Chapter Seven

WARFARE IN THE INFORMATION AGE*

Bruce D. Berkowitz

Pentagon officials and defense analysts have a new topic to add to their list of post–Cold War concerns: information warfare, or IW, in the usual manner of military-speak. The term refers to the use of information systems—computers, communications networks, databases—for military advantage, either by the United States or by a variety of unfriendly parties.

IW is drawing increasing attention for at least two reasons. First, the United States is potentially vulnerable to IW attack. The United States, in civilian as well as military matters, is more dependent on electronic information systems than is anyone else in the world. In addition to the possibility that computer and communications systems might prove to be a vulnerable weak link for military forces, there is also a danger that hostile parties—countries, terrorist groups, religious sects multinational corporations, and so on—could attack civilian information systems directly. Attacking these systems could be easier, less expensive and certainly less risky than, say, sabotage, assassination, hijacking or hostage-taking, and a quick cost-effectiveness calculation may make IW an aggressor's strategy of choice.

The second reason why the defense community is so intrigued with IW is that it may be as much an opportunity as it is a threat. The United States may be able to develop new military strategies using

*Bruce Berkowitz, "Warfare in the Information Age," *Issues in Science and Technology*, Fall 1995, pp. 59–66.

IW that are perfectly tailored to world conditions following the Cold War. Information technology is a U.S. strong suit, and military forces could use this know-how to improve our defense capabilities, perhaps dramatically, against hostile attack and to defeat any aggressors—and to accomplish both missions at the lowest possible cost. Indeed, U.S. military planners are already taking the first steps in this direction.

Yet, despite all of the attention the IW is receiving, several basic questions about information warfare remain to be resolved. These include:

- What is the actual IW threat, and how much should the United States worry about it? IW aficionados have suggested a number of scenarios in which IW might be used against us, but other observers think at least some of them are far-fetched.
- If the IW threat is real, what does the United States need to do in order to protect itself? Conversely, what must we do in order to make the most of the IW opportunity?
- As a practical matter, how should information warfare be integrated into overall U.S. defense planning? Will IW replace some military capabilities or merely supplement them? Should IW be considered "special," like atomic weapons or chemical weapons, and kept separate from other military forces, or should IW be part of the military's overall organization and planning process?
- What are the implications of IW for current concepts of offense, defense, coercion, and deterrence? For example, is it more difficult to deter an IW attack? Does information warfare automatically escalate to conventional warfare, or vice versa?
- What is the relationship between the military and civilian society in preparing for information warfare? Also, how can the nation protect democratic values—namely, freedom of expression and personal privacy—while taking the measures necessary to defend against an IW threat?

These are very basic issues. We have experience in dealing with similar questions in other areas of defense policy, but information warfare is in many ways quite different. So, if the world is indeed entering an Information Age and IW has the potential to improve, un-

dermine, or just generally complicate U.S. military planning, we need to address such issues now.

ORIGINS OF THE THREAT

Military weapons and military strategy usually reflect the politics, economy, and—most especially—the technology of any given society. Even the writers of scripture understood the technological relationship between plowshares and swords, and we take for granted the two-sided nature of nuclear power, long-range jet aircraft, and rockets. Thus, today's improvements in computers, communications, and other electronic data-processing systems that are driving economic growth and changing society are also changing military thinking and planning.

Armies have always used information technology—smoke signals in ancient days, telegraphs at the turn of the century, precision-guided munitions today—but until recently information systems were second in importance to "real" weapons, such as tanks, aircraft, and missiles. Today, information systems are so critical to military operations that it is often more effective to attack an opponent's information systems than to concentrate on destroying its military forces directly.

Also, because modern societies are themselves so dependent on information systems, often the most effective way to attack an opponent is to attack its civilian information infrastructure—commercial communications and broadcasting networks, financial data systems, transportation control systems, and so on. Not only is this strategy more effective in crippling or hurting an opponent, but it often has some special advantages of its own, as will be seen.

Some recent books and films have raised the issue of information mayhem, although they may have exaggerated the dangers. High school students cannot phone into the U.S. military command-and-control system and launch a global thermonuclear strike (à la the 1984 movie *War Games*), and it would be hard for a band of international cyber-terrorists to totally eradicate a woman's identity in the nation's computer systems (as in this year's screen thriller *The Net).*

But consider some of the scenarios that the Department of Defense has studied:

- Approximately 95 percent of all military communications are routed through commercial lines. U.S. troops depend on these communications; in some cases, even highly sensitive intelligence data is transmitted in encrypted form through commercial systems. Although hostile countries may not be able to intercept and decipher the signals, they might be able to jam the civilian links, cutting off U.S. forces or rendering useless numerous intelligence systems costing hundreds of millions of dollars.
- The United States buys most of the microchips used in military systems from commercial vendors, many of which are located in foreign countries. The chips are dispersed throughout a variety of weapons and perform a range of functions. Some experts are concerned that someone might tamper with these chips, causing the weapons to fail to perform when needed.
- One lesson of Operation Desert Storm is that it is unwise to provoke a full-scale conventional military conflict with the United States and its allies. A more subtle alternative might be to send several hundred promising students to school to become computer experts and covert hackers. Such a cadre could develop the training and tactics to systematically tamper with U.S. government and civilian computer systems. But unlike pranksters, they would play for keeps, maximizing the damage they cause and maintaining a low profile so that the damage is hard to detect.
- Some strategic thinkers believe that "economic warfare" between countries is the next area of international competition. This may or may not be so, but it is possible for government experts, skilled in covert action, to assist their countries' industries by well-designed dirty tricks. For example, a bogus "beta tester" could sabotage the market for a new software product by alleging on an Internet bulletin board that the prerelease version of the program has major problems.
- Modern military aircraft, such as the B-2 bomber and F-22 fighter, are designed without a single blueprint or drawing. Rather, they use computer-assisted design/computer-assisted manufacturing (CAD/CAM), in which all records and manufac-

turing instructions are maintained on electronic media and shared on a closed network. This makes it possible for plants across the country to share databases and to manufacture components that fit together with incredible precision. But it also makes these programs dependent on the reliability and security of the network, which might be compromised by an insider with access.

- Like many large-scale industrial operations today, the military uses "just-in-time" methods for mobilization. That is, to cut costs and improve efficiency, the military services trim stockpiles of spare parts and reserve equipment to the minimum, and they use computers to make sure that the right part or equipment is delivered precisely when needed to the specific user. If the computers go down, everything freezes.
- There is a hidden "data component" in virtually every U.S. weapon system deployed today; this component may be in the form of targeting information that must be uploaded into a munitions guidance system or a "signature" description that tells the guidance sensor what to look for on the battlefield (for example, the distinctive infrared emission that a particular type of tank produces from its exhaust). If this information is unavailable or corrupted, even the smartest bomb regresses into stupidity.

DOD and think tanks have in recent years been actively studying the national security threats that these and other IW scenarios present to U.S. security. But it is also important to remember that, in addition to the threat to military forces, many of these same vulnerabilities apply to commercial industry and the civilian infrastructure. Virtually all communications systems are computer-controlled. Virtually all aircraft and land vehicles have computer-based components. Most transportation systems—aircraft, railroads, urban transit—are directed by remote communications and computers. Thus, virtually all of these civilian systems are also vulnerable to IW attack and could become targets to unfriendly parties.

THE CHANGING FACE OF WAR

One way to understand the impact of IW on military thinking is to recall the evolution of mechanized warfare. Beginning in the mid-1800s, the Industrial Revolution made it possible to develop new weapons that were much more capable than anything produced before: mass-produced machine guns, steam-powered armored warships, long-range artillery capable of hitting targets from several miles away, and so on. The military also benefited from technology that had been developed mainly for civilian purposes, such as railroads and telegraphs, which vastly improved the ability of military forces to mobilize and to maneuver once they arrived at the battlefield. War became faster, longer-ranged, and more deadly. Just as important, new technology also created new targets. Military forces became critically dependent on their nation's industrial base—no factories, no mass-produced weapons, and no mass-produced weapons meant no victory. So destroying a nation's industrial base became as important as destroying its army, if not more so.

The result was not just an adjustment in military thinking but a complete rethinking of how to wage war. Military planners began to understand that the faster, longer-range weapons offered the opportunity of leapfrogging the front lines on a battlefield in order to destroy an enemy's factories, railroads, and telegraph lines directly. A classic case in point is the progression from the invention of the airplane to the development of the entirely new doctrine of strategic bombing. Moreover, these military planners realized that such an expanded warfare plan was not only a possibility; in many cases, it was likely to be the dominant strategy.

Today's information revolution presents a similar situation. And just as new theories and doctrines were developed for industrial-age warfare, so have thinkers begun to develop a theory and doctrine of IW. As with mechanized warfare and strategic bombing, where it took awhile for military thinking to catch up with technology, IW concepts have required a few years to mature. In fact, just as aircraft had been in use for almost three decades before the doctrine of strategic bombing was invented, the roots of IW also go back many years. For example, most of the tactics envisioned for attacking an opponent through its information systems—destruction, denial, exploitation, and deception—can be traced to classical military and

intelligence fields, such as signals intelligence and cryptography, electronic countermeasures and jamming, "black" propaganda and disinformation, and measures for concealment and camouflage.

What stands clear today is that information technology has reached critical mass. Information systems are so vital to the military and civilian society that they can be the main targets in war, and they can also serve as the main means for conducting offensive operations. In effect, IW is really the dark side of the Information Age. The vulnerability of the military and society to IW attack is a direct result of the spread of information technology. Conversely, IW's potential as a weapon is a direct result of U.S. prowess in information technology.

Indeed, many of the problems of dealing with IW are linked to the nature of information technology itself. The most important feature may simply be the falling cost of information processing; since the 1950s costs have declined at a rate of about 90 percent every five years, and most experts expect this trend to continue for the foreseeable future. One result is that information technology—and, with it, the ability to play in the IW game—is constantly becoming more available, and quite rapidly. Unlike nuclear weapons technology or aerospace weapons technology, which have been spreading steadily but slowly, the diffusion of IW technology is likely to accelerate. If a party cannot afford some form of information technology and IW capability today, it probably will be able to afford the technology tomorrow. This is evidenced in the spread of dedicated military electronic systems, but even more in the availability of commercial information technology such as computer networks, satellite and fiber-optic communications, cellular telephone systems, and so on. All of these can be used for hostile purposes, and can be attacked by a hostile power.

A second feature of information technology that affects IW is that as the technology becomes cheaper and cheaper, it becomes less and less efficient to control information from a central authority. Indeed, one reason for the current increasing pressure in society to decentralize government, corporations, and other organizations is that low-cost information technology makes it affordable and feasible to decentralize. The demand and incentives for decentralization are following the technological opportunity.

This trend runs counter to several centuries of military tradition and experience, which are based on hierarchical command structures, rank, and centralized control. The new technology does not support the traditional military model. Also, the trend toward decentralized information systems changes the government's ability to interact with the commercial sector. As result, national security officials and military planners must find new ways of issuing instructions and implementing policies.

DEALING WITH INFOWAR

With these characteristics in mind, it is possible to discuss some specific issues and problems the United States will face in dealing with information warfare.

The IW threat will grow because entry costs are low. As the cost of information technology falls, a greater number of foreign governments and non-government organizations will present a potential IW threat to the United States. Countries that could not match the United States and its Western allies in expensive modern weapons systems, such as tanks, aircraft, and warships, will be able to buy the computers and communications systems necessary to carry out IW.

One defining feature of the post–Cold War era has been that the single, large threat of the Soviet Union has been replaced by a greater number of lesser threats. The declining cost of information technology has facilitated this trend, and many of the new threats will take the form of IW. As a result, the U.S. military will need to think about IW threats coming from a number of different directions.

To complicate matters further, each threat will probably be somewhat different. One terrorist group might like to fiddle with transportation control systems; another might be dedicated to compromising DOD databases. In the past, the United States has tailored its forces and plans to deal with the single Soviet threat, and has assumed that, if it could defeat the Soviet Union militarily, it could also deal with what the Pentagon calls "lesser included threats." In the IW world, threats are likely to be as varied as tailored software, and U.S. military forces will need to deal with each on its own terms.

There will be an international learning curve. Not only will more players engage in IW, they will steadily get better at it. Because information is so easily transferred, everyone can quickly learn from the IW mistakes that others make. For example, Desert Storm was essentially a situation in which one side fought a classical 20th-century conventional war while the other side fought a classical 21st-century IW war. The Iraqi army was not out-gunned: indeed, it had a numerical edge, as well as the advantages of fighting from prepared defensive positions and its experience in battle gained during Iraq's decade-long war with Iran. The U.S. advantage was in information technology—intelligence, communications, precision-guided munitions, night vision equipment, stealth technology, and electronic countermeasures. As a result, the United States and its coalition partners were well-coordinated and could adjust their operations in real time, whereas Iraqi forces were isolated, disorganized, and blind.

It's unlikely future foes will repeat Iraq's mistakes and permit opponents such a free hand in the contest for what DOD has taken to calling "information superiority" on the battlefield. Indeed, a country or organization with even a rudimentary knowledge of IW could take countermeasures that can greatly reduce the U.S. advantage. The upshot is that the United States will have to work hard and persistently in order to maintain its present IW advantage. Also, because the U.S. advantage could potentially be tenuous and fleeting, it will be necessary to monitor the changing IW threat and develop the systems and expertise necessary to deal with it.

THE CHANGING FACE OF DETERRENCE

During the past 50 years, a well-developed body of theory about conventional and nuclear deterrence has accumulated. Although Star Wars advocates may quibble, most strategic thinkers would agree with U.S. military analyst Bernard Brodie, who noted in 1947 that it is hard to mount a foolproof defense against nuclear attack, so the more plausible strategy is to deter a nuclear attack through the threat of retaliation. Alas, the problem seems doubled for IW. So far, evidence suggests that not only will defense against IW be difficult; even an effective plan for deterrence will be hard to pull off.

One of the greatest difficulties in deterring a would-be IW threat is that an attacker may be anonymous. A country or nongovernmental

group could tamper with U.S. communications and computer systems just enough to cause damage, but not enough so the perpetrator can be identified. To paraphrase a metaphor offered by Thomas Rona, a long-time IW thinker, we will be unlikely to find a smoking gun because our opponents will likely use smokeless powder. With no "attacker ID," it would be hard to determine who deserves retaliation, and without the threat of retaliation, deterrence usually fails. Indeed, a truly diabolical enemy would most likely adopt the strategy of an unseen parasite, quietly causing problems that would be attributed to normal glitches we routinely accept with software and information systems. (Have you tried installing OS-2 Warp or Windows 95 on your computer? Many people simply expect electronics to be difficult.)

Another problem for deterrence is that, even if an IW attack is identified, it may be difficult to develop an effective option for retaliation. As one DOD official has said, "What are we going to do, nuke them for turning off our TVs?" An IW attack may be just crippling and expensive, rather than lethal, so conventional retaliation (say, an airstrike) may be unpopular. On the other hand, because the United States is so dependent on information technology, we would likely come out on the losing end of a game of IW tit for tat. And mere diplomatic responses are likely to be ineffective.

Who will be responsible for IW? In the past, the usual response of the military to a new technology has been to assign responsibility for it to a new organization; for example, the Strategic Air Command (now simply Strategic Command) was created to assume responsibility for long-range bombers and missiles. Indeed, within DOD responsibility for information technologies has historically been assigned to specific organizations—the National Security Agency (NSA) in the case of signals intelligence and information systems security, the Central Intelligence Agency (CIA) in the case of covert operations such as black propaganda and covert political action, the National Reconnaissance Office (NRO) in the case of surveillance satellites, and so on.

Currently, each of the military services is developing an IW strategy to assist it in developing new weapons and doctrine, and commanders of U.S. military units deployed in the field are developing plans for IW in their theater of operation. DOD officials have mused—

briefly—whether to consolidate responsibilities for IW in a single organization. Most have quickly concluded that this would not make sense. Not only would there be turf battles among existing organizations; such an organization would be inconsistent with the trend in which information systems are, in fact, becoming more decentralized.

Indeed, the more appropriate question may be why we need large operating organizations such as NSA and NRO when information systems are becoming cheaper, networked, and decentralized. It may soon be more efficient for military units to operate their own signals intelligence and even reconnaissance systems. There already is some movement in that direction; for example, Army and Navy units operate their own reconnaissance drone aircraft.

The objective should be to permit IW technology to spread throughout the DOD organization while ensuring that IW operations are coordinated so that they are consistent with national policy and the strategy of military commanders. At the same time, DOD needs to ensure that IW systems in the military can operate with each other and with those in the civilian world, without creating an unwieldy bureaucracy or body of specifications.

PLANNING FOR IW "CIVIL DEFENSE"

Planning for IW requires cooperation between the defense sector and the commercial sector. Civilian information systems are prime candidates for attack. So just as cities are targeted in strategic bombing, in future wars we can expect civilian information systems to be hacked, tapped, penetrated, bugged, and infected with computer viruses.

Another reason for cooperation is that DOD itself depends heavily on the civilian information infrastructure. As noted earlier, not only does the military use civilian information systems for "routine" activities such as mobilization; sometimes even the transmission of sensitive intelligence data is routed through commercial links. Obviously, it would be impossibly expensive for DOD to make the entire civilian information infrastructure secure to military standards. And even if it were affordable, the passwords, encryption systems, and

other security measures would make it incredibly inconvenient for public use.

Moreover, the government's ability to control or influence the civilian information industry is limited. DOD lacks the leverage it has enjoyed in other situations. For example, the Air Force can influence the design of spacecraft because it is the largest operator of space systems, but DOD's share of the total computing and communications market is quite small compared with commercial users. Also, today's commercial information industry is often ahead of the defense industry in developing new technology. So, whereas DOD once could effectively create industry standards in order to enhance security through its leading-edge role in research and development and its buying power, standards are now being set by companies in the market. Add to this the burgeoning information industry worldwide and DOD's influence is diminished further.

The upshot is that DOD cannot use traditional-style directives or specifications to improve the ability to defend the nation against the IW threat. If it tries, no matter how well-intentioned, it will likely fail. As evidence, consider the recent Clipper Chip episode, in which the federal government tried to cajole and coerce the information industry to adopt a NSA-developed encryption system. The Clipper Chip was supposedly indecipherable, but critics claimed that any system designed by the government would permit the government to read messages using the code (in cryptography parlance, this is called "back door access"). According to the critics, the government's objective was to preserve the ability of NSA and law enforcement agencies to read encrypted communications that they intercepted.

Not only did the industry reject the Clipper Chip, but the government was unable to prevent private computer programmers from developing and illegally distributing their own encryption systems that the government supposedly could not crack or systems (such as SATAN) that can detect "back doors." The lesson of the Clipper Chip is that DOD must use a more sophisticated, less heavy-handed approach to get the civilian sector to take measures to protect itself against the IW threat. Because directives and standards usually will not work, DOD officials need to learn how to use incentive systems instead.

For example, simply informing industry and individuals that they could be IW targets will often lead them to adopt "street smart" information behavior to protect themselves from both foreign and domestic attack. DOD officials themselves have suggested that the government could encourage insurance companies to charge appropriately higher rates to corporations that did not take reasonable steps to protect their data or information systems (again, on the assumption that making the insurance companies aware of the damage an IW attack could cause will generally suffice). In cases in which DOD is critically dependent on a civilian information link, it may even make sense for the government to subsidize the civilian operators so that they adopt protective measures.

In other cases, the government may need to face that some of its traditional activities will simply no longer be possible—for example, easily reading most transmissions that it intercepts. Instead, the government could concentrate on providing industry with the means to protect its information system. Indeed, in at least some cases it would seem that using the government's technical expertise to give U.S. industry an edge in the IW wars may do more for national security than collecting and decoding signals.

ENSURING DEMOCRATIC CONTROL OF IW POLICY

Reconciling information security obviously collides with allowing easy access to information systems and freedom of expression. However, IW presents another problem for American democracy.

It is possible to imagine ways in which offensive IW tactics might cost less or be more effective than conventional military options; suffice it to say that almost all the tactics ascribed to our opponents could, at least potentially, be considered for adoption by the United States. Yet the defense community rarely discusses the offensive use of information warfare. The reason for this reticence is that, like intelligence plans and systems, IW options are easily compromised once the opponent learns about them. Even in the case of defensive IW, some government officials are reluctant to discuss the threat, thinking that raising attention to U.S. vulnerabilities will encourage new groups to target the United States.

The problem is that it will be hard to integrate IW into U.S. defense planning without building public support. Citizens will need to understand why the government is undertaking IW programs and how the programs may permit other military programs to be phased out. Without public discussion and understanding of how IW capabilities might replace some conventional military systems, the nation may needlessly spend money for both conventional and IW programs. Secrecy also tends to increase costs by limiting competition and reducing the ability of DOD to draw on unclassified and commercial programs. One reason why commercial information technology is usually equal or superior to its military counterparts, and almost always less expensive, is that greater competition in the private sector forces innovation and pushes down prices.

Unless U.S. leaders deal with the problem of reconciling secrecy and democracy, IW will likely remain a marginal asset. In fact, the political system has considerable experience in dealing with such issues; nuclear weapons, intelligence operations, and covert action are all routinely reviewed by Congress and, at a more general level, are discussed in the public media. It seems reasonable that the nation can also have a public debate over the place of IW in U.S. defense policy without compromising the policy itself.

PRESCRIPTIONS FOR PREPAREDNESS

Dealing with the IW threat and especially with aggressive attackers who use IW as their main weapon against the United States will require new approaches. In most cases, it will probably be impossible to build a foolproof defense for the civilian information infrastructure. But it should be possible to prevent "cheap kills" by informing the general public and industry of the threat through formal and informal networks for government-civilian cooperation.

In the case of vital military communications links and computer systems, it may be possible to build hardened "point defenses," taking extra steps to thwart attackers. These could include, for example, building dedicated transmission lines for communications, isolating critical computers from all outside networks, and using hardware and software security systems that might be excessively expensive or inconvenient for commercial use but which are necessary for vital DOD systems. These measures would also need to be repeated in the

production of hardware and software, and in some cases dedicated production lines might be necessary for the most sensitive systems.

Yet, because defense and deterrence are both so difficult to achieve in IW, the best strategy to protect the most vital information systems may be stealth—keeping the very existence of such an information system a secret so that it does not become a target. Of course, "secret information system" is the ultimate oxymoron, which is another way of saying that such systems will also likely be among the most expensive, inefficient, and difficult to use.

The most challenging measures, though, are likely to be political, economic, and cultural. IW requires new concepts within DOD because traditional approaches to military planning and military command and control will not work for it. And the same is true across society, where the measures for countering the IW threat will often collide with the essential features of the democratic, free-market system that an IW policy is intended to protect.