NATIONAL DEFENSE UNIVERSITY

INSTITUTE FOR NATIONAL STRATEGIC STUDIES

WHAT IS INFORMATION WARFARE?

MARTIN C. LIBICKI

THE CENTER FOR ADVANCED CONCEPTS AND TECHNOLOGY

Directorate of Advanced Concepts, Technologies, and Information Strategies (ACTIS)

The Directorate of Advanced Concepts, Technologies, and Information Strategies (ACTIS), at the Institute for National Strategic Studies of the National Defense University, focuses on the future composition and employment of instruments of national power by Departments, Agencies, and organizations that comprise the national security establishment. ACTIS is responsible for developing an understanding of the mission challenges that the United States will face and the technological capabilities that will be available to meet these challenges. ACTIS consists of the Center for Advanced Concepts and Technology (ACT) and the School for Information Warfare and Strategy.

❖❖❖

Center for Advanced Concepts and Technology (ACT)

ACT identifies and develops approaches to critical operational problems of command and control. The Center pursues a broad program of basic research in command and control theory, doctrine, and use of emerging technology. It also develops new concepts for command and control in joint, combined, and coalition operations other than war. Additionally, the Center promotes the study of command and control at all service schools. To complement research, the Center provides a clearinghouse and archive for command and control research, publishes books and monographs, and sponsors workshops and symposia.

What Is Information Warfare?

Martin C. Libicki

THE CENTER FOR ADVANCED
ACT
COMMAND CONCEPTS AND TECHNOLOGY

August 1995

Center for Advanced Concepts and Technology
Institute for National Strategic Studies

NATIONAL DEFENSE UNIVERSITY

NATIONAL DEFENSE UNIVERSITY

- *President:* Lieutenant General Ervin J. Rokke, USAF
- *Vice President:* Ambassador William G. Walker

INSTITUTE FOR NATIONAL STRATEGIC STUDIES

- *Director:* Dr. Hans A. Binnendijk

DIRECTORATE OF ADVANCED CONCEPTS, TECHNOLOGIES AND INFORMATION STRATEGIES (ACTIS)

- *Director:* Dr. David S. Alberts

CENTER FOR ADVANCED CONCEPTS AND TECHNOLOGY

- *Director:* Captain William H. Round, USN
- Fort Lesley J. McNair, Washington, DC 20319-6000
- Phone: (202) 287-9310 ♦ Facsimile: (202) 287-9239

Opinions, conclusions, and recommendations, expressed or implied, are those of the authors. They do not necessarily reflect the views of the National Defense University, the Department of Defense, or any other U.S. Government agency. Cleared for public release; distribution unlimited.

Library of Congress Cataloging-in-Publication Data
What is Information Warfare / Martin C. Libicki
1. Information Warfare. I. Title
U 163.L53 1995
355.3'43—dc20

95-32983
CIP

First Printing, October 1995
Second Printing, March 1996
Third Printing, September 1996

For sale by the U.S. Government Printing Office
Superintendent of Documents, Mail Stop: SSOP
Washington, DC 20402-9328 • Phone: (202) 512-1800

Contents

TABLES

ACKNOWLEDGMENTS

The author gratefully acknowledges the very kind help of the following people who provided information for or reviewed and commented on previous versions of this report:

David Alberts
John Alger
Kenneth Allard
Dorothy Denning
Seymour Goodman
Delonnie Henry
Stuart Johnson
Brian McCue
Anthony Oettinger
Capt. Richard O'Neill
Ellin Sarot
Marilyn Z. Wellons

Acronyms

AWAC	airborne warning and control system
C2W	command and control warfare
CD-ROM	compact disk/read-only memory
CDMA	code division multiple access
CIA	Central Intelligence Agency
CNN	Cable News Network
DBS	direct broadcast satellite
DES	Data Encryption Standard
DoD	Department of Defense
EIW	economic information warfare
EW	electronic warfare
FLIR	forward-looking infrared
GPS	Global Positioning System
HARM	High-speed Anti-Radiation Missile
IBW	information based warfare
IR	infrared
JCS	Joint Chiefs of Staff
JSTARS	Joint Surveillance, Targeting, and Radar System
MILSPEC	military specification
MOP	Memorandum of Policy
NASDAQ	National Association of Securities Dealers Access Quotation
NIST	National Institute of Standards and Technology
NSA	National Security Agency
OODA	observe orient decide act
PBX	private branch exchange
PC	personal computer
PKE	public key encryption
SAR	synthetic aperture radar
SOF	special operations forces
STU	secure telephone unit
TS	top secret
UAV	unmanned aerial vehicle

Preface

In recent years, a concept known as "information warfare" has become popular within certain circles of the U.S. defense establishment. The concept is rooted in the indisputable fact that information and information technologies are increasingly important to national security in general and to warfare specifically. According to this concept, advanced conflict will increasingly be characterized by the struggle over information systems. All forms of struggle over control and dominance of information are considered essentially one struggle, and the techniques of information warfare are seen as aspects of a single discipline. Those who master the techniques of information warfare will therefore find themselves at an advantage over those who have not; indeed, information warfare will, in and of itself, relegate other, more traditional and conventional forms of warfare to the sidelines. If it takes information warfare seriously enough, the United States, as the world's preeminent information society, could increase its lead over any opponent. If it fails to do so, proponents argue, it may be at considerable disadvantage, regardless of strengths in other military dimensions.

This essay examines that line of thinking and indicates several fundamental flaws while arguing the following points:

- Information warfare, as a separate technique of waging war, does not exist. There are, instead, several distinct forms of information warfare, each laying claim to the larger concept. Seven forms of information warfare—conflicts that involve the protection, manipulation, degradation, and denial of information—can be distinguished: (*i*) command-and-control warfare (which strikes against the enemy's head and neck), (*ii*) intelligence-based warfare (which consists of the design, protection, and denial of systems that seek sufficient knowledge to dominate the battlespace), (*iii*) electronic warfare (radio-electronic or cryptographic techniques), (*iv*) psychological warfare (in which information is used to change the minds of friends, neutrals, and foes), (*v*) "hacker" warfare (in which computer systems are attacked), (*vi*) economic information warfare (blocking information or channelling it to pursue economic dominance), and (*vii*) cyberwarfare (a grab bag of futuristic scenarios). All these forms are weakly related. The concept of information warfare has as much analytic coherence as the concept, for instance, of an information worker.

- The several forms range in maturity from the historic (that information technology influences but does not control) to the fantastic (which involves assumptions about societies and organizations that are not necessarily true).

- Although information systems are becoming important, it does not follow that attacks on information systems are therefore more worthwhile. On the contrary, as monolithic computer, communications, and media architectures give way to distributed systems, the returns from many forms of information warfare diminish.

- Information is not in and of itself a medium of warfare, except in certain narrow aspects (such as electronic jamming). Information superiority may make sense, but information supremacy (where one side can keep the other from entering the battlefield) makes little more sense than logistics supremacy.

1 *Is There An Elephant?*

In the fall of 1994, I was privileged to observe an Information Warfare game sponsored by the Office of the Secretary of Defense. Red, a middle-sized, middle-income nation with a sophisticated electronics industry, had developed an elaborate five-year plan that culminated in an attack on a neighboring country. Blue—the United States—was the neighbor's ally and got wind of Red's plan. The two sides began an extended period of preparation during which each conducted peacetime information warfare and contemplated wartime information warfare. Players on each side retreated to game rooms to decide on moves.

Upon returning from the game rooms, each side presented its strategy. Two troubling tendencies emerged: First, because of the difficulty each side had in determining how the other side's information system was wired, for most of the operations proposed (for example, Blue considered taking down Red's banking system) no one could prove which actions might or might not be successful, or even what "success" in this context meant. Second, conflict was the sound of two hands clapping, but not clapping on each other. Blue saw information warfare as legions of hackers searching out the vulnerabilities of Red's computer systems, which might be exploited by hordes of viruses, worms, logic bombs, or Trojan horses. Red saw information warfare as psychological manipulation through media. Such were the visions in place even before wartime variations on information warfare came into the discussion. Battle was never joined, even by accident.

This game illustrated a fundamental difficulty in coming to terms with information warfare, deciding on its nature. Is it a new art? the newest version of some time-honored features of warfare? Is it a new medium of conflict that issues from the burgeoning global information infrastructure or one to which information technologies have contributed but which originates in the wetware of the human brain? Is it a unified covey of operations, or a random assemblage of fowl perched on a single power line?

Information warfare is a hot topic at the Pentagon and unavoidable in contemplating the future of warfare. It is linked to the Revolution in Military Affairs, which has assumed almost totemic importance in the conceptual superstructure of national defense. Recent tomes such as the Tofflers' *War and Anti-War*[1] have made it an article of faith that information technologies are transforming second-wave (industrial) societies into third-wave (information-based) ones. War must follow, which offers considerable comfort to

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

those who see the United States as having supremacy in handling information while its former supremacy in the industrial arts seems to be diminishing.

Coming to grips with information warfare, however, is like the effort of the blind men to discover the nature of the elephant: the one who touched its leg called it a tree, another who touched its tail called it a rope, and so on. Manifestations of information warfare are similarly perceived. Although some parts of the whole are closely related in form and function (e.g., electronic warfare and command-and-control warfare), taken together all the respectably held definitions of the elephant suggest there is little that is *not* information warfare.

Is a good definition possible? Does having one matter? Perhaps there is no elephant, only trees and ropes that aspire to become one. Clarifying the issues is more than academic quibbling. First, as the metaphor suggests, sloppy thinking promotes false synecdoche. One aspect of information warfare, perhaps championed by a single constituency, assumes the role of the entire concept, thus becoming grossly inflated in importance. Second, too broad a definition makes it impossible to discover any common conceptual thread other than the obvious (that information warfare involves information and warfare), where a tighter definition might reveal one. Third, the slippery inference derived from loose aggregation points to the conclusion that the United States can and must seek the dominance in information warfare it currently enjoys in air warfare, as if these arenas were comparable.

Thomas Rona, an early proponent of information warfare, offered the following definition:

> The strategic, operation, and tactical level competitions across the spectrum of peace, crisis, crisis escalation, conflict, war, war termination, and reconstitution/restoration, waged between competitors, adversaries or enemies using information means to achieve their objectives.

This definition is broad, too broad: one way or another, it subsumes most human activity. In a related view, information war exists to ensure that one's own picture of a conflict is more correct than that held by the other side. This perspective is useful but incomplete. All viewpoints are incorrect, because data cannot be incorporated without a conceptual structure to hang them on. Yet even the best structures are abstractions of a complex world. Whether the structures are biased in important and harmful or trivial and harmless ways is what matters.

The Joint Staff has faced great difficulty in assigning precise responsibilities even for military forms of information warfare (nonmilitary forms, for instance, include the defense of national financial systems against hackers). Command-and-control warfare (C2W) is assigned to J-3 (the operations directorate) within the Joint Chiefs of Staff. Designing command-and-control systems for security and protection is as clearly the province of J-6 (the C4 directorate).[2] Forms of information warfare that involve establishing and maintaining systems of battlefield intelligence, reconnaissance, and surveillance naturally fall under J-2 (the intelligence directorate). Finally, because most of the interesting issues of information warfare presume that the information architecture of the future will be different from that of the present, information architecture would be associated with long-term planning, which sits in J-5 (the strategic policy and plans directorate).

This essay attempts to sort out definitions of information warfare.[3] The first part reviews seven plausibly distinct forms of information warfare, each identified by one or another expert as a defining example of information warfare. Each is examined by asking what does it do, in what sense is it war, what does it owe to silicon technologies, and how well can

---

[2]Late in 1994, the two directorates negotiated a formal division of labor. How well that division holds up as the roles and missions of information warfare come up for decision remains to be seen.

[3]Readers are also pointed to Julie Ryan, "Offensive Information War," a paper presented to the Naval Studies Board of the National Research Council (Washington, DC), 8 Sept. 1993.

the United States, compared with others, wage it? Although information warfare is often regarded as new, some forms of it are newer than others. Some have been enabled by and others altered by information technology, while still others have only marginally been affected by it.

The second part of this essay searches for underlying themes. Do the forms of information warfare cohere well enough so that as a whole they can be assigned to information warriors in the sense that naval warfare is assigned to the Navy? To what extent are traditional concepts, such as "dominance," applicable to information warfare? Are there underlying principles, grasping and, ultimately, mastery of which may provide a conceptual framework for effective prosecution of information warfare? Indeed, is information warfare truly warfare?

A caveat: Those who search for an ideal definition should look elsewhere. The typology used here is intended to subdivide a large field into tractable parts—information warfare may better be considered a mosaic of forms, rather than one particular form.

2 *Seven Forms in Search of a Function*

Seven forms of information warfare vie for the position of central metaphor: command-and-control warfare (C2W), intelligence-based warfare (IBW), electronic warfare (EW), psychological warfare (PSYW), hacker warfare, economic information warfare (EIW), and cyberwarfare.[4]

As Anne Wells Branscomb has pointed out, "in virtually all societies, control of and access to information became instruments of power, so much so that information came to be bought, sold, and bartered by those who recognized its value."[5] Branscomb could have added, stolen and protected as well. This essay examines information warfare as the struggle over

---

[4]Seminal works plural on information warfare include: George Stein, "Information War—Cyberwar—Netwar," Air War College, 1993, and John Arquilla and David Ronfeldt, "Cyberwar Is Coming!" *Comparative Strategy*, **12** (1993), 141-165. The definitions used there differ from those used here. Netwar for those authors is akin to psychological warfare against both national will and national culture; cyberwar is command-and-control warfare, which broadly includes psychological operations against opposing commanders. The title used by Arquilla and Ronfeldt suggests that cyberwar lies directly in the future, yet Genghis Khan's use of psychological warfare gets a tenth of the article as does the North Vietnam's use. Coming, as such, must perforce include Came.

[5]Anne Wells Branscomb, *Who Owns Information? From Privacy to Public Access* (N.Y.: Basic Books, 1994), 1.

information processes rather than the efforts made to acquire information. Although the information systems required to manage logistics are substantial, they enter into information warfare only if and when an opponent targets the logistics information system to degrade it; similarly, weather collection systems enter information warfare only if they are subject to attack. By contrast, IBW systems are part of information warfare because they are used to read a target that would avoid being read and that often has ways (e.g., cover, concealment, and deception) to distort readings at the source.

The critical aspects of information warfare are information denial (or distortion) and its counterpart, protection. C2, EW, hacker war, and information blockade clearly fit into this definition. IBW may be included, insofar as attacks on the instruments and integrity of collection systems become important to conventional operations. Psychological warfare also is about denial, in the sense that elevating one perception usually subjugates its opposite (e.g., a nation is either friendly or hostile). Cyberwarfare fits, too, as a grab bag in which warfare and information are jumbled.

3 *Command-and-Control Warfare*

The following is taken from a core Department of Defense (DoD) dictum on C2W and information warfare:

> C2W [Command-and control-warfare] is the military strategy that implements Information Warfare (DoD Directive TS-3600.1, 21 December 1992, "Information Warfare") on the battlefield and integrates physical destruction. Its objective is to decapitate the enemy's command structure from its body of command forces.[6]

Defined in this way, U.S. forces demonstrated mastery of information warfare in the Gulf by destroying many

---

[6]MOP-30, which is currently being revised, slices and dices information warfare out to operational units. Limited to military operations, it covers, "the integrated use of operations security, military deception, psychological operations, electronic warfare, and physical destruction, mutually supported by intelligence, to deny information to, influence, degrade or destroy adversary C2 capabilities while protecting friendly C2 capabilities against such actions"(2).

Mapped on the schema used here, MOP-30 covers C2W, the anticommunications aspect of EW, defensive IBW, and unit-level psychological operations: "these [PSYOP] forces used in C2W are, in most cases, the same forces used to conduct other aspects of warfare, and unless they represent some unique capability, will move in the same flow as the units to which they are organic" (20).

physical manifestations of Iraq's command-and-control structure. These operations have frequently been pointed to as *the* reason the bulk of the Iraqi forces were ineffectual when U.S. ground forces came rolling through.[7]

Decapitation can be accomplished by a blow to the head or by severing the neck, each thrust serving a different tactical and strategic purpose.

Antihead. Gunning for the commander's head is an old aspect of warfare. Examples abound, from the ancient practice of seizing the enemy's king to the death of Admiral Nelson, shot by a shipboard sniper, the employment of sharpshooters against opposing generals during the Civil War, the downing of Admiral Yamamoto's plane in World War II, strategic nuclear targeting theory, and attempts to find Saddam Hussein during the Gulf War or Mohammed Aideed in Somalia. What is new is that the commander's accessibility keeps shifting. Command effectiveness used to require commanders to oversee and thus remain near the range of combat. In World War I wireline communications enabled commanders to operate beyond the range of enemy arms. Later, the airplane and missile returned the commanders to the target zone.

[7]An extended period of material deprivation coupled with continuous carpet bombing prior to the ground offensive has also been cited.

More important than the commander's physical location is the transformation from the commander to the command center. Today's command centers are identifiable by copious, visible communications and computational gear (and the associated electromagnetic emissions), the physical movement of paper and other official supplies, plus enough comings and goings of all sorts to differentiate these centers from other venues of military business.

An attack on a command center, particularly if timed correctly, can prove disruptive to operations even without hitting a high-ranking enemy commander. Despite the known disadvantages of single-point vulnerabilities, most commerce in messages tends to circulate within very small spaces. Fusing data and distributing them to harmonize everyone's situational awareness requires either a central set of ganglia or a major redesign of legacy systems. Determining the location of a command center permits juicy targets to come within gunsight—an opportunity rarely passed up. Correctly timed attacks can disrupt and distract operations beyond the immediate effect of destruction.

Iron bombs are not the only way to attack command centers. Systems can be disabled by cutting off their power, introducing enough electromagnetic interference to make them unreliable, or by importing computer viruses, yet none of these means is foolproof or cost-effective compared with iron bombs on target. Most soft-kill weapons require knowing the location of the target. Although some of them have a larger effective radius than conventional munitions, the difference is limited and finding before firing remains equally essential.

How long will command centers remain visible? Bunkering can protect headquarters, but at the cost of mobility (and newly perfected penetrating ordnance requires deep and comparatively immobile bunkers). Control of the signature of the command center may be a better strategy. Computers can be shrunk to the desktop, emissions of communications gear masked by electronic clutter (both deliberate and ambient) or offloaded through multiply redundant cables or line-of-sight relays away from headquarters, and paper will yield to the paperless, perhaps optical, society (someday). Networks can generally be decentralized.[8] Comings and goings and congregations that create valuable targets can be reduced through videoconferencing and whiteboarding.[9] Power supplies can be supplemented by bunkered generators or, more ingeniously, by relying on dispersed photovoltaic collectors for electricity (which should be scattered so their presence will not reveal the command center).

[8]Physical (weak) and virtual (strong) decentralization are different: physical decentralization retains a centralized information architecture but protects the system by dispersing and replicating memory and processing; virtual decentralization makes subunits capable of operating on their own but uses coordination with the center to strengthen the quality of their decisions.

[9]Whiteboarding is a network application that permits what is put on one person's screen to come up on another's.

These means can keep command centers indistinguishable from any other inhabited space. Failing this result, the degree to which an enemy is hurt by being struck will depend on backup architectures (e.g., which nodes supply what information, what information is vital for battlefield decisions).

Dispersion will take time; reconfiguration costs time and money and increases the difficulty of command. Proponents may need real-life demonstrations, rather than theoretical arguments, to convince commanders that dispersion is needed and that a given level of dispersion will suffice against attack. But the transformation will eventually happen everywhere. How soon militaries in other countries will make the shift will depend on technological sophistication, the degree to which current command centers feel vulnerable, the extent to which authority is vested in personal contact or in ostentatious displays of silicon, as well as miscellaneous cultural factors. In the long run, war planners would be foolish to base their strategy on the assumption that the enemy's command centers can be disabled.

Antineck. Modern militaries have been knit by electronic communications since the mid-nineteenth century and by radioelectronic communications since the 1920s. Cut these communications and command-and-control is disabled, which, again, is old in warfare.[10] What is new is the size of the communications load in the information age. Air defense systems, for instance, work better when integrated across facilities than when each facility works independently. The extent to which operations depend on the flow determines whether efforts to cut communications are worthwhile.

Cutting communication links requires knowing how the other side communicates. If its architecture is written in wire, the nodes (e.g., the AT&T building in downtown Baghdad) are easily identified and disabled. Like command centers, communications systems can be crippled by attacks on generators, substations, and fuel supply pipelines (e.g., gas lines into power plants), such as U.S. forces made in the Gulf. If the architecture is electromagnetic, often the key nodes are visible (e.g., microwave towers). If satellites are used for transmission and signalling, then communication lines can be jammed, deafened, or killed.

The impact of attacks depends on how far the other side has progressed from the mainframe era. A communications grid composed of many small elements rather than a few large ones radiates less and casts smaller shadows over the landscape; it offers

[10]Part of the Southern strategy in the Civil War was to conduct raids against railroads and telegraph lines used by Union forces; by 1864, nearly half the Union strength was devoted to occupation duties and protecting its lines of communication.

greater redundancy and confounds the enemy's targeting problems.

Redundancy is an attribute of both developed and less developed states. By the end of the Gulf War allied forces had more (if less important) C2 targets left to attack than at the start, despite the number destroyed. The Iraqis, as it turned out, had many communications systems, more perhaps than even they were aware of, from radio systems that Western oil contractors had left in place to rural telephone systems that routed around major cities.

Deliberate redundancy, of course, is more efficient than accidental. Systems that replicate message traffic multiply the likelihood of a message getting through in highly degraded conditions, even if redundancy reduces the system's overall capacity. Additional robustness can be protected by new technologies such as spread-spectrum (to guard against burst errors in heavy jamming environments) and sophisticated error-correction techniques (e.g., trellis coding). A strategy of redundancy still leaves the management problem of distinguishing vital bit flows from merely useful ones. Bureaucratic, rather than technological, factors may determine the vulnerability of any data-passing system.

To what effect? The potential influence of C2W on the outcome of conflict is predicated on the architecture of command relationships among the attacked. Iraq imitated its Soviet mentor, in part for political reasons (Iraqi society rules through convictions, rather than conviction). Cutting or thinning the links between head and body could easily be predicted to immobilize the body. Front-line troops were sitting ducks for U.S. air and ground attack and showed little creative response.

Clearly, a rigid opponent like Iraq is only one end of a long continuum of possibilities. Other societies may allow local commanders more autonomy. Although the North Vietnamese also were hierarchically organized, their operatives were capable of long periods of untethered operations. An attack on central authority could conceivably release field commanders to demonstrate an initiative that would more than compensate for any lack of coordination resulting from chaos at the center.[11]

The opposite also merits thought: if the center can be induced to come to terms, the last thing wanted is for peripheral forces to continue to fight. Future General Robert E. Lees, one hopes, would surrender whole armies rather than free them to fight on in guerilla campaigns. Consider the difficulties in Bosnia: although Belgrade signed a peace agreement in July 1994, the Bosnian Serbs refused to sign and continue

[11]U.S. officers in Vietnam must often have wished fervently (though silently) that communications lines between them and Saigon were severed, or at least those from Saigon to Washington.

to fight.[12] Decapitating a military may make it less effective but more troublesome.

Much of what passes for strategy to control nuclear war[13] consists of persuading an opponent to cease operations prior to global conflagration. Attacks on command-and-control thus make sense only if enemy forces are acting under positive (e.g., don't fire until I tell you) rather than negative control. Otherwise, the strategy could backfire.

C2W may do more good degrading or compromising the enemy's ability to command forces than destroying its ability altogether. For instance, destroying secure channels may induce the use of open ones vulnerable to eavesdropping. Although a destroyed infrastructure may prompt an immediate search for alternatives, one only subtly degraded may not. Finding a way to slow down the other side's ability to react at a precise moment (e.g., the moment

---

[12]It is also possible that the supposed disagreement between Belgrade and the Bosnian Serbs may have been disinformation designed to reduce the West's pressure on the Serbian economy.

[13]See, for instance, Paul Bracken, *The Command and Control of Nuclear Forces* (New Haven: Yale Univ. Press, 1983); Bruce Blair, *Strategic Command and Control* (Washington, D.C.: Brookings Institution, 1985); Ashton Carter et al., *Managing Nuclear Operations* (Washington, D.C.: Brookings Institution, 1987); or earlier classics such as Thomas Schelling, *Nuclear Weapons and Limited War* (Santa Monica, Calif.: Rand, 1959) and Herman Kahn, *Escalation: Metaphors and Scenarios* (N.Y.: Praeger, 1965).

of attack) gets the attacker inside the other side's OODA[14] loop. All these capabilities come under the category of "nice work if you can get it." As hard as it may be to degrade a system without leaving marks (while evading periodic ping tests[15] of a system's message cycling efficiency), it is harder to know whether one's attacks have done anything—even well after the dust settles. Battle damage assessment of C2 warfare is so difficult (consisting both of what was hit and what difference the hit made) that field commanders understandably want to see visible craters to ensure they had any effect at all.

C2W clearly is a valuable aspect of military operations, but it is neither a perfect complement (or substitute) to counter-force operations nor particularly new, except in certain respects. Although the information revolution has made some military operations hostage to the integrity of the center, the continuing shift from mainframe to distributed processing is reducing the center's vulnerability. The status of information warfare may reach its apogee just as the target set is accelerating its shift out from under the bombsights.

---

[14]Observe Orient Decide Act.

[15]Sending a query to a system that is automatically answered.

4 *Intelligence-Based Warfare*

IBW occurs when intelligence is fed directly into operations (notably, targeting and battle damage assessment), rather than used as an input for overall command and control. In contrast to the other forms of warfare discussed so far, IBW results directly in the application of steel to target (rather than corrupted bytes). As sensors grow more acute and reliable, as they proliferate in type and number, and as they become capable of feeding fire-control systems in real time and near-real time, the task of developing, maintaining, and exploiting systems that sense the battlespace, assess its composition, and send the results to shooters assumes increasing importance for tomorrow's militaries.

Despite differences in cognitive methods and purpose, systems that collect and disseminate information acquired from inanimate systems can be attacked and confounded by methods that are effective on C2 systems. Although the purposes of situational awareness (an intelligence attribute) and battlespace visibility (a targeting attribute) are different, the means by which each is realized are converging.

Offensive IBW. Sharp increases in the ratio of power to price of information technologies, in particular those concentrated on distributed systems, suggest new architectures for gathering and distributing information.

Platforms that host operator, sensor, and weapon together will give way to distributed systems in which each element is separate but linked electronically. The local-decision loops of industrial age warfare (e.g., a tank gunner uses infrared [IR] sights to detect a target and fire an accurate round) will yield to global loops (e.g., a target is detected through a fusion of sensor readings, the operator fires a remotely piloted missile to a calculated location). Because networking permits the logging of all readings and subsequent findings (some more correct than others), it can generate lessons learned more efficiently than a system that depends on voluntary human reporting.[16]

The evolution of IBW may be understood as a shift in what intelligence is useful for. Traditionally, the commander uses intelligence to gauge the disposition, location, and general intentions of the other side. The object of intelligence is to prevent surprise—a known component of information warfare—and to permit the commander to shape battle plans. Good intelligence allows coordination of

---

[16]See Eliot Cohen and John Gooch, *Military Misfortune* (New York: Free Press, 1990), which argues, among other views, that the U.S. Navy's slowness during World War II to institute a centralized learning process retarded the development of proficiency in submarine and antisubmarine operations on the Atlantic front.

operations; great intelligence allows coherence, which is a higher level of synchrony.[17] The goals of intelligence are met when battle is joined; when one side understands its tasks and is prepared to carry them out while the other reels from confusion and shock—thus, situational awareness.

Today's information systems reveal far more than yesterday's could, permitting a degree of knowledge about the battlespace that accords with situational awareness. The side that can see the other side's tank column coming can dispose itself more favorably for an encounter. The side that can see each tank and pinpoint its location to within the effective radius of an incoming warhead can avoid engaging the other side directly but can fire munitions to a known, continually updated set of points from stand-off distances. This shift in intelligence from preparing a battlefield to mastering a battlefield is reflected in newly formed reporting chains for this kind of information. Although the direct reporting chain to the national command authority will continue, new channels to successively lower echelons (and, eventually, to the weapons themselves) are being etched. An apparent loss in status perceived by the intelligence apparatus (thus one resisted) is turning out to offer a large gain in functionality.

---

[17]See, for instance, Jeff Cooper, "Toward a Theory of Coherent Operations," *SRS Technologies*, 30 June 1994.

Tomorrow's battlefield environment will feature a mixed architecture of sensors at various levels of coverage and resolution that *collectively* illuminate it thoroughly. In order to lay out what may become a complex architecture, sensors can be separated into four groups: (*i*) far stand-off sensors (mostly space but also seismic and acoustic sensors); (*ii*) near stand-off sensors (e.g., unmanned aerial vehicles [UAVs] with multispectral, passive microwave, synthetic aperture radar [SAR], and electronic intelligence [elint] capabilities, as well as similarly equipped offshore buoys and surface-based radar); (*iii*) in-place sensors (e.g., acoustic, gravimetric, biochemical, ground-based optical); and (*iv*) weapons sensors (e.g., IR, reflected radar, and light-detection and ranging [lidar]). This complexity illustrates the magnitude and complexity of the task for those who would evade detailed surveillance. Most forms of deception work against one or two sensors—smoke works for some, radar-reflecting paint for others, quieting for yet others—but fooling overlapping and multivariate coverage is considerably more difficult.

The task of assessing what individual sensor technologies will have to offer over the next decade or so is relatively straightforward; globally available technologies will come in many types for use by all. The task of translating readings into militarily useful data is more difficult and calls for analysis of individual outputs, effective fusion of disparate readings, and, ultimately, integration of them into seamless, cue-filter-pinpoint systems. If the Army's demonstration facilities at Ft. Huachuca are indicative,[18] the United States has done a good job of manually integrating sensor readings in preparation for the next step—which is automatic integration. Automation removes the labor-intensive search of terrain through soda straws and takes advantage of silicon's ability to double in speed every two years. Automatic integration will depend, in part, on the progress (always difficult to predict) of artificial intelligence (AI).

Defensive IBW. Equally difficult to predict (or to recognize when they succeed) are defenses developed to preserve invisibility or, at least, widen the distance between image and reality on the battlefield. IBW systems can be attacked in several ways. On one hand, an enemy would be well advised to make great efforts against U.S. sensor aircraft (such as AWACS or JSTARS). On the other, using sensors that are too cheap to kill may be wiser (e.g., it is expensive to throw a $10,000 missile against a $1,000 sensor). Sensors can also be attacked by disabling the systems they use (e.g., hacker warfare), and their systems can be overridden or corrupted (e.g., EW).[19]

---

[18]See Charles A. Robert, "Digital Intelligence Extends Army Force Projection Power," in *Signal*, **48**, 12 (August 1994), 33-35.

[19]Giving every soldier the commander's view of the battlefield can create a major vulnerability. Capturing a soldier and his equipment can give the enemy the same view. This could nullify, with one stroke, whatever prior advantage the other side had at information-based warfare. It also would reveal *how* such a view was obtained, and thus the capabilities—or even better, the blind

The most interesting defense, in relation to likely opponents of the United States in the next ten or twenty years, would be to use a variant of the traditional cover (concealment) and deception with an admixture of stealth.[20] When sensor readings are technically accurate (that is, when the readings reflect reality), countering IBW requires distorting the links between what sensors read and what the sensor systems conclude.

In high-density realms (e.g., urban areas, villages crowded together, forests, mountains, jungles, and brown water) counterstrategies may rely on the exploitation or multiplication of the confusing clutter.[21] In realms where the assets of daily civilian commercial life are abundant, military assets would need to be chosen so they could be confused with civilian assets (which tend to be more numerous and less directly relevant to the war effort and so are not

---

spots—of the other side. This creates a major problem. How does one explain to troops at risk that information on the enemy that, as they see it, may affect their survival must nevertheless be withheld from them, even though its transmission is physically possible, and, indeed, easy? Efforts to control such information are more likely to be frustrated from within than from without.

[20]Although most modern platforms will probably evolve to reduce observability, cost considerations are likely to relegate stealth to specialized uses (e.g., deep attack, support to special operations forces), and traditional forms (e.g., submarines).

[21]In lower density realms—plains, deserts, blue water—a man-made object, particularly a military one, will stand out as not belonging there, so, to avoid becoming a target, an object should, instead, resemble the background, rather than ambient man-made clutter.

such valuable targets—contrary rules of engagement notwithstanding).

Decoys, broadly defined, will probably be popular, on the theory that hiding a tree in a forest may be more practical than surrounding it with an obvious brick wall. The success of such measures will vary with the architecture of the IBW systems they are designed to fool. Systems based on multiple and overlapping sectors are more difficult to elude than single-sensor systems.

For the foreseeable future, battlefield sensors will not be able to look at all information at the same time in sufficient detail.[22] Thus, the sensor system will need to use a combination of cuing, filtering, and pinpointing (e.g., as a JSTARS system does to indicate a group of moving vehicles so UAVs can be dispatched to identify each of them). What sensors would be assigned which functions? Would ambient sensors (e.g., acoustic, biochemical) be used to cue while electro-optical ones pinpoint? Would IR readings be used for cuing, neural with net devices as filters and ambient sensors as discriminators? Which sensor readings would be discarded as least reliable? How

---

[22]As an example, a reasonably detailed (.1 meter resolution) multispectral (8 bits x 8 bands) image of a typical theater of operations (400 kilometers on each side) generates an image that, uncompressed, takes up a million billion bits of information. Even with compression and selective intelligent updating, the bandwidth required to send the same information over the air to a location behind the lines does not exist in the electromagnetic spectrum.

would the system compensate for areas of relatively weak coverage?

An object may look like a duck, walk like a duck, but honk like a goose; which is it? By carefully offering fowl for examination by the other side and then noting which are classified as ducks and which as geese, defenders may be yielded a clue to how an observing system draws conclusions. Conversely, an observing system observed may deliberately let ducks dressed as geese go free to promote an illusion of its own inability to distinguish between them. This is an old technique in the game of intelligence: IBW inserts the ethos, tendencies, and practices of intelligence insistently into the battlefield.[23]

Information technology can be viewed as a valuable contributor to the art of finding targets; it can also be viewed as merely a second-best system to use when the primary target detection devices—a soldier up close—are too scarce, expensive, and vulnerable to be used this way. Open environments (tomorrow's free-fire zones) aside, whether high-tech finders will necessarily always emerge triumphant over low-tech hiders remains unclear.

---

[23]As a perhaps apocryphal illustration, although Winston Churchill was said to know through Britain's Enigma system of codebreaking that the Germans would bomb Coventry, he decided to abjure countermeasures that might reveal that the British had broken the German codes.

5 *Electronic Warfare*

The first two forms of information warfare discussed here deal with attacks either on systems (C2 warfare) or by systems (IBW). The third form is EW, or operational techniques: radioelectronic and cryptographic, thus war in the realm of communications. EW attempts to degrade the physical basis for transferring information, while cryptographic warfare works between bits and bytes.

Neither type of EW is truly new. In tandem, they underlay Britain's success in defending its island against the Luftwaffe. In recent years, as information warfare has acquired a certain cachet, efforts have been made to reinvent EW under this new moniker.[24] Its supposed current rise in status is occurring just as technologies are being developed that will favor the bits (like the bomber of yore) getting through.

---

[24]Consider the close alignment between what was formerly named the Joint Electronic Warfare Center in San Antonio, Texas, and now the C2 Warfare Center and the co-located USAF Information Warfare Command.

Antiradar.[25] A large portion of the EW community deals with radars (both search and target) and worries about jamming and counterjamming. Offense and defense keep coming up with new techniques. Traditional radars generate a signal at one frequency; knowing the frequency makes it easy to jam a return signal. More modern radars hop from one outgoing frequency band to the next. To counter radars, today's jammers must be able to acquire the incoming signal, determine its frequency, tune the outgoing jamming signal accordingly, and send a blur back quickly enough to minimize the length and strength of the reflected signal. Jamming aircraft that are riding in formation with attack aircraft often wipe out return signals (which weaken as the fourth power of the distance between radar and target) by overpowering them, but doing so makes jammers very visible so they must protect themselves. Coalition forces in the Gulf developed new synergies using jamming aircraft en masse. Radars make themselves targets because of their outgoing signals; antiradiation missiles (e.g., the HARM) force radars either to be turned off or to rely on chirping and sputtering. The aborted Tacit Rainbow missile was designed to loiter in an attack area until a radar turned itself on; the

[25]Antiradar techniques can be generalized to antisensor techniques (e.g., the use of flares to confuse IR-guided missiles). The important characteristic of radar is that it receives *reflected*, as opposed to passive, electromagnetic radiation; radar signals can be attacked coming or going.

outgoing signal gave the missile an incoming beacon, and away it went. As digitization improves, radar can acquire a target by generating a transient pulse and analyzing the return signal before a false jamming signal overwhelms the reflection.

The cheaper digital manipulation becomes, the more logic favors the separation of an emitter from a collector. Emitters, the targets of antiradiation missiles, would proliferate, to ensure the survival of the system and to act as sponges for expensive missiles. The missiles would create a large virtual dish out of a collection of overlapping small ones. Because outgoing signals will be more complex, collection algorithms too will grow in complexity, but the ability of jammers to cover the more complex circle adequately may lag. Dispersing the collection surface will also make radars less inviting targets.

Anticommunications. EW against communicators is generally more difficult to wage than EW against radars. The signal strength of communications weakens with the distance to the transmitter squared (versus the fourth power with radar). While radars try to illuminate a target (and therefore send a beam into the assets of the other side), communicators try to avoid the other side entirely and thus point in specific directions. Communicators move toward frequency-hopping, spread-spectrum, and code-division multiple access (CDMA) technologies, which are difficult to jam and intercept. Communications to and from known locations (e.g., satellites, UAVs) can use digital technologies to focus on frontal signals and discard jamming that comes from the sides. Digital compression techniques coupled with signal redundancy mean that bit streams can be recovered intact, even if large parts are destroyed.

EW is also used to geolocate the emitter. The noisier the environment, the more difficult the task. One defense is to multiply sources of background electronic clutter shaped to foil intercept techniques that rely on distinguishing real signal patterns.[26] A thorough job, of course, requires expending resources to scatter emitters in areas where they may plausibly indicate military activity. Doing so diverts resources from other missions.

As suggested above, the work of finding targets is likely to shift from manned platforms to distributed systems of sensors. Despite the impending necessity of distributed systems, their Achilles' heel is the need for reliable, often heavily used communications links between many sensors, command systems, and

[26]Voice calls have certain patterns in terms of who talks when and what percentage of the time is filled with blank time (e.g., listening). Encryption techniques can mask blank time patterns. False emitters can generate false conversations from random locations.

dispersed weapons.[27] In sensor-rich environments, EW—expressed by jamming or by soft-kill—can assume a new importance. Interference with communications from local sensors, for instance, can create virtual blank areas through which opposing systems can move with less chance of detection. The success of this tactic critically depends on the architecture of the distributed sensor system to be disrupted. A system that relies *exclusively* on distributed local sensors (intercommunicating or relaying signals by low power to switches) is the most vulnerable. A system that interleaves local and stand-off sensors, particularly where coverage varies and overlap is common, is more robust.

Cryptography. By scrambling its own messages and unscrambling those of the other side, each side performs the quintessential act of information warfare, protecting its own view of reality while degrading that of the other side. Although cryptography continues to attract the best minds in mathematics, sadly for an otherwise long and glorious history, contests in this realm will soon be only of historical interest.

Decoding computer-generated messages is fast becoming impossible. The combination of technologies such as the triple-digital encryption standard (DES) for

---

[27]In a trivial comparison, an F-18, with its pilot, FLIR sensors, and attached weapons, can link all three with wires or in the pilot's mind and is therefore far more resistant to jamming.

message communication using private keys, and public key encryption (PKE) for passing private keys using public keys (so set up communications remain in the clear) will probably overwhelm the best code-breaking computers. The basic mathematics is simple: for any key length x, for DES data encryption the power required to break the codes[28] is $A*N^x$ (where x is the key length, A is positive, and N exceeds 1) and the power required to make the codes is $B*X^m$ (where B is positive and M exceeds 1). Regardless of the quantity of A, B, M, and N, as soon as x exceeds some number, breaking a code is harder than creating one and becomes increasingly harder as x grows.

Although encryption is spreading on the Internet and all communications are going digital, the transition to ubiquitous encryption will take time. Analog will certainly persist in legacy systems, although its lifetime is limited. Cheap encryption, coupled with signal-hiding techniques such as spread-spectrum and frequency-hopping, will seal the codebreaker's fate.

---

[28]For single DES, with its 56-bit key, $x = 56$. Triple DES is comparable to an 80-bit key, or $x = 80$. The formula works differently on PKE, because the challenge to the code breaker is to factor a product of two prime numbers rather than guess a correct key. Although today PKE software can support key lengths of 1,024 bits (and thus unbreakable in the foreseeable future), PKE is roughly a thousand times more computationally inefficient than DES and is best used to pass DES keys back and forth.

Digital technologies will make spoofing—substituting deceptive messages for valid ones—nearly impossible. Digital-signature technologies permit recipients to know both who (or what) sent the message and whether the message was tampered with. Unless the spoofer can get inside the message-generation system or the recipient cannot access a list of universal digital keys (e.g., updates are unavailable to that location), the odds of a successful spoof are becoming quite low.[29]

[29]If the timing of the message is part of its content (e.g., Global Positioning System [GPS] timing signals), a system could be fooled when its original message would be blocked and retransmitted at a slightly different time—provided the recipient lacked an accurate clock.

6 *Psychological Warfare*

Psychological warfare, as used here, encompasses the use of information against the human mind (rather than against computer support).[30] There are four categories of psychological warfare: (*i*) operations against the national will, (*ii*) operations against opposing commanders, (*iii*) operations against troops, and—a category much respected abroad—(*iv*) cultural conflict. Psychological warfare prompts the same questions asked about information warfare: Is it war? is it new?

Counter-will. The use of psychological war against the national will through either the velvet glove ("accept us as friendly") or the iron fist ("or else") is a long and respected adjunct to military operations, with antecedents found in the writings of Thucydides. The recurrent "peace offensives" and May Day parades of the Soviets showed that they were familiar with its uses, as are we.

---

[30]Otherwise, every aspect of war might be included, because breaking the enemy's will is generally the fundamental aim of military operations (e.g., the Coalition's use of carpet bombing against Iraqi positions prior to ground operations had an immense and perhaps decisive psychological impact).

The Somali clan leader Mohammed Aideed appears (if symposia hosted by the DoD are an indication) to be a master of the uses of psychological warfare. In a confrontation that cost the lives of nineteen U.S. Rangers, Aideed's side reportedly lost fifteen times that number—roughly a third of his strength. Photographs of jeering Somalis dragging corpses of U.S. soldiers through the streets of Mogadisho transmitted by CNN to the United States ended by souring TV audiences at home in the U.S. on staying in Somalia. U.S. forces left, and Aideed, in essence, won the information war.[31]

Global broadcasters, CNN a leader among them, ensure that events anywhere on the planet, whether authentic or arranged for show, can be delivered to audiences in many countries. Those CNN broadcasts indicated the immediacy satellites can now provide to news organizations, but, this feature aside, the concept of international news was not invented by CNN. More than twenty-five years ago, the Vietnam War was broadcast nightly to U.S. living rooms, time-delayed for the dinner hour.

Using direct broadcast satellite (DBS), the leader of one nation does not need permission from overseas

[31]Aideed's ingenious use of tom-toms, satellite terminals, and radio transmissions that bounced off city walls and so were difficult to geolocate has been cited as an indication that he understood other aspects of information warfare.

counterparts to speak live directly to the people in other nations. This capability is now available to anyone at low cost. The two-satellite 150-channel DBS constellation the Hughes company launched over North America, which began service late in 1994, cost roughly $1 billion, and subsequent versions will probably cost less. A DBS transponder over Asia might be profitably leased for an annual fee of perhaps $2 million (U.S.), well within the range of, say, Kurds, radical Shiites, Sikhs, or Burmese mountain tribes, who could then afford to broadcast their messages to an enormous audience twenty-four hours a day.

As the five hundred channels of a supranational information superhighway eventually become reality, the proliferation of microbroadcasters may promote a precisely opposite effect of localizing, rather than globalizing, the way world events are viewed—a de-CNNization of perception. Communities of interest, too small to be reached profitably by mass media, could be reached by targeted means. As each community's version of the news becomes subject to its own filters and slants, manipulating mass audiences will become increasingly difficult. Viewers might maintain computer agents, who would roam the Net to extract news and commentary of interest to them from archived and real-time material which they could then reshape into an individual's own news broadcasts. Affluent societies may soon suffer from Me-TV.

Given CNN, the arrival of DBS, and the possibilities of microbroadcasting and Me-TV, how far will one side go to manipulate news to affect the other. Affluent countries (and attractive victims) receive more attention than less well off nations, accessible news stories are covered better than inaccessible ones (starvation in Somalia compared with starvation in, for example, Sudan), and video cameras follow good pictures and human-interest stories. Staging demonstrations to maximize video coverage has a long history.

Yet, random, understandable biases do not equal a consistent ability to manipulate the presentation of events in a specific direction. The international media are a powerful and systematic influence in war but they rarely consistently favor one side or the other. Many in the DoD complain that unscrupulous opponents of the United States can persuade the American public by judicious manipulation of the media. The truth is that television is ubiquitous and that the United States gives as good as it gets (e.g., it exports political consultants and public affairs services, which together are a good proxy for skill at this enterprise).

Oddly enough, given time the media may come full circle. As such movies as "Forrest Gump" or "Jurassic Park" have profitably shown, synthetic, manipulative events are possible (morphing figured prominently in the advertising of both sides during the 1994 Congressional races). Sophisticated newswatchers already understand how to use one channel to confirm flash reports on another; if manipulation goes further, the notion of a personally trusted news source may supersede current concepts of public news sources. The side wishing to manipulate the other through the media would find part of the target population predisposed to believing anything, part believing nothing, part predisposed to believe the opposite of whatever the media put out, and the rest floating in worlds of their own.

Counterforces. The use of psychological methods against the other side's forces offers variations on two traditional themes: fear of death (or other loss) and potential resentment between the trench and the castle (or home front). In the Gulf War, Coalition forces convinced many Iraqis that if they abandoned their vulnerable vehicles they would live longer. The Coalition's persuasiveness was fortified by weapons that had just destroyed such vehicles during the fighting.

How will technology alter the ability of one side to speak to forces of the other? Getting electronic messages to the other side dates back at least to World War II (e.g., Tokyo Rose). Like short-wave radio, DBS can beam from space to local TVs but with far greater effect. Battery-powered TVs can be taken into the field. Whether TV is more effective than radio is debatable; clearly, images offer an immediacy and credibility sound alone lacks. The burgeoning field of personal computer-based television (e.g., video toasters) permits special units in the field to assemble complex, believable video material for broadcast behind enemy lines.

The great shift in counterforce psychological operations would come when information technology permits broadcasts of threats or resentment-provoking information to *individual* opposing troops. When the destruction of a target identified by location can be made near-certain, surviving warfare will be a matter of evading detection, rather than evading firepower. What would happen if vehicle operators could be told they had been seen and were about to be targets of deadly munitions unless they visibly disabled the vehicles? The first few times the technique was used, demonstrations, rather than actual attack, might be used to indicate that discovery is the cousin of destruction and that warnings would be ignored at peril to life and limb. With every demonstration, the correlation might become clearer. Such psychological warfare might save ammunition (and avoid subsequent broadcasts by CNN of a grisly reality). Yet the demonstration must reflect underlying realities, not create them.

By the same logic, telling soldiers that their wives and lovers are sleeping around is more effective if those at home can be identified by name. Gathering the data on individuals in primitive societies might not be possible, but it would be easier in advanced societies, which these days generate enormous computer-kept files on almost everyone (e.g., from credit card histories, medical histories). Broadcasting information to individuals might be less difficult than it appears at first (even without the ability to locate individuals within units). No one needs to watch TV every minute to receive second-hand news of what is being said by the other side. At thirty seconds per soldier (the length of a typical TV advertisement), an entire division could be covered within one week of broadcasting without anyone losing sleep.

Counter-commander. Nothing so much suggests the imminence of defeat than confused and disoriented commanders. Yet confusing them with words alone is a difficult task. In mass societies, commanders are the instruments that translate the will of those to whom they report into the duties of those they command. The commander neither originates the ends, nor, in theory, allows personal considerations to get in the way of optimizing military decisions. A good commander should be able to transcend unnecessary emotion and proceed directly to the tasks at hand.

Confusion and disorientation are cognitive as well as emotional states. Commanders make decisions on the basis of unexpected events. If reality is different from the basis used for decisions, it is difficult and time-consuming to reconstruct a cognitive structure (e.g., facts that lead to implications, actions based on conclusions) based on the new reality (rewiring interpersonal relationships and organizations to match the new reality may be almost impossible). Simulation, thought experiment, and generalized what-if thinking, which can prepare a commander to recognize wide alternatives (each with its own decision logic), would facilitate coping with the unexpected, but at a high price. Contemplating an assortment of possibilities necessarily detracts from contemplating deeply those presumably probable. Events of low probability are discarded entirely; should they occur, few know how to cope.

Because unfavorable events always offer the possibility of unhinging the commander[32] introducing them deliberately may be a good tool. How possible is it to compound a disorientation that events on the grand scale would have caused in any case? If so, among otherwise comparable courses of action, logic would seem to favor the course that would exacerbate differences between what the other side expects to see and what it actually sees.[33] In a World War II-ish metaphor, a direct tank assault may have a higher

[32]Masterpieces of the military art, according to Winston Churchill, contain "an element of legerdemain, an original and sinister touch, which leaves the enemy puzzled as well as beaten" (*The World Crisis*, 1915 [London, 1923], 21).

[33]Although unexpected success can be disorienting, it is easier on the ego and unlikely to induce a disturbing reevaluation of one's competence (few people dwell on an inability to forecast their triumphs). The unexpectedly successful are also unlikely to be forced into subsequent decisions.

probability of success of throwing the enemy back compared to a parachute-led assault. If the opposing commander is confident that a parachute-led assault against him would fail, being wrong could force him to rethink the assumptions of his strategy. How accurate must this psychological portrait be before a parachute assault becomes the preferred approach? How likely is the commander's disorientation, and what is it worth in outcomes? The decision to adopt a strategy that trades immediate outcomes for increased confusion depends on how data affect the other side.

The attempt to mislead the other side's commander at the operational level is an important part of information warfare[34]. Historically, such deception has worked best when one side has a good idea of what the other side will and will not do.[35] In World War II, for example, the Germans were convinced that the Allies would try to breach the Atlantic Wall at Calais; the Japanese believed equally strongly that U.S. forces would strike from the Aleutians. In both cases, Allied forces played to those fears, keeping the opponent's forces pinned down where the opponent would need them least when the ultimate attack came. Similarly, Iraq was led to believe that the United States

---

[34]See defensive intelligence-based warfare for mention of deception at the tactical level.

[35]Thanks to George Kraus (Science Applications International Corporation) and Allen Carley (CIA) for suggesting this line of argument.

would use aerial warfare for only a limited time and only to soften the field immediately prior to ground attack (rather than, as it turned out, for forty days and nights). Iraq also believed that the United States would try to recapture Kuwait from the sea. U.S. quasi-public commentary carried over international media, such as CNN, was shaped to support the first belief; more conventional devices (e.g., having ships sail up and down the coast) supported the second.

Information warfare can also be applied to the everyday task of deceiving opposing bureaucracies—diplomats and spies—about one's intentions and capabilities. Weapons can be said to be more or less efficient or speedy than they actually are. A nation's preparations for war can either be highlighted for effect or downplayed for soporific value. Such activity is so common and historical that labelling it warfare rather than the everyday business of statecraft it has always been would prove difficult.

How could advancing information technology accentuate or mitigate operational deception? Institutions (e.g., CNN, again) and tomorrow's technologies (e.g., DBS) ease the dissemination of deception. In the future, a transition from CNN to narrowcasting might create the possibility that one side could generate different (perhaps even incompatible) messages to competing components of the other side's polity. Proliferating media would permit promulgation of confusion. As technologies of inspection become increasingly ubiquitous, however, more details must be correct to achieve deception.[36]

Kulturkampf. Whether cultural struggle is a form of psychological warfare is a rich topic, yet many non-Western nations are disturbed by the extent to which their traditional cultures are being invaded by Western—that is, largely U.S.—popular culture (e.g., fast food, Hollywood movies, blue jeans). More than one seer has forecast a coming clash of civilizations[37] arising not because countries will take issue with the Madonna but, for example, because her present-day namesake is seen as assaulting a traditional value structure. The trip from fear and loathing to accusations of direct cultural attack is short.

Is cultural warfare a creature of the new information technologies? Hardly. The outcome of the cultural struggle between the Hebrews and the Syriac Greeks is celebrated every December, and fears of U.S. cultural imperialism certainly predate network television. Cultural challenges are facilitated by such instrumentalities as the multinational corporation (which require advanced communications to function),

---

[36]When cryptography was weak, one method of deception was for one side to let a message fall into the other side's hands as though as it were an accident. Now that cryptography is strong, such serendipity is likely to be met with more suspicion.

[37]Samuel Huntington, "The Clash of Civilizations?" *Foreign Affairs*, **72**, 3 (Summer 1993), 22-49.

the Internet, satellite video feeds, or, most recently, DBS.

Is cultural warfare a form of war (that is, again, policy by other means)? Not as seen from Peoria. First, the entire concept of national culture simply remains alien to most Americans, bred, as they are, to the idea that this nation is defined by norms of political and social behavior, rather than by cultural habits. The U.S. Constitution (with antecedents in English common law) may be the best single expression of this socio-political behavior. Americans tend to be impatient with the whole notion of culture, unlike the French, who, at least to American eyes, imbue their language, arts, and cooking with heavy national responsibility. Steeped in national myths of pioneer and immigrant, Americans readily defend the right to pick and choose—or invent—cultural choices rather than settle for one set of them. If the Japanese, say, wish to try to sell Americans on calligraphy, family bathing, daikan, or karaoke here, they are as welcome as anyone else is to try.

Cultural warfare is something the United States is more likely to do to others. Cultural products are one of the only categories in which the United States enjoys a consistent export surplus. When the French or Canadians complain about U.S. cultural exports to their countries, the United States sees those complaints as threats to world trade and refuses to treat such cultural concerns as legitimate. Yet U.S. policy wants to see U.S. *political* culture (e.g., majority rule, minority rights) exported and adopted overseas; trade rules aside, policy is completely and properly silent about other cultural influences.

7 *Hacker Warfare*

Winn Schwartau,[38] among others, uses the term information warfare to refer almost exclusively to attacks on computer networks. In contrast to physical combat, these attacks are specific to properties of the particular system because the attacks exploit knowable holes in the system's security structure.[39] In that sense the system is complicit in its own degradation.

Hacker warfare varies considerably. Attackers can be on site, although the popular imagination can place them anywhere. The intent of an attack can range from total paralysis to intermittent shutdown, random data errors, wholesale theft of information, theft of services (e.g., unpaid-for telephone calls), illicit systems' monitoring (and intelligence collection), the injection of false message traffic, and access to data for the

---

[38]Winn Schwartau, *Information Warfare* (N.Y.: Thunder's Mouth Press, 1994; not necessarily recommended, but indicative). The literature on computer crime and security is extensive. Much of what sells is of the bogeyman variety, but serious works exist, for instance, one from the Computer Science and Technology Board of the National Research Council, *Computers at Risk* (Washington, D.C., National Academy Press, 1991).

[39]Many holes persist because they are concomitants of desirable features. Passwords, for instance, chosen by users are easier to remember but they are also easier for hackers to guess.

purpose of blackmail. Among the popular devices are viruses, logic bombs, Trojan horses, and sniffers.[40]

The hacker attacks discussed here are attacks on civilian targets (military hacker attacks come under the rubric of C2 warfare).[41] Although attacks on civilian and military targets share some characteristics of offense and defense, military systems tend to be more secure than civilian systems, because they are not designed for public access. Critical systems are often disconnected from all others—"air gapped," as it were,

[40]A logic bomb is a program that some time after it is inserted destroys a computer's programs and data. A Trojan horse is a program taken in by a host computer which is then subject to attack from it. A sniffer sits on a host network and collects passwords and other similarly revealing information.

[41]According to *U.S. News and World Report*'s *Triumph Without Victory: The Unreported History of the Persian Gulf War* (N.Y.: Times Books, New York, 1992). the U.S. was able to hack Iraq's air defense computers by slipping several cooked electronic microchips into a French-made computer printer smuggled into Iraq during Desert Shield (224-225). The chips contained a virus that disabled computer systems by making it difficult to open a "window" on the computer screen without losing data. Because a peripheral device is rarely the site of a virus, it was a good entry point for insertion. Unfortunately for an otherwise amusing tall tale, a printer is rarely checked for a virus because it is designed to send control codes (e.g., "printer out of paper"), not operational codes, back to the computer; an attempt to send bits running code would be treated by the printer as erroneous or irrelevant to printer control codes. Had this incident been a good hack as the tale suggests, the United States might have wanted to do it again, so why would anyone talk about it?

by a physical separation between those systems and all others.

From an operational point of view, civilian systems can be attacked at physical, syntactic, and semantic levels. Here, the focus is on syntactic attacks, which affect bit movement. Concern for physical attacks (see above, on C2W) is relatively low[42] (although some big computers on Wall Street can be disabled by going after the little computers that control their air-conditioning). Semantic attacks (which affect the meaning of what computers receive from elsewhere) are covered below, under cyberwarfare.

Hacker warfare can be further differentiated into defensive and offensive operations. The debate on defensive hacker warfare concerns the appropriate role for the DoD in safeguarding nonmilitary computers. The debate on offensive hacker warfare concerns whether it should take place at all. In contrast to, say, proponents of tank or submarine warfare, only a few hackers argue that the best defense against a hacker attack is a hacker attack.

Whether hacker warfare is a useful instrument of policy is a question that defense analysts and science fiction writers may be equally well placed to answer.

---

[42]Schwartau discusses "bit flipping," the use of microwave beams as a method to attack computers so that they generate random errors but in a work characterized by anecdotes none is offered on this subject.

Hacker warfare would, without doubt, be a new form of conflict, but it raises not only the usual questions—is it real, is it war—but also a third: should the United States wage it?

Is it real? Perhaps emblematic of the new concern about hacker warfare among defense analysts, in November 1994 the dean of the breed, Eliot Cohen, mentioned it three times in an analysis of the future defense posture of the United States.[43] Incidents of network penetration by hackers are on the increase, rising faster than the total population of the Internet. The total cost of silicon fraud is several billion dollars (although most of that total consists of toll-call fraud perpetrated through private branch exchange [PBX] telephone switches).

---

[43]Eliot Cohen, "What to Do about National Defense," *Commentary*, **98**, 5 (November 1994), 21-32. Cohen argues that "the networking of military organizations by electronic communications will...create new opportunities for warfare by...computer worms and viruses..." (23). He adds that "Future tools of information warfare will include satellite television broadcasts, the disruption of financial systems, the forging of all kinds of electronic messages, and the corruption of databases" (31), and goes on in the next paragraph: "Elite command units worry about their members—trained in the black arts of breaking and entering, not to mention other, far nastier, criminal skills—going bad. It has rarely happened, in part thanks to successful screening and training; but as the military breeds more information warriors, one wonders if such screening will continue to be effective. The temptations of computer hacking are far wider and stronger (among other things, it is much less violent and can be far more lucrative) than, say, assassination for pay." See also Peter Schwartz's interview with Andrew Marshall in *Wired*, **3**, 4 (March 1995), 138.

It seems excessive, however, to extract a threat to national security from what, until now, has been largely a high-tech version of car theft and joy-riding. Even though many computer systems run with insufficient regard for network security, computer systems can nevertheless be made secure. They can be (not counting traitors on the inside), in ways that, say, neither a building nor a tank can be.

To start with the obvious method, a computer system that receives no input whatsoever from the outside world cannot be broken into. If the original software is trusted (and the National Security Agency [NSA] has developed multilayer tests of trustworthiness), the system is secure (whether the system functions well is a separate issue). A system of this sort is, of course, of limited value. The real concern is to allow systems to accept input from outside without at the same time allowing core operating programs to be compromised. One way to prevent compromise is to handle all inputs as data to be parsed (a process in which the computer decides what to do by analyzing what the message says) rather than as code to be executed directly. Security then consists of ensuring that no combination of computer responses to messages can affect a core operating program, directly or indirectly (almost all randomly generated data tend to result in error messages when parsed).[44]

Unfortunately, systems need to accept changes to core operating programs, all the time. The trick is to draw a tight curtain of security around the few superusers granted the right to initiate changes. Although they might complain, their access methods could be tightly controlled (they might, for instance, work only from particular terminals that were hardwired to the network, which is an option in Digital's VAX operating system). The rapid speed and greater bandwidth of today's computers have made ubiquitous use of encryption and digital signatures possible. A digital signature establishes a traceable link from input back to the user attempting to pass rogue data into the system, and although it will not prevent all tampering (e.g., bugs in the parsing engine), it can eliminate most avenues of attack on a system.[45]

---

[44]One of the more outrageous fallacies to have garnered serious research dollars was the concept that U.S. forces could somehow broadcast viruses into enemy computers. It might be possible if the computer systems of the opposition were designed to accept over-the-air submissions of executable code, but who would design a system to do that?

[45]In theory, a communications system can be jammed—rendered inoperable by having its nodes flooded with meaningless messages that prevent meaningful traffic from getting through. In practice, jamming requires knowing the precise architecture and capacity of the system nodes and links. Straightforward jamming is difficult to accomplish without leaving a fat bit-stream trail pointing back to the perpetrator.

Stringent security may make certain innovations in the global network difficult to implement, such as the practice of communicating by exchanging software objects (which bind potentially unsafe executable code to benign data). Systems can (with work) be designed to retain full functionality in face of necessary restrictions. Security comes with costs, particularly if legacy and otherwise reliable operating systems (e.g., Unix) must be rewritten in order to minimize security holes. If the threat is big enough, the dollars spent to protect mission-critical national systems may not seem so large. At present, civilian mission-critical systems can, for policy purposes, be limited to those that run phone lines, energy, and other utility systems, transfer funds transfer networks, and maintain safety systems.

One reason computer security lags is that incidents of breaking in so far have not been compelling.[46] Although many facilities have been entered through their Internet gateways, the Internet itself has only once been brought down (by the infamous Morris worm). The difficulty in extrapolating from the current

---

Some networks can be rendered inoperative by "alert storms," in which a glitch in the system causes the network nodes to send out alert messages that slow the system and thus make it generate yet more alert messages. Attacking a system this way, though, requires perhaps a better knowledge of the system than its designers had.

[46]Computer security experts whisper darkly that banks have buried large losses due to computer fraud but have, of course, kept silent on the subject.

spate of attacks on the Internet is that the Internet was designed to trust the kindness of strangers. If it is to be considered a mission-critical system for which compromise is a serious problem, it must evolve and will necessarily become more secure.[47]

Although the signalling systems that govern the nation's telephones have permitted hackers to affect service to specific customers, the system itself has yet to experience a catastrophic failure from attack. None of the few broad phone outages that have occurred has been shown to have been caused by anything other than faulty software.[48] No financial system has ever had its basic integrity become suspect (although intermittent failures occur, such as NASDAQ's frequent problems). An analogy has been drawn between the threat of hacking and the security of the nation's rail system: train tracks, especially unprotected tracks in rural countryside, are easy to sabotage, and with grimmer results than network failure, but such incidents are rare.

Although important computer systems can be secured against hacker attacks at modest cost in

---

[47]In an important exception to that generalization, the Internet has become a conduit for a large chunk of the DoD's nonsensitive but, in bulk form, essential logistics traffic.

[48]The January 1991 incident, during which phone service in the northeast United States was crippled, was traced to a specific piece of software from one vendor.

usability, that does not mean that they will be secured. Increasing and increasingly sophisticated attempts may be the best guarantor that national computer systems will be made secure. The worst possibility is that the *absence* of important incidents will lull systems administrators into inattention, allowing some organized group to plot and initiate a broad, simultaneous, disruptive attack across a variety of critical systems. The barn door closes but the prize racehorse has been lost. Are today's hackers doing us a favor? Not everyone thinks so; Dorothy Denning, of Georgetown University, has argued that today's volume of random hacking raises the sophistication of hackers, thus raising the cost of recapturing the desired level of systems security.[49]

Is it useful to test systems against hackers the way new software is tested against computer illiterates? Probably. Much of hacking is determining the construction of a system—which rarely is obvious to the outside user—that is, finding where the holes are and pinpointing and exploiting them. Testers could be given the source code that says how the system works. With that they could look for the kind of holes that hackers need to find before they know if they can punch through. If the testers's job is to make systems foolproof, they can test faster than hackers can hack (but if it consists of obscuring faults, the thorough knowledge of the system prevents them from testing

[49]Conversation with author at NIST, 9 March 1994.

how well the system can protect itself through self-obfuscation).

Perhaps the most pernicious aspect of hacker warfare is that by creating a dense aura of magic around hacking it raises the status of professional paranoids. One particularly egregious hobgoblin has whispered that deliberate flaws are planted from overseas in a popular computer chip or operating system and that the flaws can disable the world's microcomputer systems just when the United States will be confounded by an opponent's military challenge. Getting two such events to coincide would in itself be an engineering tour de force.[50]

All told, hacker warfare appears to be a problem that is not a problem until it is a problem, when it will shortly cease to be a problem.

Is it war? Hacker attacks on military information systems can reinforce conventional military operations as well as any other form of information warfare. Crucial military systems are supposed to be designed with sufficient security and redundancy (and sufficient

[50]More plausibly, a component in a military item meant for field use may, on receiving a signal at a given frequency, either die or go crazy. Similarly, equipment tied to networks may have trap doors available to the original vendor. Both situations are more plausible security faults than poisoned chips in commercial use.

separateness from the rest of the world) to defeat such attacks.[51]

Hacker attacks on commercial information systems, precisely orchestrated, can distract the political leadership from national security duties. How effective are hacker attacks as warfare? That is, what power do hacker attacks have to affect the power of the state to defend its vital interests?

A flurry of hacker attacks can rival terrorist attacks for annoyance value, and, indeed, can disrupt the lives of more people. Is annoyance without political content an act of war? Can hacker attacks force change any more than terrorist attacks do? If so, repeated terrorist attacks would have to tire the target populace and erode support for countering those for whom the terrorists work. Yet hacker warfare depends for effect on specific, thus remediable, characteristics of the target system. Repeated attacks presume either a population of doltish systems administrators or increasingly clever hackers. Can either be counted on? Applying the terrorist model, again, perhaps hacker

---

[51]Military systems vary, of course, in security regimes—most are office automation systems. A recent red team test suggests that a moderately skilled hacker could assume superuser status on a surprisingly high percentage of systems used by the DoD. In almost all of these cases, penetration was not discovered. One reason is that computer systems administration (hence security) is not a career track in the military. The Defense Information Security Administration (DISA) has been given almost $1 billion to lower those percentages.

attacks could force change by inducing repressive state countermeasures, which then would alienate uninvolved citizenry. But hacker warfare is not liable to set off random repression of undesirables. Although populations may chafe a bit at computer security measures instituted in the wake of attacks, such measures are a long way from invading houses and hauling the usual suspects off to police headquarters.

In its ability to bring a country to its knees, hacker warfare is a pale shadow of economic warfare, itself of limited value. Suppose that hackers could shut down all phone service (and, with that, say, credit card purchases) nationwide for a week. The event would be disruptive certainly and costly (more so every year), but probably less disruptive than certain natural events, such as snow, flood, fire, or earthquake—indeed, far less so in terms of lost output than a modest-size recession. Would such a hacker attack prompt the U.S. public to demand the United States disengage from opposing the state that perpetrated the countermove, just because of great inconvenience? Probably not. The United States is more likely to disengage from an overseas conflict in the face of opponents whose neighborhoods are judged less important than initially estimated. It is less likely to withdraw in the face of an opponent whose power to strike the U.S. economic system suggests why this opponent must be dealt with harshly.[52]

Should the United States wage hacker warfare? The answer depends on whether defensive or offensive hacker warfare is intended. Defensive hacker warfare is an essential but everyday task of bolstering network security. Few doubt that military information systems should be guarded against attack (unclassified open-logistics system are of particular concern); the same is true for mission-critical civilian systems, and perhaps even for the coming national information infrastructure.

Should the government ensure the security of systems critical to the national economy? On one hand, threatening the economy by targeting its systems may affect the state. On the other hand, is systems security a problem whose solution should be socialized rather than remain private? If a foreign missile hits a refinery that blows up and damages its neighborhood, would the damage be the refiner's fault? No: the problem has been socialized in that the United States has a military to protect itself against such attacks. If a gunman hits a refinery tower and causes a similar explosion, would that be the refiner's fault? Yes and no: the problem is partially socialized through public law enforcement.

---

[52]Thus, it might not have been in North Vietnam's interest to hire hackers to disrupt U.S. systems just when the country was trying to build support in the U.S. for disengagement of U.S. forces.

Yet, the refiner—as an owner of potentially dangerous equipment—is reasonably expected to take precautions (e.g., perimeter fencing, security guards). If a hacker on the Internet gains access to the refiner's system and commands a valve to stay open, creating an explosion and damaging the neighborhood, should the refiner be at fault? Yes: it should know everything about its information systems whereas the government may know absolutely nothing. Thus, the refiner should be responsible for protecting its internal systems and ensuring that software-generated events (e.g., software bugs) cannot do catastrophic damage. If a bank's deposit records were destroyed, do the depositors lose their money? No: a deposit constitutes a promise made by the bank to replay a loan. The bank's legal obligations cannot be erased by erasing its silicon memory of these obligations.

If the government is to protect the security of non-military systems, which agency should take the lead? The NSA clearly has the greatest expertise, yet in civilian circles it is also one of the least trusted agencies because of the highly classified nature of most of what it does.[53] If and when network security receives more attention, adherence to minimal standards of security may become a precondition for

[53]Another problem is that effective tools of computer security usually require encryption and digital signatures, best served by PKE, but this technology poses the greatest threat to NSA's core competence, signals intelligence.

federal regulatory approval (e.g., phone system or power-generation franchises often carry legal obligations for certain levels of assured service), for federal contract approval (e.g., bank systems), or for handling certain records (e.g., personal health data). Care must be taken lest the criteria used to define adequate security reflect military specifications (MILSPECs) and the array of threats particular to military systems, rather than criteria more appropriate to critical civilian networks.

The question of whether to develop a U.S. capability for offensive hacker warfare echoes arguments attendant on any discussion of *nouvelle* weaponry. If the United States forgoes, will others also forgo? Analogies to atomic weaponry suggest that hacker offensive warfare is not at all like atomic warfare (where linkages existed between the level of U.S. and Soviet stockpiles and delivery systems). Nations against which the United States might be preparing hacker warfare capabilities are less likely to react to U.S. capabilities than those against whom the United States might be preparing nuclear capabilities (in part because hacker warfare capabilities tend to be developed in and need to be used in great secrecy). It is also difficult to argue that attacking a society's computers with malevolent software is especially immoral when almost all are other targets are acceptable.

The argument against developing a capability for offensive hacker warfare concerns glass houses and stones. The United States is far more dependent on computer systems than other nations are.[54] The U.S. edge in perpetrating hacker attacks may be narrower than imagined. Roughly 60 percent of the doctorates granted here in computer science and security are awarded to citizens of foreign countries, two-thirds from Islamic countries or India. Analogies to biological warfare suggest that the United States should stop contemplating certain types of attacks until it has developed antidotes for them. It would be quite embarrassing if a virus intended for another country's computer systems leaked and contaminated ours.

Defensive hacker warfare presents a fundamental barrier to offensive hacker warfare. One way to promote the security of U.S. systems is to develop and distribute tools, tests, and code that ease the burden of securing civilian systems, and, thus, many multinational systems. If the tools have merit, potential adversaries will install them, too. Trap doors could be built into these products, but pulling that off requires greater cooperation between the vendors of systems

[54]If the United States were to take down Teheran's phone lines without owning up, who would notice the disruption, given the number of times those systems ordinarily malfunction?

security and the U.S. government[55] than the current debate over the Clipper chip suggests may be possible.

As the world becomes interlinked, most defenses the U.S. might employ defend not only this country but others as well. Out of the desire to ensure that U.S. corporations deposits in banks in foreign countries are secure, the United States cannot help promoting operational practices that in turn ensure that the deposits of evil dictators in the same bank are equally secure. Because hacking is cheap, nations at war might as well see what mischief it can be used to cause, and those that fall victims to such attacks will then have only themselves to blame.

[55]Because computer security experts generally regard hacking as immoral, most of them would be reluctant to cooperate even with government hackers; and sensitive customers might want to see the source code, to assure themselves of the security of a system.

8 *Economic Information Warfare*

The marriage of information warfare and economic warfare can take two forms: information blockade and information imperialism.

Information blockade. The effectiveness of an information blockade presumes an era in which the well-being of societies will be as affected by information flows as they are today by flows of material supplies. Nations would strangle others' access to external data (and, to some extent, their ability to earn currency by exporting data services). Cutting off access would cripple the economies of those nations, bringing them to their knees.

For the next few decades at least, the United States is more likely to perpetrate rather than find itself the victim of information blockades. It is more likely to be united with the rest of the world than our rogue opponents would be; not only is it, by far, the best connected and thus would be the hardest to cut off from information flows (not to mention the most self-sufficient economically), it is also a natural exporter of information.

An analysis of information blockades raises the same questions raised by other forms of information warfare: is it real? is it war? Could the United States truly blockade information, and, if so, would that make much difference to the behavior of other nations?

Is it real? Information blockades can be understood as a variant on economic blockades. Cutting off trade in goods can affect the well-being of a country by disrupting production flows and, in the long run, eliminating the benefits of foreign trade. An information blockade works similarly by forcing the target country to work in the dark and, in the long run, by removing the benefits of information exchange. It also limits the ability of the blockaded country to engage in psychological warfare.

To blockade a nation's information flow without blockading its physical flows is to block only one avenue of commerce, the one that flows electronically. If physical flows remain intact, printed (e.g., technical manuals) material could be acquired and even large databases transferred by CD-ROM. The information blockade would interrupt real-time interactions and restrict access to very large information flows (e.g., raw satellite imagery). It would be both easier and harder than blocking the country's supply of goods. With less opportunity for physical confrontation (in contrast to, say, boarding suspect ships at sea), the odds of violence are less. For the most part, information conduits are countable (by contrast, opportunistic smugglers can penetrate the entire length of a border).

How well can electronic data flows be cut off? Physical linkages, such as copper or wire, can be cut off at the border, in the waters, or at the nearest switch. In World War I, England severed Germany's cable links to the United States. Terrestrial radioelectronic connections can be silenced either by silencing the nearest transmitter (e.g., microwave towers) or by selective jamming. Space-based communications pose a bigger problem. Even if all sources uploading to geosynchronous satellites ceased transmissions (most are institutions, such as phone companies or media services), some services such as direct broadcast satellite would be nearly impossible to block. Free channels would just radiate. The benefits and lack of penalty associated with cracking by-subscription channels (which may carry tomorrow's digital business traffic) would probably motivate enough people to try, as video piracy in the United States shows.

Eliminating person-to-person linkages (e.g., Iridium, Inmarsat) could be confounded by the efforts of those on the outside whose communications were cut off. Third parties could establish accounts on global networks to pay for users inside the country. It is almost impossible for satellites to know where signals are going and even harder to determine where they come from. Encryption would hide who was talking to whom.

Is it war? Under what circumstances would a nation be vulnerable to information-economic warfare? Those who would block information could do so only by controlling a sufficiently large percentage of information resources and by being themselves relatively invulnerable to reverse pressure. In this respect, the United States alone would have a comparative advantage.

Comparisons to economic warfare are apt. The effectiveness of economic warfare depends on the target country's need for trade (or on the scale of disruption an unexpected cutoff of trade would imply). Countries that need food (e.g., the United Kingdom) or raw materials (e.g., Japan) or that live by selling specific resources (e.g., Iraq) are vulnerable to economic warfare. Those that for ideological or geographical reasons can forgo trade (e.g., the former Soviet Union) are harder to affect. A reigning article of faith holds that economic growth requires active participation in the global economy. Any nation only beginning to integrate its economy with the rest of the world's would see chancing a blockade more as opportunities missed than as output lost; either would mean taking a risk.

For an information blockade to have power similar to that of an economic blockade, the target nation would need to be dependent on external information flows, although information exchange is only one component of trade.[56] A nation that had lost access to electronic information exchange could be hindered yet not prevented from conducting trade. Iraq, for instance, could still sell oil. Without real-time access to commodity exchanges or the ability to tap databases on usage patterns, a targeted nation might have somewhat more difficulty writing the most advantageous contract for itself—but that constitutes a far lower loss.

Conversely, dependence could arise more from importing information, rather than from exporting it. The growth of computers, communications, and simulation suggests the growing attractiveness of offering services, especially expert services, over the net. Both carbon-based and silicon-based consultants could advise farmers on crop conditions, diagnose failures in complex machinery or factory systems, navigate the shoals of global commerce and finance, prepare surgical procedures, even supply the educational system. Such bandwidth-dependent applications are especially vulnerable to blockade.

As with many forms of conflict, threats may be more effective than acts. Nations seeking greater

[56]Some information flows (e.g., television, broadcast, telephone conversation) are also a large part entertainment. Although cutting them off might hurt morale, it would remove a major distraction from the war effort. Removing imported entertainment would leave a population with no alternative to local, hence chauvinistic, sources of culture and political influence.

information intercourse (e.g., to attract industries) would be more sensitive to the risks of untoward actions to their participation in the info-sphere; but nations that decide the risk is worth taking might be less likely to come to terms once information warfare has commenced. After all, societies were known to function before television.

How dependent on information flows could nations become? Some, the Philippines and several in Caribbean, are acquiring low-tech information export sectors (e.g., credit card operations). Would ambitious countries see their prosperity linked to status as a competitive base from which to sell goods and services and still risk provoking an information blockade that could sour potential investors?

If the threat of information war is present, few countries might allow themselves to become so vulnerable. Yet, under peaceful conditions, the prospect of a blockade may seem remote. Dependence on global information links will increase, and even leaders with hostile intent may not perceive that such dependence leaves them vulnerable to retribution if and when the leadership carries out hostile acts.

Information imperialism. To believe in information imperialism means believing in modern day economic imperialism. Thus, trade is war. Nations struggle with one another to dominate strategic economic industries.

How does information play in this contest? Although it is difficult in a paragraph to do justice to a complex chain of causality,[57] the logic is as follows. Nations specialize in certain industries; some industries are better than others. The good industries command high wages and, usually, feature high growth rates. They tend to be knowledge-intensive; they require and reinforce skills against which other nations, particularly those with low-wage workforces, cannot easily compete. Acquiring and maintaining a position in these industries is a reinforcing process. Consider Silicon Valley. The advantages of working there include easier access to customers, suppliers, and to workers sophisticated in electronics. The constant exchange of information, in particular, early access to interesting technical questions and information resources, provides one an edge in coming up with interesting solutions that, in turn, increases the likelihood that the area may enjoy a like advantage in the next round of problems. National policies may reinforce virtuous cycles. Japanese automobile manufacturers, even U.S. transplants (e.g., Toyota in Georgetown, Kentucky) have been accused of giving interesting work to their friends and boring work to others; Japanese vendors are said to offer their wares to domestic buyers one or two years before the wares go overseas. U.S. firms have a hard time tapping into these networks of

---

[57]See M.C. Libicki, "What Makes Industries Strategic" (Washington, D.C.: National Defense University, McNair Paper No. 5, November 1989), which explores this logic.

opportunity, either as suppliers or buyers. Targeted acquisition policies by governments (e.g., lucrative, research-intensive defense contracts) can have similar effects promoting a particular sector.

Is this war? Analogies to *kulturkampf* may be useful here. The United States does not export movies or pop fashions with an eye to subverting other cultures; it is something it does at a comparative advantage and wishes to extend through markets in goods and services. The Japanese could argue that, similarly, they do not wish to place the rest of the world into an inferior and dependent technological position. They simply want to make enough money to pay for their imports, and they believe they have a comparative advantage in certain high-technology manufacturing. Whether characterizing trade as a country-versus-country competition is meaningful in an age of multinational corporations remains an open question. Most large manufacturing corporations[58] in the United States and Europe are rapidly losing national coloration—and, in any case, they source components globally. Japanese and other Asian corporations remain noticeably national, but they are moving in the same direction.

[58]Important exceptions include steel and military goods.

9 *Cyberwarfare*

Of the seven forms of information warfare, cyberwarfare—a broad category that includes information terrorism, semantic attacks, simula-warfare and Gibson-warfare—is clearly the least tractable because by far the most fictitious, differing only in degree from information warfare as a whole. The global information infrastructure has yet to evolve to the point where any of these forms of combat is possible; such considerations are akin to discussions in the Victorian era of what air-to-air combat would be. And the infrastructure may never evolve to enable such attacks. The dangers or, better, the pointlessness, of building the infrastructure described below may be visible well before the opportunity to build it will present itself.

Information terrorism. Although terrorism is often understood as the application of random violence against apparently arbitrary targets, when terrorism works it does so because it is directed against very specific targets, often by name. In the early days of the Vietnam War, the Viet Cong terrorized specific village leaders to coerce their acquiescence. Done well, threats can be effective, even if carried out infrequently; targeted officials can be forced to accede to terrorists and permit their reach to spread. As the term is used here, information terrorism is a subset of computer hacking, aimed not at disrupting systems but at exploiting them to attack individuals.

What would the analogy for information war be to that kind of terrorism?[59] Targeting individuals by attacking their data files requires certain presuppositions about the environment in which those individuals exist. Targeted victims must have potentially revealing files on themselves stored in public or quasi-public hands (e.g., TRW's credit files) in a society where the normal use of these files is either legal or benign (otherwise, sensitive individuals would take pains to leave few data tracks). Today, files cover health, education, purchases, governmental interactions (e.g., court appearances), and other data. Some are kept manually or are computerized but inaccessible to the outside, yet in time most will reside on networks. Tomorrow, files could include user-built agents capable of interacting with net-defined services and therefore containing a reliable summary of the user's likes, dislikes, and predilections.[60]

---

[59]*Information Terrorism*, a forthcoming book by Paul Strassmann, the former DoD czar for information systems, presents a broader view of hacker war than as personally directed attacks.

[60]An intelligent agent might be used to book flights; it would know that its owner, for instance, preferred an aisle seat in the back and, for short connections, would rather rent a car and drive than take a puddle-jumper.

The problem in conducting information terrorism is having to know what to do with the information collected. Many people, for instance, might be embarrassed if the information in their collected datasphere were opened to public view; but that does not necessarily make them good objects for blackmail. Similarly, the hassle created by erroneous entries in a person's files might be significant, but threatening to put them there has only limited coercive appeal (a person so threatened could seek to limit the damage by requesting repeated backups of existing data to archival media along with the demand that all incoming data must be authenticated).

If information terrorism is to succeed, a more plausible response than fear of compromise might be anger at the institutions that permitted files to be mishandled. Before a systematic reign of computer terror could bring about widespread compromise of enough powerful individuals it would probably lead to restrictive (perhaps welcome) rules on the way personal files are handled.

Semantic attack. The difference between a semantic attack and hacker warfare is that the latter produces random, or even systematic, failures in systems, and they cease to operate. A system under semantic attack operates and will be perceived as operating correctly (otherwise the semantic attack is a failure), but it will generate answers at variance with reality.

The possibility of a semantic attack presumes certain characteristics of the information systems. Systems, for instance, may rely on sensor input to make decisions about the real world (e.g., nuclear power system that monitors seismic activity). If the sensors can be fooled, the systems can be tricked (e.g., shutting down in face of a nonexistent earthquake). Safeguards against failure might lie in, say, sensors redundant by type and distribution, aided by a wise distribution of decisionmaking power among humans and machines.

Future systems may try to learn from their info-sphere. A health server might poll participating physicians to collect histories, on the basis of which the server would constantly compute and recompute the efficacy of drugs and protocols. A semantic attack on this system would feed the server bad data, perhaps discounting the efficacy of one nostrum or creating false claims for another. Similarly, a loan server could monitor the world's financial transactions for continuing guidelines about which financial instruments merit trust. If banking server systems work the way bankers do, a rush of business to a particular institution could confer legitimacy upon the institution, and if that rush of business were phony and the institution a Potemkin savings and loan, the rush of legitimate business, by bytes and wire, could result in a rapid decrementation of assets by supporting banks. This scenario is similar to what allowed Penn Square bank in Oklahoma to buffalo many other banks that should have known better. In cyberspace, fraud can occur more quickly than human oversight can detect.

Is a semantic attack a worrisome prospect? Few servers like those just described exist. By the time they will, enough thinking should have gone on to develop appropriate safeguards, such as digital signatures, to repel spoofing and enough built-in human oversight to weed out data that computers accept as real but a human eye would reject as phony.

Simula-warfare. Real combat is dirty, dull, and, yes, dangerous. Simulated conflict is none of those. If the fidelity of the simulation is good enough—and it is improving every year—the results will be a reasonable approximation of conflict. Why not dispense with the real thing and stick to simulated conflict? Put less idealistically, could fighting a simulated war prove to the enemy that it will lose?

The dissuasive aspect of simulation warfare is an extension, in a sense, of the tendency to acquire weapons for more demonstration than for use, the battleship being perhaps a prime example. Had the United States possessed more atomic weapons during World War II, it might have chosen to light the first off Tokyo harbor for effect rather than in Hiroshima for results. The use of single champions rather than full armies to conduct conflict has both Biblical and Classical antecedents, even if the practice has now fallen into disuse. The gap between these practices and simulated conflict, with both sides agreeing to accept the result, would be a chasm.

Unfortunately, the realities of war and the fantasies of simulation make poor bedfellows. Environments tailor-made for simulation are composed of individual elements, each of which can be characterized by behavior but whose interaction is complex; for this reason, air tunnels simulate well. In tomorrow's hide-and-seek conflict, it will be almost impossible to characterize the attributes of combat. Much of warfare will depend on each side's ability to fool the other, to learn systematically from what works well and what poorly, to disseminate the results into doctrine, and, by so doing, to move up the sophistication of the game notch after notch. These operations are precisely the ones *least* amenable to simulation.

Needless to add, in the unlikely event that both sides own up to the capability and number of their systems and the strategies by which these are deployed, would the hiding or finding qualities of these systems be honestly portrayed? Mutual simulation requires adversaries to agree on what each side's systems can do. The reader may be forgiven for wondering whether two sides capable of this order of trust could be even more capable of resolving disputes short of war.

The attractiveness of today's simulation technology is its ability to model the battlefield from the viewpoint of every operator. Marrying operators and complex platforms in simulation is being promoted just when operators and their complex platforms are shuffling off the combat stage. Information systems, and over-the-horizon weaponry are more and more what war is about; and they are largely self-simulating systems.

A less ridiculous version of the game—and one that forgoes computer simulation—tests the hiding and finding systems in the real world but replaces real munitions with virtual ones—e.g., laser tag equivalents. Private war games and the National Training Center do this. That no war in memory has ever been replaced by a war game casts doubt on whether, despite great advances in simulation, any future war will be either.

Gibson-warfare. The author confesses to having read William Gibson's *Neuromancer*[61] and, worse, to having seen the Disney movie "TRON." In both, heroes and villains are transformed into virtual characters who inhabit the innards of enormous systems and there duel with others equally virtual, if less virtuous. What these heroes and villains are doing inside those systems or, more to the point, why anyone would wish to construct a network that would permit

[61](N.Y.: Ace Science Fiction, 1984).

them to wage combat there in the first place is never really clear.

Why bring up Gibson's novel and the Disney movie? Because to judge what otherwise sober analysts choose to include as information warfare—such as hacker warfare or esoteric versions of psychological warfare—the range of what can be included in its definition is hardly limited by reality.

The Internet and its imitators have produced virtual equivalents of the real world's sticks and stones. Women have complained of virtual stalkers and sexual harassers; flame wars in the global village are as intense and maybe as violent as the village gossip they have supplanted; agent technology, coming soon, permits a user to launch a simulacrum into the net, armed with its master's wants and needs, to make reservations, acquire goods, hand over assets, and, with work, to negotiate terms for enforceable contracts. What conceptual distance separates an agent capable of negotiating terms from another capable of negotiating concepts, hence, conducting a discussion? What will prevent an agent from conducting an argument? Arguments may require the support of allies, perhaps other agents wandering the net, who may be otherwise engaged in booking the best Caribbean vacation but who have spare bandwidth available for engaging in sophomoric colloquy. Allies might then form on the other side. The face-off of allies and adversaries, of course, equals conflict and perhaps even a disposition of goods and services that will depend on the outcome. Thus, war, in the guise of information war, even while the originators of the argument are fast asleep.

Possible? Actually, yes. Relevant to national security? Not soon.

10 *Summary*

A summary evaluation of the various forms and subforms of warfare asks: which are real, for which does the United States have an advantage, which are new, and how effective each might be.

(*i*) Which wars are real and which are theoretical constructs, (which do not yet exist or, if they did, could stretch the definition of warfare)? Specifically, which are war as commonly recognized—a destructive, extralegal struggle between two forces for control of a state's powers, its actions, or its assets (e.g., territory)?

Real forms of warfare include everything under C2W, EW, IBW, and psychological operations against commanders and forces. *Arguable* forms of warfare include psychological operations against the national will and culture, as well as techno-imperialism. Hacker warfare, information blockades, information terrorism, and semantic attacks are *potential* forms of warfare. Finally, simula-warfare and Gibson-warfare are *unlikely* in the foreseeable future.

(*ii*) How would the United States fare against a prototypical sophisticated foe of the future (e.g., a middle-income country with access to global markets for electronic equipment and engineering talent)?

The United States is *powerful* at antiradar and cryptographic aspects of EW, offensive intelligence-based warfare, psychological warfare against commanders and forces, and simula-warfare; it has distinct advantages in *kulturkampf* and blockading information flows. The United States is both *powerful but vulnerable* when it comes to C2W, defensive intelligence-based warfare, hackerwarfare, techno-imperialism, and Gibson-warfare. The United States is *vulnerable* to psychological warfare against the national will, information terrorism, and semantic attack on computer networks.

(*iii*) The following table lays out which of these forms are new in whole or in part. It also sketches the effectiveness of each form of information warfare against its likely defenses.

Table 1. Information Warfare—What's New, and What is Effective

FORM	SUBTYPE	IS IT NEW?	EFFECTIVENESS
C2W	Antihead	Command systems, rather than commanders, are the target.	New technologies of dispersion and replication suggest that tomorrow's command centers can be protected.
	Antineck	Communication links are now proliferated across the spectrum and landscape.	New techniques (e.g., redundancy, efficient error encoding) permit operations under reduced bit flows.
IBW		The cheaper the silicon the more can be thrown into a system that looks for targets.	The United States will build the first system of seeking systems, but, stealth aside, pays too little attention to hiding.
EW	Anti-radar	Around since WW II.	Dispersed generators and collectors will survive attack better than monolithic systems.

FORM	SUBTYPE	IS IT NEW?	EFFECTIVENESS
	Anti-communications	Around since WW II.	Spread spectrum, frequency hopping, and directional antennas all suggest communications will get through.
	Cryptography	Digital code making is now easy.	New codemaking technologies (DES, PKE) favor code makers over code breakers.
Psychological Warfare	Anti will	No.	Propaganda must adapt first to CNN, then to Me-TV.
	Anti troop	No.	Propaganda techniques must adapt to DBS and Me-TV
	Anti commander	No.	The basic calculus of deception will still be difficult.
	Kulturkampf	Old history.	Clash of civilizations?
Hacker Warfare		Yes.	All societies are becoming *potentially* more vulnerable, but good housekeeping can secure systems.

	SUBTYPE	IS IT NEW?	EFFECTIVENESS
Economic Information Warfare	Economic Blockade	Yes.	Very few countries are yet that dependent on high-bandwidth information flows.
	Techno-Imperialism	Since the 1970s.	Trade and war involve competition, but trade is not war.
Cyber-Warfare	Info-Terrorism	Dirty linen is dirty linen whether paper or computer files.	The threat may be a good reason for tough privacy laws.
	Semantic	Yes.	Too soon to tell.
	Simula-warfare	Approaching virtual reality.	If both sides are civilized enough to simulate warfare, why would they fight at all?
	Gibson-warfare	Yes.	The stuff of science fiction.

11 *Looking for the Elephant*

Slicing, dicing, and boiling the various manifestations of information warfare produces a lumpy stew. Information takes in everything from gossip to supercomputers. Warfare spans human activities from by-the-rules competition to to-the-death conflict. Some forms of warfare use the human mind as the ultimate battleground; others work just as well even if people go home. Information warfare, in some guises, almost seems to predate organized societies; in other guises, it may continue long after human society has evolved to transcend today's organization whatsoever.

With the background of the first part of this essay, it seems reasonable to return to the underlying issue of information as a medium of conflict. Is information warfare sufficiently coherent to permit the emergence of information warriors? Does information dominance have any meaning, and, if it does, is that dominance the core goal of information warfare or a distraction that either applies so selectively that it is only one of many possible viewpoints or so broadly that further discussion is useless?

Naval War Is to Navies as Information War Is to What? Can information be considered a medium of conflict parallel to other media? If so, is a separate service needed to house information warriors, however defined? There is a certain logic, for instance, to organizing a corps capable of managing the sensor-to-shooter cycle.[62] It could develop and organize the elements of the system, oversee their emplacement, interpret their emanations, maintain their integrity, and convey the results generated to the units that need them. This task would encompass IBW directly; the defense of the cycle would complement other information warfare efforts, such as defensive C2 warfare, counter-EW, and antihacker warfare. If information architectures are similar across competing militaries, than this corps may have the best feel for how the other side goes about developing its own sensor-to-shooter cycle. Conceivably, this corps would *contribute* to broader efforts in offensive C2 warfare, EW, and hacker warfare (as industrial economists helped pick targets of the U.S. strategic bombing campaign in World War II), but it would not conduct the war.

As the author can attest, the notion of an information corps falls short of intuitive obviousness. Even true believers understand that many forms of information warfare transcend the DoD: from certain aspects of intelligence collection, to the defense of civilian information systems, to most psychological

[62]See, for instance, Martin C. Libicki and CDR Jim Hazlett, "Do We Need an Information Corps?" in *Joint Force Quarterly*, **2**, 88-97.

warfare, to almost all economic information warfare, and to who knows what percentage of cyberwarfare. No DoD corps, regardless of how broadly constituted, could have cognizance of more than perhaps half the territory of information warfare.

Even within that subset, however, the notion of an information warfare corps defined in terms of in its medium is problematic. Corpsmen of all stripes tend to see their primary job as facing off against their opposites. Tank drivers know that the best weapons to engage tanks are other tanks; ditto for submariners. Jet drivers may be last to recognize how few countries believe their own jets can win air-to-air engagements with U.S. forces.[63] Denizens of the U.S. Space Command admit only grudgingly that their role in life is to help air-breathing commanders; given their druthers, they would rather conduct dustups with the space systems of other countries.

Unless an information corps is continually oriented to supplying (and protecting) information to support operations (a mission that overshadows the possession of raw firepower in determining conventional engagements), it may be tempted to orient itself against its counterparts. How ironic it would be if an

[63]Even though potential opponents of the United States are likely to try almost everything (e.g., ground-to-air systems or target stealth and hardening) *but* air-to-air combat to neutralize U.S. air power, the U.S Air Force's desire to purchase the F-22 for air supremacy persists.

information corps took defeat of the other side's systems as its mission—just when such warfare becomes increasingly difficult to pursue, unproductive of results, and generally irrelevant to outcomes.

Is Information Dominance Possible? Is information warfare a struggle for control of the information battlespace? Does information dominance—a counterpart of, say, maritime supremacy, air superiority, or territorial control—make sense as a goal? A nation claiming maritime superiority demonstrates its strength when its vessels have unquestioned right of passage over open oceans and can deny the same to enemy vessels. Similar claims to air superiority, or air supremacy, arise when one side can send its warplanes everywhere in the heavens while the other cannot even guarantee its birds' survival on the tarmac long enough to launch them.

Information warfare admits of the concept of superiority. One side in a conflict may have better access to information than the other. It has more sensors in better places, more powerful collection and analytical machines, and a more reliable process for turning data into information and information into decisions. It can rely on the integrity of command-and-control systems, while the enemy might have only a probabilistic set of weak links over which its messages pass. This state of affairs does not mean that one side's systems can keep the other side from functioning (in contrast to England's ability to bottle up the German surface fleet after Jutland).

Does the possibility of superiority say anything about supremacy? Only in some cases. One side's jamming device may be powerful or agile[64] enough to block radioelectronic emissions from the other side, yet this superiority would be local and may not imply that its devices can transmit without interference. Because radiation falls off to the square of distance (to the fourth power for reflected radar), a wide-area superiority translates poorly into local unintelligibility. Even so, one side might overcome power using such techniques as nulling, directional antennas, or spread spectrum (hiding a narrowband signal in a broadband swath). The result might not be to silence the other side but to reduce its bandwidth to only essential messages.[65] More likely, both sides' bits get through.

Can psychological warfare be understood as a zero-sum contest over mind-share? If two messages are opposed to each other, one side's message may dominate the other's, whose bits are received but

---

[64]That is, it can detect and counter the frequency hopping, spread spectrum, or chirping systems of another side quickly for the same effect.

[65]For instance, if 1.2 KHz bandwidth signal (sufficient for an STU-3 digital signal) is spread over a 120 MHz band, then a blind jammer must be roughly a hundred thousand times as powerful as the original signal generator (assuming the distances are the same) to do its job.

whose messages fade. In practice, debates are not usually conducted as a direct clash of opposites (crime is down versus crime is up) but through selective emphasis or deemphasis (crime is up versus educational scores are up). Given enough conflict, listeners could resolve the issue by saying they're both lying.

Overarching concepts such as an information warfare corps or information dominance end up having limited application over the entire or even a large segment of whatever falls under the rubric of information warfare. A comparison can be made to logistics supremacy; clearly one side's trucks do not prevent those of the other side from getting through. Opposing information systems can probably each expect to go about their business without overwhelming or even corrupting the other.

Conclusions: First, almost certainly there is *less* to information warfare than meets the eye. Although information systems are becoming more important, they are also becoming more dispersed and, if prepared, can easily become redundant (e.g., through duplication, compression, and error-correction algorithms). Other *commercially employed* techniques, such as distributed networking, spread spectrum, and trellis coding, can ensure the integrity of messages. The growth of networking systems has created new vulnerabilities, but they can be managed once they have been taken seriously. A strategy that strangles the other side by applying pressure on its information pipe may be self-defeating; if the other side's bureaucracy is well understood it may be defeated even more easily by flooding it with more information than it can handle.

Second, information warfare has no business being considered as a single category of operations. Of the seven types of information warfare presented here, two—information blockade and cyberwarfare—are notional and a third—hacker warfare—although a real activity, is grossly exaggerated as an element of war viewed as policy by other means. Disregarding these as premature forms of information warfare, and associating EW techniques with whatever ends they support (e.g., C2W, IBW), three forms remain: C2W, IBW, and psychological operations, each of which can stand as a separate discipline. As it so happens, command-and-control systems are vulnerable because they tend to be centralized, while IBW systems are vulnerable because they rely on communications to unify a decentralized sensor architecture. C2W and IBW are linked in that EW techniques can be used against both command and intelligence systems.

Third, most of what U.S. forces can usefully do in information warfare will be *defensive*, rather than *offensive*. Much that is labelled information warfare is simply not doable—at least under rules of engagement the United States will likely observe for the foreseeable future. Information systems are more important to

U.S. forces than they are likely to be to opposing forces; what the United States might do in offensive operations is limited by the restrictive rules of engagement it operates under; and the United States's open information systems are by their nature more likely to be understood than systems of other countries.

Information Warfare and Information Architecture: One concept that recurs in almost all forms of information warfare—and thus offers a unifying subtext—is that the details of a system's architecture determine the effects of attacks on it—far more than details, of say, a city's architecture determines the effects of its being bombed.

Following Sun Tzu, the side that understands its enemy better is better prepared for conflict. Understanding the enemy's culture and the ways in which its society uses information remain important. These days, grasping the way the enemy uses information systems—notably, communications networks, databases, and, someday, systematic knowledge algorithms (e.g., neural nets)—is equally important.

At the core physical level, architecture incorporates sensors and emitters and their power, acuity, availability, and reliability. At the network level, architecture encompasses the interconnection of those elements: do they feed into the core processor directly, are they filtered through particular systems (algorithmic or human or some combination) or intermediate nodes (e.g., whether a field processor extracts semantic information and passes it along or just filters bits). At a higher level are the integrity systems: encoding and encryption, message prioritization (e.g., filtering systems to replace what hierarchies used to do; useful for heavy EW environments), access (who can see what), digital signatures (to ensure that a sensor's readings come from a sensor or that commands come from a valid source), and redundancy (at the levels of bytes and semantics).

Architecture speaks to the way bits are transformed into information. A commander in one headquarters may pay attention to little else but the three top aides (who apply intuition to what they hear from lower echelons). The commander in another may insist on a large group of analysts who examine raw data, the relative influence of each analyst varying with the commander's estimate of their ability and with the correlation between the analysis and reality. Yet a third commander may reserve looking at slightly massaged bit streams for himself; analysts at this headquarters may suggest interpretations, but the analysis would get its due only if it is both out of the box but within the ballpark. Clearly, each commander has a different decisionmaking style, and a campaign of C2 warfare would have very different effects on each command apparatus.

Architecture links information to decision: how readings are interpreted, what readings are correlated to one another, what constitutes recognition, where boundaries are set to eliminate false positives and false negatives, and under what circumstances sensor bit streams are given higher relative priority. Are data from heterogeneous streams melded to influence decisions or to support them after the fact? The sensor-to-shooter complexes of tomorrow are but one channel; other channels include political direction, rules of engagement, and the status of one's own forces.

Information warfare waged without regard for the architecture of decisionmaking is no better than a shot in the dark. U.S. forces in the Gulf exploited a long period of preparation figuring out how Iraq's leadership was thinking: extracting from Soviet doctrine and from recent Iraqi history (e.g., the tenets of Baath ideology, lessons from the war against Iran), listening to intercepted messages, exploring Soviet equipment, perhaps even feinting to test Iraqi systems. By 17 January allied forces had a fairly good feel for the way Iraq used information.

Architectural issues pervade civilian systems under attack from tomorrow's hackers. Most issues of access and security are essentially questions of who the system will let talk to it. How are messages and messengers are linked—for example, by digital signature (proposed for electronic commerce) or telltale threads[66] (proposed for intellectual property protection)? Issues of whether others can feed the system executable code or parsable text are questions of what the system can absorb without rejecting. Unerasable archiving schemes are connections between the possibly corrupted present state of a system and its past, presumably uncorrupted state. To say that a system is hackable because it is physically open is scarcely to offer an adequate description of a system with complex and often correctly thought-out architectures.

Psychological warfare must correspond to media architectures, in multiple dimensions, if it is to have an effect. The first issue is the seemingly simple one of how to inject bit streams into the media mesh of another country: directly (e.g., through DBS), indirectly (e.g., through CNN), or reflection (e.g., through media reaction to particular events). Is the target population "pre-media" (e.g., when information mainly is word of mouth), mass media (e.g., one or, at most, only a few outlets), or "post-media" (e.g., five hundred channels or even Me-TV)? How do most people treat information—as gospel, as advertising claims, as reliable indications of the opposite view

---

[66]According to this concept, a piece of intellectual property (e.g., a video) would be altered or salted slightly with pseudo-random bits for each customer, who may then choose to copy the product illegally for a friend. If the friend's copy is found, enough bits in the original will indicate the original (and guilty) party.

(e.g., popular reaction to Soviet newscasts)? How do official news sources respond to anomalous information—ignore it, flood it, refute it, suppress it? In this example, architecture has both a simple technical component and a more complex cultural one.

The dependence of information warfare on the other side's architecture suggests that its effectiveness is only as good as its intelligence on that architecture. To conduct C2W requires, minimally, knowledge of who talks to whom about what using which systems wired how. Equally necessary is a feel for the way command systems operate under stress or in degraded mode. To say that this information is difficult to collect (let alone verify) is an understatement. With the Cold War over, the number of countries needing to be mapped is larger and the resources to do it smaller than while the Cold War raged.[67] In contrast to the forty plus years the United States spent studying the Soviet Union, new enemies now can arise in weeks. Yet, most potential enemies of the United States have acquired information systems from Western firms, a source of intelligence that was not available about the Soviets. If the knowledge required to conduct and assess attacks on the other side's command systems is sufficiently below what the United States has or can get, resources devoted to such attacks may be wasted.

[67]Worse, the Services are cutting back on Foreign Area Officers, so that the cultural context of this wiring may be missing.

Now, consider that foreign defense systems designed to interoperate with U.S. IBW collection systems will be easier for the United States to understand should the tides of friendship ebb. The international assimilation of computers and communications through the global information infrastructure is giving rise to information systems that respond to a variety of requests and generate a variety of answers (e.g., airline reservations systems, environmental monitoring systems, interbank fund transfers)—and perform in relatively understandable ways. This situation leads to several conclusions.

First, to know the other side's systems in wartime, it may be enough to know them in peacetime. Is it too much to expect that other people's peacetime systems will be influenced partly by their need to interconnect with U.S. systems during years when they and the U.S. enjoy mutual comity?

Second, little will help the United States to know the other side's architecture in peacetime better than helping to shape it. Other nations' systems are strongly influenced by the extent to which their architectures are subsystems of those of international systems, (hardware, software, content, and systems integration).

Third, the shrewdest U.S. national security strategy may be expressed through support for the development of a global information infrastructure. Favorable pricing policies, accessible software and technology, and mutually accepted standards offer one method. Common networks help; so, too, does global availability of services both for data dissemination and for intelligent dataprocessing. Sensors and other space information systems for which common interfaces are available and global access promote a shared visibility of the earth. Public key infrastructures and interlinked ambient monitoring systems can assist information security. The exact architecture of such emerging information systems need not be detailed immediately, but its most important feature—a global system that is an extension of the U.S. system—remains.

*U.S. G.P.O.:1996-405-201:40011