

War, Information Technologies, and International Asymmetries

S. E. Goodman

The modern computing era was born during World War II (in Germany, Great Britain, and the U.S.) and the first decade of the Cold War (in the U.S.S.R. and several NATO and eastern European countries). During the more than four decades of the Cold War, the U.S., the U.S.S.R., and most other industrialized countries continually increased the application of the information technologies (IT) to the development and use of military power. A case can be made that differences in the greatly expanded use of IT played a major role in the U.S. winning the mainline military-technological confrontation with the Soviet Union [5].

Since the end of the Cold War, there has been an acceleration in the development and global diffusion of IT, and many changes in the make-up and relative power among potential adversaries around the world. To what extent and to what ends is this influencing the structure and use of military power? An examination of the use of and investment in IT for military purposes reveals varying effects and pronounced asymmetries among the world's players.

An IT-fueled Revolution in Warfare?

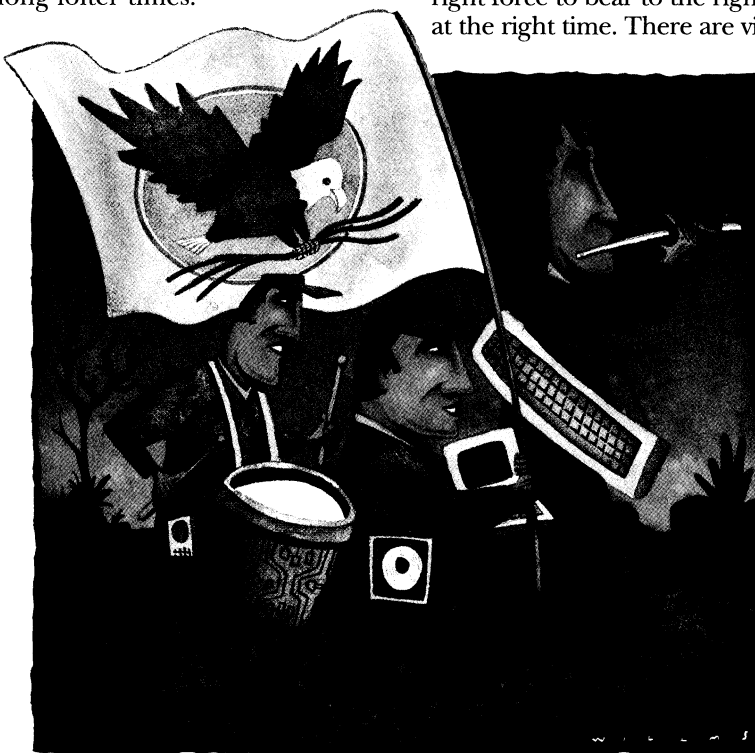
Many analysts believe an IT-based, transformation of warfare is in the making [1, 2, 4, 9]. These views have been massively and publicly reinforced via TV coverage, com-

puter games, and movies glorifying high-tech military conflict.

Indeed, IT seems to have extraordinary applicability to military and intelligence functions. IT improves performance and permits new capabilities. For example, it affords greater resolution for sensors, as in signal processing in anti-submarine warfare or image processing from satellites or unmanned aerial vehicles; it enables more precise targeting; and it provides logical control in space and other military environments hostile to human presence or which require staying alert for long loiter times.

Additional applications areas include cryptography, military-grade weather forecasting, conflict simulations, and training functions. High-tech military systems often contain elements of IT that, at a small fraction of the overall costs, contribute disproportionately to functional capabilities, such as stealth aircraft, which are not capable of stable flight without their onboard computers.

Beyond such specific functions, IT is seen as crucial to integrated battlefield management, multinational force coordination, and force multiplication, that is, bringing the right force to bear to the right place at the right time. There are visions



international perspectives

of "information dominance" and nothing short of "battlefield omniscience" [4, 10]. IT is central to the war-fighting futures sought by both the big platform advocates, who favor such weapons as tanks, submarines, and bombers, and more radical thinkers who foresee, for example, a battlefield covered with many small, smart, sensors operating under an integrated battle management system that summons brilliant weapons from long distances to surgically destroy their targets.

Downside Problems

In contrast to all of these sought-after capabilities, heavy reliance on IT in the military also often brings

under stress, fell short even in the extraordinarily asymmetric force and technology imbalances of the invasion of Grenada, and for several relatively uncomplicated incidents where single ships were (or were not) attacked: *Pueblo*, *Liberty*, *Mayaguez*, *Vincennes*, and *Stark* [6].

Even the Gulf War, where almost every American IT-based system looked like it worked, arguably owes its success as much to other factors. These include a long and uninterrupted set-up and shake-out period necessary to get many IT-based systems to work properly [3], and a cooperative, formerly adversarial U.S.S.R. that in effect permitted the U.S. to use a large fraction of

opment of IT was nurtured for military, space, and other major national-level applications, the current drivers and consumers are overwhelmingly commercial and civil. As a result, high-performance computing, satellite imagery, crypto technologies, and other forms of militarily useful IT, once almost exclusively available to the governments of the most powerful nation-states, are now much more available globally, including to private companies and individuals.

With the end of the Cold War, and the profusion of so much enabling technology, the world has become a more confusing place with regard to potential military conflicts, including civil wars. A sample of recent armed conflicts include Iran and Iraq, Iraq

The U.S. probably outspends the rest of the planet combined on high technology, and particularly on IT, for military and intelligence purposes.

greater cost and support problems, new forms of technical failures, organizational absorption and dependency problems, and new vulnerabilities to hostile intent.

Moreover, the performance of high technology in actual conflicts has been mixed. Starting with the early 1960s, roughly the same time that computers began to be extensively used, in many cases high technology was not decisive, or technically backward foes with predominantly low-tech weapons and infrastructure defeated or neutralized far more technologically sophisticated opponents. The success of the Gulf War stands in contrast to the French-Algerian War, Vietnam, Somalia, and the Soviet experience in Afghanistan, among other examples. Furthermore, the performance of command, control, communications and intelligence (C3I) systems, and their users

the forces created to deter or fight a world war for a much more modest regional conflict.

Superior technology does not insure military success, even if it is cutting edge or perfectly utilized. An extreme contrast occurred with the Israelis in Lebanon in 1982. One of the most striking electronic warfare victories in history—the air battle against Syria—was followed by a no-win, demoralizing ground struggle with the Palestinians, an asymmetric, low-tech, foe. This may be a premonitory example questioning the value of IT and other advanced technology in the occupation or pacification of an enemy's territory, or in military activities other than war, for example, peacekeeping or humanitarian operations.

The International Playing Field

Although much of the early devel-

and Kuwait, a progression of several in the former Yugoslavia, Russia-Chechnya, and others in Africa and elsewhere. Wars hardly seem to be a thing of the past.

However, an examination of who is investing in IT for military purposes reveals less than might be expected from all of the hype and potential, and some extreme asymmetries. The world of potential adversaries may be ordered into six categories on the basis of decreasing military capabilities, and command and force centralization:

- *The U.S.* The defense sector has been developing and adopting IT systems at a rate and to an extent that it will soon be almost impossible to find a military component of any size, combat or noncombat, without computers, telecommunications, or microelectronic sensors. The U.S. probably

outspends the rest of the planet combined on high technology, and particularly on IT, for military and intelligence purposes. The U.S. certainly generates more words and imagery about an IT-fueled revolution in military affairs and information warfare than the rest of the world put together.

- *Countries with the ability to project military power regionally.* Countries in this category have large conventional armed forces based overwhelmingly on mechanical and electrical industrial age technologies. A sample includes Brazil, China, Egypt, France, India, Iran, Iraq, North Korea, Pakistan, Russia, and South Korea. The forces of these countries may be increasingly augmented by IT-based systems and possibly nuclear, chemical, or biological weapons. However, overall military IT capabilities of the most technologically advanced countries, such as Israel or Japan, fall far short of those of the U.S.
- *Most other countries.* These typically have fairly low-tech, modest-sized military forces that may be as important for keeping internal order as for dealing with foreign threats. A few, including Singapore and some of the Nordic nations, are well endowed technologically, but without the total assets or potential missions of the major regional powers.
- *Countries in name only, 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, as in Bosnia, Chechnya, Chiapas, Lebanon, Peru, and Somalia. Some conflicts in these places have been notable for the way the technologically weaker combatants have used their opponents', or the worldwide, IT infrastructure to their advantage, for example, by Somali warlords against the U.S., or the rebels in Chiapas

against the Mexican government.

- *Substantial international or transnational, distributed, coherent organizations with sustained financing and havens.* Some of these are increasingly using IT. International bodies, such as the UN and NATO, have no standing forces of their own, but use the military forces of others, often needing sophisticated C3I systems. Other examples include elements of transnational organized crime and terrorist networks supported by national governments.
- *Fragmented, distributed, decentralized groups or individuals.* Their loosely coupled or independent elements are usually very small, but their abilities to do damage or gain advantage have been enhanced by technology and access to the infrastructures of their enemies. Examples include network crackers and fringe terrorists. Although not usually associated with military conflicts, such people, with mobile loyalties, may be increasingly useful to potential adversaries in pre-combat, intelligence, or specialized marginal roles.

At least two striking features emerge from this discussion of players and the recent and potential use of IT in warfare. Both are essentially concerned with asymmetries. First, the preponderance of the world's high technology in the military and intelligence domains is concentrated in the U.S., proportionately more so than for IT in the civil sectors. Second, a little high technology may provide leverage to a numerically or technologically weak combatant against a much larger or more advanced adversary.

Means Toward What Ends?

The U.S. thus has the technological fuel to pursue some kind of IT-based military revolution or at least an extensive IT-intensive rearming of its forces, but notice-

ably absent are military-technological peers providing the threat and a convincing rationale to that end. Is this a solution without a suitably challenging problem? What then might be the rationale for this quest, and how might the other players pursue their interests under the circumstances?

No doubt U.S. domestic political and budgetary factors are important, but this is not the place to consider them. From an international perspective, we speculate on three reinforcing possibilities:

1. With regard to potential direct military threats, the U.S. is trying to leave the rest of the world so far behind in military technology that few, if any, other countries will catch up, much less directly challenge the U.S. in a war. This contains a strong deterrence element, not unlike policies of the Cold War—build to deter the kinds of wars you least want to fight.

A less ambitious variant of this reasoning argues that as long as the U.S. has conventional forces, they should be made more cost-efficient, lethal, and functional for their primary missions: dealing with the military actions of the other categories of players. Although no peer threat exists now, one may emerge in the long term. Therefore the U.S. 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. The U.S. may have enough technological and experiential advantage and lead time over any prospective threat to continue to do this without the urgency and at a fraction of the cost now being pushed. But, as we have seen, there are some serious arguments suggesting caution against rushing toward too much reliance on an IT-

international **perspectives**

based security posture.

2. With the global diffusion of IT, cyberspace is itself generating new or exacerbated threats or missions. Like the geographical domains of military conflict—land, sea, air and space—cyberspace is the locus of valuable national assets and activities and is an important medium of passage. It thus needs defending and can be used to attack others. However, the possibility, and indeed probability, that future antagonists will attempt to disrupt each other's information infrastructures does not equate to the need of IT-intensive military preparations, although it would call for better security measures for protecting these infrastructures. This would not necessarily be a military mission, although there are dimensions that are of unquestionable direct concern to the armed forces, for example, offensive operations against C3I systems and other military, intelligence, and psychological warfare activities that comprise part of what is called information warfare [1, 4, 8].

Another 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 U.S. involvement [7].

3. The third line of reasoning argues it is precisely the major changes in international players and missions that requires the extensive use of IT. The U.S. would like to lead an as-yet unclear new world order. So far, in spite of an early post-Cold War euphoria over the spread of democracy, international trade, economic well-being, and

global networking, this new order has been slow in clearly identifying itself and has suffered setbacks. In the meantime, it is in the interests of the U.S., its allies, and perhaps most of the UN, to prevent the breakdown of too much of the old world order.

To these ends, a unique super-power military capability may be necessary for deterrence, containment, or coercion of last resort. Such power is also necessary for the nucleus of international coalitions for regional conflicts and large-scale peacekeeping or humanitarian missions. Even if most current strife or potential conflicts around the world do not seriously and directly threaten U.S. national security, if too many take place and some get too big, it will weaken world order over the long term, inevitably leading to serious national security problems. In the eyes of the U.S., the existence of additional military superpowers would not provide a useful form of checks and balances, but would be a likely source of much greater problems. To pursue this view of world order, the U.S. needs a suitable force, and taxpayers are the chosen people to foot most of the bill.

In this context, compared with Cold War threats, the U.S. defense establishment is faced with lesser but more varied and numerous threats that are difficult to explain to the average person. So the overriding task is to provide an armed force that can be used to respond to changing threats and missions under historically unprecedented demands and constraints. Some of these demands arise from general considerations of likely missions, for instance, rapid deployment, a reduced reliance on fixed foreign bases, and the desire to have improved C3I with foreign coalitions. Other constraints are self-

imposed by politicians, society, and the news media. These include the needs to have almost no U.S. 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 at a 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 not the best way of trying to cope with this tasking. The changes in players and global circumstances have resulted in reduced threats and smaller missions against adversaries who would likely be at great technological disadvantage. The imposed constraints essentially preclude 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 or a sweeping rebuilding of a defense establishment.

Advocates of this line of reasoning might argue that the only recourse is to respond with technology. In theory at least, IT does help address most of the demands and constraints. For example, the quest for a one-way transparent battlefield, with the hoped-for ability to rapidly bring one weapon to bear against one target, with high precision, supports the apparent need for a short battle with minimal casualties and collateral damage. All of the failed or unproved systems, the lack of other players using the same script, and the other problems discussed notwithstanding, this may be the only broadly viable approach the U.S. military can take if they are expected to deliver results and be held accountable under the postulated defense and foreign policy mandates.

These arguments do not apply to any other country or player to

anywhere near the same extent. Undertaking the high-technology military game on a large scale is very expensive and risky, and no other sovereign country or non-sovereign entity is in a position to pursue extensive development on its own. So where does that leave everyone else? Can they acquire and apply IT appropriate to their perceived needs, unfettered by the Cold War legacy of a large military-industrial complex or an obsession for push-button warfare?

The answer obviously partly depends on how the players in question stand in relation to the U.S. Friendly countries may gain directly from technology transfer or protection under a U.S. umbrella enhanced by IT-enabled systems that might be more readily used than nuclear weapons or large numbers of soldiers. (So far this has not been the case; most recent U.S. interventions have been manpower intensive.) The U.S. may even provide common interfaces to C3I systems for the coalition *du jour*.


Other conflicts not likely to have direct intervention by the U.S. military high-tech behemoth can proceed using conventional mechanical-electrical means and with modest acquisitions of IT through a buyer's market or limited indigenous efforts. Most warfare has been conducted without much IT, and this is likely to suffice as long as no other players have the money, will, or infrastructure to go into a U.S.-style warp drive toward high-tech weaponry. Past and perhaps future examples of adversarial pairings in such conflicts include Iran-Iraq, India-Pakistan, India-China, China-Russia, Russia-Chechnya, and Hutu-Tutsi. In some cases, local arms races may be intensified as potential combatants seek decisive IT-based battlefield advantages. But the greater technology-related worries here are nuclear, chemical, and biological.

Players who are unfriendly to the U.S., or who simply want to be left

alone to do harm to their neighbors without U.S. interference, face more challenging problems.

Approaches to dealing with this situation range from the very risky business of acquiring nuclear or biological weapons in the hope of deterring the U.S., to trying to leverage asymmetric capabilities or a little high technology against the unique battlefield sensitivities and vulnerabilities of the U.S.

They may also try to move at least part of the conflict off the conventional battlefield, where they could find U.S. high technology overwhelming, onto other platforms more favorable to themselves [8]. The information technologies provide some of these platforms. Ironically, as the U.S. military tries to use IT to extend its global reach, some of what it originally helped create—satellite communications, microprocessors, ARPANET-Internet, the Global Positioning System—provides others with new means for penetrating the long-standing geographical sanctuary of the U.S. itself. More generally, such platforms include the great stage of worldwide TV, the virtual labyrinths of the international computer networks, opportunities for innovative alliances among members of the six categories of players, and various forms of IT-enhanced terrorism.

Furthermore, two of the characteristics of information-intensive warfare are that some aspects do not require high technology, for instance, strategic deceptions such as the Vietnamese Tet offensive in 1968, and that significant forms of IT-based capabilities may be transferred in a matter of months, rather than the years or decades required for other forms of military capabilities. The net result is that almost anybody can find a place to play in this game. 

References

1. Arquilla, J. and Ronfeldt, D. Cyberwar is coming! *Compar. Strat.* 12 (1993), 141–165.

2. Campen, A.D., Ed. *The First Information War*. AFCEA International Press, Fairfax, Va., 1992.
3. Demchak, C.C. and Goodman, S.E. Computers as substitute soldiers? *Commun. ACM* 38, 2 (Feb. 1995), 154.
4. FM 100-6. *Information Operations*. Field Manual. Headquarters, Department of the Army, Washington, D.C., forthcoming (1996).
5. Goodman, S.E. The information technologies and defense: A demand-pull assessment. Center for International Security and Arms Control, Stanford University, Stanford, Calif. (Feb. 1996).
6. Jenkins, W.M., Jr. The DOD's changing roles and missions: Implications for command and control. Draft report, Center for Information Policy Research, Harvard University, Cambridge, Mass. (Jan. 1995).
7. Libicki, M.C. Emerging military instruments. Draft report, National Defense University, Washington, DC, Jul. 1995.
8. Rona, T. Techniques of future warfare. Directorate of Net Assessment. Office of the Secretary of Defense, Washington, D.C. (Dec. 1993).
9. Toffler, A. and Toffler, H. *War and Anti-War*. Little, Brown, Boston, Mass., 1993.
10. West 96. Technology and tactics: Meeting the fuzzy threat. Armed Forces Communications and Electronics Association Conference and Exhibition, San Diego, Calif. (Jan. 24–26, 1996).

Follow-Up

Portions of this essay were adapted from [5]. Thomas Rona, former Deputy Presidential Science Advisor, helped improve an earlier draft. Thanks to Gary Geipel, Lawrence Greenberg, Lawrence Press, Kevin Soo Hoo, and Ross Stapleton for their constructive reviews.

Views on this subject are solicited particularly from readers outside of the U.S., with the intention of presenting them in the future. These should be sent to:

Sy Goodman
CISAC 320 Galvez
Stanford University
Stanford, CA 94305-6165
Fax: 520-621-2433
sgoodman@leland.stanford.edu

Sy Goodman is a Carnegie Science Fellow at CISAC and a professor of MIS at the University of Arizona.

© ACM 0002-0782/96/1200 \$3.50