Chapter Four

INCORPORATING INFORMATION TECHNOLOGY IN DEFENSE PLANNING

Martin C. Libicki

Inherent in the human condition is the fact that although we will live the rest of our lives in the future, every decision we make is based on what we have learned from the past. For defense planners, this is more than a nominal or philosophical conundrum. Those who plan defense programs face the very real possibility that the world in which these programs reach fruition will be different from the one in which they were planned.

This chapter introduces some guidelines for, if not predicting the future correctly, then at least coming closer to a correct prediction than do those who unconsciously assume the future to be equal to the present. We can think logically, but only time will tell how correctly, about the future. This fact is demonstrated by taking something that can be predicted—the information revolution—and thinking through its likely effect on conventional warfare and the extent to which new forms of warfare, such as information warfare, make sense.

MODEST PROPOSITIONS ABOUT THE FUTURE

Those who fear error should avoid forecasting. Many an expert has been famously wrong about prospects of one or another technology. Yet defense planners are called on to make decisions that will depend on the world's state 10, 20, and 30 years out. Undertakings that bear fruit years hence—long-lived investments, promises hard to back out of, self-reinforcing institutions, standards, and visions—are

examples of long-range decisions that have yet-to-be-determined outcomes.

Forecasters make mistakes, it is true. But the effort of forecasting is still valuable if it makes *explicit* statements about the future that are closer to reality than the *implicit* assumptions that too often guide long-term policies. But how is this to be done? Naive forecasters are heir to three clichés: that change is linear, that the pace of change is accelerating, and that complexity is thus increasing.

Not all trends run forever. The rapid progress that characterized aerospace, from Kitty Hawk to the moon landing, was universally expected to continue; it was commonplace for equipment deemed revolutionary upon its introduction to be scorned as obsolete 10 years later. Yet this was not what happened. People did not have an exceptional need for great speed, and by the late 1960s there were few radical technologies that had not yet been discovered. So progress slowed down. The SR-71, the F-15, the Boeing 747, the Concorde, and the Saturn may have been surpassed, but not by very much even *30 years later*.[1] Yet *technical* progress made through 1970 still echoes in terms of *social* and *economic* changes. Pacific air travel, for example, still doubles every seven years because cheaper, faster travel has fostered global institutions and linkages that, in turn, drive the demand for more travel.

Information technology has now become hot, but it is easy to forget what has cooled in the meantime. Today's office environment would be unrecognizable to someone arriving fresh from 1979, but many of the computer systems that most affect our lives—for business management, financial transactions, process control, and transportation scheduling—have been around for twice as long. Indeed, in many ways, overall change may be decelerating. Boomers born in the 1950s and 1960s had a different childhood than their kids are having, but the differences between boomers and their parents are greater—whether measured by income, education, transportation, mass media, or the likelihood of reaching age 60. And the social impact of the

[1]The same can be said for plastics (see *The Graduate*, 1968). Every bulk plastic in use today had already been invented by then. Within 10 years, growth rates in demand had fallen from 10 percent to 3–4 percent—just slightly faster than the overall economy.

birth control pill, introduced in 1963, has yet to be exceeded by anything in biotech.

The reason the past often appears simpler than the present is that great issues, once resolved, lose their complexities. In some ways, life is simpler now. Today's personal computers are easier to use than those of the mid-1980s, which, in turn, were far simpler than those of the mid-1970s. Automatic transmissions are simpler than stick shifts. Airline schedules are easier to understand than train schedules.

Having shed the clichés of naive forecasters, the next step is to wring as much as possible from domains where the future is clear, only then moving to the speculative. A fruitful path from easy to hard starts with demography and works through technology, the environment, and economics before chancing the social and political realms. Such a flow follows causality. Technology changes society, but society can only modestly alter the vector of technology. After all, technology must obey physical law.

Demography is a good place to harvest the unexpected from the inevitable. Clearly, for instance, the number of 30-year-olds in the year 2025 cannot exceed the number of 8-year-olds alive today (2003). Better yet, because most 8-year-olds have a high likelihood of reaching 30, and most will mature in the country where they are born, the number of 30-year-olds in 2025 can be forecast with some confidence. This simple generalization suggests that greater Europe, which had four times the population of the Middle East in 1978, will have fewer 30-year-olds come 2025. Even if the long-standing birth dearth in Europe and Japan ends, the size of the productive age group will shrink unless there are large immigration flows—inconceivable in Japan, and possible only at the expense of great change in Europe.

In *technology,* the most fundamental theme over the past 25 years has been the shift from ever-larger to ever-smaller as the driver of change. Progress used to mean size: world-scale factories to serve global markets, taller buildings, heavier supertankers, wider roads, longer runways, gigantic rockets, and multimegaton warheads. Circa 1975, energy shortages, pollution, integrated circuits, and scanning tunneling microscopes heralded a new direction. Today's new factories, buildings, supertankers, roads, runways, rockets, and warheads

are not particularly larger than they were 25 years ago. Progress since then has come from the ability to engineer features and to control defects at the micro scale: microelectronics, microbiology, and micro-electromechanical systems (MEMSs).

Microelectronics—measured via processor speeds, communications throughput, and storage capacity, all now doubling every two years or faster—should continue to make progress. Personal devices will continue to be the prime beneficiary, especially with improvements in untethered energy sources: efficient batteries, miniature fuel cells, and photovoltaic devices. Major appliances may soon be network-ready right out of the box, perhaps even looking to link to any network they can find.

As for microbiology, with the human gene now being read and its mapping into folded proteins to follow, scientists are learning a great deal about how life works, how life fails, and the pathogenic and genetic correlates of disease. Easier and earlier disease detection will yield more effective treatments. Research on the human stem cell suggests that organs for transplant will be grown rather than acquired. Such techniques are close to what human cloning requires, making it a near-certain event.

Microstructures are apt to proliferate and become more useful. MEMSs, whose structural features are similar in scale to prior-generation electronic chips, are useful for detecting movement as well as subtle visual, thermal, acoustic, and biochemical features of the environment. Microwatt transmissions from small devices have been demonstrated. So have very small combustion chambers that yield power devices with 10 times the energy density of batteries.

All of these technologies can be used in sensors that have potential military applications: small cheap microphones, electro-optical charge-coupled devices (CCDs), biochemical detectors, and pocket radars for security, biomedical, and controller applications. Sensors the size of pennies may be littered across the battlefield, coupled with MEMS-aided transmitter-receivers that can operate in a remote area for weeks or months. Biosensors on chips or natural sensors on insects may find suspicious chemicals in the air or on surfaces. This confluence suggests that sensors will be key to what tomorrow brings.

Technological vectors have underlying causes. The ability to scale up physical devices reflected steady improvement in knowledge, which, at some point, reached diminishing returns. Nothing so important, one is tempted to conclude, is likely to be realized from macro-scale technologies. No such diminishing returns are apparent from the trends toward miniaturization. Cheap electronics, for instance, fed a global demand for communications, which spurred the launch of communications satellites, which faced a primary constraint of spectrum, which is being relieved through techniques such as beam forming and phased array antennae, which led to a secondary constraint of power radiation, which is spurring the next generation of 25-kW satellites. If technology favors small things, it will favor many of them, and the problem of controlling multitudes will loom. With only a dim prospect of radical advances in the writing and debugging of software, complexity theory, which posits that the right rules can induce complex behavior, can prove its value for simulation and control.

REAL REVOLUTIONS ON THE PHYSICAL BATTLEFIELD

So are there fundamental changes under way in warfare? And, if so, what are their essential characteristics and limits? In 1978, Under Secretary of Defense William Perry noted that DoD would very soon have the ability to see everything of interest on the battlefield, hit everything that could be seen, and kill everything that could be hit.[2] "Very soon" always has to be taken with a grain of salt, but Perry *was* on to something important.

Hitting What Can Be Seen

What does precision mean? Although a tank within 3 km of its target is a precise weapon, attention has rightfully focused on the precision guided munitions (PGMs), which come in three basic types, distinctions among which show how information technology may influence warfare.

---

[2]From Philip Morrison and Paul F. Walker, "A New Strategy for Military Spending," *Scientific American,* Vol. 239, No. 4, October 1978, pp. 48–61. For another early treatment, see "The New Defense Posture: Missiles, Missiles, Missiles," *Business Week,* August 11, 1980, pp. 76–81.

Man-guided PGMs require that the targeter be within visual range and thus a few kilometers of the target. Examples include the TOW (tube-launched, optically tracked, wire-guided) antitank missile, and laser-guided artillery shells and bombs (which date from the end of the Vietnam War). Although the reliability of the PGMs is usually good, their accuracy is only as good as the targeter (who can be distracted by being shot at).

Seeker-guided PGMs find targets using their own sensors. Early types included radar-guided anti-aircraft missiles, heat-seeking missiles, and acoustic torpedoes. The United States has PGMs for acquiring and tracking many types of signatures, and these weapons can usually be fired from standoff ranges. But only so much sensor capability can be put in a small package, and miniaturization that exceeds what is commercial practice tends to be costly. As a result, PGMs are expensive and thus, under current doctrine, available only for use against high-value targets.

Point-guided PGMs, directed to a specific location in real space, include ballistic missiles that rely on inertial guidance, terrain-following cruise missiles, and, more recently, PGMs guided to a specific latitude and longitude by reference to global positioning system (GPS) signals (the Tomahawk [Block IV] cruise missile and the Joint Direct Attack Munition [JDAM]). DoD supposedly lacks munitions that go to a moving point on a map, but there is no technical reason why they cannot be produced. It helps that the United States is working hard to map every object to within 5 or 10 m in absolute coordinates and 1 m in relative coordinates. GPS satellites make it possible for a receiver to know its location to within 18 m, and far closer relative to reference points. If the locations of the target and the PGM seeker are known, the seeker's course can be programmed so that it hits the target.

Why belabor these distinctions? Because they have everything to do with where the "smarts" must reside within the system. Does the sensor go in with the targeter, inside the weapon, or remain external? Giving PGMs their own sensors makes them more robust and shortens the sensor-to-weapon loop. But with limited sensor capability, thanks to cost and carriage factors, they are more vulnerable to deception and have difficulties acquiring targets at long range. The use of off-board sensors to generate target tracks not only provides im-

proved range, tracking, and identification, but also complicates strategies for PGM deception. But point-guided PGMs need a reliable link to both sensor information and the overall command-and-control (C2) system.

Ironically, this technical disadvantage—the need for a reliable link—has political advantages. For instance, the United States supplied surface-to-air missiles (SAMs) to the Afghan rebels in the 1980s and, by doing so, lost control over them. When the Soviets left, the United States started worrying that the SAMs would appear as terrorist weapons.[3] Had these weapons needed externally generated flight track information to work, the United States could have removed this information to devalue them. With self-contained PGMs, power rests with the operator; with point-guided PGMs, it rests with those who control the intelligence system. PGMs, notably point-guided PGMs, also shift the locus of power internally. It is a simple fact of war that if one can kill everything one can see, it pays to see as much as possible of the other side and, equally important, to keep oneself hidden. This ability to seek and to hide, more than the ability to mobilize forces and deploy them into battle, determines outcomes, and thus determines which job contributes more to military outcomes. Here is an application of exponentiation. The existence of precision weapons creates a need for precision information.

The process of seeing is transformed by the growing profusion of sensors in space, on aircraft both manned and unmanned, on and under water, and on the ground. The first effect of using many sensors rather than relying on one super-sensor is the potential for great flexibility in deployment. A penetrating aircraft can survive if it flies below radar, but if microphones are placed under the aircraft's probable path, defenders can detect where the aircraft was flying and perhaps even track it. Flexibility permits one to adapt to the operational challenge of conflict. If the nature of conflict and of the enemy changes, sensors ought to change as well. The variety of sensors becoming available makes it more likely that the battlefield can be made so transparent that the first part of Bill Perry's vision can be realized. Yet transparency will vary greatly. On water and in the

[3]The SAM aimed at a commercial airplane flight out of Kenya (November 2002) was actually a Russian model.

desert, nothing large can be hidden for long; on plains and chaparral, some cover is available. Forest and jungle, and finally cities, are progressively more opaque. But in cities, the searching, while more difficult in some aspects thanks to greater cover and the presence of civilians, can be partly accomplished by friendly residents who supply eyes to do much of the work.

The second effect of quantity is that it has its own quality. DoD has many sensors that can illuminate the battlefield with a high degree of precision. Satellites in low earth orbit can take very accurate photographs, conduct strategic reconnaissance, and chart static formations, but they cannot track and target moving objects. If acuity requirements can be forsworn, the purchase and use of many satellites would permit continual, perhaps continuous, target tracking from space. And unmanned aerial vehicles (UAVs) can provide both accuracy and continuity. The Clementine spacecraft, launched by the U.S. Naval Research Laboratory (NRL), proves that many good sensors can be placed on a $50-million satellite. In theory, hundreds of cheap satellites could, along with UAVs, provide continuous coverage for spotting and tracking fleeting targets, at least under favorable weather and lighting conditions.

Another effect of using many small sensors (and one that may ultimately prove to be the most decisive factor) is that it offers better survivability. Having many small sensors rather than a few large ones lessens sensor vulnerability as would-be foes become able to see the battlespace better—an example of how two-sided change carries far different implications than does one-sided change. JSTARS (Joint Surveillance and Target Attack Radar System) and AWACS (Airborne Warning and Control System) are extremely capable sensors, easily the best in their class. But both are mounted on large and not terribly stealthy aircraft. They survive by flying behind front lines, which works only until enemy missiles can range hundreds of kilometers, or enemy shooters can penetrate front lines in the air or on the ground.

A constellation of UAVs would be more able to survive. An individual UAV is not as capable as either of the two aircraft, but UAVs could collectively illuminate the skies. UAV suites include the electro-optical, infrared, synthetic aperture radar, passive millimeter wave, and light detection and ranging sensors. Similarly, although an Aegis cruiser can see surface targets tens of kilometers away and air targets

perhaps ten times farther, it is, compared to aircraft, even less stealthy, more complex, and costlier, and it may some day compete with buoy-hosted sensors that individually are less capable but collectively could be less vulnerable. Ground sensors—microphones, remote cameras, and other sensors that can measure seismic, gravitational, biochemical, or magnetic phenomena—may be the ultimate in distributed searching. Some of the detectors coming out of the medical field are small, precise, and intelligent. Ground sensors in development are expensive, but commercial technology suggests that far lower costs are feasible. The wholesale cost of a PC-mounted camera is, for example, about $10; the wholesale cost of a microphone is well below that of its batteries.

The fourth effect of using many sensors is that it puts a premium on data coordination, correlation, and fusion. One sensor may excel at locating an object but not at identifying it. Another may be able to distinguish whether an object is a pickup truck or a tank but not be able to find the object precisely. Using different sensors not only reduces the uncertainty of where the object is, but also helps identify it more confidently. With the importance of sensor coordination across not only phenomenologies but also media, there is no good alternative to thinking about battlefield illumination in a joint context. Jointness is not simply a matter of warfighters with different-color uniforms working together; it now includes asking their machines—which are a good deal more finicky and far less clever—to do so.

If one can see from afar, why shoot from up close? Targets can be hit from 20 km with air-launched munitions, unattended remote-controlled weapons, or pop-up, or even shoot-and-scoot, platforms that are hard to shoot back at. Targets can be hit from 200 km with weapons such as the Army's Tactical Missile System (ATACM), stealth aircraft, and UCAVs; and they can be hit from 2,000 km with ballistic and cruise missiles. Are PGMs too expensive for most warfare tasks? Today's cruise missile costs $600,000. The United States fought the Vietnam War as a war of attrition (wisely or not), spending $1.2 to $1.5 million to kill each enemy soldier. If, as is typical in aerospace manufacturing, each doubling of quantity lowers unit costs by 20 percent, cruise missiles purchased at the rate at which enemy soldiers were killed in that war would cost $100,000 to $200,000 each. Using even expensive weapons to kill three people around a campfire hardly adds to war's costs. Reaching farther than the enemy can

reach back is a comparative advantage even—especially—in a perfectly transparent world. And the ability to build long-range propulsion systems is likely to be something the United States and its allies can do well and likely adversaries cannot.

The need for standoff range illustrates today's strategic asymmetry between the United States and its likely opponents. In a slugfest where dollar is traded for dollar, the United States will come out ahead—it can expect to enjoy ten, and more typically, one hundred times more gross national product (GNP) than any of its likely opponents for a long time to come. But if the United States finds itself trading life for life, it will lose.

From Contingency to Necessity

What is suggested when one puts sensors and weapons together is that modern militaries should wage war by using sensors to find targets and using PGMs to prosecute them. But *should* does not imply *will*. The United States and its allies can also go to war in the old-fashioned way—mobilizing force against force—and still do fairly well, as Desert Storm illustrated. But for how long? Which is to say, how great a divergence can arise between what technology promises and what its users grasp?

In Desert Storm, the coalition went to war against Saddam Hussein, an enemy who was fairly blind to what information technology could do. Previous RMAs (such as the dreadnought, blitzkrieg, and nuclear weapons) were built on items not found at local stores, but the current RMA is based on what comes from commercial sources as well as what comes from military labs. What if an adversary opened a checkbook and bought PGMs from the French or the Russians; UAVs made by any of 20 countries, plus digital cameras or digital videocameras (particularly after the successful advent of high-definition television with its thousand-line resolution) to put on them; space-based imagery, terrain data, and software to meld the two into fly-through quality virtual reality sets; digital video disks (today's 4.7 gigabyte drives can hold an image of all of Yugoslavia accurate to 2 m); portable personal computers; palmtop cellular phones; access to global communications; GPS receivers-on-a-chip; and night-vision goggles—all to provide a fine ground-level complement?

Now take Desert Storm and run it against this enemy, which, armed with these information technology tools, is far more sophisticated than Iraq was. The coalition did three big things to win in Desert Storm: ship in a mountain of material, take out Iraq's C2 capability, and run free over the battlefield, first in bombers and then in armor. The same war fought the same way against a sophisticated adversary—maybe not rich but smart enough to wire itself up in advance—may work poorly, for the following reasons.

First, having to ship in a mountain of material is a recipe for disaster, because most of the elements of the logistics infrastructure—ports, bridges, ships, airlifters, and logistics piles—are highly vulnerable and poorly hidden. Logistics can be attacked by volleys of PGMs.

Second, the coalition could cut Iraq's ability to talk because Iraq used centralized systems such as mainframe computers and central office switches. The world today is moving toward cellular phones and local area networks (LANs), a more distributed architecture and one far harder to knock out.

Third, although maneuvering is more attractive than sitting and dying, maneuver entails moving, and moving disturbs an environment, creating signature and thus making one a target for destruction. Walking into Desert Storm II against a sophisticated enemy could mean a great deal of trouble—and this is without even considering weapons of mass destruction (WMD) being used against massed forces.

This raises the question of platforms—a question that is an unintended but logical result of the information revolution. Today, platforms rule: the Air Force is built around aircraft; the Navy, around ships; and four of the five Army combat branches (artillery, tanks, air cavalry, and air defense), around platforms. Platforms have grown more capable, but only by also growing more complex and costly. As they become more costly, fewer are bought; with fewer in the inventory, owners want them better protected. Self-defense systems are thus needed, raising costs further. As the number of acquisition programs under way declines, each community in DoD becomes more desperate to get its requirements adopted in the new platforms—which retards the acquisition cycle, meaning that fewer can be started at any one time—hence, two vicious circles. Norm Augustine,

before becoming CEO of Lockheed-Martin, observed that current trends would leave the U.S. military with one aircraft by the middle of the next century: an aircraft flown three days by the Navy, three days by the Air Force, and on Sundays by the Marines.[4] By contrast, UAVs can be cheaper for owners to replace than for adversaries to shoot down.

Distributed sensors and weapons that are redundant and overlapping are not worth risking lives for, because they are built on civilian specifications and thus benefit from great economies of scale. Although it is harder to deal with a mosaic of smaller pictures than with one big one, only computer power stands in the way of converting the one into the other, and computer power is getting cheaper every day.

The Coming Architecture of Military Organization

Information technology suggests that it may be logical to convert from a platform-based to a knowledge-based military (see Figure 4.1). In the former, operators, local sensors, weapons, and self-protection are all bundled as platforms that work together but are each essentially an autonomous fighting unit. They are given intelligence, but once in combat they usually work with data they collect themselves.

In a knowledge-based military, fused data from networked sensors go into creating a shared knowledge base of the battlefield. All of the battlefield appears in low resolution, and some parts of it appear in high resolution; the two views come in and out of focus as need dictates. Such knowledge, in turn, feeds the weapons, because it generates the targets and tracks they are aimed against.

This architecture permits the separation of information and operations, so those who find the target need not be those with the trigger. Such a separation offers opportunities to build vertical coalitions, in which the United States supplies to local allies information they can use to conduct a war. Why build such coalitions? First of all, they

---

[4]Norman R. Augustine, *Augustine's Laws and Major System Development Programs* (rev. and enl. ed.), American Institute of Aeronautics and Astronautics, New York, 1983.

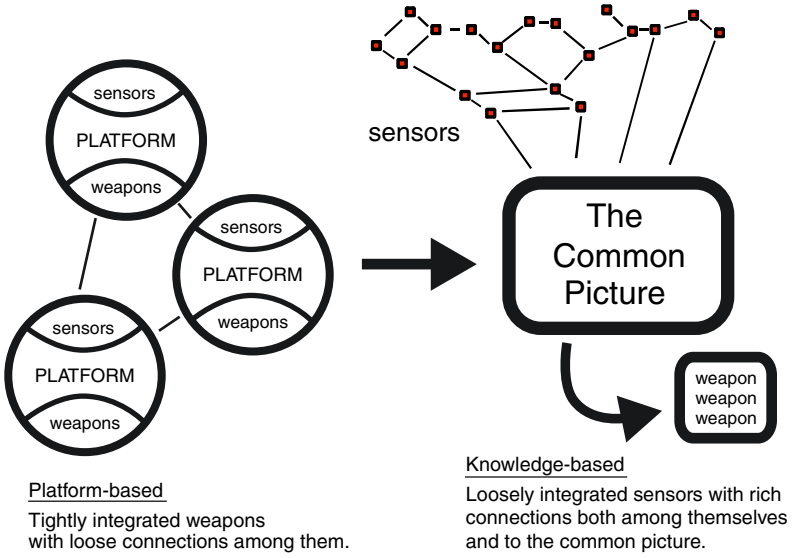

Figure 4.1—The Move from Platform-Based to Knowledge-Based Warfare

would enable the United States to avoid some of the many disadvantages associated with its going to war. For example, the large logistics infrastructures its force structure requires are, as noted, vulnerable, and the large fingerprints left by U.S. operations often work against its political interests. Moreover, if the United States can outfit its friends with PGMs (some have them already), and then provide the requisite information on targets and other enemy dispositions, the friends could prevail in what otherwise would be an evenly matched contest. As an illustration of how this would work, replace "weapons" (lower right corner) with "friends" in Figure 4.1. The United States gives its friends the common picture.

Vertical coalitions also offer other opportunities for altering the nature of the U.S. role and presence. During the Bosnian conflict, NATO was eager to bring Serbians to the bargaining table, but the Serbians would not quit as long as they believed they were militarily superior to the Bosnian and Croatian forces. By presenting the latter with a usable picture of the battlefield, NATO could have tipped the balance against Serbia without setting foot in the Balkans.

In the 1970s, as Egyptian and Israeli forces disengaged, the Sinai was wired to give both sides early warning of an invasion. In the future, DoD could fashion technology to generate not only early warning, but targeting information as well, creating an effective no-man's-land between the two combatants. Violators would show up as targets, putting them at immediate risk.

Information can be the glue behind security arrangements. Countries joining NATO could get a jump-start on interoperability if their C4ISR (command, control, communications, computers, intelligence, surveillance, and reconnaissance) infrastructures and NATO's were compatible beforehand. Were, for instance, Poland and its border areas well illuminated, Poles could feel better about their security without necessarily having to arm themselves heavily or see large numbers of troops deployed on their soil. Information can reassure friends of the United States who eye each other with suspicion. Were Asia better illuminated, each nation could justifiably feel confident that it could see something coming or conclude that nothing was. Belligerence could be further dampened if access to such illumination depended on how each nation behaved and thus postured its military.

The ability to flood the battlefield in lights also carries great implications for force structure. DoD has traditionally scaled its forces for warfare according to enemy strength. But what if the real question is what it takes to illuminate the battlefield, and then how many weapons it takes to shoot the foes? Most of the sensing infrastructure, notably satellites, is not expended but, rather, an investment. Expendable sensors ought to be cheap. Munitions, if bought in quantity, are also cheap; at the height of the 1980s buildup, PGM procurement accounted for only one of every 40 defense dollars. As for platforms and their units—the traditional metric of power—their job would be to haul sensors and weapons closer to the battlefield. Costs, as it turns out, would depend little on how many enemies exist, or how many tanks, planes, and soldiers enemies have. Instead, they would more likely depend on an adversary's sophistication and experience at deception; these two factors would indicate how much redundancy is needed in sensors and weapons.

Conventional War, Hyperwar, and Mud Warfare

Traditional warfare à la Desert Storm, hyperwar, and mud warfare place fundamentally different demands on military information systems because each has its own set of problems that information must be used to solve. To generalize, in traditional combat, what and (broadly speaking) where the enemy is are known. In this case, information systems need to generate data to provide situational awareness to operators. Complexity must be mastered to conduct large operations, and speed helps because it permits action before the adversary can react.

Conventional warfare pits superior force against force. The new logic of warfare, at least for the United States, is to scan the battlefield, sift through fields of data looking for targets, sort them by priority, and then strike those worth hitting. This approach has broad potential for stopping an approaching military and then wearing it down so that more-traditional combat approaches can be used to eventually push it back by successively occupying territory. In some cases, land occupation may not be necessary. If it is, successive attrition makes the job far easier—and, as noted, land forces need not wear U.S. uniforms.[5] Even in nonlinear combat, the ability to illuminate the battlefield can inhibit the enemy from massing forces and thereby from carrying out operations that require doing so. Since everyone makes mistakes, the ability to spot and exploit those mistakes quickly enough permits one to take advantage of them. It may be possible to know which locations the enemy is paying no attention to and thus where friendly forces can operate. Illumination allows supplies to be interdicted more successfully and permits the battlefield to be divided into smaller and smaller cells, each of which can then be attacked.

This capability is a goal and, as NATO operations in Kosovo imply, not yet a reality. Post-war analyses suggest that military assets were hidden in forests and villages and were not easily detected if they

[5]This presumes that the interests of the United States and its allies are sufficiently similar. Such is not always the case, as Operation Anaconda revealed. The United States was far more interested in destroying Al Qaeda than its Afghan allies were.

were not moving at the time. That noted, rendering them immobile might have been half the battle won. Unfortunately for the United States, it is precisely the prospects of such warfare that may compel adversaries to think of war in other terms—an example of how innovation for one can spark counterinnovation for others.

One response, termed mud warfare, is likely to be characterized by operating in dense environments, hiding in clutter, wielding civilian-looking material, taking hostages, and using terrorism. Mud warfighters have to learn what to look for and then where to look. Information plus training should prepare warfighters to distinguish patterns of hostile activity from everyday backgrounds. They must know where to intervene quickly when order is tipping over to chaos or enemy control. Because mud warfare features small unit operations, the locus of command is best moved down.

In hyperwar, warfighters know what to look for but not exactly where to find it. Complexity is associated with picking high-value targets from the clutter. Speed is necessary to track and engage such targets while they are visible. The availability of global information and the ability to bring any and all weapons within an ever-larger radius into simultaneous play tend to move command up.

Table 4.1 suggests how the three types of warfare affect C4ISR requirements. Paradoxically, while mud warfare appears crude, the information architecture required to conduct it is, in fact, much more complex than that for hyperwar. Such is the ability of future technology to shape competition that, in turn, reshapes the requirement for technology.

Table 4.1

C4ISR Requirements for Conventional War, Hyperwar, and Mud Warfare

	Conventional War	Hyperwar	Mud Warfare
Environment	Knowns	Known unknowns	Unknown unknowns
Purpose	Data/imagery	Information	Understanding
Complexity	Running ops	Finding things	Sensing patterns
Speed	Gain cycle-time edge	Find fleeting targets	Preempt tipping points
Command	Today's mix	Moves up	Moves down

FALSE REVOLUTIONS ON THE VIRTUAL BATTLEFIELD

If the real revolution in information technology lies not in its continual improvement but in the *form* that its improvement takes—distributing processing power into smaller packages and amalgamating it, in turn, into more powerful networks—does war follow commerce into cyberspace, pitting foes against one another for control of this clearly critical high ground? Does this comparison have a basis in tomorrow's reality, much less today's?

The Defense Science Board seems to believe it does:

> The objective of warfare waged against agriculturally-based societies was to gain control over their principal source of wealth: land. . . . The objective of war waged against industrially-based societies was to gain control over their principal source of all wealth: the means of production. . . . The objective of warfare to be waged against information-based societies is to gain control over the principal means for the sustenance of all wealth: the capacity for coordination of socio-economic inter-dependencies. Military campaigns will be organized to cripple the capacity of an information-based society to carry out its information-dependent enterprises.[6]

What Is Information Warfare?

The purpose of information is, was, and always will be to inform decisions; if not, it is just entertainment. Prior to World War II all these decisions were made by people. With the advent of digitized information systems, an increasing share of decisions—choices made among alternative actions—are made by machines. But they are decisions nonetheless.

Because conflict has always involved decisions, information has always been a part of conflict. Information warfare can thus be defined as the actions taken to influence the enemy's decisionmaking processes so that its decisions are bad or too late or good for your side (e.g., deciding to stand down rather than fight). Seen in this light,

---

[6] *Report of the Defense Science Board Task Force on Information Warfare—Defense,* Office of the Under Secretary of Defense for Acquisition and Technology, Washington, DC, November 1996, p. 2-1.

quintessential human activities such as deception, propaganda, and targeting the other side's commanders are hardly new to warfare.

What is new is that many of today's decisions are made using more information, and that information is richer, generally more timely, and often more widely disseminated. At first glance, this tendency supports a belief that information has become a center of gravity for military operations—and, as such, more deserving of attack. Attack methods, it would seem, now merit greater resources. At second glance, however, the logic is a bit odd. It is as if to say that the task of toppling someone sitting on a stool is more likely to call for breaking the stool's legs if they number eight rather than if they number three. Sound strategy requires looking not only at an opponent's *demand* for information but also at its *supply*. The latter is determined by long-term trends in technology, and these trends are not especially conducive to information warfare. The exception is computer warfare: because computers are everywhere and connected, defending them is harder.

To demonstrate as much requires that information warfare be decomposed. Consider the following information flow: Information is gathered by sensors, relayed to decisionmakers through the electromagnetic spectrum, and reaches the command center, where it is entered in a computer for further processing, the results of which inform decisionmakers. Figure 4.2 shows the primary related forms of information warfare: attacks on sensors, electronic warfare, C2 warfare, computer (hacker) warfare, and psychological operations. Note, again, that with the recent exception of the computer, and the half-century exception of the spectrum, none of this is particularly new, especially if sensors are considered today's version of yesterday's cavalry pickets.

What does the future tell us about the efficacy of information warfare? Modern militaries *are* increasing their dependence on the ability to generate and use information gathered and exploited from well over the horizon. But the industrial-era paradigm of concentrating value in a few machines of increasing complexity may have peaked and, with it, the vulnerability of modern systems, even military systems, to information warfare. Again, computer warfare is an exception, one dealt with below.

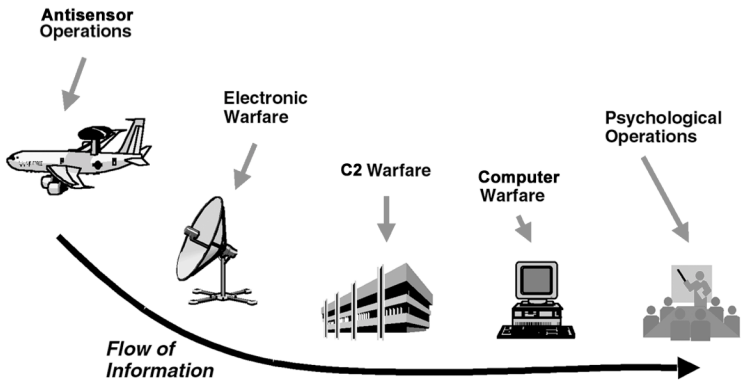

Figure 4.2—Five Types of Information Warfare

Antisensor Operations

The flow of good information into sensors can be disrupted in one of three general ways: (1) destroy the sensor itself, (2) use arcane electronic methods to spoof the sensors into seeing the wrong set of bits, and (3) use cover, concealment, and deception to fool those who interpret these bits into not seeing what is really there (or into seeing what is not there). The second method is specific to electronic equipment (notably radar-based equipment); the other two clearly predate electronics. The primary reason antisensor warfare may be more attractive today is that sensors are more important to warfare than ever before; the growing ability to hit targets at a distance depends on being able to detect and identify them from comparable distances.

The vulnerability of U.S. sensors to attack depends on the attacker. The primary long-range sensors in the U.S. inventory include reconnaissance satellites, aircraft (e.g., JSTARS, AWACS, Rivet Joint, Cobra Ball, the U-2), large radars (e.g., the Aegis system), and UAVs. So far, only Russia can attack a reconnaissance satellite (although China may soon have some capability). Similarly, aircraft and ships can be

protected by operating 100 km or more behind the lines and using a protective screen (e.g., F-15s) to keep adversaries at bay.

Twenty years out, the survival of such assets may be dicier, especially against an opponent that determinedly invests to neutralize a decisive source of U.S. advantage. Reconnaissance satellites are expensive, few in number, and fly rather close to the earth. A spruced-up Scud-like rocket on direct ascent may be able to intercept their orbits, and lasers may be employed to blind at least the optical sensors on such spacecraft. Radar-based aircraft are large, hard to maneuver, easy to detect by watching for their energy output, and not at all stealthy. If they have to track deep targets or if front lines are poorly held or defined, they may be vulnerable, particularly to very long range missiles. The Aegis cruiser is at risk because naval fleets are developing increasingly sophisticated defenses against cruise missiles but usually lack the stores to completely counter a sufficiently large attack volley. UAVs are somewhat better protected due to their stealthy characteristics, their ability to fly high, and their small size.

UAVs, however, foretell the coming futility of direct antisensor operations. As electronics get cheaper, the prospect of putting formidable electro-optical capabilities on increasingly smaller and less-expensive UAVs suggests a long-term strategy of employing such sensors in large profusion. Sufficiently cheap but increasingly sensitive UAVs cost less to replace than to destroy. Finally, if unmanned ground sensors approach the low cost of consumer electronics (e.g., microphones, digital cameras) they can provide an even more robust method of collecting signatures.

The fate of electronic spoofing follows a similar logic. It is far easier to spoof a single sensor of known phenomenology (e.g., radar, electro-optical, hyperspectral, passive millimeter wave, acoustic) than to fool a suite of sensors that are in multiple locations and use various phenomenologies to produce readings that can be correlated to develop an increasingly detailed view of the battlespace.

This leaves the opponent with the age-old techniques of making the hostile appear benign (e.g., putting troops in vehicles normally assigned to hospitals) and feeding the preconceptions of adversaries so as to persuade them to classify the normal as threatening. These techniques, in large part, predate technology.

Electronic Warfare

Can messages be stopped, corrupted, or intercepted between nodes in the system? Jamming, message spoofing, and interception—all were the stuff of the so-called Wizard Wars conducted between Britain and Germany in the early 1940s.

One form of jamming works by putting an emitter between two enemy communications devices so that the noise blocks the message. As a general rule, the cost of transmitting a signal of given strength (being largely a matter of power chemistry) may not change very fast. However, the adroit use of digital waveforms, the ability to exploit spread-spectrum and frequency-hopping to hide a narrowband message within a wideband slice of spectrum, and the reduced cost of making receivers are lengthening the edge enjoyed by message senders over message blockers. Tomorrow's phased-array receivers should be able to focus on a transmitter of known location and tune out interference from the side. Thus, if the jammer does not sit between the receiver and the transmitter, it can get in the way only by generating far more power. Phased-array receivers may well become commercial items (the increasingly scarce spectrum can be reused if receivers can be pointed at a specific transmitting antenna to the exclusion of others around it).

Radar jamming still has some life, however, because the source of the signal, as it were, is the reflection off the target, near which the jammer can fly, sail, or stand. The nearness of jammers and targets obviates the line-of-sight defense available to communicators. Radars may instead emit constantly changing pulsed digital waveforms and collect an electronically unique signature, coupling that with mathematical techniques that help separate signal from noise.

As for spoofing and interception, any message as long as a short paragraph may be protected with cryptographic techniques. Transmitters equipped with a private digital key can add a signature tag to a message; this tag can authenticate the transmitter's identity and the fact that the message has not been corrupted.[7] (If the message is

[7]The message is mapped into a unique 128-bit hash, which is then processed together with the private key to form a signed block. The receiver takes the public key, reverse-processes the block, extracts the hash, and checks for consistency between the

time-stamped, it cannot be echoed deceptively, either.) Encryption is a well-known defense against eavesdropping. Until recently, encoding everything would have been computationally burdensome, but cheap electronics have ended that problem. Barring some unforeseen mathematical breakthrough or the development of quantum computers of sufficient size (unlikely before 2020), the time required (even by a palmtop) to encode a message will fall—regardless of whether corresponding advances in supercomputers require longer keys to preserve message confidentiality.

In sum, while electronic warfare has always been a seesaw affair, developments over the next 20 years will continue to favor the bits getting through and will generally favor their being read.

Command-and-Control Warfare

The third target for information warfare is the command center itself, using shot and shell to disable the commanders, destroy the command apparatus, or sever the wires and fibers to fielded forces. Electronics are also vulnerable to such soft-kill techniques as microwave bursts and electromagnetic pulses. Apart from the obvious ability to put a precision weapon anywhere within an identified command center, the really new feature of C2 warfare is the modern military's dependence on keeping information systems going—a dependence whose importance, in some respects, even surpasses the importance of keeping individual commanders safe from harm.

But here, again, the vulnerability of command centers may have already peaked because of the proliferation of digital electronics. The traditional architecture of information systems involved large, complex central office switches and mainframe computers. But trends everywhere are toward dispersion. Central office switches are being replaced by routers of decreasing size and increasing number; fixed routing is being replaced by packet switching, thereby permitting every packet to take a different route. Network trees can be replaced by network meshes. Large computers are being replaced by conglom-

---

message and the hash. A time-stamp confounds problems that could arise if the interceptor were to echo the original message back. Similar techniques using private and public keys can be used to exchange other keys that permit more-efficient and harder-to-break symmetric code breaking to be performed.

erations of smaller ones. Fixed storage is being replaced by redundant arrays of independent disks capable of being distributed throughout a network. From late 1993 to late 2002, for instance, the cost of hard storage fell by a factor of 1,000, a drop roughly twice as fast as that for the cost of processors (as measured in dollars per instruction/second). Although the cost of laying a line of fiber is unlikely to decline much, the capacity of that fiber is nearly limitless. If redundant lines are paid for and used, only one line need survive to support all the traffic needed, as long as increasingly sophisticated routing algorithms can redirect traffic at a moment's notice. Finally, dispersed power sources, such as photovoltaics and fuel cells, promise to make information systems at least somewhat independent from the still-vulnerable power grid.

Technology even offers a way to protect the command hierarchy. Given the growing realism of videoconferencing, the utility of whiteboarding[8] tools, and shared access to databases, people no longer need to be physically drawn together for command conferences. This limits the vulnerability of a force's leadership to a lucky strike. And so, the bottom line remains the same. Whereas modern militaries are increasingly dependent on information systems, the technological advances that have made dependence so attractive are also available to protect such systems with increasing confidence.

Psychological Operations

What of decisionmakers themselves? Here the ancient truism comes to the fore: to make adversaries yield, it helps if they are convinced that the benefits of cooperation are high, the cost of resistance is destruction, and that they are operating against the will of the heavens. As a general rule, the dependence of militaries on human factors is no greater than it always has been.

Psychological operations may be defined as the use of information to affect human decisionmaking. They range from attempts to influence the national will, to deception against the opposite commander, to propaganda against opposing forces. The broader term, *psy-*

[8]Whiteboarding is the ability to put a word, picture, etc., on a screen that then appears on all screens of all people in a session.

chological warfare, refers to all aspects of combat that affect the willingness of people to fight above and beyond any physical harm that befalls them. Ultimately, however, there is no form of warfare that is not, to one degree or another, psychological warfare.

Some aspects of psychological operations perforce vary with specific circumstances and power relationships (e.g., among politicians, military officers, and military forces). Other aspects reflect pervasive trends. One such trend is the growing openness of societies to external influences—from cable television, direct broadcast television and radio, and the Internet. Over the next 10 years, the proliferation of space-based multimedia broadcast satellites, the continual spread of fiber optic lines, decent language-translation software, the proliferation of remote sensing satellites in commercial hands, and the possibility of agents and bots that can transfer satisfying answers to vaguely worded questions should increase permeability much further.

Will technology make psychological operations more rewarding? Citizens, soldiers, and commanders will be subject to a vast array of data sources, making it harder to cut them off from what the world is saying and to cut the world off from what they are saying and seeing. Further, media dominance by a handful of major networks is moving toward an era of 500-channel television and into Me-TV, where the low cost of creating a video feed and the ability to mix and match sources mean that everyone's news sources are different. The more the potential sources of information cover any one incident (think the random videotaping of the Rodney King incident), the harder it becomes to put out a single effective story line.

The saving grace for the information warrior who wishes to deceive others is still the human tendency to jump to conclusions, willingly consuming supporting evidence, and filtering out everything else. A case in point is Hitler's certainty that the Allies would invade Europe at Calais. Here, too, the evolution of information technology is of little help to tomorrow's information warrior.

The Ghost in the Machine

The most insidious form of information warfare, and the one that has garnered the most media and high-level policy attention, is the abil-

ity to get inside information systems in order to render them dysfunctional. If subverted in this way, an information system may work poorly or collapse, permit the entry of corrupted information, or reveal its secrets. Possible hacker entryways include surreptitiously inserting code into the machine at birth (e.g., through deliberately queered circuitry) or later (e.g., viruses), and assuming the identity of an authorized user—or, better yet, a systems administrator—and issuing malicious commands.

For this type of information warfare, cost factors that lead to a proliferation of nodes work against defenders. The more nodes on a system, the more doors for a hacker to try and the more difficult to find the hacker's entryway and where the corruption actually lies. The ability of one node to transfer instructions or control to another permits, among other things, very agile routing around damage, but it also permits vicious viruses, bad bots, and aggravating agents to spread quickly throughout a system.

Clearly, therefore, hacker warfare is more likely to be effective in at least the near future than it has been in the past. But does that mean that hacker warfare can be anything more than a minor annoyance or the source of random damage? That was the case for the April 1999 Chernobyl virus and the October 2001 Code Red Worm, even though both caused hundreds of millions of dollars of damage.

In gauging the effectiveness of future hacker attacks, it is useful to classify information systems into castles and agoras. *Castles* are a nation's critical infrastructures—military C4ISR systems, funds transfer, safety regulation, power plants and similar industrial facilities, telecommunications switching systems, and energy and transportation control points. They are, or should be, generally self-contained units, access to which can and ought to be restricted. *Agoras* are the great consumer marketplaces of cyberspace, in which increased vulnerability to malice, accident, and dysfunction is the price paid for the dense interactions and potential learning experiences that contact with strangers permits. It is as hazardous to use the rules of the agora to govern the castle as it is constricting to enforce the castle's norms on the agora.

In the short run, predicting the course of information security almost requires predicting where the next set of mistakes will be made.

Complexity seems to swing the advantage toward the hackers, who know that finding just a single breach may open the floodgates. But complex systems need not necessarily be insecure. You, the readers, who are several orders of magnitude more complex than any man-made system, are proof of that. No combination of bits that you can read right now could wreak havoc in your operating system. I, the author, have no authority to make you do stupid things. You process these words not as instructions to be obeyed but as data to be analyzed.

Processing inputs as information is the key here. As systems grow more sophisticated, they are likely to become more humanlike. They will be able to absorb data from beyond themselves, filter those data, and analyze them with a sophistication that grows with everything learned—just as humans do. True, critical castle systems can and probably should still be isolated. But the agora systems are fair game. And so, information systems will be heir to the more subtle faults. A computer that analyzes intelligence on a country, for instance, may absorb the content of Web-based newspapers, police reports, crop statistics, tax records, and local bulletin boards to draw conclusions.

These conclusions may, for their part, be influenced by what others—often self-serving and sometimes hostile—post, and computers will have to filter out the chaff to get the nuggets. Learning systems, such as neural nets and knowledge engineering devices, may be corrupted by bad information introduced at an unknown time, the discovery of which may leave administrators wondering how much good learning has to be erased to remove the bad learning. But this is essentially no different from what humans do, and, so far, humans have coped. The result is that hacker activity will express itself not as looming catastrophe, but as the certainty of at least some level of pollution. And pollution is not warfare.

THE LESSON OF SEPTEMBER 11

Peter Schwartz, founder of the Global Business Network, once observed that even futurists consistently underestimate the effects of

technological inputs on the course of history.[9] What is underestimated is not the extent of change—i.e., seeing 1, forecasting 2, and realizing 4—but its breadth and depth. Were the problem a question of extent, the fix would be easy: double everything. But insufficient breadth and depth come from not seeing the variety of change, a failure that an overactive imagination cannot easily fix.

The events of September 11 remind us of the inevitability of surprise. Suicide bombers, the use of airplanes to attack symbolic monuments,[10] the anti-American sentiments held by fundamentalist Muslims, and the special animus against the World Trade Center—none of these was particularly new on that day. One prominent futurist who asked what the worst thing a terrorist group could do to America was, was repeatedly told by security experts that it could crash a 747 into the World Trade Center. He thus learned to dismiss this scenario as a cliché. But the event, itself, was still a surprise. Had something of this magnitude taken place in cyberspace rather than in real space, several information warfare gurus would have proclaimed, "I told you so." But they are not right, yet.

The success of the U.S. campaign against the Taliban regime validated, at least in that context, the hopes of believers in the current RMA. While neither the Taliban nor Al Qaeda is assuredly destroyed for all time, precision warfare, carried out in concert with willing if initially less-powerful allies, did in three months what the Soviet Union could not complete in 10 years.

---

[9]Peter Schwartz, *The Art of the Long View: Planning for the Future in an Uncertain World,* Doubleday, New York, 1996.

[10]Several years earlier, French security forces forestalled a plot to launch a jet into the Eiffel Tower.