the rapid and extensive infusion of new technology into military systems, but without fundamental change in the way these systems are used. An RMA is more ambitious in that technological and other new capabilities would fundamentally change the way military power is assembled and used. The changes would affect what military power could do to advance national interests and to control the relations between and the behavior of other nations. One way or the other, the United States is building the world's first IT-based, postindustrial military establishment.

This essay aims to provide a short, somewhat speculative, discussion of the value of IT in the defense of the United States.[8] This is an initial, wide ranging, exploratory effort to try to understand how and why so much IT is finding its way into the U.S. national security domain. It is concerned primarily with the balances between demand-pull and technology-push drivers of the use of IT in the U.S. military, and with some of the implications of the imbalances. Demand-pull factors stem directly from foreign threats or other tasking of the military arising from U.S. foreign policy initiatives, such as peacekeeping missions. Technology-push factors stem from the IT means and opportunities that have been or could be created in response to demands other than foreign threats or missions. Examples include the desire to create commercial markets, or to build more efficient industrial processes or organizations. To greater or lesser extents, demand-pull and technology-push iteratively and interactively reinforce each other.

During World War II and the first few years of the Cold War, military demand essentially pulled digital computing into existence. Since that initial demand-pull created a pull-push imbalance, the situation has shifted to the point where the imbalance is now heavily on the technology-push side. This shift at first took place gradually, but has rapidly accelerated since the early 1980s. The reasons include revolutionary changes in both IT and the set of foreign threats and missions. The sections that follow will try to address questions related to this shift and the ensuing weakness of the demand-pull side.

Section 2 provides a brief, IT-centric history of the Cold War. Did these technologies have much of a role in "winning" the military-technological confrontation with the U.S.S.R.? How did the American and Soviet IT demand-pull and technology-push environments differ and compete?

The end of the Cold War removed the U.S.S.R. as a competing global superpower in the military and intelligence fields. Section 3 considers what continues to drive the extensive infusion of IT into the U.S. defense community. Does some combination of foreign threats directly and convincingly motivate the pervasive use of IT?

The U.S. government seems driven to employ IT to enhance its military and intelligence capabilities for dealing with a wide assortment of conflicts and instabilities around the world. These uses are discussed in section 4. How many of them have been amenable to IT-based solutions so far? What limits the use of IT for such purposes? The United States went through the Cold War with enormous IT-related advantages over every other country. Has the accelerated global diffusion of these technologies in the post-Cold War period augmented or eroded these advantages, and increased or decreased vulnerabilities?

The diffusion of IT has enabled "information revolutions" in the American economy and society. Section 5 considers the extent to which the IT-induced civil revolutions feed technology-push or demand-pull into any prospective RMA. If the United States increasingly has an information society and economy, then where are they located, who threatens them, and who will defend them? Is the collective IT-based medium (cyberspace) itself a location for conflict that is much different from the traditional geophysical media (land, sea, air, and space)?[9]

The United States seems intent on pursuing an IT-based MTR or RMA although nobody else is following suit to anywhere near the same extent. Sections 5 and 6 discuss why and how some kind of technological revolution might be accomplished without the demand-pull of comparable military competition. Is there a compelling, demand-pull basis for a sweeping, near-term, IT-based MTR or RMA with a 12-digit price tag?

2. A Brief History of the Information Technologies in the Cold War

World War II and its immediate aftermath provided the demand-pull for the dramatic development and use of high-technology military systems, including nuclear weapons, ballistic and cruise guided missiles, jet aircraft, radar, and electronic warfare. Military demands also drove the creation of the first operational, large-scale, digital computers.[10] Given the extraordinary complexities of building these machines, it is not clear how or when they might have been built had it not been for the wartime, and the immediate postwar, national-security-driven efforts in the United States, Great Britain and, to a lesser extent, Germany. By the mid-1950s, electronic digital computers were also operational in the Soviet Union and Eastern Europe.[11]

Many of the advanced technologies to emerge from World War II became crucial to U.S. and NATO policies and strategies of deterrence, containment, and war fighting during the Cold War. Nuclear weapons became the foundation of deterrence and military standoff with the U.S.S.R. Nuclear-driven strategic needs provided much of the imperative for new IT-based military systems, for example continental air defense, the command and control of nuclear forces, more accurate ICBMs, ABMs, and space reconnaissance systems. The most powerful computers available were used extensively for the design of nuclear weapons and their delivery systems. The rapidly improving cost and performance characteristics of computing and telecommunications led to increased use in other parts of the U.S. defense establishment, such as administration, aircraft design, and communications intelligence.

To a great extent, U.S. national security concerns were driven by a single, monolithic foreign threat. Advanced technology became a basis for much of the U.S. military response to the U.S.S.R. The United States could focus intelligence on Soviet efforts and the defense community could concentrate on a "countervailing strategy" of building and fielding "new systems of overmatching capabilities."[12] With this policy of "performance at a premium," cost was secondary because the global threat was ultimately one of national survival.[13] Increasingly, performance at a premium took the form of microelectronics and microelectronics-based IT, in which rapidly improving advantages might be obtained in speed, size, control, and power consumption. These technologies became important enabling or enhancing elements for most of the overmatching systems.

This policy of technologically outpacing a clearly identified foreign threat was complemented by an export control policy designed to protect the advantages thus gained by slowing the transfer of military and dual-use technologies to adversarial countries. To this end, the United States and its similarly threatened, technologically advanced allies established the CoCom framework to form a common front that tried to prevent most of the world's high technology sources from transferring products and know-how to a common set of potential adversaries. Over the history of CoCom, from 1950-1994, microelectronics, computers, telecommunications, and computerized manufacturing systems commanded most of the attention among the dual-use technologies.

This double-edged, technology-based policy turned out to be effective because both sides played the same high-technology systems game at the core of their military confrontation. The United States took a technology-based approach to being a global military superpower immediately after World War II, and the Soviet Union followed suit. The Soviets were given little choice by both technological and political-economic factors. How could they remain a global military power without trying to match U.S. strategic capabilities? And how could the U.S.S.R., the expansionist "vanguard of the world's most advanced and scientific political and industrial system" beg off from an industrially based contest for global supremacy with its arch-rival, especially when the threat of "militaristic capitalism" was used as one of the great legitimizers of the Soviet political-economic system? Each side saw itself demand-pulled, that is, threatened, in similar ways by the technology-push of the other.

The scope of the military-technological confrontation expanded, notably into space and across an increasingly comprehensive spectrum of advanced conventional systems. The militaries on both sides continued to take a leading role in the initial development, production, and use of many emerging dual-use technologies, including electronics, semiconductors, space vehicles, communications satellites, computer hardware and software, and systems security. Some of the most visible technologies of the Cold War–for instance, nuclear weapons, rockets, missile submarines, and main battle tanks–stayed exclusively in the military domain, or in other limited, large-scale, essentially governmental domains, such as the atomic energy and space agencies. The most singular exceptions were the information technologies, which took on an increasingly expansive and useful presence in the larger U.S. economy and society.

Many IT advances were driven by the U.S. national security establishment in ways that more effectively transferred technology to the civil sector than was the case in the U.S.S.R. Since the end of World War II a number of important private sector advances in IT have come as by-products of defense contracts. One of the most notable examples is the technology for the Defense Department's ARPANET which, from its origins in the late-1960s, has been transformed into the world's Internet.[14] Several companies, including IBM and AT&T through its Bell Labs, derived commercial benefits from R&D for the DoD. Over time, as the applications and value of IT to the general economy grew, product and technology transfer increased in both directions, with the civil-to-military flow arguably growing faster.

By the mid-1970s, computing had significantly more of a presence outside the U.S. military and its direct, focused, industry-supporting infrastructure than inside. IBM and Digital Equipment Corporation had transformed the computer industry and market with their System 360/370 upwardly compatible family of mainframes and the PDP minicomputers, respectively. These companies were producing on the order of 10,000 machines annually, with the great majority going to civilian end-users. AT&T had developed many advanced telecommunications technologies and a continental-scale network that provided incomparable access for a large civil population. Similarly, much of the U.S. software development and consumption effort was shifting to the civil sector.[15] The dynamics of the much larger, and richer, civilian commercial, industrial, and scientific sectors were providing more of the drive behind the development of these technologies than was the national security sector. Heretofore, the development and use of computing had been limited to scattered pockets around the world. The end of the 1960s witnessed the beginnings of a large-scale diffusion across the largest and most advanced national economy. In the early 1960s, the DoD consumed most of the world's production of advanced electronics; today it constitutes less than one percent of the American market.[16]

As IT became more valuable to the U.S. economy and society as a whole, most of the increases in R&D, national diffusion, and production continued to shift to civil sectors. The American national security establishment was a major beneficiary in many ways, especially from access to a much larger infrastructure of capabilities and technological talent that was developing IT in ways and at a pace that the DoD could not drive, manage, or afford on its own. This more general national base in high technology made for a strong form of technology-push that drove IT into a broad array of higher performance strategic and tactical military systems in ways the Soviets could not match, but which clearly mattered by the criteria of the game both were playing. Overall, IT-related national infrastructural differences were critical to the creation of increasing gaps between the United States and the U.S.S.R. in the existence and performance of a broad and growing spectrum of military systems. By the end of the Cold War, important qualitative gaps favoring the United States extended even to tanks, a core bastion of Soviet military advantage going back to the 1930s. For tanks, IT is fundamental to armor and anti-armor design (the most computationally intensive application in the U.S. Army), fire control, and command and control.

The technology infrastructure of the former U.S.S.R. was large, but unbalanced and poorly interconnected. It had an extensive tertiary educational system, some of it outstanding, for example, it produced a large, world-class mathematics community. It was able to focus resources, and did so successfully in areas such as the development and production of weapons of mass destruction (WMD) and submarines, and the covert collection of foreign technology. But because these strong sectors were more isolated from the larger domestic economy and from the world technological community, serious deficiencies occurred with regard to IT as compared to the way these technologies developed in the West and Japan. Although the Soviet and American militaries were playing the same game with regard to their military-technological confrontation, the two civil IT sectors were playing in very different games. The structure and priority-setting mechanisms of the Soviet economy in general, and of the military-industrial sector in particular, made for an abysmal environment for internal technology transfer, both from the military-industrial to the civil sector and vice versa.[17]

In contrast, the U.S. DoD operated much more in the active, overt, strongly interconnected technology transfer domains.[18] A case can be made that the Soviet and American militaries were both dipping at the same international technology troughs, mostly located in America, as the R&D, production, and market strengths in microelectronics and IT shifted from the military to the civil sectors in the 1970s and beyond. The Soviets were forced to substitute the American civil IT sector for the technology-push their economic-political system had failed to develop at home. Neither military establishment could develop and support such a large and dynamic high-technology sector on its own. These American advantages and Soviet disadvantages were reinforced by the effects of export controls. Even good Soviet covert collection mechanisms, much bemoaned by the U.S. defense and intelligence communities, often resulted in weak transfer when the collected technology was poorly absorbed by the first receiver, and then even more poorly transferred internally within the U.S.S.R.[19] As these diffusion trends accelerated, the relative Soviet weaknesses were magnified more broadly systemically.

The most important IT-related examples of Soviet use of American technology were the massive ES (Ryad) and SM programs of the Warsaw Pact countries to duplicate functionally the IBM System 360/370 family of mainframes and part of Digital Equipment Corporation's lines of PDP and VAX minicomputers. Overall, the attempts lasted two decades, starting in the late 1960s. After some belated success, the programs could not be sustained at the same rates of technological advance as the continuing American efforts. In spite of extensive covert and overt technology collection, the Soviet and East European computers never achieved comparable levels of technology (including peripherals), reliability, production levels, or forms and quality of distribution.[20]

Because of greater American infrastructural strengths supporting and pushing technological development and transfer, the scale and visibility of what was happening, and the comparative ease of collecting intelligence against the United States, the Americans set the pace in more areas as the Cold War progressed.[21] The Soviets saw themselves as being impelled by U.S. military-technological threats, with the Strategic Defense Initiative (SDI) as an especially high-profile example. Performance gaps were appearing and widening in almost every military systems area where IT figured prominently. Ultimately the Soviets could no longer run, or afford to run, a full-spectrum competitive race in military systems.[22]

The complementary American Cold War policies of technologically outpacing military adversaries and slowing undesirable forms of transfer to them supports another premise that pervades U.S. national security policies. This is essentially that having superior high-technology systems prevents the kinds of wars they would decisively win, or at least decisively precludes the other side from winning. During the Cold War, with the enormous risk and destructive potential of possible wars between the superpowers, the nuclear and electronics/IT approach to defense arguably deterred a large part of the potential conflicts the United States most wanted to avoid.

3. Beyond the Cold War: Technology-Push and Defense

Since the mid-1940s, the U.S. defense sector has developed and absorbed IT systems at a rate and to an extent that it will soon be almost impossible to find an American military component of any size, combat or non-combat, without computers or telecommunications of some kind. Important IT-based systems have already provided advantages in post-Cold War conflict.[23] These systems range from the fire control system and armor of the M1A1 Abrams tank, to sophisticated surveillance systems, such as the Airborne Warning and Control System (AWACS) and the Joint Surveillance Target Attack Radar System (JSTARS).

However, many IT-based systems, including most that helped "win" the military-technological battle of the Cold War, have remained unproved or shown themselves deficient in actions against foreign targets, for example the Patriot missile in the Gulf War and the Aegis cruiser system against a misidentified Iranian airliner. DoD and the intelligence agencies are littered with the remains of expensive IT systems that never amounted to much.

What is often not as fully appreciated is the increasingly pervasive role of IT in the life cycle of virtually every important military or intelligence system, not only in its operation. In one form or another there is an IT presence in the sequence that includes design, initial development, advanced development, testing, production, maintenance, training, and modification, and the various feedback loops between these stages. It has gotten to the point where some things, like the design and production of many integrated circuits or the design and control of high-performance or stealth aircraft, and certain intelligence functions such as breaking code keys, cannot be done without computers.

The IT content is also rapidly expanding within strategic and tactical systems. For example, the F-16C produced in the late 1980s required about 230,000 lines of on-board software code; the F-22 will require an estimated 2 to 4 million lines.[24] IT also figures prominently in the system-countersystem dynamics in successive generations of military technologies, for instance, an electronic targeting system, electronic countermeasures against this system, and electronic counter-countermeasures. Furthermore, IT is not something, like new truck tires, that just gets plugged into existing systems. It involves an extensive process of absorption, including modifying doctrine, retraining, reconfiguration that can severely stress organizations.[25]

Consider, for example, the computer needs for the F-117A, the first stealth combat aircraft, which performed dramatically as a light bomber during the Gulf War. A large mainframe computer was heavily used for its design. Limitations in computing power in part necessitated a focus on the low cross-section against certain radar frequencies at the expense of other design factors. The focus and limitations seriously affected aerodynamics and resulted in a design that was unstable in flight. These problems had to be corrected with on-board flight control computers performing thousands of aerodynamic micro-adjustments per second, thus making it possible for the aircraft to fly. Human pilots simply could have not controlled the aircraft, and it would have fallen out of the sky without these computers. They were made quadruple-redundant to ensure survivability and reliability. Moreover, computer-controlled machine tools were necessary for the precision manufacture of parts of the aircraft. The F-117A also had an innovative, fully computerized flight program. This program could actually fly the airplane from takeoff, control the entire flight to the target and back, and accomplish the final landing. The pilot was not essential. This flight program permitted unprecedented accuracy of location and timing. To stay stealthy, the F-117A could not carry much in the way of its own radar, defensive weapons, or a large bomb load. Weapons were limited to precision guided munitions. The computing requirements for more advanced stealth aircraft programs, the F-22 and the Joint Air Strike Technology (JAST), have become much more demanding.

Stealth aircraft is an important example of a weapon whose development was originally demand-driven by the extensive and deep Soviet air defense network. Air defense was a major asymmetry of the Cold War, since the United States had very little continental anti-aircraft defense for the last decades of that conflict. Stealth airplanes were intended to neutralize and penetrate the Soviet system.[26]

These brief statements of "what is" describe only part of the picture. I have barely mentioned the "what is intended to be" part, such as the extensive efforts to create truly global and integrated C4I[27] systems at every level: within each armed service, between armed services ("joint operations"), and between U.S. and allied forces ("coalition"). Ignoring the questions of how well they will work, what they will cost, whether or not they are needed, or what is driving their creation, the DoD C4I programs are technically and conceptually impressive and ambitious. More generally, there are largely IT-based, expansive visions of a sweeping MTR or RMA (to be considered further in sections 5 and 6).

The Department of Defense is not the only part of the U.S. national security establishment to become highly dependent on IT, although its large size and singular role distinguishes it above all others. The CIA, DEA, FBI, NASA, Department of Energy, and others have integrated IT-based systems into a wide spectrum of their functions.

During the Cold War the United States saw an understandable, clear (perhaps more so with successful hindsight?) correlation between a threat to national survival and a high-technology-based approach to protecting its security. The pervasive infusion of IT into defense, as just briefly sketched, is a major consequence of that approach. The high-technology strategy of both running faster and slowing transfer to adversaries played an important role in "winning" the Cold War military confrontation. Direct military vindication can also be drawn from the technologies used by both sides in Desert Shield/Storm, which in a military-technological sense might be seen as the last Cold War conflict as much as "the first information war," as it is often portrayed. The United States was working with a complete and balanced push-pull set: a full spectrum foreign "superpower" threat with comparable military values and goals provided the demand-pull, and a powerful national infrastructure furnished a complementary technology push. Now half of this complementary relationship that shaped American defense posture has been greatly reduced, and the potential threat and conflict spectrum has significantly changed.

Yet, the IT-intensive approach to defense continues, and perhaps has even accelerated. Why? The obvious and most compelling first place to look for answers is on the demand-pull side. To what extent are foreign threats driving the infusion of so much IT throughout the U.S. national security community?

With the collapse of the overarching communist threat and the global diffusion of technology, the make-up and complexity of national security concerns has changed dramatically. Roughly speaking, the mean value of the threat distribution is much reduced, but the variance is increased.[28] Among other things, the demise of the Soviet Union has reduced what in retrospect was an important element in controlling the undesirable diffusion of technology for WMD, especially nuclear weapons; reduced the clear set of high-value targets appropriate for U.S. IT-based systems; reduced the consensus focus on a security threat widely shared by the American public and allies; and reduced the level of defense cost the Congress and public are willing to support. Other factors, including the proliferation of IT and other capability-enhancing technologies, have increased the number, variety, and lethality of a new spectrum of problematic transnational and sub-nation-state entities. These include assorted ethnic minorities, well-armed rogues, international bank robbers, drug cartels, and a wide variety of terrorists.

In the current politically messy, technology-enabled world, how does one define and identify a threat to U.S. national security? We broadly define national security to include the safety and well being of American society *vis-à-vis* foreign threats. This would include all the traditional military threats, significantly decreased by the lack of a comparable global adversary, but with additional worries about the proliferation of WMD to regional military powers.

Beyond these threats, candidates for inclusion become more debatable and more numerous. For example, what about threats to crucial portions of the national infrastructure, such as terrestrial and satellite telecommunications, the national air traffic control network, power grids, the banking system, and law enforcement systems? These systems have all come to be of great importance to the national economy, are used extensively by the military, and would be more crucial during crises. In the "old industrial era," direct foreign threats to infrastructure consisted of something like a saboteur bombing a railroad station and producing very localized damage. Such attacks would usually be mounted by foreign governments. Not so any more. Attacks to IT-based infrastructure, including all the above systems, can now be much more extensive, often with far less physical damage, and can be much more varied in possibilities beyond simple physical destruction.[29] They may also be conducted by a multitude of foreigners, not to ignore troublesome Americans, outside of traditional national military establishments. Do the international drug cartels, and global organized crime more generally, qualify as threats to national security? They have become extensive and in some cases sophisticated users of national and international infrastructures, especially telecommunications and banking, and have developed effective global infrastructures of their own. Illegal drugs in America arguably do more damage to the safety and well-being of society than anything else inflicted by organized foreign entities.

It is beyond our scope to consider what should officially be included in the set of national security threats. The immediate question is whether some combination of such threats are now directly and convincingly driving the pervasive use of IT in defense.

The most compelling form of affirmative answer should be based on the demonstrated decisiveness, or at least great effectiveness, of IT-based systems across a spectrum of conflicts short of what would have been World War III. However, a brief look at the cost and performance of high technology in actual military operations against foreign adversaries reveals a mixed set of results. Starting with the heavy U.S. involvement in Vietnam, chronologically roughly the same time that computers began to be diffused extensively in the United States, in many cases of conflict high technology was not decisive, or foes with low-tech weapons and infrastructure defeated or neutralized far more technologically sophisticated opponents.[30] The success of Desert Storm stands in contrast to Vietnam, Somalia, and the Soviet experience in Afghanistan, among other examples, where the technologically much more advanced superpower combatant came out the loser. It is worth noting that the Iraqi-Allied technology gap was smaller than those between combatants in the other conflicts.

Even Desert Storm, where almost every IT-based system worked, arguably owes its success as much to other factors. These include a long and uninterrupted set-up and shake-out period that proved necessary to get many IT-based systems to work properly.[31] Another factor was a cooperative former adversarial superpower that in effect permitted the United States to use most of the forces put together to deter or fight a world war for a much more modest regional conflict. Furthermore, the performance of C4I systems, in particular, left much to be desired even in the extraordinarily asymmetric force and technology imbalances in the invasion of Grenada, and for several important ship-related military incidents (for example, with the ships Pueblo, Mayaguez, Vincennes, and Stark).[32] The fragility and complexity of many IT-based systems and their users under stress has been such that we should be thankful that the mainline military-technological conflict of the Cold War remained mostly “cold.”

Superior technology does not necessarily insure success, even if it is cutting edge or perfectly utilized. Perhaps the most extreme contrast occurred with the Israelis in Lebanon in 1982. One of the most striking electronic warfare victories in history–the air battle with Syria[33]–was followed by a miserable, no-win, demoralizing struggle with an asymmetric low-tech foe. One might question more generally the value of all the advanced technology systems in the advent of an aftermath of a high-technology-based military victory, such as an occupation or pacification of a defeated enemy’s territory. Certainly the Israelis do not have much of a positive story to tell. U.S. forces were also prematurely pulled out of Lebanon after an unsuccessful stay that included the loss of over 240 Marines in one extremely low-tech blow.

Similar questions arise with regard to the value of high-technology systems in comparison to that of the other measures against national security threats, such as advanced technologies used by the DEA and other law enforcement agencies, or what the $1 billion DoD effort has tried to bring to bear, to fight the drug war. Clearly, it is not generally the case that the value of high-technology systems scales down very well along the spectrum of levels of conflicts or technological levels of combatants.[34] Nor does it seem obvious that many such systems are developed, or can be cost-effectively developed, with such scalability as a goal.

Arguments may be put forth to explain each failure: that yet more high-technology systems were needed in these conflicts to overcome the deficiencies of the systems actually used, or that development programs did not start early enough, or that the systems were not used properly, or that the politicians would not let them be used appropriately, or that the wrong battle was fought in the wrong place, or that the full potential or synergistic possibilities of IT had not quite been realized yet, or whatever.[35] But there should be more concern that high technology in general, and IT-based systems in particular, may leave the United States short of what is needed to deal with future foreign threats much different from the nearly ideal situation presented by Saddam Hussein. What is particularly disturbing is the large fraction of real conflicts and incidents where advanced technology-based systems proved to be seriously inadequate in one way or another. Perhaps too much reliance on IT might produce another form of the impotent and pitiful giant, that is, the nuclear- and airpower-rich superpower effectively beaten by the oppressed people, or warlords, or whomever, in Vietnam and more recently in Somalia.

No other country is spending nearly as much as the United States on advanced technology for national security. The United States outspends the next five countries put together on defense, and possibly outspends the entire rest of the world put together on national security-related IT in all of its forms.[36] Furthermore, the range of IT-using applications the United States pursues is far greater than that of any other country. It is possible that all of the different kinds of IT-dependent national security systems in the rest of the world together would not match the U.S. inventory.[37] The United States seems to feel compelled to outperform the combination of everyone else across the spectrum of current or prospective high-technology military systems. It is not easy to find historical precedents for such global disparities in defense spending.[38]

As subsequent sections discuss, there is a weaker match between defense technological strengths and new demand-pull realities than was the case during the Cold War. Significant IT-based strengths that were then well-matched with threats are now directed at less threatening adversaries or are almost irrelevant, for example, blue water anti-submarine warfare, or SSBN and ICBM targeting. Furthermore, all the possible adversarial countries put together are probably not investing in such defense systems to the same extent as the United States. This is not to say that there are not threats to U.S. national security, nor that IT-based systems cannot be valuable assets in countering those threats (I will argue later that they had better be, because the United States is not generating much in the way of alternatives). But such systems are not well proven in past and recent operations against actual adversaries or against the new world of foreign threats and conflicts. It is far from apparent that successful adjustment to new demand-pull conditions explains most of the continuing massive infusion of IT into the national security sector.

So what is driving IT into the U.S. national security establishment? The answers span a broad range of collectively reinforcing arguments and interested parties.[39] Not surprisingly, most of the answers offered by these interested parties derive from the basic advantages IT may bring to systems of military importance: the ability to communicate much more completely, and the capability to provide unprecedented, autonomous forms of distributed sensory capacity, logic, and control. At the next level of granularity, a representative list of these functions or advantages, and a sample of military activities that are perceived to benefit, includes:

- To perform functions, especially those that require frequent repetitive computations, much faster and more accurately than humans, for example, the continuous tracking of multiple, high speed targets, or the breaking of codes.

- To be used in environments very hostile to humans, as are sensors in space or the bottom of the ocean.

- To "stay alert" more consistently than humans and provide intelligence in systems that need to loiter for very long times, as with arms control verification.

- To perform critical functions in more desirable packages, especially in contexts where weight, volume, cost, and human casualty constraints are severe, as in the case of battlefield reconnaissance.

- To target precisely, permitting the "surgical" use of weapons, limiting undesirable collateral damage, cutting down on the need for multiple missions risking high-value American platforms, and so on; an example is the hitting of small, critical, heavily defended targets.

- To organize and control large volumes of data in predictable, distributed, and usable ways, for instance keeping track of the locations and movements of friendly forces.

- To provide reliable information recall from a variety of sources, for example, for intelligence applications.

- To provide suitable means for intrusive actions, lessening or eliminating the problems of extraction of human U.S. intruders; such actions include deep reconnaissance or precision penetration missions.

- To afford greater resolution or sensitivity for sensors of various kinds, as in acoustic signal processing in anti-submarine warfare (ASW) or satellite image processing.

- To exploit vulnerabilities in the use of IT by adversaries, for instance, in wiretapping by the FBI or communications exploitation by the National Security Agency (NSA).

- To offer a wider range of more secure or higher volume forms of communication, for example, so downed pilots or special operations groups can get more timely help.

- To provide C4I-based force multipliers, to enable the concentration of forces at the right place at the right time with the right weapons, even though the enemy might have more traditional numerical advantages. More general arguments along these lines view IT as the glue and neurons that will bind many systems together into a system of systems that make for an integrated whole greater than any sum of the parts.

- To allow real time or very short turn around access to vast, diverse, and changing sources of information, for instance, by providing commanders with a more transparent battlefield including more timely information on the results of recent actions.

These functions form essential building blocks in the DoD's efforts to define and rationalize future generic military capabilities. DoD leadership sees these capabilities coming together in a synergy that they hope will provide nothing short of a revolutionary transparency of the battlefield.[40] This "dominant battlefield awareness," knowledge, and ultimately "omni-science" is to provide the means whereby U.S. and allied forces will have unprecedented control over the battlefield, enabling everything from the avoidance of fratricide to the ability to find and engage all worthwhile targets in great depth, with high precision, and in short times.

Another set of reasons for technology-push derives from budgetary pressures. So far, there does not seem to be any fundamental questioning of the "need" for U.S. military technology to surpass everyone else's across the board. However, cost is now a more pressing and more independent variable, largely the result of weakened traditional demand-pull, that is, the lack of a peer military competitor.

Much of the economic pressure shows up in seeking greater efficiencies, such as reduced cost and the substitution of technology for people. Downsizing, or borrowing the more positive-sounding *rightsizing* term from industry, is a fact of life for most government agencies. Difficult political battles are inevitable when money becomes tight. Means are sought to cut costs while maintaining or shortening times to field new advanced technology systems. For example, most IT development now takes place in an increasingly internationalized civil industrial sector working on shorter product-cycle time scales than has been the case for the DoD. Therefore, the DoD feels the need to expand and improve the effectiveness of its product and technology transfers from the private sector, for instance by improving the acquisitions process and seeking lower cost and more frequently upgraded technology.[41] An additional appeal of IT to traditional platform advocates is that, absent the money to create many completely new platforms, these technologies can be used to upgrade the capabilities of existing platforms at lower costs, as with making the M1 tank into the M1A2, developing successive generations of B-52s, and adding ASCM defenses to ships.

However, one might seriously question the extent of success in achieving all these desired functions, or of doing so in efficient, cost-effective ways. Many IT systems are extraordinarily complex and often more fragile than most people think. They are susceptible to electromagnetic pulses, freaky software interaction errors, and so on. It is combinatorially impossible to test large systems (or often, not-so-large systems) for all possible uses. Problems frequently arise in several general forms, including: (i) data-overload for digitally hooked-in commanders; (ii) severe cost and schedule overruns, and (iii) surprise failures in system interactions under untested and stressful use.[42] It would be difficult to find many major IT-based defense systems that have not suffered from one or more of these problems.

A mixed bag of other reasons for the continued high-tech push into defense might also be postulated. A military based on high technology makes for a "clean" public and recruiting image. IT-based simulations and computer-aided instruction support relatively low-cost, flexible, accident-free peacetime training and exercises. Some of these simulations can be conducted on scales that would be financially and logistically out of the question as real exercises. Especially after the demonstrations of Desert Storm, high technology gives the U.S. arms industry an international competitive advantage, thereby improving balances of payment, keeping defense skills employed, and providing the U.S. military with economies of scale. IT-based weapons cut down on casualty exposure to enemies who do not possess the long reach of American systems. It is much more attractive for defense leaders and thinkers, both now and for their longer term legacies, to be high-tech fueled visionaries than to deal with miserable problems like downsizing and WMD proliferation. High-tech infusion continues some post-World War II trends that have become "natural," such as a large role for scientists and an R&D-oriented military-industrial complex. High-tech training and management are good experience for peacetime careers, and provide postenlistment or postretirement job opportunities for military personnel and civilian government employees.

With so much uncertainty about the extent and forms of foreign threats, and with budget-based threats all too real, it is natural for the existing parts of the national security community to seek their own marriages of doctrine, deployment and technologies. This results in efforts to "fight the last war better," bureaucratic politics to protect programs, and speculation about enemies who might arguably be dealt with by using a favored system or platform. In what is otherwise a negative DoD atmosphere pervaded with concerns about the proliferation of unpleasant forms of WMD and reductions in personnel, bases, and mission grandeur, the elements of modernization and high-tech "revolutions" provide a much needed positive programmatic dimension and future-oriented outlook.

With the end of the Cold War, the balance of demand-pull and technology-push for the use of IT shifted dramatically, yet the infusion of IT continues, perhaps even at an accelerated pace, for a variety of mutually reinforcing, mostly technology-push reasons. But the spectrum of conflicts the United States wants to deter or successfully conclude has changed significantly. It is questionable whether the post-Cold War set of potential conflicts and operations is well covered–either substantively or cost-effectively–by what is still essentially a downsizing Cold War defense establishment.

We turn now to some IT-related concerns about these conflicts and missions that beg further consideration.

4. Computers as Substitute Soldiers?

Given the capabilities and aims of prospective near- and intermediate-term adversaries, little of the spectrum of potential conflict and other military operations is going to look much like the Cold War, World War III with the Soviets, or Desert Storm. It is by no means clear how much of the new set of military problems is going to be amenable to IT-based solutions.

The intermediate-term set of potential adversaries appears roughly as follows, ordered in terms of decreasing traditional military capabilities and command and force centralization:

(a) Regional military powers with large, industrial military forces. They may be increasingly augmented by IT-based systems and possibly WMD, but overall military IT capabilities fall far short of what is available to the United States. China and Iran are examples. This category might be extended to include more technologically advanced powers like Russia.

(b) Other less-developed countries (LDCs), fragments of failed nation-states, and ethnic or otherwise cohesive groups within a country or region. Their forces are usually mixes of “pre-industrial” and “industrial” elements, with some use of IT, as in Bosnia, Cuba, and Somalia.

(c) Substantial transnational, distributed, coherent organizations, with access to sustained financing and havens. Examples are elements of global organized crime and guerrilla or terrorist networks supported by (or supporting) foreign governments.

(d) Highly fragmented, distributed, decentralized groups. Their loosely coupled or independent elements are usually small, but their abilities to do damage have been enhanced by technology and access to the infrastructural elements of their enemies. Network hackers and fringe terrorists are instances of such opponents.

A wide spectrum of conflicts, peacekeeping operations, forms of information warfare, and so forth that would require the presence or use of U.S. national force can be envisioned with this adversarial set. This spectrum, and the emerging forms of interactions between such widely different players, should arguably be the most important driver in any forthcoming revolution in U.S. national security affairs.

Given this adversarial set, we can consider the basic short- and intermediate-term U.S. defense goals and constraints with an eye toward assessing the demand-pull for IT-based military capabilities. Gone are the days when the U.S. military can convincingly proclaim goals such as protecting American shores from foreign military invasions, or being the bulwark against the sweep of well-armed world communism, or deterring a civilization-ending nuclear holocaust. With less than a perfectly clear idea of where the United States wants to lead the world, that more or less leaves dealing with various forms of incursions into the United States by something other than large foreign armies, interventions for selective U.S. interests, helping allies, being the world’s best armed coalition partner for major regional contingencies (MRCs), and serving as the police of last resort. The United States might also hope to discourage other countries from getting too strong militarily. This is done by making them feel that a build-up is either not worth the cost, or not necessary because the Americans are already watching out for them, or that it will not get them anywhere because an unbeatable United States is going to war if they cause trouble.

Many of the prospective national and international security-related encounters with the foregoing type (b), (c) and (d) entities are not even called *war*. Among other things, these activities include peacekeeping, police actions, counter-terrorism, counter-proliferation, military-assisted evacuations from trouble spots, unconventional warfare (such as guerrilla insurgencies), and ferreting out destructive hackers on the Internet. For want of a more imaginatively descriptive term, U.S. officials refer to most of this work collectively and by default as operations other than war (OOTW) or low intensity conflicts.

There are serious constraints on the long-term pursuit of such roles and missions. It is doubtful if any postindustrial society, and the United States in particular, could raise and frequently use a large, perhaps conscript, industrial army to engage in regional wars or relatively low-intensity military or OOTW undertakings that are not perceived to seriously threaten national security. Reasons range from an at least current public and media aversion to sustaining even minimal American casualties, to deeper and more extensive social changes that have occurred in the United States as it is undergoing the transition from an industrial to a postindustrial society.[43] The United States is severely constrained by cost, social factors, and public opinion against putting a lot of Americans in harm's way, or against getting involved in questionable, remote conflicts requiring extended commitments and sacrifice, often likely without the kind of conclusive closure (that is, total victory) most Americans desire.

Thus, if the U.S. government wants to maintain a military capacity to deal with a wide assortment of conflicts and instabilities around the world, it will have to do it with a postindustrial military. This will require a serious rethinking of how to organize, distribute, and use military force. However one may try to envision what that would look like, given the near- and long-term national strengths and constraints, the United States is going to have to try to use more computers to augment or substitute for current forms of surveillance, fire power, mobility, logistics, and soldiers.

This need for IT is arguably both a demand-pull consequence of factors affecting the way the United States will have to adjust to the post-Cold War potential conflict spectrum, and a technology-push consequence of the options available to make that adjustment. Furthermore, almost everyone seems inclined to at least implicitly buy into this argument. Advocates of one program or another, ranging from big platform traditionalists to radical "information warriors," essentially see computers in one form or another as necessary to deal with enemies across a broad spectrum of missions and at the same time to keep human soldiers safe. The performance enhancing features of IT in military systems discussed in section 3 all point toward shifting functions from people to computers. So does cost-motivated downsizing. It is also easier for the national command authority to commit force if the effort does not involve the time and risks of using lots of people, or calling up the reserves for extended periods. Few people care if computers are "killed" in combat or accidents in some remote part of the world.

The United States has been moving towards such substitutions for some time, although on a far less extensive scale than we are now seeing and are likely to see in the future. Many uses of IT in strategic systems have decreased the ratios of people to other factors, such as lethality, cost, and deliverability. For example, manned U-2 flights over the former U.S.S.R. were replaced by IT-intensive satellite-based "national technical means" of reconnaissance. Precision-guided munitions used during the Vietnam and Gulf Wars cut down the number of human-flown sorties needed to destroy well defended targets and word processing cuts down the need for clerical staff in the Pentagon.[44]

The use of machinery in industrialized armies generally has taken the form of the mass production and large numbers of machines and very large numbers of people to operate them. Computers provide the qualitatively different option of reducing the number of humans in combat yet keeping or adding to the functions they have performed.

So, in an environment where arms control and disarmament get lip-service, we may expect to see a comprehensive, IT-based, re-arming of the United States. One of the major features will be the substitution of computers for many things, notably people. This is a near certainty, regardless of who wins the internal battles in the Pentagon. The computerization will take many forms ranging from digitally rebuilding existing platforms, to greater qualitative and quantitative changes in the way we conduct military operations, for example, the replacement of traditional forces with stand-off, precision weapons integrated with extensive sensor-based intelligence and targeting systems and remote battlefield-management systems.[45]

Having said this, it is by no means clear exactly how IT-based systems are going to be used across the spectrum of prospective conflicts and operations. As we have seen, high technology systems have often proven either unnecessary or less than decisive in a mixed bag of wars and other operations outside of the mainline superpower conflict. A wide range of possibilities and real difficulties exists.[46] The rest of this section offers a few basic observations and proto-conclusions. These fall into four categories: (1) the lack of broadly viable alternatives, (2) coverage of the demand-pull-driven conflict and operations spectrum, (3) increased U.S. vulnerabilities, and (4) selected policy issues.

Lack of alternatives. In one way or another, IT-based systems are going to play a central role in any U.S. military posture. This is because they already do, because the mind-sets and precedents are well-developed for the many reinforcing reasons discussed in section 3, and because such use derives from more general U.S. economic and technological strengths. There is little in the way of broadly applicable alternatives, given the combination of national goals, strengths, and constraints. Budget limitations, and the relatively low values the American public would place on parts of the potential conflict and operations spectrum, do not permit other approaches that require the frequent use of large numbers of people.

Conflict coverage. Considering the prospective foreign encounters involving the use of the U.S. military, and the set of technological and doctrinal legacies from the Cold and Gulf Wars and those under development, one comes to the not surprising conclusion that existing IT-based systems best prepare the United States for conflicts that look like the Gulf War with modest sized type (a) adversaries. The value of current and new near-term systems decreases as we traverse the set of potential conflicts from an almost ideal situation against a poor type (a) proxy for the Soviets to various forms of people-intensive OOTW.

Some parts of the post-Cold War conflict spectrum are more immediately and compellingly foreign-threat-driven than others. They include the proliferation of WMD, terrorism, drug trafficking, and some forms of information warfare (IW). The latter is primarily concerned with defensive and offensive activities in which IT-based resources–either the systems themselves or the information that resides or flows in them–are targeted.[47] These forms of conflict involve small, hard-to-find, targets that may be time-sensitive, dispersed, and located among innocent or friendly people. Foreign military adversaries are also going to learn lessons from the Gulf War and make their assets harder to find. The expensive systems the United States used to make the Gulf War battlefield more transparent than any other in history were unable to help find a few warlords in Somalia who eventually brought about U.S. withdrawal.

With a reduced global force structure and a post-Cold War conflict and adversarial set likely to stress target location and identification under difficult timing and geographical demands, there will be an added premium on IT as a "force multiplier." In essence, force multiplication requires capabilities to get the necessary force to precisely the right place at the right time, and related intelligence capabilities necessary to determine the right place and time. The prying, demanding, and unforgiving eyes of the world's IT-based news media create additional pressures on civil and military leaders that require better command and control, and the wherewithal to "do something" in response to horrors portrayed on the nation's TV screens.[48]

The information technologies, almost by definition, or at least by default, seem to be the "natural" technologies for all these functions. IT-based approaches to surveillance and intelligence have worked better than anything else in other contexts, for example, for surveillance across the vast surfaces of the oceans and the former Soviet Union. IT-based surveillance systems also performed fairly well in the Gulf War, and are likely to be improved over time so that they may be valuable in less ideally set regional conventional wars. Whether IT-based systems will prove to be of comparable importance in other forms of conflict remains to be seen.[49]

However, there is not much of a positive historical record for IT-based systems in OOTW or low-intensity conflict outside the basic communications domain. Since the systems for intensive forms of conflict do not generally scale down well, there have been calls for special nonlethal high-technology systems for OOTW.[50] It is not clear what these would be, outside of some limited possibilities with obvious narrow utility, for instance, implanting tiny microelectronic "beepers" in the bodies of pilots and others who might need to be found and evacuated from unfriendly places. What IT systems would have made a decisive difference for the Israelis in Lebanon, the United States in Somalia, the Russians in Chechnya, or anybody in Rwanda? These operations tend to be people-intensive, sensitive to collateral damage, and problematic in terms of moral and political delicacies and will. Not much should be expected in the way of substituting computers for people in many such operations.

The claims of some techno-advocates and contractors aside, the information technologies to date have not shown as much flexibility and universal applicability as might be desired. So far, IT-based systems have not generally transferred well from one level of conflict to another, or have proven brittle or ineffectual. There is not much need for F-22s or highly digitized M1A2 tank formations against type (b) to (d) adversaries. The most valuable use for so-called smart and brilliant weapons is against sizable, high-value targets. In most prospective conflicts involving the United States, it will be the combatant with the largest number of the sizable, high value targets, or perhaps the only such combatant. Finally, high-tech military systems do not have much of a record in the aftermath of a conflict. So the United States may find itself best suited for projecting a quick, long-range, hard blow against certain kinds of targets, and then it will find itself unable to deal well with the resulting mess, for example, deterioration to guerrilla or civil war, occupation, cleanup, or collapse of local authority.

Increased vulnerabilities. The enormous disparities in investments in advanced military technologies noted earlier guarantees that any conflict between the United States and any adversary will be extremely asymmetric in this regard. But there are enough historical examples to indicate that such asymmetries do not guarantee a decisive or satisfactory conclusion. Ironically, as the absolute IT and military gaps between the United States and everyone else grow, IT may be proportionately more of an equalizer for all four types of adversaries described above.

This effect comes in essentially two forms: (i) IT produces increased vulnerabilities for the United States and other advanced industrial countries, and (ii) IT provides greater empowerment for the asymmetrically weak through the use of infrastructure built by the more advanced countries.

(i) Some recent conflicts, particularly that in the Falklands, illustrate discomforting vulnerabilities of expensive high-tech platforms to cheaper, more easily diffused, less high-tech systems. It is not hard to imagine how a couple of more well-equipped, Exocet-carrying squadrons, and a couple of skillfully used, modern, diesel submarines, could have produced a different outcome in that war. A small number of Stinger anti-aircraft missiles produced an extremely leveraged effect against the U.S.S.R. in the war in Afghanistan. Similar weapons would have caused the United States enormous problems in Vietnam. No existing high-tech systems provide much in the way of defense against several forms of low-tech WMD delivery.

One can project more problems to come. As noted earlier, stealth aircraft were born from the demand-pull of penetrating an extensive Soviet air defense system. Now that form of pull is a pale shadow of its former self, and the United States has such dominant air superiority that no potential enemy could do much flying for any purpose during a conflict against it. Ironically, stealth aircraft, perhaps flying at night and armed with cluster bombs, provide potential adversaries with a viable, proportionately more valuable, and potentially very damaging counters against the U.S. threat. Similarly, modern unmanned aerial vehicles (UAVs) would be disproportionately valuable to American enemies, who could not possibly keep manned AWACS or JSTARS equivalents in the air.

Such modestly high-tech weaponry, increasingly available from multiple suppliers in a post-Cold War buyer's market, may provide an otherwise weak asymmetric combatant with serious striking power against the expensive targets of a more technologically advanced, target-rich foe. The United States is singularly well-endowed with expensive targets and singularly sensitive to losses. The situation has gotten to the point where extensive multi-billion dollar defensive packaging is necessary for the U.S. Navy to deliver two dozen attack aircraft or a couple battalions of Marines against anyplace with comparatively minimal modern technology for defending itself.

(ii) Additional problems include more vulnerable national assets that are widespread and easily accessible (for example, communications and banking systems), or because of political and social sensitivities (for instance, high-visibility losses seen by large audiences through the IT-based media).

There is an equally large set of undesirable uses of increasingly worldwide infrastructures by type (a) through (d) adversaries. Many of these problems are the consequences of the extraordinary global diffusion of IT that is unprecedented in the history of technology in terms of both its rate and its extent. These uses include dipping into the large weapons and dual-use technologies industries established by the advanced industrial countries (such as for the purchase of anti-ship cruise missiles, fissile materials, or powerful microprocessors), and the use of global telecommunications, transportation, and banking systems. The latter include, for example, global organized crime's laundering and transfer of something on the order of $500 billion a year,[51] hackers on the Internet, the widespread availability of the DoD-developed Global Positioning System (GPS) for other people's military uses, and the increasing availability of high-quality satellite imagery formerly accessible to only a few major national governments.[52]

Another kind of global diffusion-based vulnerability results from the fact that some products are no longer made in the United States, or are made here in much smaller quantities. There is concern that the U.S. military could be embargoed, or not given priority, at critical times by foreign manufacturers.[53]

There are also vulnerabilities, or what amount to additional demands to maintain existing capabilities, that take the form of IT-driven disproportionalities. These appear as requirements for countermeasures against more modest adversarial capabilities. For example, strong forms of encryption are possible with easily obtainable computing power. Breaking such codes requires enormously greater computing power, and may in effect be prevented altogether through fairly easy measures like frequent key changes. The IT needs of SCUD-like ballistic missile systems are much less than those of anti-missile systems. The use of multiple, smart, stealthy ASCMs against large ships requires extraordinarily demanding real-time computing for defense.

Selected policies. The Cold War high-technology complementary policies of running faster and controlling technology transfer were well matched to those parts of the conflict spectrum that were most imperative to avoid and deter. Now, there is no comparable adversary to run against, and the global diffusion of IT is such that most of it is increasingly beyond effective control.[54]

What may remain is the corollary policy to the effect that having superior high-technology systems prevents or contains the kinds of conflict they would decisively win, or which are most desirable to deter, or at least forces conflicts to lower levels of destructiveness. Advanced conventional weapons, it is argued, will provide a more effective strategic deterrent than WMD because they are more likely to be used, and the United States would use them in a much broader spectrum of conflicts than would have ever been considered for WMD. In a period when problems and adversaries are changing across short time scales, a case may be made (perhaps in the absence of anything better?) that IT-based systems provide the most flexible means of projecting American power and defending American interests as quickly and as hard as possible.

In attempting to apply deterrence to the spectrum of conflicts, problems arise because the possibilities are so varied and fragmented, and thus not conducive to broad matches between technology-push and threats. There seems to be a fairly good match with regard to Gulf War size MRCs. But there is not a particularly good history of past attempts to find high-technology military solutions to the kinds of difficult, grungy, tenacious people problems encountered in other conflicts. Even the hope that type (b), (c), and (d) adversaries would be properly intimidated by incomparable U.S. military-technological superiority may not last long. In Somalia, initial awe gave way to something considerably less, and warlords in one of the world's most backward places learned to use American sensitivities and IT infrastructure to drive us out. The Somalians were hardly unique in this regard. Others not long intimidated by "overwhelming" military-technological superiority include Lebanese, Palestinians, Afghanis, Vietnamese, Chechnyans, and drug cartels.

Real and spectacular improvements in technical parameters and capabilities–such as for computational power and bandwidth, often doubling values or halving costs over product cycle times of 12-24 months–have not been effectively applied to changing military operations in remotely the same proportions and rates. This has never been the case in any major applications area, and it never will be. But at no previous time has there been such an increase in the number of new technology product time cycles that fit into national security policy and doctrine time cycles. Making hardware such as faster chips is simply an easier and more focused undertaking than making the hardware serve important functions in a messy, peopled world, especially if some of the people will be seriously resistant. In addition to battlefield foes, resistance comes from many of the people and organizations who would have to absorb the new systems.

So, at this point, there is at least a temporary mismatch between technology-push, that is, the kind of high-technology military the United States may be best able to build and sustain, and demand-pull, that is, a suitable set of prospective conflicts and adversaries driving the United States in that direction. This makes existing and proposed force structure and budget levels less than obviously justified. It is thus one of the most striking changes in U.S. military affairs since the end of the Cold War.

5. Revolutions: Clapping with One Hand?

Many people believe that some kind of revolution in military affairs is or needs to be taking place, and that much of whatever it may be is enabled by the military applicability of IT. There are two other, or one combined, much proclaimed, IT-based "revolutions" going on: in business, and in American or global society generally. Common wisdom has it that major technology-based changes in the military are closely linked with those in economies and societies more generally, or that the "ways of war follow the ways of revolution." So at least in these senses the time may be ripe for an RMA. To what extent do the IT-induced revolutions in the American economy and society tell us what the next (underway?) military revolution may look like? Do they feed much technology-push or demand-pull into any prospective RMA? Are there other "revolutionary" feeders?

Given the influence of business on the DoD and the American economy, it is natural that some of the RMA thinking should explicitly echo that of the IT- and foreign-competition-driven revolution in business. The DoD is going through some of the same traumas as American business: cost cutting, downsizing, organizational and process re-engineering. Economic globalization in its various manifestations, notably foreign competition and international market and infrastructure expansions, provides a strong threat and opportunity demand-pull package for business. Responses have included extensive and deep organizational changes, such as flatter organizations with less middle management; high-tech approaches to new products, services, and processes; and many efforts to promote efficiency and cut costs. IT pervades all of these responses. American business invested $1 trillion in IT during the 1980s, and investment remains high halfway through the 1990s. Remarkably, considering the extraordinary bottom-line orientation attributed to American businesses, there is still no clear verdict on what $1.5 trillion in IT investment has done for productivity or other quantitative measures of success over the last 15 years.[55]

Thus American business may provide the DoD with models, experience, detailed examples, and some unresolved questions. However, there are significant differences between defense and business,[56] many of which, of course, relate to differences in adversarial relations. For example, business may do well to invest in a few high-cost, reliable facilities like a semiconductor manufacturing plant in order to benefit from economies of scale, or to use cheap foreign labor. As competitive as international markets may be, few businesses expect the competition to try to physically destroy their facilities, so they do not build in redundancy or take other factors into account to protect against physical attack. That is usually not the way wars work. Nor would the United States seek to build its own army out of foreign troops. The most striking difference between the business and DoD technology-fed revolutions is that the DoD is scrambling because of the loss of its comparable foreign adversary, but business is trying to respond to the global diffusion of both expanding markets and more capable competitors as demand-pull drivers.

The greater emerging American, and increasingly worldwide, "information society" that is the outcome of the "information revolution" lacks a widely accepted precise characterization.[57] For our purposes, a central fact is that the massive and continuing infusion and diffusion of IT is changing the ways many millions of people spend their time at work and at home, and the ways they entertain themselves. IT is changing how people and organizations function, and how wealth is being created and distributed. This is happening on such a scale that a case can be made that it constitutes a revolution, just on the basis of the fraction of the nation's total person-hours spent in one way or another with IT in all its forms. The rate and extent of development and diffusion of IT to fuel something so diverse on such a large scale has been nothing short of awesome. With the possible exception of the advent of the internal combustion engine, no preceding military revolution has had so much technology to use so pervasively.

So the American economic and social information revolutions are generating the technology-push means for a sweeping, ambitious, expensive, and so-far not very clearly defined MTR or RMA. Any such revolution would also produce a military establishment more “in sync” with its societal surroundings. But the military and national security community more generally should not be free to simply follow the best business practices or grow and change similarly to society as a whole. They are charged by that society with the basic mission of protecting it against foreign threats. The American polity may not long be tolerant of paying hundreds of billions in tax dollars simply for military systems with impressive performance characteristics that are built and used with more efficient business practices. These systems must clearly be capable of advancing national interests and of addressing credible foreign threats to the national well-being.

Past military revolutions came complete with balance on the demand-pull side of the equation. Previously, countries leading an MTR or RMA had to contend with other nation-states, with comparable resources, picking up on the same technologies and applying them to comparable military forces. For example, Great Britain’s path-breaking use of a confluence of technologies to produce dreadnoughts, thereby changing the character of naval warfare, soon produced similar developments in the United States, Japan, Germany, and elsewhere.[58] American and Japanese naval thinkers who used the breathing period between the world wars to work out the then-revolutionary future of carrier-based warfare had a good notion that Japanese and American fleets would be fighting in the deep waters of the Pacific. During the same time, the Germans who brought the world the military-technological blitzkrieg package also had a strong sense of where, and against whom, it would likely be used. So did the U.S. Marine Corps thinkers who developed the essentials of amphibious warfare. All were thinking in terms of major, focused conflicts, with huge geostrategic stakes. Before and during World Wars I and II, and during the Cold War, there was no lack of comparable military-industrial powers building and modernizing military forces and doctrine on the basis of then-advanced technologies. These national powers had similar understandings of what military power could do to advance national interests.

The current situation is different. Nation states comparable to the United States with comparable military-technological efforts or interests are notably missing. The current high-profile quest for the next military revolution has a hollow ring to it because of the imbalances on the demand-pull side of the equation. Militaristic states like North Korea or Libya just do not cut it in the same ways as Imperial or Nazi Germany, Imperial Japan, or the Communist Soviet Union. No armed forces of an advanced industrial nation are remotely comparable to those of the United States. Some analysts are working hard trying to make the Chinese or Iranian armed forces into near-term, credible, near-peer-level threats to the United States. However, even with today’s downsizing and excluding close allies, the DoD may be outspending the rest of the world put together on advanced military technology.

So the United States has the technology-push capabilities to pursue a major IT-based RMA. But there is little in the way of traditional prospective peer foes or foreign missions driving it to this end. Is this, then, a solution without a suitably challenging problem?[59] Is the undertaking tantamount to clapping with one hand?

Let us briefly consider two current, IT-specific approaches to the search for a second hand. First, what threat concerns emerge directly from the civil information revolution? Second, how might the United States unilaterally pursue an RMA that would provide a coherent set of capabilities to address the unprecedented threat circumstances?

What does the civil information revolution generate in the form of national security concerns? What possibilities relate most directly to the prospective adversarial set discussed in section 4? The infrastructure being created to support the information economy and society amounts to a substantial and expanded medium for conflict, and one to which almost anyone can obtain access. This situation makes for an enormous new playing field for adversaries who do not play by the old rules of nation-states. It also makes for the more extensive worldwide dispersal of American people and interests, and those of allies, which may have to be defended. The accompanying global diffusion includes comparatively small amounts of advanced technologies, which are, nevertheless, enough to enable disproportionately great leverages against the United States by what would otherwise be militarily weak enemies. All of this is visible enough to make impressions on many people around the world who are left out or alienated by what they see, or who have other agendas not compatible with American interests.

If the United States increasingly has an information economy and society, then where are they located? And who will defend them? The IT-based medium is now the locus of an enormous quantity and variety of American assets, the means for transforming and moving these assets around (often adding value), and also the place for conducting an increasing amount of economic and social activity. These developments are becoming more important to other countries, including most allies, as well. As such, cyberspace is also becoming a zone for serious conflict. The broad set of possible adversaries who want to take advantage of American assets in undesirable ways will go after what they want where it can be found. It is no longer exclusively located in the traditional geophysical zones of conflict: land, sea, air, and space.

Traditionally, the U.S. military has been concerned with protecting American people and property against threatening foreign military forces operating in the geophysical media against Americans and American assets located there. The collective IT-based medium arguably is itself a different, but significant, additional medium for conflict. A case can be made that the nation also needs to be defended in cyberspace, in other words, that assets and passage need to be protected as is done with the other primary loci of conflict. In addition to defense, growing IT dependencies among adversaries provide offensive opportunities against others. So here is a vast and rapidly expanding new medium for conflict, with a complex and growing potential adversarial set.

We do not yet understand the extent and forms of the problems, risks, and threats faced, although this has not prevented a good deal of hype and speculation on the subject.[60] The border-based factors that have traditionally defined defense responsibilities get very fuzzy. Some borderless adversaries thrive on taking advantage of the border-based constraints of the old world order. Domestic laws and international agreements are notably lacking. Jurisdictional and enforcement questions abound, with little in the way of answers. It is not even clear what would be appropriate responses to attacks by very asymmetric foes. Risks are low, and deniability and payoffs are disproportionately high for small, stealthy groups with newly enabled long reaches who may or may not be working for foreign governments or type (c) entities. It is at least clear that cyberspace provides expanded access to more U.S. assets by more foreigners than has ever been the case before, and that the traditional sanctuary of the geographical United States is not what it used to be.

Broadly speaking, much of this conflict might go under the heading of information warfare. In spite of the apparent potential magnitude of the problem, its qualitatively different features from other forms of conflict, and the use of the term *warfare,* how much of a "second hand" IW provides for an RMA remains to be seen.[61]

The DoD certainly has a major direct defensive interest because it has extensive assets as potential targets, notably including all its C4I systems. These vulnerabilities are increasing as IT continues to be rapidly and pervasively infused into the U.S. military establishment. The military has a direct interest in the well-being of the national infrastructure, since 95 percent of normal DoD and the intelligence agencies' voice and data traffic use the public channels, and such use would likely be expanded during crises.[62] Although much of the overall U.S. military structure is highly dependent on IT, little of the current force and support structure would be directly involved in IW, except perhaps as targets. Moreover, it is likely that most of the defensive responsibilities on a national scale will ultimately fall to nonmilitary organizations, including nongovernmental groups like the telecommunications providers, and to those most directly threatened. Forms of self-defense, such as more seamless encryption and other computer security measures, might extend to every user level, down to individual citizens in their homes. In contrast to the public attitude to national defense in the geophysical media, many of those potentially threatened might have problems with too much of a domestic DoD (or other government agencies') role in the defense of this medium and concerns about intrusions into privacy.

Offensive IW against the IT-based assets of adversaries would also not be in the exclusive domain of the DoD, although there is clearly a large role for the military in existing and growing forms of IW, such as EW or command and control warfare. In the offensive IW arena, too, little of the existing military organization would participate, and large U.S. forces would not be created to pursue such conflict. There is not likely soon to be an equivalent of a new, full fledged army, navy or air force, for this medium.

A case can be made that the global diffusion of IT and the attendant information revolution have been such that technology is increasingly available in enough forms for even small and backward entities to deter or inflict what may be serious damage on the United States. The preceding sections contain a number of examples. None of them has as much destructive or deterrence potential against the United States as WMD. But significant new possibilities exist, and most have low thresholds for use before or during conflict, for example, attempts to damage the U.S. civil infrastructure, or new intelligence opportunities for foes as the United States fills up the multidimensional battlespace with information that could be valuable in the wrong hands.[63] But some of these systems, and American tolerance for damage to them, may be more robust than threat speculators think. The systems and the prospective threats are not yet well enough understood to tell, although the possibilities are so extensive that it seems likely that nasty surprises are in store for the United States.

It might be possible for unfriendly entities to do hundreds of millions of dollars worth of damage to American interests through IT-based attacks or use. It may even turn out that IW in its various forms will eventually become a form of perpetual warfare directly affecting the civil population of the United States, and will have to be dealt with on a continuous basis like terrorism on the streets in Israel. However, cyberspace does not generate enough demand-pull to justify much of a military force on its own, much less a large fraction of a $250-300 billion defense budget.

What if the United States pursues an RMA but nobody else follows suit to anywhere near the same extent?[64] How is an RMA accomplished without peer-level military competition?

Much of the perceived foreign threat and potential spectrum of conflicts and operations is now being created by fertile imaginations in the United States, rather than by enemies abroad. In the absence of compelling, concrete, peer-level, attention-grabbing military threats, and with the proliferation of so many lesser and poorly understood possibilities, significant parts of the U.S. defense community are now generating a “second hand” on their own. This pursuit of a suitably motivated military revolution is proceeding almost unilaterally, hopefully anticipating threats until the time when real foreign demand-pull catches up.

The net result is that the U.S. national security establishment is putting together a large set of threat scenarios whose sum is likely greater than that of the real (but so far perhaps embryonic, unseen, or unappreciated) threats that will show up in the future. Just enough real history of these forms of demand-pull exists to make longer term worries plausible. Almost everyone groping around in the pursuit of a military revolution is participating. This includes everyone from the armored forces people who think the future holds more massive tank battles with regional military powers, to the defensive IW people.

The latter exemplify a group who see their interests as necessary parts of an RMA, but who do not have much in the way of traditional conflict histories to support their views. Their problems go beyond those faced by other newcomers in military-technological history, such as the strategic bombing advocates after World War I. The current problem is more complicated than a debate as to whether long-range guns or airplanes are better suited to destroy ships, buildings, or the will of the enemy to continue to fight. The IW people have to make a case for new forms of threats and warfare in a new medium where there has been little so far in the way of suitable, visible, verifiable threats and targets. They must also make the case that they understand the threats well enough to cope with them and elevate those threats to compete with other, more traditional and visible military concerns. Absent some form of “electronic Pearl Harbor,” without generating, simulating, or extrapolating suitable threats from bits and pieces of real world instances, little danger will be perceived by other national security constituencies.

The scale and diversity with which such demand-pull is being pursued is unprecedented. This is the result not only of the unusual situation of, in effect, not having choices made for us by peer-level military competitors, but also of the enormous geographical and operational spectrum of possibilities that might conceivably deserve consideration. In addition to its other roles in defense, IT has become increasingly pervasive in the threat conjecturing, modeling, and response training process. Increasingly, much of this process occurs through computer-based simulations.

This combination of a dramatically changed threat environment, the response of self-generated demand-pull, and the use of IT to enable pursuit of the latter in so many ways is itself a key element of the IT-based MTR. The United States is building IT-based simulation capabilities to construct and exercise many scenarios. Computers help substitute for enemy soldiers and systems (as well as our own) and thereby provide at least a virtual second hand. At one end of the scale, it includes very detailed physical modeling of weapons system performance in complex and hostile environments, as in a ballistic missile interception. At the other end, it includes modeling global political-military conflict scenarios, as in the war games played at Newport involving hundreds of role-playing participants. Just about everything in between is also possible, one example being the laser and computer system enabling brigade-sized combat field exercises at the National Training Center. Someday, commanders about to be shipped to someplace they have barely heard of will be able to “drive” their vehicles down accurate simulations of beaches or roads in those places, plan their operations “on site,” and at least partially neutralize the terrain knowledge advantages of local adversaries. First class “enemies” can be generated from fertile American minds to provide opponents who will stress any level of U.S. command in ways that were not possible a dozen years ago. Joint or coalition command and control structures that have never been put together may be simulated and worked out before the unit configurations are assembled. Networking technologies potentially provide great expansions of scale and access. The U.S. is turning these overall capabilities into a pronounced asymmetry in comparison with the military of any other country.[65]

Arguably simulation is part of what the defense community should be doing in an effort to restore more balance between technology-push and demand-pull. It should be done from the standpoints of both seeking to justify relevance and resources, and improving the likelihood of anticipating and being able to deal with what may eventually have to be confronted. In a suitably competitive environment, one tempered by emerging international pressures and budgetary stresses, the two standpoints should complement each other during a controlled defense draw-down in a still-worrisome world.

However, there is something mechanistic about the way a large part of the spectrum of RMA visions represent adversaries, partly because of the simulations. There may be too much focus on a single, decisive engagement on the traditional battlefield. Much of what is seen in the

> …concept of war under the MTR/RMA banner resembles a shooting gallery, a static firefight in which superior U.S. firepower is concentrated on a relatively defenseless opponent. The objective, similar to that in the Gulf, is simpl[y] to win the firefight, to break the enemy force, leading to a return, more or less, to the status-quo-ante.[66]

The most frequently specified proto-enemies tend to look like the forces of Iraq or the former Soviet Union. These enemies do not persevere; they do not “take a licking and keep on ticking.” The resources, resourcefulness, staying power, and tenacity of most nation states, or other powerful foreign entities, may often be undervalued.

There is an ironic reversal here. In the mid-1940s, defense demand pulled computer technology out of a near void. Today, with a partial vacuum in defense demand-pull, computers are being used to help create another hand's worth of foreign threats within the confines of the U.S. national security establishment.

6. Remaking Defense?

With the end of the Cold War and the explosion of IT applications in the American civil information revolution, there is a mismatch between technology-push, that is, the kind of high-technology military the United States may be best able to build, and demand-pull, namely, a suitable set of adversaries and missions driving us in that direction. Yet the momentum of the infusion of IT into defense continues and has perhaps accelerated for a variety of reinforcing reasons discussed in sections 3 and 4. The spectrum of conflicts and other missions the United States may want to or have to deter or successfully conclude has changed significantly, but it is questionable whether the intensive pursuit of so much high technology in the military provides either substantive or cost-effective coverage.

Many important existing and proposed force structures, budget levels, and acquisitions are thus less than obviously justified. Does the defense establishment need an IT-based MTR or RMA to remake itself to deal with what is clearly the most striking change in U.S. military affairs since the end of the Cold War? Is the quest doing much to help provide the United States with $250-300 billion worth of national security against a credible and hefty conflict spectrum?[67]

During the Cold War, defense tasks could be divided into three missions: strategic nuclear war with the Soviet Union (a very hefty potential conflict), conventional war (the prime example being a massive Warsaw Pact attack on Western Europe), and unconventional war (mainly guerrilla, covert, and intelligence warfare with communist adversaries). Most of the American defense budget went into the second category, with far less going to the first, and the relatively small remainder to the third. This was not a bad balance. We worried global nuclear war to deterrence and stalemate; did not do well with unconventional war (or, in the most singular case, tried to turn it into conventional war in Vietnam); and prepared to deter or fight conventional war. The latter was arguably the mission that maximized the combined factors of probability of occurrence and geostrategic importance to U.S. national security.

As discussed in section 2, one heavy infusion of IT into the U.S. military is far along, and was well-integrated with the defense tasks of the Cold War. It started during World War II and has rapidly accelerated since the early 1980s. This infusion was both bound to the nuclear-based RMA and also had a life of its own. Over the course of the Cold War, it arguably amounted to more of an RMA, rather than an MTR, because it had substantial effect on how nations related and behaved with regard to the use of armed force for national purposes. This effect is most evident in how the United states and the U.S.S.R. played the same competitive game and assessed each other's capabilities, and ultimately in both essentially deciding that the United States had won the mainline military-technological confrontation. Fortunately, this confrontation was conducted mainly through a cold war of arms races, perceptions, and minor engagements rather than a hot war that would have severely exercised all of the unproven and fragile IT-based systems on both sides. That cumulative change is evident in comparisons between the composition and operations of the U.S. military of 1991 with that of 1941 or 1971. The differences are also apparent in comparison with any other military force in the world.

What has become of these national security tasks in the mid-1990s and will become of them in the early twenty-first century? The threat of global nuclear war between large, technologically sophisticated forces has been greatly reduced, supplanted by much different and more modest worries about WMD proliferation. There is even less motivation to fight unconventional wars now that they are unconnected to global military and ideological conflict. The national security of the United States cannot easily be tied to such warfare. And the United States and its NATO allies have little in the way of near- or intermediate-term plausible enemies for conventional war at the world-war levels that justified their Cold War forces. An MRC on the scale of the Gulf War, with similar geostrategic importance (and perhaps approximate location) remains a consideration.

What of the new or growing forms of demand? Despite the rhetoric or embrace of OOTW, or, more generally, operations short of a conventional MRC, it is hard to construct a convincing set of such missions that is worth a large fraction of a $250-300 billion annual defense budget. The geostrategic, economic, and national security justification of one or two Somalia- or Haiti-type operations a year over coming decades is weak. The case for billions more for high technology for such missions is even harder to make. As for dealing with the vulnerabilities created by the civil “information revolutions,” and type (c) and (d) threats (transnational crime, network warriors, and such), these are not missions for which militaries are well trained or well placed to perform. Whether or not another few billion dollars goes to the FBI, DEA, Treasury, or CIA to deal with these threats is one matter, but putting this much, or more, into the military for these purposes begs a convincing argument. There is a growing demand-pull case for IW and the defense of IT-based national and military infrastructures, but this does not constitute demand for an RMA on anything approaching the scale of projected defense budgets.

Circumstances are much different from those that prevailed after World War II. Then, technological developments–nuclear weapons in particular–so clearly dominated possible war between two very large, global military powers that the technology essentially dictated an RMA by itself. The information technologies are driving a revolution in the ways nations and other large and small international or transnational entities relate and behave in the economic, political, and social spheres. But IT does not provide such self-evident dominance across the spectrum of military conflict in today’s and tomorrow’s messy world. One has to work harder to find reasons for so much infusion of expensive technology into defense under such changed threat circumstances.

The last question of this essay must therefore be: Is there a demand case for an IT-based RMA, or at least a continued MTR?[68] Three possible answers can be cobbled together from the observations and arguments of the preceding sections.

The first is straightforward. As long as the United States has conventional forces, they should be made more cost-efficient, lethal, and functional for their primary missions, dealing with the overt military actions of other states or international entities. Left to their own devices, the conventional warfare and administrative parts that make up a great majority of the DoD will continue to contend among themselves and spend as much as they can get from Congress to aggressively apply IT, for all the reasons discussed in sections 3 and 4. Successive generations of military systems will become more IT-intensive, and computers will be substituted for American soldiers, sailors, and airmen. Demand will be cited on the basis of the now-modest set of real type (a) and (b) unfriendly entities, or simulated possibilities.[69] The quest for a transparent future battlefield, U.S. "battlefield omniscience", and winning the information war may be used to justify an overarching revolutionary banner.

This likely will be a continuing form of MTR. Rhetoric aside, the U.S. conventional military is not likely to create much of an RMA because they do not see a threat problem that a sweeping RMA is necessary to solve. The wrenching changes that institutional revolution may require to meet more demanding threats tend to be avoided when not driven by necessity. Right now, budget cuts, and the human and organizational difficulties of effectively absorbing the continuing infusion of IT are enough wrenching change for most.[70] Potential adversaries are far behind the United States in any thrust to a technology-based MTR or RMA, and do not provide much of the traditional prodding in this regard. Changes in how the United States goes to war will be evolutionary although, as was the case during the Cold War, the cumulative effects of so much technological infusion and integration may prove revolutionary.

Desert Storm showed that the United States could take a high-technology military force built to fight a conventional or minimally nuclear form of World War III and use it spectacularly to win an MRC in the Third World. Much of what is being done in the Pentagon, either within the separate armed forces or under the now-emphasized "joint" and "coalition" banners, appears intended to continue to provide the capability to fight this kind of MRC (or 1.5 to 2 of them simultaneously[71]) at almost World War III prices. Something appears to be wrong. A combination of the following possibilities seems to pertain:

- The United States should be leveraging technology more efficiently to pay much less for much less value to its national security;

- The United States greatly underestimated what it would have taken to fight a conventional World War III and fortunately did not have to find this out the hard way;

- It is getting to the point where no single postindustrial society can afford to continuously maintain a ready, high-tech-based, military to do most of the work in a remote MRC, even against a technologically inferior foe;

- The United States is explicitly deciding to unilaterally provide itself with a very expensive military to enable it to respond frequently with military assets to an expanded set of politically or media driven and constrained foreign missions involving little direct threat to national security. (This possibility is considered more explicitly in the third answer below.)

Second, what of longer-term peer or new forms of threats? Although no peer threat exists now, one may emerge in the long term. Therefore the United States must maintain a viable military core, a watchful eye on the rest of the world, and long-term programs, so that there is a foundation for a more capable military force and military-technological industry than any prospective peer threat could produce. This argues for the intellectual spade-work and many forms of experimentation for what might become an RMA. The United States now has enough advantage and lead time over any prospective peer threat to continue to do this without the urgency and at a fraction of the cost now being pushed.

Almost by definition, the more embryonic demand areas are modest in budget size and footprint across the current defense establishment. IW is one of these areas, and it is trying to emerge from the current hype and campaign for recognition in the internal Pentagon wars. Part of the tactics for recognition is to try to find a leadership role in the charge for an RMA. A relevant general question is whether IT can be used to create significantly new tools of national military power that simply cannot effectively exist without the technology. Criteria might include the ability to influence, more through information than firepower, a variety of distant conflicts without extensive direct American involvement.[72]

The third answer is aggressively internationalist, explicitly arguing that the revolution in foreign demand-pull circumstances requires an MTR or RMA. In this case, the United States would like to promote an as-yet unclear new world order that is conducive to its interests. So far, in spite of an early post-Cold War euphoria over the spread of democracy and economic well-being, this new order has been slow in identifying itself and has suffered many setbacks. In the meantime it is in U.S. interests to prevent the breakdown of too much of the old world order, and to protect itself and others from emerging threats.

To this end, a strong form of unique superpower military capability is arguably necessary for deterrence, coercion, containment, or enforcement of last resort. Such power is also necessary as the only candidate for the nucleus of international coalitions for MRCs and other large-scale missions. Even if most current strife or potential conflicts around the world are not seriously and directly threatening to U.S. national security, if too much of this goes on, it will weaken world order over the long term, and that would inevitably lead to serious national security problems. In American eyes, the existence of additional military superpowers would not provide a useful form of checks and balances, but would be unnecessary and also undesirable as a likely source of much greater problems in the long run. To preserve or promote this view of world order, the U.S. defense establishment needs a suitable military force, and the U.S. taxpayers are the unilaterally chosen people to foot most of the bill.

In this context, DoD is faced with much decreased physical threats, and the clarity of the remaining and emerging threats is foggy. The threat spectrum is made up of more diversified potential adversaries, and is truly worldwide, “fuzzy”, and “difficult to explain to the average American.”[73] So the overriding DoD task is to provide the United States with an armed force that can be used to respond to a variety of changing threats and missions under historically unprecedented demands and constraints. Some of these demands arise from generic considerations of the likely missions, for instance, the need to rapidly take effective military force to anywhere in the world, and the desire to have much improved joint and coalition operations. They also include the need to be able to deal with any emergent peer military power that might arise. Other constraints are self-imposed by American politicians, society, and the news media. They include the needs to have almost no American casualties, to bring any shooting conflict to a rapid and successful conclusion, to avoid collateral damage, to look good on TV, and to do everything efficiently and at lower cost. These constraints are perceived as necessary to keep the taxpayers' interest and support, or at least their acceptance.

Simply scaling down the Cold War force structure is arguably not the best way of trying to cope with this tasking. The U.S. military has to deal with a revolutionary new set of foreign threats and missions. That usually is a self-evident reason to pursue an MTR or RMA. But the current change in demand-pull has resulted in reduced threats and smaller missions, most likely against adversaries who would be at far greater technological disadvantages than the U.S.S.R. in the Cold War. The imposed constraints essentially prohibit the military from responding in manpower-intensive ways, and dictate unprecedented protection for anyone who may be put in harm's way. The net result of these demands and constraints makes for very peculiar circumstances for a military revolution.

Advocates of this third answer might argue that the only recourse under these circumstances is to respond with technology, a general approach that was well established during the Cold War. The most broadly applicable and available technology at hand is IT. In theory at least, IT does help address most of the demands and constraints. For example, the electronics-based quest for a transparent battlefield, with the hoped-for ability to rapidly bring one weapon to bear against one target, with high precision and probability of kill, supports the apparent need for a short battle with minimal casualties and collateral damage. All the disappointments, unproved systems, the lack of other players using the same script, and all the other problems discussed throughout this study notwithstanding, this may be the only broadly viable approach the U.S. military can take if they are going to be expected to deliver results and be held accountable under the postulated overarching defense and foreign policy umbrellas.

Abbreviations and Acronyms

ASCM – Anti-Ship Cruise Missile

CoCom – Coordinating Committee for Multilateral Export Controls

COMINT – Communications Intelligence

C4ISR – Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance (the current maximum sequence; predecessors include: C2, C3, C3I, C4I, and C4I2).

DoD – U.S. Department of Defense

EW – Electronic Warfare

GPS – Global Positioning System

HPC – High-Performance Computers/Computing

IW – Information Warfare

LDC – Less-Developed Country

IT – Information Technology/Technologies

MNC – Multinational Corporation

MRC – Major Regional Contingency/Conflict

MTR – Military-Technical Revolution

NGO – Non-Governmental Organization

NIC – Newly Industrializing Country

OOTW – Operations Other Than War

R&D – Research and Development

RMA – Revolution in Military Affairs

WMD – Weapons of Mass Destruction

Notes

[1] This definition is used elsewhere in academia and industry. The scope of this paper might be extended to include microelectronics more generally, various satellite and sensor technologies, robotics, certain office equipment, and the broadcast media in the (rapidly decreasing number of) cases where such systems do not include any computers. However, there is no convenient term for this larger aggregation, and there would be instances when disaggregation would be awkward in the context of this study.

[2] Michael May has given a similar short characterization of nuclear weapons: they made it possible to inflict massive destruction faster and more cheaply than before. Such short characterizations almost seem to trivialize these exceptionally important technological developments, but they do arguably capture their essence.

[3] Roughly, an *industrial* military is one based on weapons and infrastructure that essentially reflect the industrial revolution and society. This more-or-less describes the U.S. military from the mid-Civil War to the Vietnam War. Some characteristics include large, conscript armies using mass produced, mainly mechanical, weapons. Other writers use *modern* or *second wave* essentially synonymously with *industrial*. Similarly, *pre-industrial (premodern, first wave)* refers to agrarian societies and militaries, and *post-industrial (postmodern, third wave)* to those societies and militaries that have been transformed by the *information revolution*. Given the extent of today's global diffusion of arms, any so-called *preindustrial military* is equipped with at least *industrial* automatic weapons, light vehicles, etc., and perhaps some more sophisticated IT-using weapons such as anti-aircraft missiles. One might try to more explicitly define a *postindustrial* military or defense establishment as one at least half of whose members are primarily *information workers*. The U.S. Department of Defense probably meets this criterion, which is based on a commonly used definition of an *information economy* (Porat 1977, 1978). The *waves* terminology was popularized by the Tofflers, most relevantly in (Toffler and Toffler 1993).

The best available single volume history of technology in military affairs may be (van Creveld 1989). So far, little has been written on the macro-history of the military use of computing. Respectable technical histories of several important early systems and projects may be found in the *Annals of the History of Computing*, a journal of the Institute of Electrical and Electronics Engineers.

[4] (Nitze 1994).

[5] (Ricks 1995).

[6] The abbreviations *MTR* and *RMA* are often used generically and interchangeably to denote whatever an author thinks a given vision will eventually produce. (Cooper 1995) defines and ranks MTR, RMA, and RSA (Revolution in Security Affairs) by increasing comprehensiveness and macro-impact. As might be expected with trying to discretize what is essentially a continuum, the exact point when incremental change becomes "fundamental" can be endlessly debated.

[7] Both the national security and IT communities of scholars and practitioners are filled with more than their shares of jargon, picky details, abbreviations, and acronyms. The combination of both sets of alphabet soup is potentially appalling. However, I have made a determined effort to keep to a minimum, to facilitate the reading comfort of the wide audience this study addresses. A short appendix of abbreviations and acronyms is provided, as well.

[8] Some important issues that could have been included under the wideband title of this study are not considered or are only touched on minimally. For example, flows of information are fundamental to the effectiveness of any organizational structure. Military organizational structures have historically been mostly hierarchical for many good reasons. However, some argue that the military of the future needs to be more intelligence-based and decentralized, that such functions are better supported by flatter and more networked organizational structures, and that IT is now available to make both the functions and more appropriate organizational structures possible.

[9] The term *cyberspace* is commonly used to describe the medium of the Internet. However, the Internet does not constitute the totality of the IT-based media; for instance, it does not include important parts of the world's military networks and C4I systems. Because there is no well established term for the entirety, this article uses *cyberspace* by default.

[10] The histories of nuclear and digital computer technologies have initial parallels that eventually diverged orthogonally. Both matured into viable and militarily important products as a result of isolated, protected projects during World War II. The atomic bomb project was a massive undertaking that culminated in the dramatic and enormously destructive war-ending explosions at Hiroshima and Nagasaki. The much smaller project for the ENIAC, the first all-electronic, digital computer, at the University of Pennsylvania, had the more modest and much less dramatic goal of producing artillery firing tables, and the computer was not fully operational until the war was over.

After the war, nuclear weapons became the highest profile element in the American and Soviet arsenals, and the peaceful uses of "limitless" atomic energy in the forthcoming "atomic age" were widely discussed with great expectations. By the early-1950s, there were still only a few digital computers in the world–including a noteworthy Soviet computing effort (Crowe and Goodman 1994)–and forecasts of the numbers needed were in the single and double digits. For a history of the early influence of the U.S. military on the development of computing, see (Cohen 1988).

Today, the nuclear legacy is an unhappy one, without the extensive use of peaceful nuclear power that was once predicted. It includes serious accidents and safety problems at nuclear power plants, a Cold War residue of tens of thousands of nuclear weapons, discomforting prospects for their safe disposal, and frightening possibilities of nuclear weapons proliferation. In contrast, since the early 1980s, computers and other forms of IT have become the world's technological "darlings" with hundreds of millions of computers in use, more at the personal level than were imagined decades ago, and with IT at the center of visions of a revolutionary societal era comparable in importance to the agricultural and industrial transformations so important to the history of humankind. It remains to be seen to what extent, and it will happen to some degree, the "information revolution" will turn sour.

[11] For descriptions of early Soviet computing capabilities, see (Rudins 1970, Davis and Goodman 1978, Goodman 1979, and Crowe and Goodman 1994). Most East European members of the Warsaw Pact also had nontrivial (given their sizes and economic conditions) computer development efforts during the 1950s. For a description of the eventual partial integration of the Soviet and East European industries, see (Goodman 1984, and Geipel, Jarmoszko and Goodman 1991).

[12] For example, a statement of how this strategy was applied to Soviet naval developments:

> the way to deal with the increase in Soviet surface ships is by a combination of greatly improved ocean reconnaissance, so that we can locate Soviet ships at sea, and by greatly increased deployment of anti-ship cruise missiles. By the same token, the way to deal with our numerical disadvantage in submarines is not by doubling or tripling the number of submarines we have in our force, but by continuing to exploit the very great advantage that we have in submarine

> detection. By combining the technology of very sophisticated processing of underwater acoustic signals, we are able to detect and locate Soviet submarines at ranges several times greater than they can detect our submarines.

Similar statements were made about dealing with the full range of Soviet military capabilities (Perry 1984, 9-11).

[13] The last two quoted terms are from (Kaminski 1995).

[14] The ARPANET, started in the late 1960s, was fully "civilianized" by the mid-1980s, and was the source of the development and first large-scale working proof of much of the technology upon which today's global networks are based. It is inconceivable that any other military in the world could have had such a role in the creation of what has become one of the most remarkable grass roots technological diffusions in history.

Another general, high-value, military utility is the Global Positioning System (GPS) for very precise position location and related functions. This system would appear to be useful to almost all of any potential conflict and operations spectrum, including most intelligence, counter-proliferation, and counter-terrorism, operations. Like the Internet technology, GPS is an IT-based "gift" to the entire world from the DoD, one with extensive utility beyond military applications.

[15] This transformation did not take place uniformly across the spectrum of IT. For example, supercomputing continued to be relatively much more strongly driven by national security applications, especially for communications intelligence and nuclear weapons, than other forms of computing.

We might note that tens of millions of comparably powerful computers and microprocessors are now manufactured each year. Intel alone expects to produce over 30 million microprocessors a year in 1995 and 1996. A very small fraction ends up in defense systems.

[16] (Economist 1995a).

[17] (Goodman 1985).

[18] (Goodman 1990). Activeness is a measure of the degree of participation of the source in the transfer. In more active transfers, the source is available on a teaching and feedback basis that continues until the receiver successfully absorbs the technology. The most passive technology transfer mechanisms do not have any feedback participation by the source, for example, reading the open technical literature. Sometimes a passive source can be made more active, for example, by using the Internet to contact the author of a paper to obtain some clarification. The terms *overt* and *covert transfer mechanisms* refer to the degree to which the source is knowledgeable that the transfer is taking place and the legality of the transfer from the standpoint of the technology-originating country. Active and covert transfers are possible, for instance, when knowledgeable engineers work with a foreign government to pass technology without their employing company or national government knowing of the transfer.

[19] There are cases of effective technology transfers. For example, the combination of intelligence acquisitions and illegal imports of sophisticated computerized machine tools from Japan's Toshiba resulted in significant quieting of Soviet submarines.

[20] (Davis and Goodman 1978). Many covert transfers involved considerable delay and additional cost. For example, the ALMAZ enterprise near Moscow, maker of the "Soviet Patriot" S-300 missile among other things, tried to acquire covertly a large printed circuitboard manufacturing system

through European intermediaries. After the Soviets had spent at least two to three times the normal cost for the system starting in the mid-1980s, the system had yet to successfully produce any boards by the end of 1991 (and the end of the Soviet Union).

[21] Starting in the late 1970s, part of the Soviet response to what they were seeing in the United States was the impotent rhetoric and theory of the Military Technological Revolution (MTR). Earlier forms of ineffectual rhetorical and theoretical responses to American IT in the Soviet Union and Eastern Europe were concerned with cybernetics in the 1950s and 1960s, and with the so-called Scientific Technological Revolution starting in the 1960s. Well after the musings about cybernetics declined in the United States, the Soviets were still creating or continuing such entities as entire Institutes of Cybernetics. Perhaps for want of more concrete forms of IT-based threats, the Soviet MTR became part of the demand-pull for the U.S. intelligence community. An irony is the current use and fascination with terms like *MTR* or *RMA* in the U.S. military and national security communities. (FitzGerald 1994) provides a recent description of some of the content of this Soviet MTR.

[22] The Soviet general economy was much less able to support the cost of this military-industrial race. They may have devoted 18 to 20 percent of their GD/NP to the effort. The more technologically robust American economy was also stressed, but at only 5 to 6 percent. These estimates are from Jeffrey Lehrer and Judith Sedaitis, Defense Conversion Project, CISAC.

[23] For examples, see (Campen 1992).

[24] (Defense Week 1994). Current plans supposedly call for the F-22 to carry two 9000 MTOPS (millions of theoretical operations per second, a measure of computing power used extensively for export control purposes) high-performance computers. Each of these machines has more raw computational power than a Cray Y-MP8 (3700 MTOPS), a top-of-the-line supercomputer circa 1991. It is not entirely clear why the F-22 “needs” so much computer power, but the technology is rapidly progressing to a point where such power may be supplied in an appropriate on-board package in a few years.

[25] See also note 36. More generally, there seems to be no study where an extensive case has been made for the pervasiveness of IT in U.S. military systems. The case could be made credibly by an almost unlimited litany of examples. Overall, IT is used in the DoD in so many forms that it is essentially unquantifiable. The closest common denominator of measurement might be the percentage of time the total population of the DoD spends using, building, and maintaining IT in all of its forms, including those listed in note 1. But even that becomes a questionable measure when we consider how many important IT-based systems are “on duty” without human attendance. The desired analysis is much easier for other technologies, for example, for armored land warfare. This is because tanks and armored fighting vehicles are much more localized within the DoD organizationally, and it is simpler to make cost estimates using the acquisition, personnel etc. budgets for a few dominant organizations.

[26] Ironically, the design of the first U.S. stealth aircraft was based on Soviet scientific research. This work was essentially ignored in the U.S.S.R., presumably at least partly because of the air defense asymmetries.

[27] For example, (Horton 1995). As of mid-1995, senior defense officials were starting to use the concatenation/exponentiation of Command, Control, Communications, Computing, Intelligence and Information (C4I2). But this sequence appears short-lived, and as of early-1996 the expanded sequence was C4I plus Surveillance and Reconnaissance (C4ISR) (Cebrowski 1996). Over the years, the progression has moved through C2, C3, C3I, C4I, C4I2, and C4ISR. For the most part, the C4I abbreviation is used in this study.

[28] The potential conflict and operations spectrum could be partially quantified, and probably was in some form during the Cold War. For each kind of operation, for example, a full Soviet blitzkrieg toward the English Channel, a probability distribution could be assigned, as well as measures of the severity of the conflict or operation, such as a distribution for casualties or other forms of damage. For this particular example, one might guess that the probability of occurrence has dropped by at least a factor of 100, and perhaps more, since its maximum value during the Cold War. Estimates of severity would also have to be lessened considerably, given the condition of the Russian military, the longer distances they would have to travel, and so on. This example would go from a big spike on the Cold War conflict spectrum distribution to a small bump on the new one. Operations might also be partially ordered by scale, intensity of action, and the like. The new distribution would show a much greater variance and a greater likelihood of assorted low-intensity conflicts, operations other than war (OOTW), and conflicts with global organized crime and network-based criminals.

[29] The intents of these varied attacks are often described by *D* words: *deny, delude, disrupt, deceive, destroy, disable, decoy, delay, distort, disclose.* Some members of the U.S. information warfare (IW) community like to use the term *weapons of mass disruption* for the means of doing widespread nonlethal damage via electromagnetic and information technologies, such as electromagnetic pulses against integrated circuits, and viruses against computer networks.

[30] A particularly striking example is the Cu Chi tunnels in Vietnam. More than 200 miles of hand-dug tunnels stretched from Saigon to the Cambodian border and served multiple purposes for Viet Cong and North Vietnamese forces. They formed an exceptionally crude, but also an exceptionally effective, military infrastructure for communications, information, transportation, and operations. They were a major factor for years, defied all sorts of high-tech efforts, and were eventually destroyed through wasteful use by Hanoi, hard-nosed U.S. human intelligence and psychological warfare programs, and B-52 carpet bombing (Mangold and Penycate 1985).

[31] (Rochlin and Demchak 1991, Demchak and Goodman 1995).

[32] Some of these incidents are discussed in (Jenkins 1995). From the standpoint of clutter, terrain conditions, collateral damage and other factors complicating the use of IT, there should be a lot less “fog of war” on the ocean surface than on the ground. The fact that a large fraction of real, fairly simple, IT-intensive, naval conflicts came out badly is discomforting.

[33] (deArcangelis 1985).

[34] There are some dubious “rules of thumb.” For example, postindustrial military systems almost always will defeat industrial systems, but may not do well against preindustrial foes.

[35] Among the people interviewed during the course of this study, an Army colonel took the strongest “technology can solve any problem” position. He felt that the United States could have won the Vietnam War if R&D and production had started earlier on night vision and thermal sensor technologies.

[36] According to 1993 statistics cited from the U.S. Arms Control and Disarmament Agency, the top ten spenders were: (1) the United States ($298B), (2) Russia ($114B), (3) China ($56B), (4) France ($43B), (5) Japan ($42B), (6) Germany ($38B), (7) Britain ($34B), (8) Italy ($21B), (9) Saudi Arabia ($21B), and (10) South Korea ($12B) (Economist 1995a, S7). Other than for the United States, Russia, and South Korea, there is not a particularly strong correlation between spending and manpower levels. China’s military manpower level was roughly twice that of the U.S., but it spent less than a fifth of the U.S. total. After the top three spenders (in reversed order), the largest militaries are those of India, North Korea, Vietnam, Turkey, South Korea, Pakistan, and Iran. (Korb 1995, 23)

cites a later study from the International Institute for Strategic Studies with even stronger contrasts. Russia remains second, but at "only" $80B. The United States alone accounts for 37 percent of global military expenditures, and its close allies (the rest of NATO, Japan, Israel, and South Korea) account for another 30 percent. The six so-called rogue countries (Cuba, Iran, Iraq, Libya, Syria, and North Korea) combined account for only $15B annually.

There are, of course, difficulties in making comparisons across such different national economies. So, for example, common soldiers come relatively more cheaply in the "rogue" countries than in the United States, but technology is relatively cheaper in the United States. Thus there is a smaller difference (or a reverse difference, as in the case of China above) in the manpower figures than the total spending comparisons would suggest, but probably a larger difference in technological capability.

The second part of the statement on IT spending is based on the presumption that the U.S. defense investment choices emphasize IT far more than any other country's, and that most others (including fairly big spenders like Saudi Arabia) import almost all their IT-based systems. If this is the case, the U.S. share of IT-related spending should be higher than 37 percent of the world total, and quite likely over 50 percent, particularly if all the nonmilitary intelligence organizations are taken into account. I know of no rigorous study establishing the second part of the statement.

[37] For example, (U.S. Army 1995) officially describes all 108 Army "weapons" systems and programs that includes everything from self heating field rations to the Patriot missile. Their functions fall into five general mission categories: Project and Sustain (17 systems), Protect the Force (22 systems), Win the Information War (28 systems), Conduct Precision Strikes (13 systems), and Dominate the Maneuver Battle (28 systems). Foreign counterparts are identified when possible. All the IW systems, most of the systems for protecting the force and making precision strikes, and a few of the others (such as the M1A2 tank under "maneuver") are IT-enabled to significant extents. No foreign counterparts were identified for more than half of these. No single country had many comparable systems. It is doubtful whether many advanced foreign IT-intensive army systems exist for which there are no U.S. counterparts. Probably, an even greater percentage of Air Force and Navy systems (not to mention those in the intelligence community) is IT-enabled to significant extents. One might also guess, given the way most other countries distribute resources among their respective armies, navies, and air forces, that comparable or greater percentages of those systems have no or far less sophisticated foreign counterparts.

[38] Perhaps the Romans during their prime empire days? But the Romans needed such an extensive and costly army to expand and maintain their classical tributary empire against fairly continuous opposition in one place or another, and that empire paid for much of the army.

[39] To some extent, this attempt to answer the question is put together from a non-trivial, but informal, survey of about 100 people and dozens of presentations at private discussions and such gatherings as AFCEA meetings and exhibitions. The people covered include military officers ranging from majors and lieutenant commanders to four-star flag officers, and a similarly wide spectrum of senior civilians in both government and industry. A partial list of these people, many of whom were also interviewed about the defense uses of high performance computing , appears in (Goodman, Wolcott, and Burkhart 1995, Appendix B).

When asked why these functions were desirable, interviewees often cited technology-push reasons (for instance, "If we have the technology to keep track of 200 targets, why would we settle for less?"). When demand-pull answers were solicited–they were almost never offered by the respondents on their own–they were either very general ("we clearly have to be able to do this better than anyone else" or "it will save lives in battle") or drew on examples from the Cold War or Desert Storm. Performance problems and system fragilities were infrequently mentioned in the responses.

[40] Admirals Owens and Cebrowski, the Vice-Chair and the J-6 of the JCS respectively, are among the most responsible, articulate, and evangelical military proponents of this view; see, for example, (Owens 1996, Cebrowski et al. 1996, and West 1996). The Army plans to publish a major Field Manual on "Information Operations" which is likely to emphasize information dominance (FM 100-6 1996).

More generally, policies in the DoD are aiming for five Future Joint Warfighting Capabilities that are expected to be met substantially with technological means (Defense S&T 1994). As of September 1994, these goals were:

1. To maintain near perfect real-time knowledge of the enemy and communicate that to all forces in near real time.
2. To engage regional forces promptly in decisive combat, on a global basis.
3. To employ a range of capabilities more suitable to actions at the lower end of the full range of military operations which allow achievement of military objectives with minimum casualties and collateral damage.
4. To control the use of space.
5. To counter the threat of WMD and future ballistic and cruise missiles to the continental U.S. and deployed forces.

[41] For examples, see (Kaminski 1995, and Scott 1995).

[42] Many examples have been collected in (Neumann 1995). The important considerations regarding how well IT-based systems actually work, and problems of delays in development, cost overruns, and safety, and organizational problems of absorption are not considered further in this study. Unfortunately, they are not given sufficient coverage in either the technical or policy literature.

[43] For discussions, see (Luttwak et al. 1994, and Coker 1995). This sensitivity to battlefield casualties stands in stark contrast to a remarkable tolerance for carnage on the streets in the forms of automobile accidents and crime. If American lives and property are of primary value, a good cost-benefit analysis would probably show that tax dollars put into automobile safety have a much higher return than those put into most defense categories now that World War III is much less likely.

[44] The use of new technology may be more costly and less effective in the short term than older, more people-intensive, approaches. In some applications it may also be more costly over the long term because of the shorter times between new generations of IT products and the perceived need to upgrade frequently. But computers do not get retirement or G.I. Bill benefits or other forms of entitlements.

[45] For one view of what this might look like, see (Libicki 1994a and 1995b).

[46] For a mixed set of recent examples, see (Demchak 1995, Goure 1995, Horton 1995, Libicki 1995a, Metz and Kievit 1994, Owens 1995, and TRADOC 1994). Not surprisingly, in the current, budget-frightened, revolution proclaiming, DoD environment, one sees less discussion of the pitfalls and shortcomings of high technology used for defense.

[47] For a taxonomy of the forms of IW, see (Libicki 1995a). Libicki's taxonomy is as complete and self-explanatory as any: "(i) command-and-control warfare (which strikes against the enemy's head and neck), (ii) intelligence-based warfare (which consists of the design, protection, and denial of systems that seek sufficient knowledge to dominate the battlespace, (iii) electronic warfare (radio-electronic or cryptographic techniques), (iv) psychological warfare (in which information is used to change the minds f friends, neutrals, and foes), (v) 'hacker' warfare (in which computer systems are attacked), (vi) economic information warfare (blocking information or channeling it to pursue economic dominance), and (vii) cyberwarfare (a grab bag of futuristic scenarios)."

[48] IT has also acted as a kind of "power multiplier" for the news media, giving them expanded, more powerful, and more complicated roles in national security affairs. For example, it can be argued that the news media got the U.S. military into Somalia, and then forced withdrawal. Considerable discussion of the role of the news media in covering military operations followed the Gulf War; for instance, see (Hopkinson 1992).

The media also give rise to a great contrast in the national security dimensions of IT. On the one hand, IT can be used to provide small unit commanders with enormous power in terms of controlling the local battlefield and calling on very sophisticated weapons whose use could have major consequences. On the other, the news media may be very quickly aware of what is happening as a result, and can take the consequences directly and immediately to millions of citizens and the highest levels of the U.S. government, including the president. Those highest levels may have no alternative but to drop everything and deal with the decisions of a commander of a small unit. The downing of the Iranian airliner by an Aegis cruiser is one example. This dichotomy of so much decentralized capability and so much centralized responsibility has become a factor in national security operations.

The use of so much IT in the military, especially in C4I, also provides more access points for media prying into plans and operations. Defensive IW may also have to be practiced against the world's media, who have the resources to practice what might be considered a form of offensive IW.

[49] On a per capita basis, the intelligence community probably has a higher investment in IT than the DoD. There is the possibility that the intelligence agencies are using all of this technology very well across the full spectrum of adversaries discussed earlier, but that this author is not fully appreciative because of classification restrictions. There is also the possibility that the essentially Cold-War-configured intelligence community may not be structurally or functionally in good shape to deal with the kinds of nonbattlefield demand-pull generated by these adversaries.

[50] For examples, see (Metz and Kievet 1994), and J. Epstein's forthcoming CISAC report on nonlethal weapons.

[51] Other estimates are half or double this one (CSIS 1994).

[52] For detailed discussions of the GPS national security versus civil applications tradeoffs, see (Lachow 1995); for the quality of satellite imagery, see (Gupta 1994).

[53] (Moran 1990, Bitzinger 1994).

[54] Recent studies on the decreasing effectiveness of export controls for computing include (Harvey et al. 1995, and Goodman, Wolcott, and Burkhart 1995).

[55] For example, see (Gillam 1994, Economist 1995b, S10-S12, and Landauer 1995). For some applications, notably the automation of manufacturing, a general case can be made for productivity increases. Not so for services and white collar sectors, or for the value of IT in changing organizational structures. The jury is still out, although many business people seem to feel that so much investment in IT is paying off, and that it can be defended on a case-by-case basis.

Today some argue that the best overall justification took time to arrive. When international competition and other business problems forced downsizing, all the IT in place enabled companies to lay off many people without losing much in short-term functionality, productivity, or profitability. Is the essence of IT in the RMA similar, that is to improve the traditional performance characteristics of legacy or new weapons systems while cutting back the labor force needed to maintain and use these weapons, or to simply cut labor costs in the quest for budget-driven efficiencies?

[56] For a more extensive discussion, see (van Creveld 1989).

[57] See (George et al. 1996).

[58] In the process, Britain's achievement wiped part of the naval slate clean, arguably negating much of its previous advantage. Something similar might eventually happen with the U.S. and stealth aircraft.

[59] Throughout history, militaries and other national security organizations without much in the way of foreign enemies have managed to find "another hand" domestically. Many countries in Central or South America provide cases in point. Perhaps some militaries without peer threats just expand to the limits of their management abilities and society's budgetary tolerance?

[60] For example, in decreasing order of hype: (Schwartau 1994, Toffler and Toffler 1993, and Arquilla and Ronfeldt 1995).

[61] Although a great deal of talk is devoted to information warfare at high levels of government, as of November 1995 the highest ranking military officer under the Office of the Secretary of Defense (and perhaps in all of the DoD?) who was fully occupied with IW was a colonel (O-6).

[62] (Joint Security Commission 1994, NCS 1994).

[63] For example, one vision of a digitized U.S. Army is to provide all forces, including very small units, with enough information to make the battlefield "transparent," for example, maps with the precise locations of friendly forces to facilitate coordinated maneuver or avoid fratricide. IT will soon exist that will make this goal technically feasible. Then a lot of information that could be of crucial value to the enemy will be flowing around the battlefield. It could be protected, for instance, by encryption. But such protection is neither simple nor infallible, and resourceful enemies may find ways to get access without revealing themselves.

[64] This question suggests another: What would happen if the United States did not pursue a comprehensive RMA at all?

[65] There are, of course, problems with this approach. For example, the levels of accuracy and fidelity of the models could be inadequate. Programming errors might produce poor or misleading results. Simulated opposition may be culturally constrained, and not as motivated, as innovative, or as desperate as real enemies. Simulations also have been of very limited value with regard to assessing protracted conflicts against tenacious enemies. There may also be weighting toward more tractable and traditional threats (like enemy tanks or aircraft), neglecting the more complicated, less well understood type (c) and (d) adversaries. One might also question whether lessons learned and risks taken during physically safe computer simulations would really apply as well to a psychologically much more intense and physically much more dangerous battlefield. For further discussion of these problems during the Gulf War, see (Demchak and Goodman 1995).

Simulation is not the real world, but often cost, logistics, time, and other factors would make physical exercises impossible (and physical exercises are also not real-world conflicts).

[66] (Goure 1995b). In some ways it appears that the United States is trying to build a twentieth/twenty-first century counterpart of the British army and navy of the post-Crimean War nineteenth century. This would be a relatively small, technologically superior force that could go anywhere and do anything to the locals without fear of serious loss. Many British actions during those times also amounted to shooting galleries. But Britain arguably had a clearer understanding of what they

wanted from those armed forces versus the "second hands" of the time than the United States does now. The technologies and practices of the nineteenth century were also such that England itself was safe from attack by adversaries from less developed parts of the world.

[67] The June 1995 joint Congressional budget resolution for called for $262 billion in 1995, rising to $281 billion in 2002 (Korb 1995, 22).

[68] There are at least two extremely negative views on the continuation of the current IT-based RMA/ MTR. (Peters 1995) states that it is over, and that it does not help much in dealing with the most important foreign threats, namely the breakdown of the old order among nation-states and the growing importance of the menagerie of global and regional criminals, warlords, terrorists, and the like. (Goure 1995b) believes the extensive reconnaissance-strike-C4ISR approach to an RMA/MTR is a "counter-revolution" to the nuclear/ballistic missile RMA of the Cold War, in that the latter did a better job of optimizing the classical military objective function of balancing time, distance, mass, firepower, and cost.

[69] The combination of real threat conditions and budgetary pressures seems to be leading to some major decisions on force structure and operations. For example, the approach to "just in time" logistics using IT to manage highly centralized storage facilities in the United States is clearly a result of budgetary considerations. It also reflects a presumption of strategic invulnerability, in other words, that no adversary will be in a position to seriously contest the movement of these supplies before they arrive at the theater.

[70] Some of this cost- and IT-induced organizational change may produce other than the intended effects in the military. For example, (Demchak 1995) argues that the Army's effort to build a cost-efficient, taut, and tightly coupled "high-reliability organization" will produce an IT-bound ground force too brittle to accomplish the kinds of missions it may have to face above the brigade level. It may prove to be expensive and efficient, but not very robust. Tight coupling and a lack of slack may result in the networked magnification of problems and an inability to respond well to surprising conditions, of, for instance, terrain or enemy action, unexpected behavior of very complex IT-based systems. This could leave the United States with ground forces that could only be used confidently under very well defined and constrained circumstances.

[71] The C4I, logistical, and other such demands of two simultaneous MRCs have been used to justify the need for more IT in defense. During the Cold War, even when the United States was engaged in the Korean or Vietnam Wars, the communist "bloc" never got their act together to pursue two simultaneous MRCs against the United States. It is hard to assign much probability to the notion of Saddam Hussein and either Fidel Castro or Kim Jong Il getting together to seriously threaten U.S. national security with two simultaneous MRCs that would not ultimately leave them big losers. The U.S. defense budget may be almost 20 times that of the six combined so-called "rogue states" (Korb 1995, 23), and the disparities in technology and allies may be even greater.

[72] One nascent possibility may be via an extensive system for the selective provision of information to others (Libicki 1995b). The United States used its unique IT-based intelligence capabilities to significantly aid the British during the Falklands War.

[73] "Fuzzy" according to (West 1996); "difficult to explain to the average American" according to (White 1995).

References

(Arquilla and Ronfeldt 1995) John Arquilla, David Ronfeldt, “Information, Power, and Grand Strategy,” (July 1995), draft report.

(Bitzinger 1994) Richard A. Bitzinger, “The Globalization of the Arms Industry: The Next Proliferation Challenge,” *International Security*, Vol. 19, No. 2 (Fall 1994), 170-198.

(Campen 1992) Alan D. Campen, ed., *The First Information War* (Fairfax, VA: AFCEA International Press, 1992).

(Cebrowski et al. 1996) Arthur K. Cebrowski, Michael Pestorius, John H. Tilelli, Thomas L. Wilkerson, “Battlefield Omniscience...,” Special Address and Panel Session, in (West 1996).

(Cohen 1988) I. Bernard Cohen, “The Computer: A Case Study of Support by Government, Especially the Military, of a New Science and Technology,” in (Mendelsohn et al. 1988), 119-154.

(Coker 1995) Christopher Coker, “The Demodernization of War in the 21st Century,” CISAC special technical seminar, March 22, 1995.

(Cooper 1995) Jeffrey Cooper, “Another View of Information Warfare: Conflict in the Information Age,” (June 25, 1995), draft report.

(Crowe and Goodman 1994) Gregory D. Crowe, Seymour E. Goodman, “S. A. Lebedev and the Birth of Soviet Computing,” *IEEE Annals of the History of Computing*, Vol. 16, No. 1 (Spring 1994), pp. 4-24.

(CSIS 1994) Center for Strategic and International Studies, Conference on Global Organized Crime, Washington, DC, Sept. 26, 1994.

(Davis and Goodman 1978) Davis, N. C., and Goodman, S. E., “The Soviet Bloc’s Unified System of Computers,” *ACM Computing Surveys*, Vol. 10, No. 2 (June 1978), pp. 93-122.

(de Arcangelis 1985) Mario de Arcangelis, *Electronic Warfare* (Dorset, UK: Blandford Press, 1985).

(Defense S&T 1994) *Defense Science and Technology Strategy* (Washington, DC: Department of Defense, Sept. 1994).

(Defense Week 1994) “Perry is Warned About Potential F-22 Software Woes,” *Defense Week* (Sept. 26, 1994), reprinted in the *Early Bird* (Sept. 27, 1994).

(Demchak and Goodman 1995) C. C. Demchak, S. E. Goodman, “Computers as Substitute Soldiers?” *Comm. of the ACM*, Vol. 38, No. 2 (Feb. 1995), 154.

(Demchak 1995) Chris C. Demchak, “High Reliability Implications of Military Modernization: When Defense Leaders Get What They Ask For, They Won’t Want What They Get,” (Sept. 1995), draft report.

(Economist 1995a) “Defense Technology: The Information Advantage,” *The Economist* (June 10, 1995), Survey 1-20.

(Economist 1995b) “American Business: Back on Top?” *The Economist* (Sept. 16-22, 1995), Survey 1-18.

(FitzGerald 1994) Mary C. FitzGerald, “Russian Views On Information Warfare,” *Army* (May 1994), 57-60.

(FM 100-6 1996) Field Manual FM 100-6, *Information Operations* (Washington, DC: U.S. Army TRADOC, expected 1996).

(Geipel, Jarmoszko and Goodman 1991) Gary L. Geipel, A. Tomasz Jarmoszko, Seymour E. Goodman, “The Information Technologies and East European Societies,” *East European Politics and Societies*, Vol. 5, No. 3 (Fall 1991), 394-438.

(George et al. 1996) Joey F. George, Seymour E. Goodman, Kenneth L. Kraemer, Richard O. Mason, “The Information Society: Image vs. Reality in National Computer Plans,” to appear *Information Infrastructure and Policy*, (1996).

(Gillam 1994) Paul Gillam, “Pressure to produce: Is IS making us more productive? The answer, finally, may be yes,” *Computerworld Premier 100* (Sept. 19, 1994), 10-12.

(Goodman 1979) Goodman, S. E., “Soviet Computing and Technology Transfer: An Overview,” *World Politics*, Vol. XXXI, No. 4 (July 1979), pp. 539-570.

(Goodman 1984) Goodman, S. E., “Socialist Technological Integration: The Case of the East European Computer Industries,” *The Information Society*, Vol. 3, No. 1 (1984), pp. 39-90.

(Goodman 1985) S. E. Goodman, “Technology Transfer and the Development of the Soviet Computer Industry,” in (Parrott 1985), 117-140.

(Goodman 1990) Seymour E. Goodman, “Trends in East-West Technology Transfer,” *Computer (IEEE)* Vol. 23, No. 7 (July 1990), 94-95.

(Goodman, Wolcott and Burkhart 1995) Seymour Goodman, Peter Wolcott, Grey Burkhart, *Building on the Basics: An Examination of High-Performance Computing Export Control Policy in the 1990s*, (Stanford, CA: CISAC, November 1995).

(Goure 1995a) Daniel Goure, “Testimony before the Procurement SubCommittee, Senate Armed Forces Committee,” (May 5, 1995), Unpublished manuscript.

(Goure 1995b) Daniel Goure, “The Non-Revolution in Military Affairs: The MTR as Counterrevolution,” (July, 1995), Unpublished manuscript.

(Gupta 1994) Vipin Gupta, *New Satellite Images for Sale: The Opportunities and Risks Ahead* (Livermore, CA: Center for Security and Technology Studies, Lawrence Livermore National Laboratory, Sept. 28, 1994).

(Harvey et al. 1995) John R. Harvey, Cameron Binkley, Adam Block, Rick Burke, *A Common Sense Approach to High-Technology Export Controls*, (Stanford, CA: CISAC, February 1995).

(Hopkinson 1992) Hopkinson, Nicholas. *War and the Media.* (London: Wilton Park Paper 55, June 1992).

(Horton 1995) F. Barry Horton, "Future Directions for C3I," presentation at CISAC, Stanford University, Feb. 21, 1995.

(Jenkins 1995) Will M. Jenkins, Jr. *The DOD's Changing Roles and Missions: Implications for Command and Control* (Cambridge, MA: Center for Information Policy Research, Harvard University, January 1995), Draft Report.

(Joint Security Commission 1994) Joint Security Commission, *Redefining Security,* A Report to the Secretary of Defense and the Director of Central Intelligence (Feb. 28, 1994).

(Kaminski 1995) Paul Kaminski, Technology Challenges Address, West '95 Conference and Exposition on Operations Other Than War, AFCEA & U.S. Naval Institute (Jan. 19, 1995).

(Kerr et al. 1984) Donald M. Kerr, Karl Braithwaite, N. Metropolis, David H. Sharp, and Gian-Carlo Rota, eds., *Science, Computers, and the Information Onslaught* (Orlando, FL: Academic Press, 1984).

(Korb 1995) Lawrence J. Korb, "An Overstuffed Military," *Foreign Affairs* (November/ December 1995), 22-34.

(Lachow 1995) Irving Lachow, "The GPS Dilemma: Balancing Military Risks and Economic Benefits," *International Security* Vol. 20, No. 1 (Summer 1995), 126-148.

(Landauer 1995) Thomas K. Landauer, *The Trouble with Computers: Usefulness, Usability, and Productivity* (Cambridge, MA: MIT Press, 1995).

(Libicki 1994) Martin C. Libicki, *The Mesh and the Net: Speculations on Armed Conflict in a Time of Free Silicon,* (Washington, DC: National Defense University, March 1994).

(Libicki 1995a) Martin C. Libicki, "What is Information Warfare?" (Washington, DC: National Defense University, 21 July 1995). Draft report.

(Libicki 1995b) Martin C. Libicki, "Emerging Military Instruments," (Washington, DC: National Defense University, July 1995). Draft report.

(Luttwak et al. 1994) Edward N. Luttwak, Jessica Tuchman Mathews, Frank Press, and John D. Steinbrenner, “Environment, Economics, and National Security,” *Issues in Science and Technology,* X, 4 (Summer, 1994), 41-49.

(Mangold and Penycate 1985) Tom Mangold and John Penycate, *The Tunnels of Cu Chi* (London: Hodder and Stoughton, 1985).

(Mendelsohn et al. 1988) E. Mendelsohn, M. R. Smith, and P. Weingart, eds., *Science, Technology and the Military, Vol. XII* (Kluwer Academic, 1988).

(Metz and Kievit 1994) Steven Metz and James Kievit, *The Revolution in Military Affairs and Conflict Short of War,* (Carlisle Barracks, PA: Strategic Studies Institute, U.S. Army War College, July 25, 1994).

(Moran 1990) Theodore H. Moran, “The Globalization of America’s Defense Industries: Managing the Threat of Foreign Dependence,” *International Security,* Vol. 15, No. 1, (Summer 1990), 57-99.

(NCS 1994) National Communications System, *The Electronic Intrusion Threat to National Security and Emergency Preparedness Telecommunications: An Awareness Document* (Arlington, VA: NCS, Dec. 5, 1994).

(Neumann 1995) Peter G. Neumann, *Computer Related Risks* (Reading, MA: Addison-Wesley and ACM Press, 1995).

(Nitze 1994) Paul H. Nitze, “The Front-Line Duty of Conventional Arms: America’s Strategic Deterrent May Need to Shift from Nuclear to Smart Weapons,” *The Washington Post National Weekly Edition* (Jan. 24-30, 1994), 23.

(Owens 1995) William A. Owens, *High Seas: The Naval Passage to an Uncharted World* (Annapolis, MD: Naval Institute Press, 1995).

(Owens 1996) William A. Owens, Keynote Address, in (West 1996).

(Parrott 1985) Bruce Parrott, ed. *Trade, Technology and Soviet-American Relations* (Bloomington, IN: Indiana Univ. Press, 1985).

(Perry 1984) William J. Perry, “Technological Innovation: The Key to Our National Security,” in (Kerr et al. 1984), 7-11.

(Peters 1995) Ralph Peters, “After the Revolution,” *Parameters* (Summer 1995), 7-14.

(Porat 1977) M. U. Porat, *The Information Economy: Definition and Measurement* (9 vols.) (Washington, DC: U.S. Government Printing Office, 1977).

(Porat 1978) M. U. Porat, “Global Implications of the Information Society,” *Journal of Communication* 28, 1 (1978), 70-80.

(Ricks 1995) Thomas E. Ricks, "How Wars Are Fought Will Change Radically, Pentagon Planner Says," *Wall Street Journal* (July 15, 1994), A1, A5.

(Rochlin and Demchak 1991) Gene I. Rochlin and Chris C. Demchak, "The Gulf War: Technological and Organizational Implications." *Survival, Journal of the International Institute of Strategic Studies*, 33(3):260-73, London.

(Rudins 1970) George Rudins, "Soviet Computers: A Historical Survey," *Soviet Cybernetics Review* (Jan. 1970), 6-44.

(Schwartau 1994) Winn Schwartau, *Information Warfare* (NY: Thunder's Mouth Press, 1994)

(Scott 1995) William B. Scott, "'Information Warfare' Demands New Approach," *Aviation Week & Space Technology* (March 13, 1995), 85-88.

(Toffler and Toffler 1993) Alvin Toffler and Heidi Toffler, *War and Anti-War* (Boston, MA: Little, Brown, 1993).

(TRADOC 1994) "Force XXI Operations: A Concept for the Evolution of Full-Dimensional Operations for the Strategic Army of the Early Twenty-First Century," US Army TRADOC 525-5 (1 August 1994).

(U.S. Army 1995) United States Army, *Weapons Systems 1995* (Washington DC: OASA (RDA), 1995).

(van Creveld 1989) Martin van Creveld, *Technology and War* (New York: The Free Press, 1989).

(West 1996) *West'96*, "Technology and Tactics: Meeting the Fuzzy Threat," AFCEA Conference and Exhibition announcement (Jan. 24-26, 1996).

(White 1995) John White. Address to the General Meeting of the U.S. Army Science Board, Ft. Hood, TX (Oct. 25, 1995).