NATIONAL DEFENSE UNIVERSITY
INSTITUTE FOR NATIONAL STRATEGIC STUDIES

DEFENDING CYBERSPACE AND OTHER METAPHORS

MARTIN C. LIBICKI

THE CENTER FOR ADVANCED
CONCEPTS AND TECHNOLOGY

Defending Cyberspace and Other Metaphors

Martin C. Libicki

Directorate of Advanced Concepts,
Technologies and Information Strategies
Institute for National Strategic Studies

National Defense University
Washington, DC

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
- Fort Lesley J. McNair, Washington, DC 20319-6000
- Phone: (202) 685-2209 ♦ Facsimile: (202) 685-3664

Library of Congress Cataloging-in-Publication Data

Defending Cyberspace and Other Metaphors / Martin C. Libicki.
p. cm.
ISBN 1-57906-031-5
1. Information Warfare—United States. 2. Information Superhighway—United States. I. Title
U163.L52 1997
355.3'43—dc21 96-53238
CIP

First Printing, February 1997

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

Contents

Figures

Introduction

Information warfare, as any casual observer of the Pentagon can attest, remains a hot-button topic in the military community.

Broader claims for it have been toned down,[1] and few now argue that all aspects of warfare are now revealed as information warfare, but an ideology of information warfare has nevertheless wended its way into the heart of defense planning. The Air Force's *Cornerstones of Information Warfare*, for example, has approached the status of doctrine. The spring 1996 establishment of the 609th Squadron (at Shaw Air Force Base) dedicated to information warfare offers further evidence of the seriousness with which that ideology is maintained. In 1996 the National Defense University (NDU) ended its two-year experiment of offering a forty-four-week program on Information Warfare and Strategy after forty-eight students were graduated, but what has replaced it is a broader thrust in teaching the all four hundred students the rudiments of information warfare (and offering related electives). In 1995–96 large portions of the Defense budget were designated information operations (although only a small portion represents information warfare).

Intellectually speaking, what clarity has been gained by the discovery of information warfare?

Some Insights: On the one hand, several insights have been brought to attention. One insight recognizes the deification of the observation-orientation-decision-and-action (OODA) cycle and maintains that an information warfare strategy that retards the enemy's decision cycle without physically destroying it may nevertheless be worthwhile.

---

[1]On the theory that once a trend hits *Time* magazine it has already peaked, the cover article of the 21 August 1995 issue was "Cyber War," by Mark Thompson and Doug Waller (38-46).

Another insight is based on the near-tautology that one should not rely on capabilities on which one cannot depend (which is to say, defend). The U.S. military depends increasingly on computers and networks, particularly radio-electronic networks. This emphasis inevitably creates new vulnerabilities unless it is matched by attention to systems protection (e.g., defensive electronic warfare and operational security) or at least dependence management. How much security and protection are needed, what the tradeoffs are in security, cost and functionality, and to what extent technology favors offense or defense all are empirical questions, but the need to address them is beyond reasonable argument.

A third insight is that global computer and media networking carries risks, even if these risks are easily exaggerated. Computer networks might permit enemies to use hackers to attack the information infrastructure of the United States, rather than its military forces. The conventional defense establishment has been described as a Maginot Line, in which hackers are equivalent to Guderian's Panzer Korps, wheeling past prepared defenses to strike at the nation's unguarded flanks. Television networks are conduits through which foreign interests can wage psychological warfare using a mix of traditional propaganda, manipulation of truth by human and technical means, and even the exploitation of micromedia (e.g., specialized cable channels, mailing lists, or Web sites) to set one part of a target population against another.

New Threads: A previous monograph[2] made limited progress toward a theory that would unite the various aspects of information warfare. Because information turns out to be pervasive in human activity, segregating it as something

[2]Martin C. Libicki, *What Is Information Warfare?* (Washington, D.C.: National Defense University Press, 1995). It divides information warfare into (1) command-and-control warfare, (2) intelligence-based warfare, (3) electronic warfare, (4) psychological warfare, (5) hacker warfare, (6) economic information warfare, and (7) cyberwarfare.

particular over which combatants can struggle appears to be an unproductive approach. But as information warfare wanders off the military reservation, the question of whether it is indeed warfare grows increasingly urgent. Even though most techniques of information warfare have appeared in earlier wars, much of what is called information warfare may so fundamentally act at variance with warfare as to be a fabric woven from completely new threads.

One thread is that understanding how the other side uses information is critical to knowing what aspect of the enemy to attack. Because success in information warfare is strongly influenced by the quality of intelligence about the other side, most forms of it are highly opportunistic, with effects difficult to predict. Consider some examples. Success in decapitating the other side's command structure requires knowing where the command centers are (and who is inside it) and where are the lines that run from commanders to the field. If cryptographic codes are unbreakable, then signals collection requires waiting for opportunities arising from human error, such as talking in the clear or mishandling keys.[3] Computer systems can be entered because of uncorrected mistakes, so success in breaking and entering into them also varies widely.[4] The other side's commanders are more easily fooled if they cling to certain prior judgements about the nature and contents of the battlefield. Luck and circumstance play great roles in information warfare, while brute force seems to be a smaller factor.

A second thread, which echoes the critical role of intelligence in enabling information warfare, is the difficulty of battle damage

---

[3]See for instance, Gustuvus J. Simmons, "Cryptanalysis and Protocol Failures" in *Comm. ACM* **37**, 11 (November 1994), 56-65; and in the same issue, Ross J. Anderson, "Why Cryptosystems Fail," 32-40.

[4]Whether breaking into *one* part of a complex system means access to the *whole* depends on such factors as internal firewalls, the ways some parts of the system grant privileges to other parts, and the ways multilevel security is implemented. Thorough security systems are redundant and compartmented.

assessment (BDA). Damage assessment is a frustrating exercise even when it cannot be masked or exaggerated—as it can be with human and computer information systems. Was the particular command center that was identified and destroyed, for instance, really the intended one? Did a virus really disable the computer? How can one tell whether a microwave burst really put a tank's electronics out of action? Has every frequency used by a radar been covered by a jamming signal?

Some techniques help address the BDA problem. The human intelligence that relayed the identity of the command structure may be available to confirm destruction. The crippling of an air defense radar can be assumed by inactivity when one's own aircraft are overhead. Communications sent through secure channels may be diverted into the open when preferred channels are taken out. The destruction of a utility's switch can be inferred by the sudden blackout. Observers can report whether a propaganda barrage against a populace is having an effect. Yet, the victim may be able to mask the real damage. A system under hacker attack can generate false effects. The newly purloined data, were they valuable or was the enemy's grip purposely loosened so deception might be spread? Files might be established that appear valid, even files that correlate to other files but which are phony—the cyberspace version of "The Man Who Wasn't There," (a ruse the British used during World War II to plant phony war plans on a corpse left for the Germans to find). Replicating fictive digital documents throughout a system is easier than replicating real ones (a few keystrokes suffice and storage space is cheap). A system could show false signs of failure by appearing to slow down or malfunction.

A third thread is the impact of information warfare on the need for force. The world's most successful coercive organization, which extracts more than a trillion dollars from a public that would just as soon keep its money, is the U.S. Internal Revenue Service (IRS). The IRS works almost entirely in the information realm. Those who choose to work against the IRS manipulate or withhold information, while the IRS develops information-

gathering mechanisms to fill the national exchequer. Behind a vast information apparatus lies the law that compels taxation, and behind that lies the threat of physical force as a collection device and as a general deterrent. The taxpayer who calculates the correlation of forces before filing a 1040 is rare, and the amount of force used in the collection of taxes is small. Still, the taxpayer perceives its lurking presence, and were force absent, the flow of taxes might be greatly reduced. Force also remains the stone in the snowball of tomorrow's high-tech militaries. The ratio of stone to snow grows smaller. It may not even be our stone (the United States might supply targeting information to an ally that did the actual shooting), but without a stone, military force would have no meaning.

A fourth thread is the mutability of the information medium. The eternal seas and their geological, physical, and meteorological characteristics are immutable foundations of naval warfare. The art of air combat rests on the immutable aerodynamic characteristics of the earth's atmosphere. The characteristics of space satellites descend from immutable laws of orbital mechanics. For the most part, even the land terrain precedes ground combat and is the context for what works and what does not work in war. The information domain, however, is almost entirely man-made.[5] Thus command-and-control warfare may attack the enemy's command structure but the command structure, itself, can be shaped, almost at will. Hacker warfare proceeds entirely over a terrain of the defender's making—be it hardware, networks, operating systems, applications, or access architecture. The success of attempts to deceive the other side's system of systems are a function of its makeup from one year, day, or minute to the next. Psychological warfare against enemy commanders or troops works best when it works off preconceived notions they share. Warfare, in general, has been likened to chess in which two players contest over a fixed board using pieces with predetermined behaviors. In information

[5]The physical properties of the electromagnetic spectrum (e.g., the permeability of the elements to various wavelengths) constitute an exception.

warfare each side brings its own board; one which each can change as much or as often as it needs to.

So To Metaphor: These threads suggest that information warfare remains a phenomenon that must be understood separately from warfare as a whole. Yet people rarely think about information warfare from first principles; for the most part, information warfare involves phenomena few people have experienced. It is warfare by virtue of analogy, or, better, metaphor. It is warfare because it resembles activities that surely are warfare. Used properly, a metaphor can be a starting point for analysis, a littoral, as it were, between the land of the known and the ocean of the unfamiliar. A good metaphor can help frame questions that might otherwise not arise, it can illustrate relationships whose importance might otherwise be overlooked, and it can provide a useful heuristic device, a way to play with concepts, to hold them up to the light to catch the right reflections, and to tease out questions for further inquiry.

But before analysis proceeds and policy recommendations can be justified, metaphors must be put back into the box from whence they came so that issues can be understood for what they are, not what they look like[6]. To use metaphor in place of analysis verges on intellectual abuse. It invites the unquestioning extension of a logic that works across the looking glass but lacks explanatory power in the real world. Those who forget this are apt to try to make their metaphors do their thinking for them. It is easy, for instance, to get caught up in the syllogism that effortlessly links stages of economic production with modalities of warfare.[7] According to the Defense Science Board,[8]

---

[6]Mark Stefick's *Internet Dreams: Archetypes, Myths, and Metaphors* (Cambridge, MA: MIT Press, 1996) argues that the metaphors used to describe the Internet may be hazardous to its development.

[7]The reference to Alvin and Heidi Tofflers' *War and Anti-War: Survival at the Dawn of the 21st Century* (Boston: Little Brown, 1993) is obligatory.

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

Thus does war follow commerce into cyberspace, pitting foes against one another for control of this clearly critical high ground. But does this facile comparison have a basis in reality?

Essays: In this iconoclastic spirit, the following six essays are characterized by a continuing search for the meaning of information warfare.

The first essay, "Perspectives on Defending Cyberspace," concedes that the United States is increasingly dependent on its infrastructure but finds that the risks to the national security from that dependence are easily overstated.[9]

The second essay, "Deterring Information Attacks," continues the examination of the metaphor that information warfare is indeed warfare by discussing the problems of retaliation and

---

[8]From the *Report of the Defense Science Board Task Force on Information Warfare - Defense* (Washington DC: Office of the Under Secretary of Defense for Acquisition and Technology, November 1996), 2-1.

[9]An earlier version of this essay appears as "Protecting the United States in Cyberspace," in Alan D. Campen, Douglas H. Dearth, and R. Thomas Goodden, *Cyberwar: Security, Strategy, and Conflict in the Information Age* (Fairfax VA: AFCEA International Press, 1996), 91-105.

asking whether an explicit policy of retaliation is workable and thus likely to deter.[10]

The third, "Indistinguishable from Magic," notes a potential gap between what information warfare can do and what it can appear to do and asks whether that gap can be exploited for psychological warfare.

The fourth, "The Retro Revolution," examines information warfare as a throwback to forms of national security that supposedly ended with the end of the Cold War. Information warfare appears to have given new life to concepts borrowed from strategic theology, from the world of strategic intelligence, and even bygone habits of defense acquisition.

The fifth, "Postcards from the Immune System," suggests more useful metaphors for information warfare than the simple connection between defenses against real viruses and defenses against computer viruses. The immune system must attack foreign antigens but not attack the human body. In refining this delicate distinction the immune system is revealed as an information-warfare machine that uses a rich selection of redundancy, fail-safe devices, stimulants, and suppressors.

The last essay, "Point, Counterpoint, and Counter-counterpoint," was inspired by a search for a new metaphor for new kinds of warfare. Conflict has classically been modeled by orthogonal lines of defense and attack. Today's asymmetric warfare is about points, blots, and gated fences, topological forms with particular applicability to information warfare.

[10]An earlier version of this essay can be found in Winn Shwartau, *Information Warfare*, 2nd Edition, (NY: Thunder's Mouth Press, 1996), 592-600.

Essay One

Perspectives on Defending Cyberspace

With every passing week, the United States appears to grow more vulnerable to attacks on its national information infrastructure (NII). As this vulnerability to attack is transformed into military metaphor, the logic of national defense is often exploited to think about security,[11] but as comforting as that logic may feel, it is the wrong way to consider the problem.

Systems security *does* matter. The Department of Defense (DOD) must assume that any enemy it engages will attack the DOD's computers to disrupt military operations. Operators of commercial systems must be aware of and thus responsible for harm done to third parties if the operators' systems become compromised. Those who introduce new commercial applications need to think through the potential for malicious use.

Yet prudence is not the same as a notion that hacker attacks will be the twenty-first century's version of strategic warfare. That notion goes against common-sense aspects of both computers and

---

[11]On 25 June 1996, John M. Deutch, Director of the Central Intelligence Agency (CIA), testified before the Senate Permanent Committee on Investigations and maintained that among the most worrisome threats to U.S. national security, hacker attacks ranked second—just below weapons of mass destruction. In response to the threat of hacker attack, he had drawn up plans for a roughly thousand-person office located at the National Security Agency (NSA) which would focus on the risks foreign hackers posed to U.S. computers. Deutch also supported plans for a "real-time response center" in the Justice Department to work against widespread hacker attacks. He noted that the intelligence community has assessed risks to the United States of such an attack, but the results were classified. Jamie Gorelick, the Deputy Attorney General, who also testified that day, opined that information warfare was the nation's premier security threat and called for a 1990s' Manhattan Project to deal with it.

national security. It also can lead to policy prescriptions so potentially controversial that proponents would pine for the halcyon days of the Clipper chip. The United States certainly does not need a response to computer risks that (in words applied to the fin-de-siècle Austro-Hungarian Empire) are "desperate but not serious."

This essay argues that the task of securing the NII must be put into perspective. The subject has attracted a wide range of opinions, but the real nature of the threat remains undefined. At this point one can only go by what has happened or not happened to date[12] and reason about the nature of information systems—how they work, what they do, and why they may be at risk. Doing so at least culls the fantastic from the plausible. In so doing this essay argues that:

- everyday threats already engender everyday defenses,
- deep threats focus the risk on attackers,
- defense is possible if taken seriously,
- vulnerability is greater than it ought to be but should not be exaggerated,

[12]Yet, the NII has yet to suffer a major attack or anything close it despite numerous smaller attacks. The opportunity for a major attack already exists: the United States has been an automated society for years. Nor does the United States have a single large enemy holding its fire until the time is right. A statistical relationship between an incident's size and its rank (Zipf's Law), suggests that for one very large incident there should be two not-so-large incidents, four lesser incidents, and so on—each category a geometric ratio of the one above it. A distribution composed of a few cataclysms and a panoply of annoyances would be anomalous. Anomalies prove nothing, but they ought to be addressed by proponents of any NII catastrophe theory.

- the strategic benefits of an information attack are unclear, and

- system owners must protect themselves; if they punt, the government cannot substitute.

What follows are recommendations for government policy.

Potential Threats to the NII

Why do people worry about attacks on the NII?

1. The U.S. economy and society are ever more dependent on information systems. Analog systems are becoming digital, and digital systems are replacing humans (e.g., automated teller machines [ATM], voice-mail systems). Staring at video screens—the portals to the "infotainment" face of the NII—may yet dominate U.S. nonbusiness hours.

2. Information systems are increasingly interconnected by phone and e-mail. Interconnection saves work hours, promotes work place collaboration, and permits remote management (e.g., supervisory control and data acquisition [SCADA] systems), but it also permits havoc to enter from outside the system's boundaries or even from abroad. When supposedly trusted systems can infect one another, malevolence becomes harder to contain.

3. Responsibility for serious work is being shifted to personal computers (PCs) and Unix machines and away from mainframes and minicomputers.[13] The last two,

[13]Yet, three-quarters of all real-time transactions are still on mainframe-based networks, according to Salvatore Salamone, in "How to Put Mainframes on the Web," *Byte* **21**, 6 (June 1996), 53.

designed to carry a company's valuable operating data, tend to make users into second-class citizens by limiting their access to software and taking security more seriously. PCs, designed to be as accessible as toasters, and Unix workstations, designed for information sharing, are more vulnerable systems. In addition, attacking a system whose interfaces are publicly available and thus well-understood is far easier than attacking a system whose parameters and interfaces are proprietary trade secrets.

4. Many innovations carry new security risks. Some Web browsers and spreadsheet macros allow the unwary to download viruses.[14] Distributing software objects and agents over networks may introduce similar problems. If systems use what they learn to reconfigure themselves continuously, the classic response to suspected corruption—starting fresh with original media—will set back system capabilities.

These four factors suggest that the challenge of computer security will matter more to America's well-being tomorrow than it does today.

But do they make protection of the NII a matter of national security? To some extent, yes:

1. The more a nation depends on the integrity of its information infrastructure, the more it can be put at risk by attacks there. The threat of massive disruption through information warfare has been posited as a potential

[14]Although the creators of Java paid careful attention to security issues when designing the language (essentially disabling some dangerous features of C++), Java remains problematic for systems with hard outer shells (which keep intruders from posing as users) but soft innards (which allow users to wreak havoc on the system). A Java-based program picked up from the Net can do almost anything a user can. Thus, an unpatched bug (e.g., sendmail), which lets users access system administration files, can also allow Java-based agents to do so.

successor to massive destruction by nuclear warfare. A milder variation holds that by threatening the NII, a militarily weaker foe may keep the United States out of its own backyard (and thus stymie the U.S. advantage in conventional warfare).

2. Information warfare is terrorism less bloody but with a potentially broader effect. As porous as the United States is to bad people, it is even more porous to bad bitstreams. A phone or e-mail connection suffices to gain access to a wide variety of computers. Hackers can hopscotch from one node to another until an important point of vulnerability is found and exploited. Because the risk of detection is low, and the risks of apprehension and punishment are even lower, a cyberspace attack can be cheap and rather free of risk.

3. The DOD depends more on the NII (95 percent of its unclassified communications go outside DOD systems at some point) as its assets are repatriated and off-the-shelf becomes the rule. An unprotected infrastructure permits foes to undermine conventional military operations.

Everyday Threats Engender Everyday Defenses

Abuse of systems comes in many forms. Commonplace abuses rely on normally common motivations (e.g., greed, thrills), and many are only high-tech versions of carjacking and joyriding. Others less common are serious and difficult to anticipate. The owners of systems can be expected to protect themselves (to an economically optimal level) against commonplace threats, the probability and patterns of which can be predicted from experience. Less common but serious threats are less liable to be watched for because they arise from motives that surface less often.

Deliberate abuse can take roughly six forms:

1. Theft of service (e.g., cellular phone-call fraud)

2. Acquisition of objective data (e.g., research results)

3. Acquisition or alteration of subjective data (e.g., a person's credit history)

4. Theft of assets (e.g., embezzlement)

5. Corruption or disruption of data in storage or motion (e.g., sabotage, vandalism)

6. Disruption of information services (e.g., telephony) or attached services (e.g., electric power distribution) for its own sake or for secondary purposes (e.g., corrupting medical data to hurt individuals, seeking control for the purpose of blackmail)

The first four types listed here are or could be commonplace, because they can be undertaken by individuals for gain. For example, because greed is eternal, the motive for robbing a bank electronically is ever present. Ditto for stealing services. Threats against individuals (as in the 1995 movie "The Net"), although a potential tool of guerilla warfare, are more probably motivated by private grudges. The fourth case, the theft of data, is simply a high-tech version of espionage—something the DOD already takes seriously every day. Fifth and sixth, corruption and disruption, however, best characterize the unexpectedness and malevolence of information warfare: attackers require an external goal and both a concerted strategy and the time to carry it out.

Systems that face a known pattern of threat (and whose owners would bear most or all the cost of an attack) can determine an optimal level of protection. There is no reason to believe that these owners provide less protection against information attacks than they do against other threats to their well-being (e.g., shoplifting, embezzlement, customer lawsuits). The real worry for such systems is an attack rarely seen in the background

environment—thus one for which there is less recognition and hence less protection.

Deep Threats Focus the Risk on Attackers

Systems can generally be attacked by errant bits[15] in one of three basic ways: (*a*) through corruption of a system's hardware or software; (*b*) through using an insider with access privileges; or (*c*) through external hacking, as well as through combinations of these (e.g., through having an insider reveal vulnerabilities that facilitate subsequent hacking). The closer the attack source is to the system's core the more trouble a defense may be; but deep threats focus suspicion on fewer potential attackers.

A typical tale of corruption could involve a rogue employee of a U.S. microprocessor firm queering some circuits in every PC chip so that they all go bad simultaneously at just the right time. How simultaneity is ensured without premature discovery is never explained. A slightly more plausible threat is the planting of a bug in a specific system (so that an external signal or specified condition makes the system go awry).[16]

From 70 to 85 percent of all serious hacker attacks involve insiders. In the era of downsizing, there is no shortage of disgruntled employees or ex-employees capable of initiating an

---

[15]Systems can also be attacked physically (e.g., jamming, microwaves, shot and shell), but only for the purpose of physical denial and associated blackmail. Physical attacks require a nearby presence and thus are akin to acts of well-understood terrorism. They carry far greater risks to the attacker than do cyberspace attacks, which can be launched from anywhere on Earth.

[16]Queering source code may, ironically, be easier if Ada (DOD's official computer language) is being used for coding. Ada is virtually self-documenting; this allows a hacker to look at the code, identify the purpose of its modules, and edit accordingly. Ada also supports information hiding so that a rogue module can be added without its code being open for inspection.

attack or being recruited to do so.[17] Exploiting corruption, whether inside the physical system or among trusted users, offers obvious advantages, particularly for use against systems secured only against outsiders, not insiders. The risks of getting caught are greater, though, because the chain of responsibility is direct (and in either case the number of suspects is smaller than the billion-plus people with phone access). The risks involved in recruiting such individuals from the outside resemble those involved in intelligence recruitment; if someone turns or is caught, a system is warned that it is targeted. The more people have to be recruited, the lower the odds of penetrating many systems undetected. Until such a conspiracy comes to light, the presumption must be that no sufficiently large attempt has yet been made. Insiders are, therefore, more liable to be the source of opportunistic or intermittent, rather than systematic, attack.

Last is the hacker route. Most systems divide the world into at least three parts: outsiders, users, and superusers. One popular route of attack on Internet-like networks is (*a*) systematically guessing someone's password, so that the outsider is seen as a user, and then (*b*) exploiting the known weaknesses of operating systems (e.g., Unix), so that users can access superuser privileges. Once granted superuser privileges, a hacker can read or alter the files of other users or those of the system; can control the system under attack; can make reentering the system easier (even when tougher security measures are subsequently enforced); and can insert rogue code (e.g., a virus, logic bomb, Trojan horse, etc.) for later exploitation.

The damage a hacker can do without acquiring superuser privileges depends on the way systems allocate ordinary privileges. A phone user *per se* can do little damage to the phone system. Computer networks are especially vulnerable to abusers when certain privileges are granted without being metered. Any

[17]Not every bad egg will harm society: during the Gulf War, sensitive war plans stolen from a car were promptly returned along with a message that the perpetrator, while a thief, was by no means a traitor.

system with enough users will contain at least one who would abuse resources, filch data, or otherwise gum up the works. Although mechanisms to keep nonusers off the system matter, from a security point of view, limiting what authorized users can do may be more important.

Another method of attack—applicable only to communications networks open to the public—is to flood the system with irrelevant communications or computerized requests for service. Systems in which either service is free or accountability can be evaded in some other way are prone to such attacks. The weakness of such attacks is that they often require multiple sources (to tie up enough lines) and separate sources (to minimize discovery), and their effects last only as long as calls come in. Because communications channels within the United States are much thicker than those that go overseas, overseas sites are a poor venue from which to launch a flooding attack.[18]

Systems Can Be Protected

Although many computer systems run with insufficient regard for security, they *can* be made quite secure. The theory is that protection is a point to be sought on a two-dimensional space (see Table 1). One dimension is the degree of access, from totally closed to totally open. A system that is secured only by

[18]This rule admits several exceptions. First, a flooder can curtail communications between the United States and a foreign nation if it can get on the links that connect the two countries. Second, a flooding attack can be aimed at large known reflector sites. Third, under some circumstances, a flow of incorrectly addressed mail, even if smaller than a link's capacity, can clog a router's memory buffers. Fourth, a flooder can try to propagate a virus among networked computers that, upon activation, floods the rest of the network from multiple and unsuspecting sources. The first cannot take down the NII; the second can be turned off; and the third requires a software fix. The fourth may be a real problem but the mathematics for the attacker (how long it takes a virus to infect enough computers to have any effect without being discovered prematurely) are daunting.

keeping out every bad guy makes it difficult—or impossible—for good guys to do their work. The second dimension is resources (money, time, attention) spent on sophistication. A sophisticated system keeps bad guys out without great inconvenience to authorized users.

Table 1
Security Choices

Security Choices	Scrimp on Security	Spend on Security
Tighten Access	Users kept out or forced to alter work habits	Users can get in with effort, but hackers cannot
Loosen Access	Systems vulnerable to attack	Users can get in easily but most hackers cannot

To start with the obvious method, a computer system in a secure location that receives no input whatsoever from the outside world ("air-gapped") cannot be broken into (and, no, a computer virus cannot be sprayed into the air like a living virus, in the hope that a computer will acquire it). If insiders[19] and the original software are trustworthy (and the NSA has developed multilayer tests for the latter), the system is secure (although often hard to use). Such a closed system is, of course, of limited value, but the benefits for some systems (e.g., nuclear systems) of freer access are outweighed by even the smallest chance of security vulnerabilities.

[19]The problem of insider sabotage is a difficult one approached through traditional security checks and compartmentalization as well as authentication methods to link effects to their authors, and, for sensitive areas, the equivalent of dual-key authorization.

The challenge for most systems, however, is to allow them to accept external input without putting their important records or core operating programs at risk. One way to prevent compromise is to handle all input as data to be parsed (the 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 the core operating program, indirectly or directly (when parsed, almost all randomly generated data result in error messages). To pursue a trivial example, there are no button combinations that can be pressed that would insert a virus into an ATM. Less trivially, it is very hard to write a virus in a data-base manipulation language such as structured query language.

Unfortunately, systems must accept changes to core operating programs all the time. In the absence of sophisticated filters, a tight security curtain may be needed around the few applications and superusers allowed to initiate changes (authorized users might need to work from specific terminals hardwired to the network, an option in Digital's VAX operating system). Another method to cut down on viruses and logic bombs is to operate solely with programs found on unerasable storage media, such as CD-ROMs. When programs must be altered,[20] they can be rewritten, recompiled in a trusted environment, and fixed onto new CD-ROMs (by 1996 the cost of equipment to cut a CD-ROM had fallen below $500).

The technologies of encryption and, especially, of digital signatures provide other security tools. Encryption is used to keep files from being read and to permit passwords to be sent over insecure channels. Digital signatures permit the establishment of very strong links of authenticity and

[20]Operational software must be complemented by data files which must be constantly change. Data files, used properly, cannot host viruses; they can be corrupted, but a corrupted data file can do only so much damage.

responsibility between message and messenger[21]. A digital signature is used to create a message hash with a private key for which only one public key exists. If a user's public key can unlock the hash and if the hash is compatible with the message, the message can be considered signed and uncorrupted. Computer systems can refuse unsigned messages or ensure that messages really originated from other trusted systems. The private key never has to see the network (where it might have been sniffed) or be stored on the system (where the untrustworthy might give it away). The use of digital signatures is being explored for Internet address generation and for secure Web browsers. Users as well as machines, and maybe even individual processes, may in the future all come with digital signatures.[22]

Firewalls offer some protection, but, even though they are the most popular method for protecting computers attached to the Internet, they need a good deal of work before they can be used reliably and without considerable attention to detail when being set up.[23] Anti-virus software also offers some protection against known viruses but whether the $3 billion a year spent on such products has been worthwhile is a different issue.

Most problems of security for systems come from careless users, poor systems administration, or buggy software. Users often choose easily guessed passwords and leave them exposed. Poorly administered systems include those that let users choose their own passwords (notably easily guessed ones), keep default

[21]Digital signatures can also inhibit some insider crime. For instance, ensuring that a data-base that can only be changed by a digitally signed entry makes it tamper-resistant; corruption is easier to trace back to a specific individual.

[22]Unfortunately, to be secure, a digital signature needs to be 512 to 1,024 bits long—thus difficult to memorize. Human use may require hardware-encoded schemes coupled with a personal information number (PIN) so that theft of the hardware will not reveal the full password.

[23]See Lee Bruno, "Internet Security: How Much Is Enough?" *Data Communications* **25**, 5 (April 1996), 60-72.

passwords or backdoors in operation, fail to install security patches, or give users access to total system resources to read or write files (particularly those that control important processes), from which they should be barred. Common bugs include those that override security controls or permit errant users to crash the system, or in general make security unnecessarily difficult or discretionary.

Client-server architectures suggest a second-best approach to security. Absent constant vigilance by all users, client computers are hard to protect. They are as numerous as their users (and often as variegated); they often travel or sit in unsecured locations, and tend to run common applications over commercial operating systems. Client computers are "owned" by their users who tend to upload their own software, use their own media, and roam their favorite Web sites. This helps propagate viruses (by one account half of the client computers used by the U.S. Army in Bosnia were infected). Traditionally, viruses infected the computers they run on and little else; but tomorrow's more intelligent versions may learn to flood or otherwise disable networks, and seek out specific information on servers in order to pass it along, or corrupt it. Servers, for their part, hold the core objects (information bases, processing algorithms, and system control functions) from which clients can be refreshed. Servers are few in number (which facilitates auditing and monitoring), and they rarely travel. They can be secured behind physical walls and semantic firewalls. They are "owned" by their institutions and thus unlikely to host unnecessary applications. They are also more likely to run proprietary or heavyweight operating systems which are inherently more secure. A strategy which solves the easier problem of protecting servers may provide information assurance; however, network servers also must be protected for assured service and they tend to run commercial network operating systems which are inherently more vulnerable.

The head of the Computer Emergency Response Team (CERT) once estimated that well over 90 percent of reported break-ins

involved exploitation of known and uncorrected weaknesses of the target system.[24] Most of the remainder used methods understood to be theoretically possible, even if the precise algorithm was unknown.

Because the operating systems of most PCs and workstations assume a benign world, rewriting them to secure them against the best hackers is difficult; the more complex the software and security arrangements, the greater the odds of a hole. In security, the primitive is often superior to the sophisticated: there are fewer configurations to test.[25]

Yet a virtual stock exchange (e.g., NASDAQ) may be secured from attack with more confidence than the real one can (e.g., the floor of the New York Stock Exchange). In the virtual world, technology permits owners of a system to control all its access points and examine in detail everything that comes through. In the physical world, public streets cannot be so easily controlled,

[24]In 1994 and 1996, hackers broke into computers at the Rome Laboratory and at Los Alamos, respectively, using a bug in the Unix sendmail program that had been used in, and thus known since, the Internet Worm incident in 1988.

[25]Security research is focusing not so much on how to make systems secure and as on proving that they *are* secure. Detecting failure modes and developing tools, metrics, simulations, and formal models are all being emphasized. It would be nice if systems could be developed that could prove software secure, but considerable effort is needed to verify even a small program. A meta-model of a software system written to highlight a system's security features may be useful, but such effort will compete with all the other meta-models a designer may be asked to create (e.g., to state rigorous architectural assumptions for later integration into other systems). Fortunately, only a small part of most programs deals with access privileges, and this part (if compact and well-identified) is more easily checked than the whole. Another approach is to hire in-house hackers, give them the source code (thus giving them a great advantage over outside hackers—except for Internet systems, whose source code is public and available), and see how far they get. A third approach is to offer a reward for cracking in (as Netscape has done, for their security software) while the product is in beta testing.

moving items cannot be so confidently checked, and proximity and force matter.

Perhaps the most misleading guide to protecting information systems is the myth of the superhacker, the evil genius capable of penetrating any system. Militaries have conventionally been built on the understanding that there is no perfect defense or offense: No wall, however thick, will withstand a battering ram of sufficient size (and no battering ram, however strong, can go through a wall sufficiently thick). The analogy to computer systems is specious. Systems are entered because they have holes open to some combination of bytes. The placement and distribution of holes is what matters, rather than how persistently or creatively an attacker forces them.

The NII's Vulnerability Should Not Be Exaggerated

How vulnerable *is* the national information infrastructure? No one really knows. Are publicized incidents of phone "phreaks," Internet hackers, and bank robbers the tip of the iceberg? Common wisdom is that victims do not talk about being had, but Citibank's decision to prosecute the perpetrators of rather than cover up a fairly large computer crime ($400,000 was transferred to and withdrawn from the accounts of the perpetrators and another $10 million had been waiting in them for withdrawal) suggests a change in perception as well as prospects for public reporting.[26]

What does computer crime cost? The Federal Bureau of Investigation's (FBI) best estimate is between $500 million to $5

[26]On 2 June 1996, the London *Times* reported that banks in London, New York, and Tokyo had paid roughly a half billion dollars in blackmail to "cyber terrorists," who had demonstrated to them that they could bring computer operations to a halt; over three years, they had made more than forty attacks. The *Times* report has proved unusually difficult to verify, because neither the banks nor the alleged perpetrators (nor anyone quoted in the report) was identified by name.

billion—in the same league as cellular telephone fraud (roughly $1 billion) and private branch exchange (PBX) toll-call fraud.[27] One should not make too much of any such estimates. Most embezzlement in the 1990s is computer crime, because computers are where financial records are kept but embezzlement predates the computer. The cost of a stolen phone call is much less than its price (most phone systems have excess capacity, the price of a call includes services such as billing, which do not apply to stolen calls, and many callers would have foregone the call if they had to pay). The cost to a corporation of having its research and development (R&D) looked at by competitors may be impossible to assess, but it is easy to assign an outsize figure to it.[28]

How frequent are Internet attacks? One way to calculate is to start with the 1,200 reports CERT received in 1995.[29] In the early 1990s, the Defense Information Systems Administration (DISA) used publicly distributed tools to attack unclassified defense systems and succeeded 90 percent of the time. Only five percent of all victims knew they were being attacked, and of those that knew only two percent reported the attack. If this 1000:1 ratio is indicative (and Navy tests echo them), then 1,200 reports suggest that the Internet suffers a million break-ins (even

[27]By comparison, the total cost of all credit-card fraud is $5 billion.

[28]Stolen intellectual property does not disappear; it is duplicated. Suppose one carmaker performed a billion dollars' worth of product development. Another company hacks into its computers and copies this information. The first company has lost no information; has the second company gained anything that might reduce the former's competitive position? It is probable that all but a small fraction of the research was specific to a particular product and thus offered little of value for the company that illicitly copied the data. SAIC surveyed 40 major corporations that confidentially reported having lost $800 million in 1995 through computer break-ins both *in lost intellectual property* and stolen money (Steve Lohr, "Ready, Aim, Zap," *The New York Times*, **CXLVI**, 50566, [30 Sept. 1996], D4.)

[29]An analysis of CERT reports, by John Howard of Carnegie Mellon University, suggested that, after growing apace with the Internet, the number of incidents peaked late in 1993 and has since remained relatively constant.

if few do real damage). Using similar methodology, DISA estimated that in 1995 DOD computers alone were attacked a quarter million times.[30]

The Internet, with its benign assumptions is hardly indicative of systems in general. It is rarely used for mission-critical tasks (with military logistics perhaps the most glaring exception), and if it were to become a mission-critical system for which compromise would be a serious problem, the Internet would need to evolve and would necessarily become more secure.[31] Were a hacker to get on the Internet, and through it, bring down the network at NDU, where I work, the consequences would be indistinguishable from the many outages occasioned by accident or maintenance problems. Anyone breaking into NDU's computers for information (none there is classified) would find, at best, only draft copies of papers that their authors would be more than pleased to have circulate on request.

One reason computer security lags is that so far incidents of breaking in have not been compelling. Although many facilities have been entered through their Internet gateways, the Internet itself was brought down only once (the 1988 Morris worm). No large phone or power distribution outage has been traced to hacking (the most serious incident affecting telephones occurred in the Northeast and Los Angeles in 1991, and it was traced to

---

[30]U.S. General Accounting Office, *Computer Attacks at Department of Defense Pose Increasing Risks* (Washington, D.C.: GAO/AIMD-96-84, May 1996).

[31]Most people are probably still loathe to entrust their credit cards to the Internet. In the 1950s, only 20 percent of the Americans polled were willing to fly aircraft. Aircraft manufacturers quickly realized that their prospects were tied directly to safety concerns. Boeing developed and implemented its "single-failure" philosophy, with the goal of preventing any single aircraft failure from resulting in a crash. Aircraft accidents declined over the next forty years despite more than a tenfold increase in takeoffs and landings. In a similar fashion, the newest version of the Internet Protocol (IPv6) can sharply reduce many threats such as source-address-spoofing, source-related routing attacks, password sniffing, and connection hijacking.

a faulty software patch). There is no evidence that any financial system has ever had its financial integrity put at risk by a hacker attack. A parallel security issue may be drawn with the security of the United States's rail system: unprotected rural train tracks are easy to sabotage, and with grimmer results than virtually any network failure, but until the Arizona train crash in 1995, such sabotage had not occurred in fifty years.

A system that is easy to abuse in one way may be difficult to abuse in another. In the U.S. phone system, it is not the thousands of switches that must be guarded but the few hundred signal transfer point (STP) computers. Phone phreaks attack by getting into and altering the many databases that indicate the status of calls and phone numbers. Presumably, with enough alterations, area telephone service could be terminated, but only as long as the databases remain altered. Planting a bug in the computer's operating system is harder. Even though STP computers are interconnected through Internet protocols, serious study suggests the difficulty of one STP computer infecting another.

Can a nation's stock market be destabilized by scrambling the trading records of the prior day (as in Tom Clancy's novel *Debt of Honor*[32])? Possibly, but it is easy to forget how many separately managed computers record most stock transfers (e.g., the exchange's, each client's, their brokers, the company itself, etc.). Archiving every transaction to an occasionally read archival medium (CD-ROM or even printouts) could foil most after-the-fact corruption, detect consistent in-the-process faults, and perhaps reveal deliberately intermittent error.

Can an individual's assets be stripped by erasing a bank account? A bank account is essentially an obligation by the bank to repay the depositor. That obligation persists even when the bank's record of an account cannot be found.

[32]N.Y.: G.P. Putnam, 1994.

Finally, the reliability of a system involves factors other than its security holes: the system's ability to detect its own corruption, the existence of backup data files and capabilities, its overall robustness (including redundancy in routing), and its ability to restore its own integrity and raise its own security level on short notice.

Yet, in spite of all the measures sketched here, and measured against plausible rather than mythical dangers to systems, the truth is that computer security remains too weak in too many places to withstand systematic attack. Systems were thought safe because really brilliant hackers were scarce. By 1995, easy-to-use tools came to circulate on informal public networks for hackers to find and use.

Information Attacks Offer Few Obvious Strategic Gains

Although important computer systems can be secured against hacker attacks at reasonable cost, that does not mean that they will be secured. Increasingly common and sophisticated attempts may be the best guarantor of the security of national computer systems. If the absence of important incidents lulls systems administrators into inattention, entrée is created for some group to launch a broad, simultaneous, disruptive attack across a variety of critical systems. The barn door closes, but the horse is gone. For this reason, a sequence of pinpricks or even a steady increase of attacks is the wrong strategy: it creates its own inoculation. Strategic effectiveness requires attacking an infrastructure in force and all at once.[33]

---

[33]Fortunately, the fog of war affects hackers as well. An all-points assault has to work almost everywhere at once; second chances may not arise. Yet, any attack so complicated is difficult to test; an attacker is forced to bet everything on one shot. True, some systems do experience nonlinear failure from relative small outages (e.g., the electric power grid in the western states); yet finding and exploiting potential cascades before they are found by systems administrators is no mean trick.

A key distinction is between a purposeless attack and a purposeful one. Japan's attack on Pearl Harbor was successful (at least in the short run) not because so many ships were sunk and sailors killed or wounded but because the United States had been immobilized while Japan conquered large chunks of Southeast Asia and the Pacific. An attack on the NII that left an opening for strategic mischief would be far more damaging than one that merely caused damage. A strategic motive for a digital Pearl Harbor could be to dissuade the United States from military operations (perhaps against the attacking country) or to hinder their execution by disrupting mobilization, deployment, or command and control.

How much damage could a digital Pearl Harbor cause? Suppose hackers shut down all phone service (and, say, all credit card purchases) nationwide. That would certainly prove disruptive and costly, but as long as recovery times are measured in hours or even days, such an attack would be less costly than such natural events[34] as a hurricane, snowstorm, flood, or earthquake—events that have yet to bring the country to its knees[35]. How much would the public need to be discomfited before demanding that the United States disengage from the part of the world the attacker cared about? More plausibly, the United States might desist before opponents whose neighborhoods were judged less worthwhile in face of difficulty of protecting them. The United States is less likely to withdraw before an opponent whose power to strike the U.S. economic

[34]By shutting down the northeast for half a week, the January 1996 snowstorm cost the economy $10-15 billion. Hurricane Andrew (1992) cost roughly $25 billion. Damage from the 1994 earthquake in Northridge, California, cost roughly $10 billion.

[35]Attacking the NII may have a psychological impact disproportionate to its real one. That being so, is the public better served by a Government that magnifies the possibility and the consequences of such an attack; or one which concedes the possibility but puts it in the same category with accidental and natural disasters—a fact of life whose costs one can minimize but never eliminate?

system provides a rationale for why the opponent must be put down.

Would it have been in North Vietnam's interest to hire hackers to shut down the U.S. phone system in 1966? Doing so would have contravened the message that it was fighting the United States only because the United States was in Vietnamese territory. Such an attack could have compromised support in the U.S. for the disengagement of U.S. forces. It would have also portrayed North Vietnam as an opponent capable of hurting the United States at home, which would have eroded the cautions that limited U.S. air operations against North Vietnam.

A more pertinent question than how much damage a digital Pearl Harbor might cause is how well hackers attacks can delay, deny, destroy, or disrupt military operations. An enemy in war should be expected to disrupt U.S. military systems as much as possible. But is there enough *military* gain from a concerted attack on the *civilian* infrastructure to warrant the risks?

Clearly, some military functions are vulnerable to attacks on certain portions of the NII. Today's wars require a large volume of communications from the field both to the Pentagon (say, to its Checkmate cell in the basement from the Black Hole cell in Riyadh) and to various support bases, control points, logistics depots, contractors, and consultants. A prolonged power, telephone, or e-mail cut-off would hurt broad command and control. Given the many communications media and dense links in the United States, such a disruption would need to be nearly complete, that is, widespread, coordinated, and largely successful, to have any effect whatsoever—and only if the DOD had little capacity to transfer vital traffic onto its own systems. Were U.S. commanders to exercise real-time control over operations that depended on commercial telephone lines, then a disruption would be a bigger problem, but establishing military operations with such long and vulnerable tethers is unwise for many other reasons.

The effect of an extended disruption on troop or supply mobilization is more difficult to gauge; these processes typically take weeks or months to bear fruit.[36] A disruption that lasted hours, rather than days, would probably affect outcomes imperceptibly. Many services can be restored in that time, unless some hard-to-replace physical item was damaged. If a logistics system cannot withstand minor disruption (overnight deliveries aside) with little ultimate impact, it can only have been badly engineered to begin with (disruptions near the point of use being, of course, an expected feature of warfare).

Can communications be sufficiently disrupted to retard or confound the nation's ability to respond to a crisis overseas? An enemy with precise and accurate knowledge of how decisions are made and how information is passed within the U.S. military might get inside the cycle and do real damage—but the enemy must understand the cycle very well. Even insiders can rarely count on knowing how information is routed into a decision; in an age in which hierarchical information flow is giving way to networked information flow the importance of any one predesignated route is doubtful.

The difficulty of crafting a credible linkage between an NII attack and national security is best illustrated by looking at the most widely quoted scenario, RAND's "Day After in Cyberspace."[37] More than twenty incidents befall U.S. and allied information infrastructures, many stretching the limits of plausibility (e.g., three separate incidents tied to identical logic bombs, the simultaneous blackout of the Washington area's heterogenous phone systems, rogue subcontractors affecting what in real life are triply redundant systems, market crashes

---

[36]Fast deployments tend to move assets under DOD control (and are easier to protect); slow deployments tend to require public facilities and reserve assets. The latter are harder to protect, but their time-sensitivity is less.

[37]Discussed in Roger Molander, Andrew Riddile, and Peter A. Wilson, *Strategic Information Warfare: A New Face of War* (Santa Monica, CA: Rand Corp., RAND MMR-661-OSD, 1996).

following manipulation of a hypothetical central computer). Yet, in the end, except for a potential for mass panic, facts on the field of combat (in this case, in the Persian Gulf) are scarcely affected.

The Provision of Systems Security Is Inescapably Private

Is systems security a problem whose solution should be socialized, rather than remain private? Consider a hypothetical scenario in which a refinery blows up and damages its neighborhood. The responsibility of the refiner for external damage ought reasonably to vary according to what caused the original damage[38] (even if the perpetrator and supporting nations or institutions share can be identified and subject to the force of law or state action).

- What if the refinery were damaged because it was shelled by an enemy military? In this case, the refiner's responsibility should be minimal. Rather than design refineries to withstand wartime attacks, it is far more cost-effective to socialize the problem of such incidents by providing a common national defense.

- What if the explosion were set off by a sniper's hit on a refinery tower? The problem of preventing crime is partially socialized through public law enforcement. Yet a refiner should make reasonable provision, so that a single-point failure would not create an uncontrollable cascade of disaster.

- Positing a random pistol wielder as attacker, rather a sniper, would widen the responsibilities of the refiner. Owners of dangerous equipment should be expected to take

[38]In practice, insurance may pay, but insurance rates would come to reflect insurers' judgements about their clients' information security programs. The net effect would be the same.

reasonable precautions (e.g., perimeter fencing, security guards) to protect the public from the acts of an occasional nut.

- Finally, what if a hacker off-site were to access the refiner's system and command a valve to stay open, causing the explosion? Because a refiner should know everything about its information systems (whereas the government may know absolutely nothing about them), the refiner has under its control every tool it needs to protect its internal systems from outsiders and ensure that software-generated events (including bugs) cannot cause havoc.

Most of the NII is in private hands; if its owners bear the total costs of system failure, they have all the incentives they need to protect themselves. But public consequences would follow the disruption of certain systems: phone lines, energy distribution, funds transfer, and safety. If the threat is great enough, then they have to be secure—even at the cost of yanking the control systems off publicly accessible networks. Often, less costly remedies (e.g., more secure operating systems) suffice. Even primitive solutions are cheap compared with other steps the United States takes to protect itself (e.g., nuclear deterrence). That said, the number of critical sectors is growing. Credit-card validation is becoming as critical as funds transfer to the hour-to-hour operation of the economy. Automated hospital systems are evolving toward mission-critical safety systems.

Should there be a central federal policymaker to guard the NII? If so, who? The DOD has both the resources and national security mission, but its expertise is concentrated in the very agency fighting the spread of one of the most potent tools of security, encryption.[39] The military's approach—avoiding new

[39]Technically, the NSA does not oversee the use of encryption in the United States, and the export of moderately hard (56-bit) encryption will be permissible if provisions are made for recovering the key pursuant to a

systems that fail to meet military specifications—is costly when applied to technology with short life cycles and difficult when applied outside command-and-control hierarchies. NIST, the second choice, has the talent but neither funding nor experience in telling other federal agencies what to do. Beyond the DOD and NIST, expertise thins and the mission fits poorly.

The concept of a single government commander for information defense is, anyway, a stretch. Any attempt to "war-room" an information crisis will find the commander armed with buttons attached to little outside immediate government control. Repair and prevention are largely in the hands of system owners, who manage their own systems, employ their own systems administrators, and rarely need to call on shared resources (so there is little need for central allocation). Little evidence exists of recovery or protection synergy which cuts across sectors under attack (say, power companies and funds transfer systems). The other problem with a single set of security policies is that each sector differs greatly not only in its vulnerabilities and in what an attack might do but, more important, in how government can influence its adoption of security measures (e.g., some sectors are regulated monopolies). Seeing to it that various private efforts to defend themselves are not at odds can help. A high-level coordinator could ensure that the various agencies do what they are tasked to do; lower level coordinators could work across-the-board issues (e.g., public key infrastructures). Beyond these, no czar is needed.

---

legitimate search requirement. However, the NSA's historic secrecy, its role in earlier digital signature and encryption controversies, the impact of restricting for-export software on the capabilities of domestic-only software, and the possibility that key-recovery requirements may obviate particular encryption methods all feed the public perception that the NSA is opposed to encryption. Negative public perception could complicate the DOD's encouragement of private efforts to protect systems.

Some Things Are Worth Doing

Because even the privately owned NII is, in a sense, a public resource, a role for the government may be warranted, but this role must be both circumscribed and focused. Here are ten suggestions for ways of doing so, all of which can be addressed simultaneously.

1. **Figure out how vulnerable the NII really is.**[40] What can be damaged and how easily? What can be damaged by outside attack; what is vulnerable to suborned or even malevolent insiders? For which systems might attacks be detected as they occur and by what means? What recovery mechanisms are already in place to recover operations after a disruption—or after an act of corruption? How quickly can systems be patched to make them less vulnerable? Similar questions can be asked about the military's dependence on commercial systems. How thorough would outages of the phone and Internet need to be to cripple military system operations and how would they do so: by affecting operations, cognitive support to operations, logistics (if so, only internal to the DOD or also external), mobilization? What alternative avenues exist for military communications to go through? What suffers when the 95 percent of military communications that otherwise go through public networks have to travel on the DOD-owned grid? Further questions concern the software suites on which the NII runs: for instance, does today's Unix need replacement, or are known fixes sufficient? How useful are test-and-patch kits for current systems?

2. **Fund R&D for enhanced security practices and tools and promote their dissemination through the economy.** The United States spends $100 million a year in this area of R&D (divided among the Defense Advanced Research Projects Agency [DARPA], NSA, and other agencies) to make operating systems

[40]On 15 July 1996, the President's Commission on Critical Infrastructure Protection was formed under Department of Justice leadership to do this. If researchers are diligent, skeptical, and well funded, they should make progress.

more robust and to develop cryptographic tools, assurance methodologies, tests and, last but not least, standards. The technology already exists to secure systems, but not how to make that knowledge automatic, interoperable, and easy to use. Cyberspace may need an equivalent of the Underwriters' Laboratory, capable of developing standard tests for the security of information systems.

3. **Take the protection of military systems seriously.** Any nation at war with the United States should be assumed to want to attack military systems (especially unclassified systems for logistics and mobilization) in any way it can—and hacker attacks are among the least risky ways of doing that. The government should assume that foreign intelligence operatives are, or soon will be, probing U.S. systems for vulnerabilities. The DOD should also be concerned about systems in contractors' hands and defense manufacturing facilities. The government could stipulate in contract that those who supply critical goods and services for the U.S. military (even phone companies) should have a reasonable basis for believing their systems are secure. Perhaps the DOD needs methods to validate a hardware or software vendor's source code that would also assure that the vendor's commercial secrets are safe.

4. **Concentrate on key sectors—or on the key functions of key sectors (telecommunications, energy and funds distribution, and safety systems).** Because the government cannot protect these systems, it may have to persuade (through technology assistance, or its bully pulpit) their owners to take security and backup seriously. Several organizations are useful for discussing mutual security concerns: Bellcore or the National Security Telecommunications Advisory Council for phones; the National Electric Reliability Council or the Electric Power Research Institute for power plants. Odd as it may sound in a digital age, critical systems should have ways to revert to manual or at least on-site control in emergencies.

5. **Encourage dissemination of data on threats and compilation of data on incidents** (CERT already does a good job for the Internet). Raw data may need to be sanitized so investigations are not compromised nor innocent systems maligned. Effective protection of the public-information infrastructure inevitably involves public policy, and public policy that relies on "if you knew what I knew" cannot long be viable.

6. **Seek ways to legitimize "red-teaming" of critical systems,** in part by removing certain liabilities from the unintended consequences of authorized testing. Nondestructive testing of security systems may be insufficient until the state of the art improves; that is, only hackers can ensure that a system is hacker-proof. Unfortunately, hackers are not necessarily the most trustworthy nor systematic examiners, and tests can go wrong (the Morris worm propagated more quickly than he intended, because somewhere in its program "N" got confused with "1-N"). Such systems should be tested both with and without on-site access permitted (the latter to simulate national security threats).

7. **Bolster protection of the Internet's routing infrastructure**—not because the Internet is itself important but because protecting it is relatively cheap. Critical national and international routers should be made secure, and the Domain Naming System should be spoof-proof. This is different from protecting every system on the Internet, which would be both very expensive and the proper purview of system owners.

8. **Encourage the technological development and application of digital signatures,** in part by applying them to security systems and not just to electronic commerce. Supportive policies may include research on private key infrastructures, enabling algorithms, and purchases that create a market for them.

9. **Work toward international consensus on what constitutes bad behavior on the part of a state and what appropriate responses might be.** Consensus would permit the rest of the world to adopt a common policy against states that propagate,

abet, or hide information attacks by limiting those states' access to the international phone and Internet system, much as international consensus permits trade restraints. That said, proof that a state has sponsored information attacks will be difficult to establish, and a state embargoed on suspicion may often be able to convince itself and others that it has been singled out for sanctions for other reasons.

10. **Strengthen legal regimes that assign liability to systems owners for the secondary consequences of hacker attacks.** Needless to add, the owners should be able, if at all possible, to recover costs from perpetrators.[41] At the current state of technology, however, it would have a chilling affect on networks if their owners were held responsible for attacks unwittingly perpetrated through their systems (e.g., a hacker gets into one network in order to penetrate a second one).

Things to Avoid

Perhaps more important than figuring out what to do is figuring out what not to do. Here are six things to avoid.

1. **Avoid harping on information warfare to the extent that warfare becomes the dominant metaphor used to characterize systems attacks** (much less systems failures). Porting precepts of interstate conflict to computer security can remove responsibility for self-defense from those whose systems are attacked. Protection from attack in cyberspace should not be yet one more entitlement from the government.

Once something is called war, the responsibility of the victim for the consequences of its negligence is dissipated. A phone

[41]Nothing prevents system owners from suing their software providers to recover the costs of a hacker attack that can be traced to deficiencies in the software. Shrink-wrapped software, however, is provided "as is" for good reasons; provably secure software scarcely exists.

company that may need to compensate customers for permitting hackers to harm service should not be able to claim force majeure as a victim of information warfare. Characterizing hacker attacks as acts of war creates pressure to retaliate against the hackers, real or imagined. Reasonable computer security is sufficiently affordable that the United States should never be forced to go to war to protect its information systems. Finally, promoting paranoia is poor policy, especially when systems crash often enough on their own.

2. **Limit the resources expended on looking for a threat.** Crime requires means, motives, and opportunity. Means—the cadres of hackers with some access to connectivity—can be assumed. Of all Ph.D. degrees awarded in computer security by U.S. universities, 60 percent went to citizens of Islamic or Hindu countries. The United States needs to put some effort into specific motive so as to forecast plausible patterns of attack by other nations (in order to know what security tasks are most urgent). Most of the information-collection effort should go toward opportunity—assessing U.S. vulnerabilities so that they can be fixed.

3. **Ignore the seductive appeal of automatic retribution software.** Militaries are built to hit back rather than prosecute; by this logic DOD systems could protect themselves by downloading a disabling virus into a hacker's computer system. Yet, assume, despite serious technical obstacles, that the approach works. Imagine, then, a hacker breaking into, say, CNN's computers, and from there into DOD. A DOD system instantly retaliates by dropping a virus into CNN, which, understandably, objects. Consequences ensue.

4. **Don't sacrifice security to other equities.**[42] It is difficult to see how the NII can be secure without the use of encryption,

[42]See, for instance, Computer Science and Telecommunications Board of the National Research Council's *Cryptography's Role in Securing the Information Society* (Washington, DC: National Academy of Science Press), 1996.

yet the government is loathe to encourage the proliferation of encryption (the Clipper chip and export controls). Controversy over encryption has complicated the government's credibility in securing the NII.

5. **Remember that too great an emphasis on adopting today's security practices may keep systems from taking advantages of tomorrow's innovation (e.g., for collaborative computing).** Some systems (e.g., those that control dangerous devices) must be secure regardless and, yes, many anticipated innovations have security problems that must be attended to. But the systems field is too dynamic for a straightjacket approach.

6. **Respect heterogeneity; it makes coordinated disruption harder to achieve and preserves alternative paths.** Common industry approaches to security matter less than standard protocols and software hooks to algorithms for standard security functions.

Conclusions

Who should defend cyberspace? The case for assigning cyberspace defense to the DOD arises from the ill-considered prediction that cyberspace attacks could become the predominant feature of 21st-century warfare (it is difficult enough to construct a scenario in which such attacks have little more than nuisance value).

Is cyberspace, in fact, a space that can be defended—or is it a set of largely private spaces that traffic in bytes from other largely private spaces? No good alternative exists to having system owners attend to their own protection. By contrast, having the government protect systems requires it to know details of everyone's operating systems and administrative practices—an alternative impossible to implement, even if it did not violate commonly understood boundaries between private and public

affairs. In cyberspace, forcible entry does not exist, unless mandated by misguided policy.

Essay Two

Deterring Information Attacks

A nation can defend its information infrastructure by denial, detection (with prosecution), and deterrence. Denial frustrates attacks by preventing them or limiting their effects. Detection followed by prosecution of the attacker inhibits attacks and takes the attacker out of circulation. Deterrence is the threat that a nation (or analogous entity[43]) can be punished for sponsoring such an attack.

Denial and detection are straightforward. No one argues that computer systems ought to be vulnerable to attack and penetration. Most detected cases of hacker warfare are crimes and therefore merit punishment.[44] Denial and detection may be less than satisfactory responses, however. Defenses, from one perspective, are good, but only up to a point. Although they can deny casual attacks, they fall before full-scale ones backed by the resources only a nation or some similarly financed transnational criminal organization (TCO) could provide. The ease by which

---

[43]If deterrence against a state is problematic, deterrence against a stateless organization is even more so (for instance, one must find something worth striking in return). For this reason, the discussion to follow considers only actions against sponsoring states as the clearest case for a viable deterrence policy.

[44]Some residents of cyberspace take issue with punishing someone who breaks into computer systems, reads information (and perhaps leaves a calling card), but otherwise does no harm. Most enforcement officials nevertheless favor prosecution. Consider an analogy to the problem of graffiti. Graffiti is minor vandalism; yet, as James Q. Wilson has theorized and the New York City Police Department has concluded, graffiti marks a neighborhood as one whose standards of conduct can be violated with impunity. Citizens feel unsafe and anxious, and the neighborhood is often marked for subsequent, more serious crime. Hacker attacks, even those that cause no damage, can mark cyberspace as a lawless environment.

hackers can attack a system from anywhere around the globe without leaving detectable virtual fingerprints suggests that the risk of punishment is low.[45] Hackers supported by foreign governments may be detected but later hidden (perhaps by allied TCOs) or discovered but not lie beyond extradition.

Should deterrence be part of a nation's information defense strategy? At a workshop sponsored by the Center for Advanced Concepts and Technologies,[46] more than two-thirds strongly replied "yes" to the question, "Should the United States have a declarative policy about its response to information warfare attacks?"

The term "deterrence" and its cousin "graduated response" appear to be leftovers from the Cold War, and if information warfare is regarded as an aspect of strategic warfare, they may well be. During the Cold War, the United States developed and adopted a policy of strategic nuclear deterrence, in essence, a warning to those who would attack to expect an attack in return.[47] Deterrence is commonly believed (if impossible to

---

[45]Hackers as motivated as suicide bombers may not be deterred by detection, but the balance of risk and reward felt by their sponsors may be righted by deterrence.

[46]Gary Wheatley and Richard Hayes, *Information Warfare and Deterrence* (Washington, D.C.: NDU Press, 1996), 24. The Defense Science Board (op.cit., ES-3) has also argued:

> In the information age as in the nuclear age, *deter* is the first line of defense. This deterrence must include an expression of national will as expressed in law and conduct, [and] a declaratory policy relative to consequences of an information warfare attack on the United States . . .

[47]Strategic nuclear deterrence is not the only form of deterrence. So-called tactical nuclear weapons were designed both to deny battlefield objectives and to raise the level of destruction so high as to deter battle in the first place. John Mearsheimer argued, in *Conventional Deterrence* (Ithaca: Cornell University Press, 1983), that an aggressor can be deterred by the prospect that victory, although likely, will be expensive. A nation that adheres to this theory might

prove[48]) to have worked—at any rate, the homeland of the United States was not attacked by a foreign force using either nuclear or conventional weapons. By analogy, analysts have wondered whether a strategy similar to deterrence could ward off attacks on critical U.S. information systems.

The argument here is that an explicit strategy of deterrence against attacks on the nation's information infrastructure is problematic and that little would be gained from making any such policy at all specific.

Need the United States declare that it reserves the right to strike back against an information attack? Any state that perpetrates harm to the U.S. homeland can already expect retaliation. After the bombing in Oklahoma City, an early false lead suggested a tie to radical Islamic states. In the Middle East the consensus was that the United States would retaliate in force if the lead were solidified by evidence: had Iran, for example, attacked an information system and caused casualties (e.g., an induced Federal Aviation Administration [FAA] outage, a badly set switch in a rail system), the United States would have retaliated as well. A destructive attack without casualties also could invite retaliation. Who would believe an attacker's protestation that reprisals were unwarranted because information terrorism was never official listed as an actionable incident?

The United States has never made clear its equation for how much harm from a violent incident merits how much retaliation. Sometimes the identity of the perpetrator makes a difference. The attack by the United States on Libya in 1986 would have incurred a greater risk if executed against a nation equipped with nuclear weapons (China) or capable of causing considerable

---

invest resources not to increase the odds of defeating aggression but to increase the odds that the aggression would be costly.

[48]See Keith Payne, *Deterrence in the Second Nuclear Age*, (Lexington, KY: The University of Kentucky Press, 1996), especially the first four chapters, for an elucidation of this point.

mischief (North Korea). By contrast, Cold War U.S. nuclear retaliatory policy could be applied against any foe; designed for use against the Soviet Union, it could easily have been applied to a lesser aggressor.

Elements of Deterrence

Richard Hayes has outlined several prerequisites to the success of a strategy of deterrence.[49] Three concern explicit deterrence:

- The incident must be well defined.
- The identity of the perpetrator must be clear.
- The will and ability to carry out punishment must be believed (and cannot be warded off).

Two concern deterrence in kind:

- The perpetrator must have something of value at stake.
- The punishment must be controllable.[50]

Should information attacks be punished by information counter-attacks? Several factors argue yes. First, punishment in kind makes obvious what is being responded to. Second, it obviates difficult questions of moral equivalence (e.g., how many lives are equal to disruption of a credit-card validation system?). Third, restricting the response to the same channel limits the

[49]Wheatley et al., 12.

[50]Such control helps keep the punishment proportional to the incident. To mete out great punishment for a modest incident might make the punishment in and of itself seem an aggressive act; it would also remove the flexibility in responding to an adversary that sees little to be lost in moving from a modest to a major incident.

action-reaction cycle (and might keep the damage below what a conventional war, much less a nuclear war, could cause). If there were an information-warfare agency to handle retaliation (as in a spy-for-spy exchange, or the expulsion of someone else's diplomat in retaliation for expulsion of one's own), that might keep more powerful and dangerous institutions out of the game. Yet hacking computers to punish computer hacking would erode any moral argument the United States might make about the evils of hacking[51]—even if it did satisfy the desire to render "a taste of your own medicine."

The two factors against retaliation in kind are asymmetry and controllability. If a nation that sponsored an attack on the U.S. infrastructure itself lacked a reliable infrastructure to attack, it could not be substantially harmed in kind and therefore would not be deterred by equal and opposite threat. North Korea, for example, does not have a stock market to take down; phone service in many Islamic terror-sponsoring states is already hit-or-miss. Controllability—the ability not just to achieve effects but to predict their scope—is difficult. To predict what an attack on someone's information system will do requires a good intelligence about how to get in it, what to do inside, and what secondary effects might result. The more complex systems become, the harder predicting secondary effects becomes—not only effects inside the system but also outside it or even outside the country. Retaliation may produce nothing, may produce a nothing that can be made to look like something, may produce something, may produce everything, or may affect third parties, including neutrals, friends, or U.S. interests. The NII, after all, is growing increasingly globalized.[52] Without the ability to

[51]As differentiated from the legal argument that in certain circumstances reprisals in kind may be legitimate under commonly accepted (e.g., Hague) laws of war.

[52]Consider the relevance of the notion that a distributed system—which is what the global information infrastructure is becoming—is "one in which the failure of a computer you didn't even know existed can render your own computer unusable" (cited from Ivars Peterson, *Fatal Defects* [N.Y.: Random

control the size or nature of effects, graduated response is almost meaningless.

The difficulties involved in the three issues remaining to be discussed here—defining the incident, determining the perpetrator, and delivering retaliation—can be illustrated by eight vignettes. Note that retaliation against physical terrorism is a cleaner concept to apply (at least based on the first two criteria[53]) than retaliation against physical terrorism; yet it has been less than clearly successful as a policy.

Defining the Incident

What criteria should differentiate an actionable information warfare attack from one that is ignored? Nuclear events (even the smallest ones) are obvious (and rare); any hostile nuclear event can be declared as actionable. Hacker attacks—information warfare in microcosm—are numerous and for the most part trivial. There may a million break-ins on the Internet every year (see page **24**). Most are home-grown although some originate overseas—a fraction of which may be state-sponsored. Most of the million are pranks and do no damage. Even if damage is done, usually it is scarcely more than an annoyance. And even if either are grounds for individual punishment, it does not necessarily follow that they are sufficiently grave grounds for international retaliation. To retaliate against every break-in (even every state-sponsored break-in) would tax the principle of

House, 1995], 121).

[53]Physical terrorism lends itself to a simple threshold: did people die (imagine terrorist incidents that would cause great damage without human casualties)? Physical terrorism also seems to be easier to link to specific perpetrators because it leaves physical evidence.

proportionality. Defining an actionable incident means determining how much harm is enough.[54]

Loss of life might be one threshold—clearly, a hacker attack on a railroad switch that caused a fatal collision would be actionable. Yet fatalities are often only indirect results of the intended damage.

Should economic loss beyond a certain threshold (e.g., stock trades muddled) trigger retaliation? A threshold may be arbitrary, and no measure of the effect of an incident may be exact. What is the cost of preventing credit card purchases for a day? If forced to use other means of payment, some customers might use cash, others might come back another day, and still others might never make the intended purchase. Which result best measures the loss to the economy? The sum of all salaries of people not working? Or of those not working productively? How would one measure the loss of corrupted data? Would it be the time required to restore the integrity of the data, or the damage to the integrity of the system corrupted? Two vignettes illustrate some of the potential problems involved.

Vignette 1. What types of information warfare are actionable? An U.S. company bids against an Asian company to supply a telephone system to a third party. A member of the Asian country's intelligence service hacks into the computer of the U.S. company, determines the amount of the U.S. bid, tells its native company which undercuts the bid, takes the contract, and costs the United States thousands of potential jobs. Is this an actionable instance of information warfare—and, if so, in what domain (e.g., is it spy-versus-spy)? When French intelligence officials were suspected of spying on U.S. firms, the United States retaliated by using its agents to acquire information about

[54]What about alternative criteria—the presence of a hostile rationale, or the attack's systematic nature? Rationales are often unknown even to historians with access to all the documents. Systematic is almost as hard to define; mere breadth of attack is inadequate.

French firms (and got caught doing so).[55] During recent trade talks with Japan on automobiles, it was revealed that U.S. signals intelligence found valuable information on the Japanese negotiation strategy.[56] Was this information warfare? Had the tables been turned, how would the United States measure damage done to its interests in order to determine whether a certain threshold that could trigger retaliation had been crossed?

Vignette 2: Can damage be measured? The control centers of the FAA suffer from serious service outages that cause increasing flight disruptions and thus economic loss. At some point, someone checks the integrity of the FAA computer system and finds signs of hacker intrusion. The hackers are identified unambiguously and so—as is rarely possible—is the time of first penetration. Even after the operating software is cleaned up, considerable controversy surrounds any attempt to determine what damage, if any, was caused by the intrusion. If the 1990s are any indication, the FAA's current system is susceptible to increasing outages. Until an outage is linked to specific alterations in the system's code, the only way to gauge the independent effect of the attack on system uptime is to use statistics. Statistical methods can produce a range of conclusions that vary with the model used to estimate downtime in the absence of attack. If the outage did not cause an accident, but might have, would creation of a potentially life-threatening hazard be grounds for retaliation?

[55]See Craig Whitney, "Five Americans Called Spies by France, Asked to Leave," *New York Times*, **CXLIV**, 49981 (23 February 1995), A12.

[56]Paul Blustein, Mary Jordan, "U.S. Eavesdropped on Talks, Sources Say," *Washington Post*, **118**, 316 (17 October 1995), B1.

Determining the Perpetrator

If an information attack were distinguished from background noise, the perpetrator caught, and a obvious chain of evidence pointing to command by or, at least assistance to a foreign government, then something actionable would have occurred. But how often can an attack be traced unambiguously? Perpetrators rarely leave anything as identifiable as fingerprints. Criminals often have habits that increase the chance of their being caught—they brag, they return to the scene of the crime, they inflexibly adopt a particular method, they do not clean up their signatures—but these are not hallmarks of professional operators. Because cold, professional hacking incidents are rare (or known ones are), the chance of detecting a carefully laid plan is unknowable. Even were the perpetrators caught, tracing them to a government is hardly guaranteed: hackers neither wear uniforms nor require enormous resources or instruments hard to find outside government hands (e.g., a tank).[57]

Vignette 3: Can the United States reliably tag an obvious foe as perpetrator? Jordan comes under military pressure from Iraq, and the United States ponders intervention. Suddenly, a series of mysterious, hacker-caused blackouts plague major U.S. cities. No perpetrator is identified, but both Hamas and Hezbollah take credit for the blackouts. It seems clear that the attacks were motivated by Iraq, as a warning to the United States not to become involved on Jordan's side. Or *was* it Iraq? Iran, to whom the United States is still the "Great Satan," might have a double motive—to hurt the United States and draw it into conflict with its own rival, Iraq. Jordan would want the United States to take the crisis seriously and intervene on its side. Israel could want the United States to support Jordan (e.g., to see a greater U.S. presence over the horizon). Adding a wild card, North Korea, having just engineered a peace offensive, could have reason to

[57]The requirement that a nation's warriors identify themselves as such (e.g., by uniforms or other official gear) reflects laws of war that entitle captured warriors to be treated as prisoners of war rather than as criminals or spies.

create incidents that make it look benign in contrast to those the U.S. government looks likely to blame. Or maybe Hamas or Hezbollah were telling the truth after all. By analogy, after Pan Am Flight 103 exploded over Lockerbie, Scotland, in 1989, Libya, Syria, and Iran were all suspected of being responsible, until Libya's refusal to extradite suspects focussed attention on its possible role. The United States lacks the luxury of a single foe assumed to be lurking behind every information warfare attack.

Vignette 4: How reliably can state sponsorship be determined? As anti-Western sentiment increases in Moscow and Russia seeks to define a foreign policy independent from the West, the U.S. telephone system is hit by disruptive outages. Hackers are caught, who prove to be recent immigrants from Russia connected to the Mafiya, in turn, connected to the government in Moscow.[58] Should the government in Russia be held accountable? Many governments have ties to transnational criminal organizations. To some extent this reflects the corruption of government by crime, but governments could also use criminal organizations in lieu of their own official organs[59]. If a government could choose between perpetrating an attack through its own organs and contracting it out, most would take the latter option quite seriously.[60] A contractors's reliability might be questionable, but contractors often have effective ways to keep their own employees in line.

---

[58]Compare the Mafiya-connected hackers in Vignette 4 to the "students" in Teheran who held the U.S. embassy hostage in 1979-81.

[59]Consider, for instance, the CIA's alleged use of the Mafia to kill Castro in the early 1960s (*Alleged Assassination Plots Involving Foreign Leaders: An Interim Report of the Select Committee to Study Governmental Operations with Respect to Intelligence Activities*, 94 Cong., 1 Sess., Report No. 94-465 [Nov. 20, 1975], 72-81, 92-97, 109.)

[60]The downside is that an organization for sale to the "red side" may also be for sale to blue. Because BDA is difficult for information warfare, blue might induce red's contractor to report back to red that blue's systems were successfully attacked when in reality little damage had occurred.

Vignette 5: Can state sponsorship be assumed even when evidence leads back to state officials? The KGB admits that the Mafiya (Vignette 4) is linked to a KGB unit. The Russian government concedes it is having difficulty reestablishing control over the unit (which says but cannot prove that it was acting on KGB orders). History is replete with examples of free-lancing intelligence tolerated because having militaries involved can complicate deniability. Russia's rationale looks plausible, so the incident is not considered actionable—but is this view accurate? If a rogue commander were to launch a nuclear weapon, a government could be held responsible for near criminal negligence in the command and control of dangerous equipment. Yet do computers used for hacking qualify as dangerous equipment? Shrugging off a rogue battalion that is invading its neighbor is more difficult, because an attack that large cannot be undertaken without government complicity. But must a serious hacking incident be that resource-intensive? A few bright hackers might suffice.

Certainty of Response

A policy of deterrence presumes incident and response are tightly linked. But is it wise policy to promise a response, regardless of the identity of the perpetrator? One would not want a retaliatory policy with no flexibility whatsoever; yet clarity is the hallmark of deterrence and sophistication tends to cause blurriness.

U.S. strategic retaliation designed during the Cold War projected a tough adversary; other potential attackers were lesser cases. In information warfare, there is no canonical foe and no lesser case. Ordinarily, retaliation serves to deter the recurrence of incidents, yet the United States is vulnerable to attacks because systems security is weak and weak systems security reflects the perception that potentially damaging attacks are rare. A sufficiently nasty attack might catch people's attention and promote security. A second attack would therefore be harder to pull off.

The next three vignettes differ only in the identity of the perpetrator as a way of exploring the nature of the response, and, as such, the certainty of a sufficiently serious response.

Vignette 6: Can retaliation be perceived as a mere excuse for military action by the United States? A hacker attack on the primary U.S. funds transfer system causes it to shut down while system faults that led to corrupted records are traced and eradicated. Before order is restored, the extended shutdown of the system leads to widespread layoffs, bankruptcies, and cascading panic. The crime is traced to agents of the Iranian government, and the United States retaliates with air strikes against Iran's nuclear infrastructure, setting back the presumed Iranian weapons program by ten years. In retaliation, Iran attempts to close the Straits of Hormuz, which the United States reopens but only after some fighting and a steep hike in oil prices at home. When the dust settles, retaliation was adjudged worthwhile because it deterred further attacks on the funds transfer system. Yet the United States has a long history of worrying about Iran's nuclear program and its potential threat to oil flows near the Straits of Hormuz. Retaliation for the attack on the funds transfer system seemed to provide a convenient pretext for doing what was otherwise useful.

Vignette 7: Are there countries against which the United States should hold their fire if even provoked? Consider that North Korea was responsible for the attack on the funds transfer attack. If sufficiently irked by U.S. retaliation, North Korea is in a position to cause considerable damage to South Korea. North Korea has artillery overlooking Seoul and forces it can and has sent southward; it probably has nuclear weapons. Is the United States willing to risk a second Korean War over an incident that might have been thwarted had a few million dollars more been invested in security? Would the United States be comfortable having to explain that calculus to anyone else? Would investing to secure the nation's critical systems be less costly and risky than planning for a retaliatory act whose consequences cannot be controlled? In the end, the United States does little (just as South

Korea did little in response to the assassination of its top officials in Rangoon, in 1983, and to the destruction of one of its airliners in 1987). Inaction was rationalized by the perception that the government of North Korea was probably declining as a threat to its neighbors and would eventually fall in due course.

Vignette 8: Are there countries whose activities ought to be ignored as short-term irritants? This time Serbians are responsible. Again, retaliation is considered and again rejected. Pressure is put on Serbia to extradite those responsible, but few in the United States expect that this request will be given high priority any more than the search for war criminals did. Officials conclude that the Serbia's enmity toward the United States will fade as the former Yugoslavia sorts itself out; there is no geostrategic rationale for risking an armed conflict that might result in a cycle of retaliation. Officials are relieved they did not institute a deterrence policy that would have required them to make good on a promise of retaliation.

Conclusions

An explicit specification requires a nation to respond to what, in the case of information attacks, could prove to be gauzy circumstances. Lack of a specification does not prevent ad hoc retaliation.

It is difficult to see how an explicitly declared deterrence policy could be made to work, but it is easier to see what the problems are in trying. A declared policy that could not be reliably instantiated would soon lack credibility. If thresholds were too low or the proof that a nation sponsored terrorism not sufficiently convincing, then retaliation would make the United States appear the aggressor. If thresholds were too high and standards of proof too strict, a policy of retaliation would prove hollow. If the United States were to retaliate against nations regardless of other political considerations, it would risk unwanted confrontation and escalation; if its responses were seen

as too expedient, retaliation would seem merely a cover for more cynical purposes.

Is it even obvious that the United States should react vigorously to information attacks? To do so might tell others that they have hit a nerve and raise the possibility that the United States could be hurt enough to be dissuaded from action in its interests or could become distracted in crisis. The opposite view, that information attacks are problems only for those too negligent to secure their own systems, would suggest that they are unlikely to alter U.S. foreign policies or its defense posture. This stance might persuade potential opponents that the results would be of no official concern to the United States—it cannot affect its policy and cannot give cheer to its enemies. Thus, it would be of no political gain to them.[61]

[61]Whether this attitude can be sustained in a hypersensitive democracy in which personal or corporate problems can turn into claims on public resources—even military resources—is a different question.

Essay Three

Indistinguishable from Magic

Information warfare strategies tend to split into those dealing with attacks on or by the use of electronic devices (as in intelligence-based warfare, electronic warfare, or hacker warfare) and those dealing with psychological warfare—bytes and memes,[62] as it were. The intersection of the two is rather small[63] yet both strategies are often lumped into the same discipline, information warfare.

These strategies, however, can also be related as follows: because ascertaining the potential of computer warfare is difficult, its psychological impact may be disproportionate to its tangible impact. The power of computers in general, and of information warfare in particular, is not well understood by the public or most military or national leaders. For this reason computer-based information warfare can play a huge role in psychological warfare; conversely, powerful techniques may lack psychological impact.

The truly skilled can exploit this dissonance between the perception and the reality of computer-based information warfare to make themselves seem more fearsome then they are and thereby expand their deterrence capabilities—that is, until their bluff is called. Others may invent an enemy whose information warfare tricks are so insidious they deter themselves.

---

[62]A term invented by Richard Dawkins (by analogy with "gene") to suggest that memes are ideas that parasitize people into propagating them much as viruses do.

[63]The most obvious connection is that propaganda spreads more slowly through a population whose information infrastructure has been crippled or destroyed.

Bosnia, Strategic Defense, and the NII

Three vignettes illuminate the penumbra of believability surrounding the core of potential.

Vignette 1, Bosnia: In 1995, in Dayton, Ohio, during the negotiations for peace in Bosnia, the United States and Serbia differed over the width of the corridor linking Moslem-controlled Gorazde (at that point, surrounded by Serbian forces) and Moslem-controlled parts of Sarajevo. The United States wanted a width of five miles, while the Serbians insisted on two miles[64]. To prove their point, U.S. negotiators put their Serbian counterparts in front of a computer using PowerScene software that simulated pilots flying through a three-dimensional image of an area. The image made plain that from surrounding hills Serbian forces could dominate a narrow valley corridor. The Serbians acceded. The software was kept running so the Serbians could see exactly what the U.S. side saw. As the software "flew" over Bosnia, the Serbian vice-chancellor realized that U.S. forces could virtually see areas where he had grown up, visited relatives, attended school or played hookey. Deliberately or not, the U.S. negotiators demonstrated that, in Mafia-speak made famous by American films, "We know where you live." Serbian observers were visibly shaken, and this demonstration may help explain why, fears to the contrary, in 1995-96, the first year they were in Bosnia, NATO peacekeeping forces were generally unmolested.

Vignette 2, Strategic Defense: In the early 1980s, many in the United States justified the construction of the B-1 bomber by citing the Soviet Union's vulnerability to air attack. So fearful were they of air invasion that they would inevitably spend more on air defense than the United States would spend on the B-1; they would be pushed that much closer to insolvency. The effect of President Reagan's announcement, on 23 March 1983, that a

[64]See Ethan Watters, "Virtual War and Peace," in *Wired*, **4.03**, 49.

strategic defense was not only possible but also imperative, on the leadership of the Soviet Union was supposedly more impressive. Richard Perle, among others, argued that Soviet Union abandoned its Cold War stance when it perceived that its strategic rocket forces would be rendered obsolete. But, would the Strategic Defense Initiative (SDI) really have worked? Some thought not. The United States had made progress on component technologies faster than the Soviet Union, but critics argued that getting the SDI to work required systems integration, which meant writing, testing, and deploying tens of millions of lines of software code. Many Western computer scientists, especially David Parnas,[65] thought no one could know whether such complex software contained flaws undetected until tested in battle. Yet, the Soviets supposedly behaved as if the system would work.

Those vignettes indicate that information warfare capabilities, broadly defined, can cast a spell over potential opponents, but the spell can work also on its proponents.

Vignette 3: As noted in Essay One, by 1996 concern for the NII's integrity, trustworthiness, and availability was high. The NII is inadequately protected, but debate centers on whether even conscientiously protected systems are safe. Although every known hole should have its plug, naysayers maintain that given the complexity of modern systems software no one could know that all holes have been found. Between the ways security can be outwitted—from imitating authorized users, to overloading buffers and delivering errant bits to a program, to sending viruses that open doors from the inside—and the almost constant invention of new methods of attack, the difficulty of ascertaining that any sufficiently complex system is safe is daunting. If no system is perfectly secure, then any sizeable effort to break in may succeed—that is, the complexity of the systems means a

[65]See David Parnas, "Software Aspects of Strategic Defense Systems," *Comm. ACM* **28**, 12 (December 1985), 1326-1335.

determined enemy will get in.[66] Self-deterrence comes from ineradicable systemic ignorance.

Information technology also reduces any nation's ability to understand the capabilities of another nation's weapons systems, even conventional ones. Actual testing of weapons allows humans or sensors to see them in practice and to gauge how well they work. With increasing sensitivity to field hazards and decreasing costs of information technology, weapons are now often tested through simulation, leaving few opportunities for those not directly involved to measure performance or gauge effectiveness. In strategic terms, a nation can suddenly become a force of surprising, even decisive, capability. According to Eliot Cohen:

> As platforms become less important and the quality of munitions, and above all, the ability to handle information becomes more so, analysts will find it ever more difficult to assess the military balance of opposing sides. If Admiral Owens (former Vice Chairman of the Joint Chiefs of Staff) is right, the revolution in military affairs may bring a kind of tactical clarity to the battlefield, but at the price of strategic obscurity.[67]

Assessing Information Warfare Capabilities

If the capabilities of specific instruments of war are harder to measure, the outcomes of potential conflict itself are harder to forecast. One may not know, for instance, which side in an

---

[66]Computer and network scientists worry about whether stringing together enough separate systems may give rise to behaviors neither predictable nor understandable simply on the basis of knowing each piece. Emergent behavior (a term from complexity theory) suggests that the DOD's system of systems, however good it looks in theory, could go haywire even without attack, a possibility that deserves examination.

[67]Eliot A. Cohen, "A Revolution in Warfare," *Foreign Affairs* 75, 2 (March-April 1996), 53.

evenly matched battle will win, but it is rare that one force defeats another more than three times its size. Even if the result of a nuclear confrontation is unpredictable, the effects of a nuclear blast can be calculated with fair confidence. With information warfare, highly asymmetric results are possible.[68]

Information warfare opens a gap between what one appears able to do and what indeed one can do. If appearance deters, actuality may be irrelevant. The counterargument—that deterrence depends on accurate mutual assessment leading to predictions of outcomes which would cause all but the clear winner to desist—is poorly supported by history. World War I broke out even though most major combatants had a good sense of the size and characteristics of the forces that opposed them. Insofar as each side understood each other's war plan each recognized:

> The Plan's limits were fixed by the railways [necessary to carry troops and supplies to the front lines].... Since each side could estimate the carrying power of the other's railways, strategy became a fairly exact guessing game.[69]

The Germans estimated that their own attacking forces had a decisive but not overwhelming edge against the French and gambled that it was enough to insure victory. During the Cold War, exact estimates of opposing strength were probably irrelevant. The Soviets and the United States both judged the possibility of nuclear exchange catastrophic and were deterred.

The need to deter others leads nations to want to appear strong, regardless of their capabilities. The royal court of Byzantium repeatedly paraded troops around its capital in full sight of diplomats of other nations, the troops changing uniforms after

---

[68]Consider how Israelis used electronic warfare to achieve an 82 to 0 exchange with Syrian jets in their 1982 confrontation in the Bekaa valley of Lebanon.

[69]Theodore Ropp, *War in the Modern World* (Durham: Duke University Press, 1959), 183.

each cycle and then going out again in order to appear more numerous, better armed, and more powerful than they actually were. Soviet military parades in Red Square were similarly intended to reassure and intimidate without revealing actual quality or amounts of equipment.[70]

Understanding the enemy's information warfare capabilities is almost a contradiction in terms—to understand a capability is to take a large step toward being able to nullify it. To know the holes in one's system through which an enemy will attempt passage is to know what needs to be plugged. To know how well an opponent can hide from one's sensors suggests what features of one's sensors are easiest to spoof or evade—and thus what needs most work. If an opponent knew how well one could counter it, that could be only because it sensed how one could do so, which creates a basis for counter-countermeasures, and so on.

To make matters worse, any measure of a nation's capability for information warfare may be meaningless unless measured against a specific opponent. One nation may be able to disrupt another's information infrastructure if that infrastructure is centralized and protected by firewalls, but not if it is dispersed and protected by redundancy. Another nation may be stymied by firewalls but operate more easily against networks. Some nations may hide their forces by stealthy technology; others may use cover, concealment, and deception. The United States, having pioneered stealth, may understand its flaws but flail helplessly before operational deception; another nation may be frustrated by stealth but know how to counter deception. Information warfare capabilities do not exist in isolation.

---

[70]In the mid-1950's, the Soviet Union used this trick to induce the CIA to overestimate how many Bison bombers it had produced (Dino A. Brugiani, *Eyeball to Eyeball: The Inside Story of the Cuban Missile Crisis*, [N.Y.: Random House, 1991], 9).

Practical Considerations

As a practical matter, how much of its ability to conduct information warfare should the United States show—in particular, its ability to see distant lands and take down the infrastructures there?

The deterrence value of information warfare echoes long-standing debates over submarines and battleships. Submarine advocates argue that this weapon is more cost-effective for critical missions. Battleship advocates counter that navies have traditionally been built to demonstrate presence. A grey hulking monster offshore was more likely to strike fear into those onshore than would a submarine lurking silent and deep. Here warfighting capability and deterrent effect could differ.

Is information warfare a battleship or submarine? If a submarine, then substituting invisible force for a visibly fearsome one lacks persuasiveness, regardless of what it may ultimately contribute to warfighting. Information dominance may need to be made visible. If, as in Arthur Clarke's frequently cited Third Law, "any sufficiently advanced technology is indistinguishable from magic," then the esoteric nature of information warfare may induce fear out of proportion to reality. Voodoo is proof of the power of magic to paralyze the human will. Information warfare may thus be the battleship.

As a corollary, the likelihood that a successful act of information warfare will shock and awe the victim is likely to depend on who they blame. If taking down an enemy's infrastructure endows the perpetrator with proof of enormous powers then such attacks may have great psychological effects. A commander who blames the incompetence of his own systems administrators for letting it happen is more likely to feel frustrated rather than terrified.

As the Bosnia vignette suggests, the United States's ability to see everything on the battlefield may prompt others to give its military a wide berth. To feed that fear, the United States

government may be tempted to show others just enough of what it can see to illustrate the point: monitoring a small area in great detail over time or demonstrating a repeated ability to catch violators and criminals in the act. Perhaps selectivity may not prove convincing to an opponent that knows that pictures of laser-guided bombs going down airshafts result from culling pictures of many misses. Intelligence capabilities are highly classified, because they reveal a nation's sources and methods. By exclusion, knowing such methods would suggest what a nation *cannot* see. At very least, therefore, the United States must imply it can see more than it lets on.

But the United States may not completely control its own smoke and mirrors because its foes will want to test its magic. The nuclear magic held, in part because no one wanted to test the capability of anyone's strategic systems. Yet, information warfare is usable in a way nuclear warfare is not—if the United States claims capabilities and does not use them, could not opponents (and interested bystanders) conclude that these capabilities have been exaggerated? On the one hand, the United States might abjure taking down another nation's information infrastructure, because that might cause unjustifiable damage to civilians without a compensating military rationale. On the other hand, how long could the United States claim information dominance if systems existed that it could not take down or forces it could not find? If an opponent can demonstrate its ability to continue military communications, preserve its information systems (primitive though these might be), or hide successfully, what of American magic?

This argument assumes a U.S. interest in making other international actors think it is more powerful than it is. With the United States so far ahead of every other nation in warmaking capability, it may wish to seem *less* scary. It may share knowledge about its strategic intentions to assure others of its interest in promoting a more transparent world or accede to a global information regime in which the United States and others yield information hitherto considered state secrets. If strategic as

well as tactical transparency are important, can or should the United States lead in putting all (or most) of its information warfare cards on the table, in an attempt to establish global rules for information in warfare?

Addressing the deterrent value of information warfare capabilities has only begun, but even the little that has emerged suggests that information warfare is not simply conventional warfare with bytes and memes replacing bullets and bombs. The magnitude of the gap between reality and magic is especially strong even if it is not clear which of the two is more powerful. Information about information warfare is itself a component of information warfare. If and when information warfare comes into its own, its effects on the calculus of capability and deterrence have to be rethought, not simply ported from familiar but misleading terrain.

Essay Four

The Retro Revolution

One of the many ironies of information warfare is its retro nature. On one hand, information warfare reflects the heady advances of information technology and anticipates the rich information infrastructure of the future we all will have to cope with and have already become dependent on. On the other hand, because metaphor, rather than experience, is the currency of discussion, the logic of information warfare often harkens back to the darkest days of the Cold War yielding the following three atavistic features:

- The vocabulary of strategic conflict.
- The ascendancy of intelligence operations in military affairs.
- Resistance to reform of acquisition and to joint systems.

These provide yet one more reason why the metaphors of past wars must be scrutinized so that their application not obscure rather than reveal the essence of information warfare.

The Vocabulary of Strategic Conflict

Can information warfare be used strategically? Proponents have argued that a well-placed attack on a nation's information infrastructure might, like Douhet's airplane, permit a nation to go around the other side's forces and strike directly at its infrastructure. The atomic bomb was the *reductio ad nihilum* of an earlier version of this dictum.

The appropriateness of Cold War strategic conflict as a metaphor can be judged by examining efforts to apply it. The concepts of

deterrence and graduated response were dissected in the last essay. Four other concepts can be considered: (*a*) indications and warning, (*b*) minimum essential information infrastructure (MEII), (*c*) defense conditions (DEFCONs) as applied to information warfare, and (*d*) reconstitution.

What would constitute indications and warning of strategic information attack? The United States thought it understood what would precede a Soviet tank surge into Germany (e.g., a mobilization of trucks) or a nuclear attack (e.g., the movement of top officials into prepared bunkers). But a strategic information warfare attack probably would not resemble anything previously experienced or planned for.

One key difference between an information attack and a physical attack is that the latter requires the expensive, observable maintenance or restoration of military resources to attack status. What, if anything would constitute attack status for information warriors? Would an information warfare attack be preceded by information probes? Perhaps such feints would force systems administrators to tighten security, only to have that security fall back as users weary of the effort needed to maintain it. Or would feints be avoided because they would induce permanent security measures (such as better software), making systems more impervious to attack?[71]

In information warfare there is no predetermined lead-time between ignition and detonation. Bad code might be inserted into a system years before it is needed simply because an opportunity to insert it arose unexpectedly. When needed, the code would be activated by external signals. True, bad code cannot sit around forever. Software upgrades may clean them out and the longer

[71]North Korea's invasion of South Korea was preceded by raids. By October 1973, Egypt had lulled Israel into a false sense of security: during the previous spring, Egypt staged feints that forced Israel to mobilize partially; the feints were revealed as such, leading Israel to conclude that Egypt's pre-invasion covering moves also were feints.

the code sits the greater the odds it is found or ignites early. Yet the cost of maintaining bad code (e.g., periodically checking on it) is probably low.

Determining a MEII for carefully defined defense scenarios may be a useful exercise. In the event of complete system failure, a compact minimum capability for each infrastructure may be needed to bootstrap recovery operations. Yet, in general, a list of critical nodes and links that would constitute an MEII will be undefinable *per se*,[72] unknowable (how can outsiders determine the key processes in a system and ensure that they stay the same from one year to the next?), and obsolete well into its bureaucratic approval cycle (the NII is changing rapidly and has a long way to go before it gels). The government lacks tools to protect only key nodes. It should have policies to encourage system owners to protect themselves; they, in turn, will determine what needs to be protected and how.

Having a DEFCON-like mechanism for hacker attacks makes a little sense. Organizations can respond to a rising threat of intrusion by increasing the difficulty of access or restricting who may access which capabilities and files. Without indications and warnings, knowing when to call for more stringent security measures is difficult.[73] The notion that an organization can relax most days because on some days it can tighten up is the wrong way to think about information assurance; by the time the threat is obvious, the viruses, worms, and Trojan Horses may well have been implanted. Most of the NII is in private hands; system owners would take a national declaration of an

---

[72]"Minimum" implies minimum for some purpose. What purpose would define an minimum infrastructure? conducting a nuclear war, protecting the ability to conduct two conventional wars, preserving the public's faith in its institutions?

[73]Information security may be tightened in line with rising DEFCONs, but the policy would be correct only accidentally (physical and information attacks are likely to have different timeliness) and the carryover into civilian systems would be, at best, hit or miss.

information warfare warning as just one piece of evidence among many in deciding their system policies.

The reconstitution[74] concept fails in the opposite direction. Whether few or many decades are needed to recover from a nuclear attack makes no difference to the outcome of a nuclear war likely to be decided over hours, days, or, at most, weeks and months. By contrast, the impact of many types of attack on the NII would be directly proportional to the duration of the outage, or, in the case of bad information, to the time required for data reconstitution.[75] An attack on a natural gas distribution system in the middle of winter, for example, that would cut off supplies for an hour might force people to wear sweaters at home, but workers in large offices might not notice at all. An interruption that would last for a full day might force people into buildings with other sources of heat and force offices to shut.

The Ascendancy of Intelligence Operations

In the Cold War, the United States's struggle against a closed society raised the need for intelligence and, with that, the status of intelligence agencies. In a more open world (even with an increase in "peace" operations), the need for intelligence would seem logically to shrink—open sources would mostly suffice. Yet

[74]Even the term RAND used for cyberwargaming, "Day After," was adapted from nuclear wargaming.

[75]Exceptions include an individual's loss of privacy, the public's loss of confidence in an institution, physical damage (e.g., an unanticipated power outage can freeze aluminum in its smelter pots), and permanent injury or death.

information warfare brings back the need[76]; hence, as noted, its supporters in the intelligence community.

As struggles over information—thus, intelligence—increasingly affect the conduct of conventional conflict, the mindset of intelligence is bound to pervade the warrior's mental constructs. In conventional combat, information on the performance of systems is only the beginning of strategy to counter those systems; a charging tank is terrifying even if the soldier knows its top speed, but data on the other side's information warfare systems constitute much, even most, of what is required to defeat those systems. The United States (and other nations) needs to hide the extent of its true capabilities (and vulnerabilities); and devote considerable effort to determining counterpart strengths and weaknesses.

Were knowledge about who can do what to whose information systems peripheral to the outcome of conflict, the public policy debate on defense can be conducted on the assumption that what is knowable both makes the real difference and can be understood (despite what intelligence operatives may think). Yet, the more the struggle for information dominance determines the outcome of a war, the more public debate grows increasingly uninformed and therefore immaterial. If public debate cannot inform, much less determine, how much information power is

[76]Information warfare is likely to have varying impacts on how information is classified. Since anything having to do with intelligence is more highly classified (e.g., top secret, codeword) than matters related to operations, the growing role of intelligence in operations raises security levels across the board. Similarly, because the *unclassified* portion of the defense information infrastructure—logistics, deployment—is most vulnerable to a hacker attack, if their vulnerabilities must be hidden, then systems management data for these systems may have to be classified—and with it, perhaps the systems themselves. Conversely, the greater the impact of media-based information warfare, the more frequently warriors must justify themselves to the media and thus the greater the pressure to declassify so as to reveal information that would indicate why, for instance, a target selected for destruction (e.g., the ostensible schoolhouse) was believed to be military.

enough, how can it address the relative costs and benefits of a particular level of effort? The issue of ends versus means figured prominently in public debate about U.S. involvement in Vietnam and, more recently, its defense of Kuwait. But public influence on the generation and use of military power—an effective secondary form of civilian control—is meaningless if insufficient information is public.

Intelligence is cousin to deception. As hiding and seeking assume larger roles in outcomes, each side will necessarily put more effort into testing the other's capabilities, to see what is and is not detectable. One side may feint, the other may fake (ostensibly responding to false negatives and allowing some positives to seem to move unscathed). Deception and counterdeception have always been part of war, but they were practiced mainly by the few while the majority operated tools of force. Tomorrow, deception and counterdeception could become requirements for all warriors, and many will have trouble thinking in ways such practice demands.

Beyond tactical deception lies operational deception, which exploits the other side's preconceived notions (e.g., Japan's belief that the United States would invade it from the Aleutians). As Admiral Wylie[77] has pointed out, military campaigns come in two types, cumulative and sequential. In a cumulative campaign (such as the antishipping campaign against Japan during World War II), each successful move has an independent effect, and no single tactical deception counts for much. In a sequential campaign, each successful move permits another (for example, the success of D-Day enabled every subsequent other military operation). A successful deception may remove the key stumbling block to a series of moves.

[77]Joseph C. Wylie, *Military Strategy: A General Theory of Power Control* (New Brunswick, N.J.: Rutgers University Press, 1967).

Retarding Reform of Acquisition

Despite strong opposition, since the mid-1980s two great shifts have started in how armed forces are provisioned: from military specification (MILSPEC) to commercial off-the-shelf systems and from Service-unique to systems that have to be designed for cross-Service internetworking. Both shifts threatened many fiefdoms that characterize defense acquisition.

Information warfare offers opportunities for retrogression. It presents two obstacles to the Services's use of commercial systems. First, neither commercial hardware nor software is today well protected against painstaking malice. Commercial communications equipment, for instance, is rarely hardened against jamming or otherwise made invulnerable to spoofing (although spread-spectrum technologies in digital cellular phones offer some protection). Commercial software systems, developed for low-threat environments, are poorly protected against rogue code. Commercial networks are penetrated all the time. The military, which needs to operate in contested realms cannot afford such vulnerability. Yet if dependent on today's commercial systems, they have no good choice but to insert security after the fact; the more security, the more often a proprietary solution is less expensive. Second, some in the Armed Services maintain that unless commercial hardware and software are rigorously inspected, no one can be sure they have not been tampered with.[78] Most commercial electronics originate, in whole or in large part, from Asia. What guarantee is there that someone there did not sneak a circuit onto a chip that, on being awakened, will send out a previously unseen signal to disable or corrupt the unit it sits in? Software provides numerous opportunities for planted bugs. RAND's "Day After in Cyberspace" scenario posited many incidents in which systems were made unsafe, thanks to rogue code inserted by a contract shop in Bangalore, India. Ought the DOD not accept software whose source code it has not itself rigorously inspected? Vendors

[78]The NSA manufactures computer chips at its own on-base silicon foundry.

of commercial software, for whom DOD is a minor customer, are likely to balk at this condition; defense software houses, whose products are often purchased in source code, would have fewer problems with it.

The threat of hacker warfare discourages internetworking systems across Service lines[79] (not to mention with allies much less coalition partners). A system run by a single organization can have a single point of contact ensure its integrity. But once systems are linked together, who becomes responsible? How does the Navy systems administrator, for instance, know that classified information sent from that office to the Army is treated there with the respect the Navy thinks necessary? How does the Army systems manager know that information received from the Air Force has not been tampered with on its journey? How does the Air Force know that what is coming in from a Navy system does not carry an insidious bug, worm, or Trojan horse? The world is full of trust-nobody security products that sit on interfaces of systems, but in practice, interconnection is felt to be tantamount to unsafe computing.

A Concluding Thought

Information warfare as a policy issue has yet to break the surface into public consciousness. If it does, the media[80] are prepared to argue that the threat of information warfare is completely

[79]The DOD does operate information systems that cut across Service lines: the Global Command and Control System, various CINC command systems or intelligence systems. The systems of tomorrow will probably be built from those of today, and many of these systems, particularly those tied to Service-specific warfighting communities, as well as weapons systems will probably be administered by Service detachments. Even in a truly joint world, ordinary bureaucratic mistrust among different communities—intelligence, operations—will persist.

[80]Based on the author's conversations with representatives of the New York Times, the BBC (British Broadcasting Corporation), and CNN (Cable News Network).

fabricated—that is, that it is the national security community's desperate attempt to recreate old threats it knew and loved so well. If the constructs of information warfare are taken from or used to revive earlier practices, its advocates will have only themselves to blame for being regarded as nostalgia buffs, and metaphor will have failed.

Essay Five

Postcards from the Immune System

> *Every living organism is confronted by continual intrusions from its environment. To survive, every organism has therefore had to develop defenses that render it resistant, or immune, to such assaults. These defenses range from physical barriers, such as a cell wall, to highly sophisticated systems.*[81]

The human immune system has often been explained by metaphors taken from war.[82] In recent years, defense analysts have returned the favor by looking to the immune system for suggestions on how to fight war. The rise of information warfare helps explain why. First, the defense of large networks against computer viruses and other illicitly entering material may be helped by understanding how the human immune system defends

---

[81]Eli Benjamini, Geoffrey Sunshine, Sidney Leskowitz, *Immunology: A Short Course* (N.Y.: Wiley-Liss, 1996), 19. Note that replacing "organism" with "nation" and omitting "cell" make the quotation speak precisely to defense.

[82]See, for instance, Robert G. Evans, "Health Care as a Threat to Health: Defense, Opulence, and the Social Environment," *Daedalus* **123**, 4 (Fall 1994), 21-42. As Susan Sontag argued in *AIDS and Its Metaphors* (N.Y.: Farrar, Straus, and Giroux, 1989), such explanations are not always benign:

> Military metaphors have more and more come to infuse all aspects of the description of the medical situation. Disease is seen as an invasion of alien organisms, to which the body responds by its own military operations, such as mobilizing of the immunological "defenses," and medicine is "aggressive" [9].... Military metaphors contribute to the stigmatizing of certain illnesses and, by extension, of those who are ill [11]...[so that] the effect of military imagery on thinking about sickness and health is far from inconsequential. It overmobilizes, it overdescribes, and it powerfully contributes to the excommunicating and stigmatizing of the ill [94].

itself against biological viruses.[83] Second, the ability of the immune system to distinguish between self and nonself (i.e., the pathogenic invader) may have parallels in the application of intelligence-based warfare and low-intensity combat (including counter-terrorism and peace operations). Third, complexity theory is gaining attention as a way of explaining warfare, and the immune system is often invoked as a highly functional complex and adaptive system.

If the immune system is to be exploited intelligently as a metaphor it must be understood in and of itself.[84] Its specifics matter, because they are what make the immune system work. To extract certain features from the immune system in isolation while ignoring the underlying complexities may be to draw analogies to an incomplete system that would not work.[85]

---

[83]See, for instance, *The Wall Street Journal*, 15 Jan. 1996, A1, or "Cyber Wars," *The Economist*, **338**, 7948, (13 Jan. 1996), 77-78.

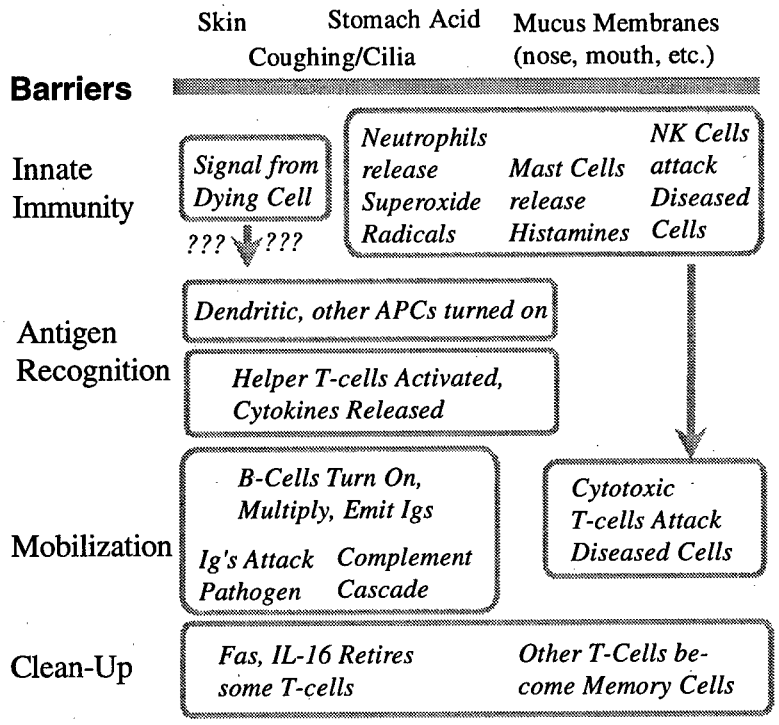
[84]Benjamini et al. provides an excellent introductory text. Also recommended are the September 1993 issue of *Scientific American* (**269**, 3), in particular: Sir Gustav Nossal, "Life, Death, and the Immune System"; Irving Weissman and Max Cooper, "How the Immune System Develops"; Charles Janeway, "How the Immune System Recognizes Invaders"; Philippa Marrack and John Kappler, "How the Immune System Recognizes the Body"; and William Paul, "Infectious Diseases and the Immune System." Subsequent articles in *Scientific American* include: Howard Johnson et al., "How Interferons Fight Disease" (**270**, 5 [May 1994], 68-75); Victor Engelhard, "How Cells Process Antigens" (**271**, 3 [August 1994], 54-61); and Martin Nowak and Andrew McMichael, "How HIV Defeats the Immune System" (**273**, 3 [August 1995], 58-65). The author also gratefully acknowledges the assistance of Dr. Amy Rosenberg (Food and Drug Administration) on this chapter.

[85]No simple sketch can adequately convey a system's complexity, and much remains to be discovered about how the immune system works. The immunologist, physician, writer, and philosopher Lewis Thomas, who died of cancer in 1995, once remarked that because the immune system is so complex, he would not know which of his cells to root for to fight his cancer (from Jimmie Holland, "Cancer's Psychological Challenges," *Scientific American* **275**, 3 [September 1996], 160).

How the Immune System Works

The human body fights a continuous invasion of pathogens from bacteria to viruses, fungi, worms, protozoa, and spirochetes. As Figure 1 illustrates, the human immune defenses entail:

Figure 1
The Immune Response



- barriers,
- innate immune defenses,
- recognition that an antigen is nonself and thus a likely pathogen (or an indicator of pathogenic activity),
- mobilization of biochemical processes to destroy the pathogen (or diseased or cancerous cells),
- returning itself to a standby state.

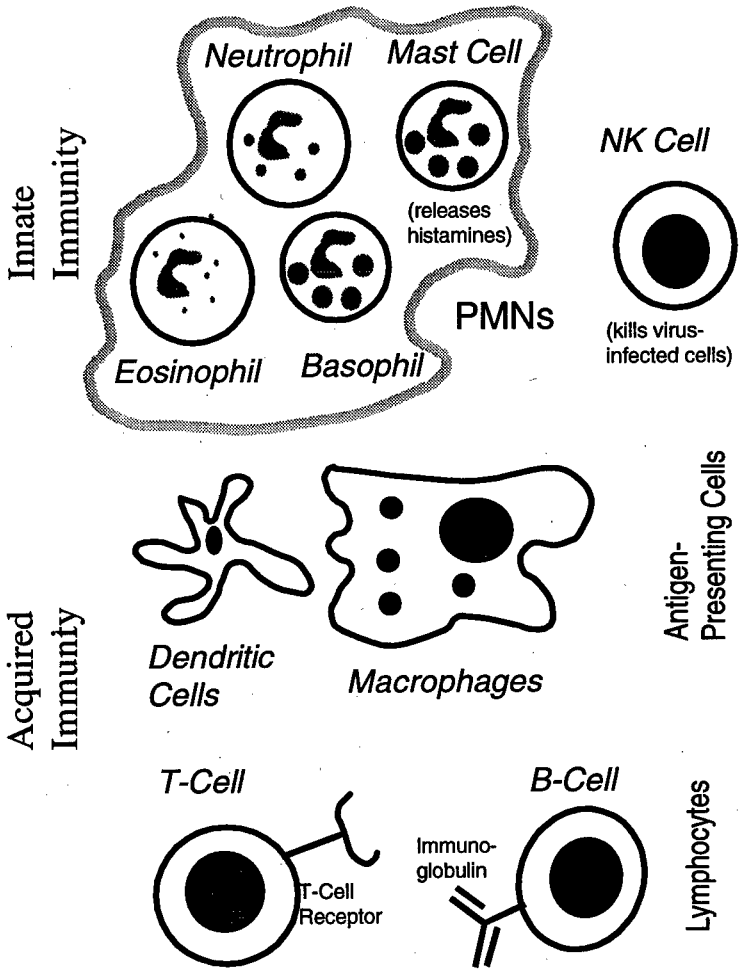
Like any good defense system, the immune system is multilayered. Skin forms the primary, but not sole, barrier to invasion. Nasal, alimentary and other passages are protected by mucus membranes, which secrete chemicals harmful to bacteria while stomach acid also is corrosive and cilia and coughing responses protect the lungs.

Because many pathogens can establish an infection despite such barriers, the immune system must be able to detect diseased cells and eliminate them to keep disease from spreading. Yet it must also be careful not to attack healthy cells or destroy its own proteins. This balancing act, which must be maintained over a lifetime, gives the human immune system its daunting complexity.

The immune system is generally discussed in terms of *innate immunity* and *acquired immunity*. Innate immunity is prompted by specific events (e.g., trauma) and directed against specific invaders that the human immune system has *evolved* to recognize. Acquired immunity works against nonself antigens which the body has *learned* to recognize. The key cells of the innate and acquired immune system are portrayed in Figure 2.

The Innate Immune System: Following a cut (or other traumas such as wounds or burns), local platelets in the blood rupture, releasing chemicals that expand the size of blood vessels and raise the local temperature. Both changes induce an influx (chemotaxis) of polymorphonuclear (PMN) cells whose hydrolytic enzymes, peroxides, and superoxide radicals are toxic to many microorganisms. PMNs (e.g., neutrophils) also clean up dead and dying cells, which otherwise would provide rich feeding grounds for bacteria.

Figure 2
Cells of the Immune System



Natural Killer (NK) cells play an early role in combating viral infections that happen to induce the appearance of glycoproteins on the surface of the affected cells. These glycoproteins attract and activate NK cells, which kill infected cells by sending them chemical agents which induce such cells to commit suicide but not release their contents—apoptosis.

The innate immune system starts work within thirty minutes to an hour after infection and works well against pathogens that elicit specific chemical reactions, but it does not otherwise distinguish between an invader and the body—that is the job of the acquired immune system, which takes longer (circa two days) to respond but is far more precise.

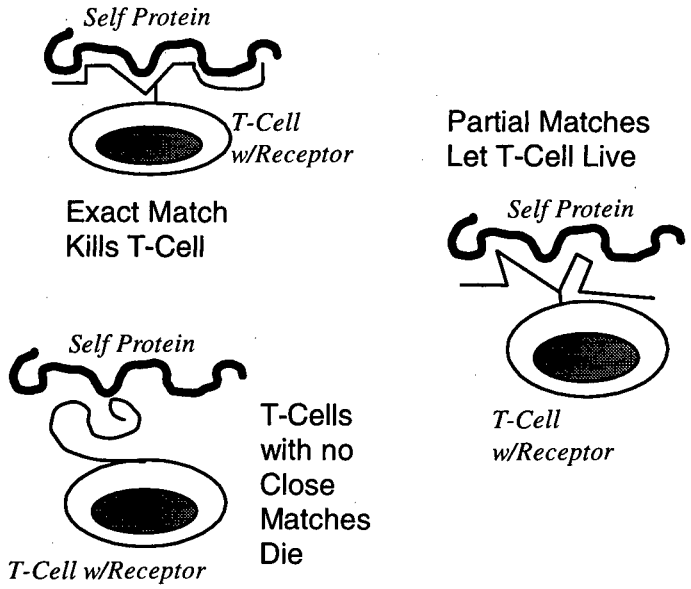
Recognizing Nonself: The key to the acquired immune system is recognizing pathogens (and related sugar groups) as different from self-proteins so as to attack only the former. Specific lymphocytes (T-cells and B-cells) are what recognize individual pathogens—more precisely, not the pathogen itself but its antigens[86] (surficial proteins or proteins that result from cellular processing) which, in turn, are recognized by their epitopes (sequences of five to seven amino acids). Recognition results from a lock-and-key match between a receptor on a T-cell or the immunoglobulin (Ig) molecule of the B-cell.

Unfortunately, there are hundreds of thousands of potential antigens in the world. The human genome is too small to code a separate receptor to recognize each antigen. Even if it could, the body would still be defenseless against something humans have never encountered. The body, it turns out, does not code a separate receptor for every potential epitope. Instead, during

[86]An antigen is any foreign material that is specifically bound by specific lymphocytes; generally speaking, it is the marker for a pathogen. Some antigens are recognized not by their own epitopes but for the enterotoxins their activity produces (e.g., a rotavirus is detected when its enterotoxin, NSP4, reacts with a T-cell). Some B-cells also recognize polysaccharides (long chains of sugar molecules).

fetal development, a basic toolkit of receptor components is reshuffled to produce up to a hundred million potential receptor combinations; then the body gets rid of those it does not want. How? In the fetal thymus, receptors constantly come in contact with the body's proteins. Lymphocytes whose receptors match the body's own proteins too well have to be discarded because they could induce an autoimmune reaction later in life[87]. Lymphocytes whose receptors fail to come close to matching the body's own proteins die by neglect probably because they would not recognize any antigen. The survivors (less than one in ten) are those that exhibit a partial match with the body's own proteins. This threefold differentiation is illustrated in Figure 3.

Figure 3
Clonal Selection of Lymphocytes



[87]By contrast, a tight match with an epitope that occurs *after* clonal selection in the thymus will energize the lymphocyte. Exactly why is poorly understood. A T-cell has a CD28 receptor which needs to be in contact with a B7 protein to be activated. Such proteins are generally absent during clonal selection, but abundant later in life. However, other mechanisms may play a larger role.

The downside of the body's producing millions of different T-cell receptors is that only one in roughly ten thousand T-cells can recognize a given antigen.[88] This is a small force arrayed against an antigen designed to replicate lustfully once it has settled in. Human survival depends on the body's ability to replicate its immune cells to compete.

Initiating an Acquired Immune Response: Almost all acquired immune responses start with an interaction involving an antigen-presenting cell (APC), an antigen, and a helper T-cell.

APCs (dendritic cells, macrophages, B-cells) tend to congregate near potential entry points (e.g., skin, lungs, stomach) or in the lymphatic system.[89] These cells can present antigen to T-cells because their surfaces can display *major histocompatibility complex*[90] (MHC) molecules and co-stimulatory proteins (e.g., the B7 protein). Dendritic cells are particularly rich in both. As Figure 4 illustrates, if there is a close match between the antigen (as held by the MHC molecule) and the T-cell receptor then the T-cell is activated.

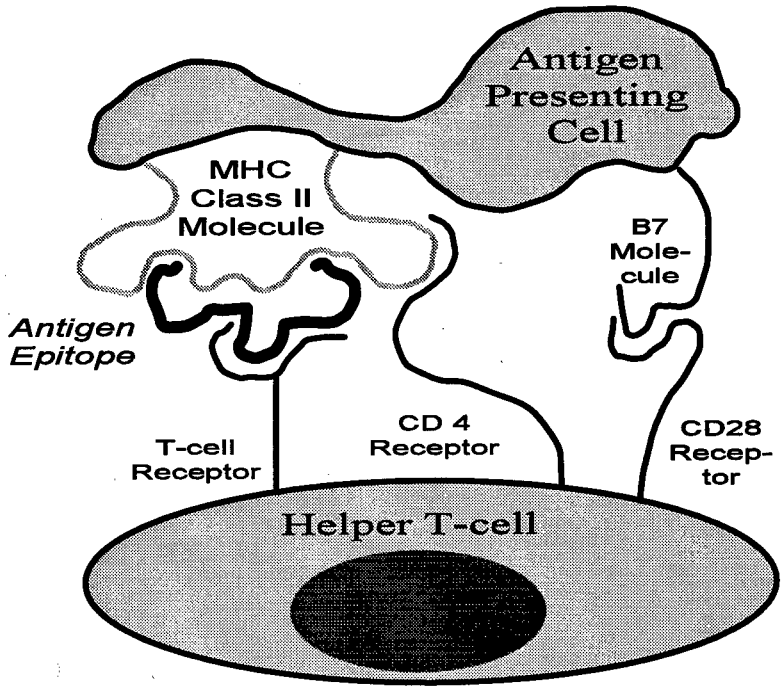
---

[88]The difference between 10,000 and a few million suggests that the average antigen can be recognized by each of a few hundred receptors. This is true probably because (*a*) antigens contain many different proteins which themselves contain many different epitopes, and (*b*) many receptors are sufficient matches for any one epitope.

[89]Research, notably by Polly Matzinger of the National Institutes of Health, suggests that to induce antigen presentation dendritic cells need to be activated by signals from other cells dying or otherwise under attack.

[90]MHC Class I molecules tend to interact with helper T-cells and their CD4 receptors. MHC Class II molecules (which have a larger groove for acquiring antigens) are more closely associated with cytotoxic T-cells and their CD8 receptors.

Figure 4
T-Cell Recognition of Antigen



MHC molecules are like pliers; they grip segments of antigens (that remain after processing by cellular mechanisms) and present them to T-cells. The shape of an MHC molecule—and the human body contains a profusion of types— determines how well it can present specific antigens to T-cells. If T-cells cannot see antigens gripped in a particular way they may not mount a vigorous immune reaction against it. Because the character of the more common pathogenic invaders changes so rapidly, human MHC proteins also have to evolve very rapidly to achieve the best grips. For that reason, populations in certain regions often have unique MHC molecules (e.g., the MHC molecules of those living near the Gambia river are specialized for ambient malaria).

When an antigen so presented achieves a correct lock-and-key match with a helper T-cell's receptor (and certain pairings occur such as those between the T-cell's CD28 receptor and a B7 protein), the helper T-cell is activated.[91] Activation (*a*) causes the helper T-cell to mature and replicate, (*b*) spit out cytokines (notably interleukins [ILs]) to activate critical effector cells (e.g., cytotoxic T-cells),[92] and (*c*) activate cognate B-cells.

Cytokines exist mostly to stimulate the immune system. Some (IL-1, IL-4, and IL-7) promote T-cell proliferation and excite B-cells. Others (IL-3 and IL-5) affect mast cells and eosinophils. Yet other chemicals attract PMNs and macrophages, which grow

---

[91]How the innate immune system reacts to the antigen determines whether T-cells mature into either Th1 or Th2 cells. Viral or bacterial stimulation of NK cells promotes Th1 cells, which emits interleukin-2 (IL-2, a T-cell growth factor) and gamma-interferon (INF-γ). The latter activates cytotoxic T-cells, NK cells, and macrophages and it stimulates the proliferation, circulation, and presentation of antigens by the Class II MHC proteins they host; this activates yet more helper T-cells. INF-γ has generic antiviral properties and helps modulate immune reactions by turning strongly stimulated B-cells on and turning weakly stimulated ones off. Mast cell and eosinophil stimulation (probably by parasites) promotes Th2 and induces emission of IL-4, IL-5, and IL-6 (all of which stimulates B-cells and immunoglobulin secretion), IL-9 (which activate mast cells), and IL-10. Path selection also affects which kind of immunoglobulin (Ig) molecule is produced when B-cells are stimulated. INF-γ (the Th1 path) favors IgG subtypes; IL-4 (the Th2 path), IgE. Once a path is selected, it tends to reinforce itself: IL-10 inhibits Th1 formation, while INF-γ inhibits Th2 formation (the Epstein-Barr virus protects itself by making a protein similar to IL-10 and thereby inhibiting the body's Th1-based defense). In Western societies, the general absence of whooping cough and tuberculosis which otherwise stimulates Th1 formation is correlated with a greater incidence of asthma which is an allergy-based condition exacerbated by IgE stimulated by Th2 formation (see William Cookson and Miriam Moffat, "Asthma—An Epidemic in the Absence of Infection?" in *Science*, **275**, 5296 [3 January 1997], 41-42).

[92]Partial matches are important in the immune response, because they cause helper T-cells to emit IL-4 which stimulates APCs. Yet, partial recognition tends put T-cells to sleep rather than stimulate their replication. See Gilbert Kersh and Paul Allen, "Essential Flexibility in the T-Cell Recognition of Antigen," *Nature* **380** (11 April 1996), 495-498.

increasingly voracious and will dissolve whatever they ingest (because activation is near an infection site, they are more likely to ingest antigens rather than random cellular material).

Lymphocytes live for a few weeks and then die. A small percentage of these cells does not develop fully and remains in circulation.[93] These undeveloped, longer lived T-cells create a reservoir of potential "memory" cells (roughly five to a hundred times more prevalent than prior to original infection). This population gives the body a head start on a counterattack the next time the antigen appears. Compared to other lymphocytes, memory cells adhere better to dendritic and other APCs and thus react to antigens more quickly. A body invaded once is therefore immune to almost all subsequent invasions[94] of a type memory cells have experienced.

The Role of the B-Cell: The helper T-cell starts the immune response, but does not itself fight the invader. It takes another lymphocyte, such as the B-cell, to release the chemicals that do this. Frequently, an antigen that has attracted a T-cell to one of its many epitopes has also bound B-cells to another of its epitopes. The cognate relationship (see Figure 5) induces replication of B-cells specific to the particular antigen and the release of their attached immunoglobulin[95] (Ig) antibodies.

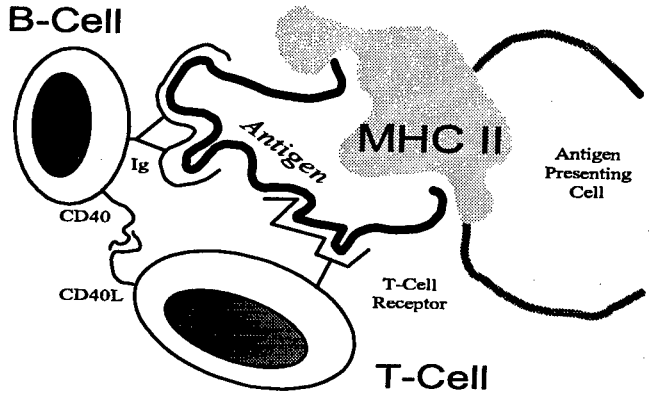
---

[93]Most memory cells (helper T-cells and B-cells: see Rafi Ahmed and David Grey, "Immunological Memory and Protective Immunity: Understanding Their Relation," *Science* **272** [5 April 1996], 54-60) are thought to need constant regeneration, a process facilitated by dendritic cells, which retain just enough antigen to induce new memory cells to replace ones that have deteriorated.

[94]This principle underlies vaccination. A dead or weakened virus is injected into the body, where its antigens stimulate an immune reaction, rather than fullblown disease, so that a subsequent encounter with a healthy live virus can be rapidly defeated. Occasionally, the second encounter overstimulates the immune system and precipitates an autoimmune response.

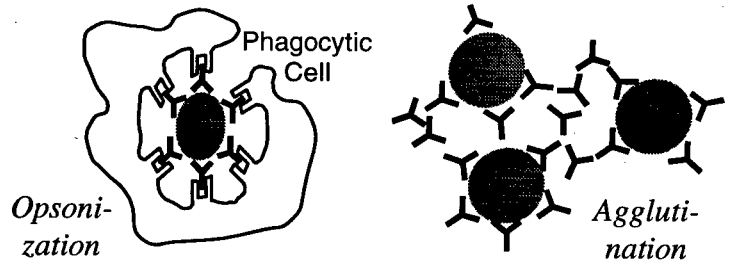
[95]The basic Ig molecule looks like one or more "Y"s connected at the stem. There are five classes of Ig molecules (with multiple subclasses). IgG is the basic workhorse; it can penetrate all body cavities. IgM (5 Y groups), the

Figure 5
Cognate Reactions Between B- and T-Cells



Ig molecules bind to antigens snugly. Opsonization is when a pathogen is coated with enough Ig molecules for a macrophage to grip it like velcro and eat it (smooth-coated bacteria are otherwise hard to grab). Ig-coated pathogens also move slower; when enough Ig (notably IgM) molecules bind enough antigens, the entire mass is agglutinized and immobile. See Figure 6.

Figure 6
How Immunoglobulin Destroys Pathogens



second most common, is the largest and first to be produced when B-cells are turned on; the presence of cytokines determines which classes the IgM is converted to. IgA (2 Y groups) is bound in mucus membranes (and thus in tears and saliva). IgE is associated with histamine response, and the functions of IgD are largely unknown. During an immune response, B-cells tend to favor those Ig classes which exhibit the highest affinity for the antigen.

Ig molecules also kill invaders by stimulating[96] the complement reaction, a complex cascade of protein activations and cleavages which yields two final proteins—one to slice a channel in the antigen and the other to widen the channel fatally. An intermediate protein in this cascade attracts neutrophils to perform clean-up. The complement reaction can also be turned on by (*a*) toxins, such as cobra venom, cell walls of gram-negative bacteria, or some yeasts or (*b*) by mannose-binding proteins emitted by the liver stimulated by IL-6. The complement reactions do not distinguish between self and nonself, but since they occur in the immediate vicinity of an antigen-Ig reaction, they are disproportionately aimed at the pathogen, rather than at the body's own tissues.

The Role of the Cytotoxic T-Cell: Cytotoxic T-cells are important defenders against viruses. A virus does not stay in circulation very long; after it invades cells it uses the cell's own chemistry for further replication of viral nucleoproteins (e.g., DNA); thus they would normally be inaccessible to the immune system. However, all cells contain MHC class I molecules, which tend to circulate internally and presents protein fragments to the cell's surface. Because cells with viral infections and some precancerous cells[97] manufacture proteins otherwise not seen in the human body, they can induce immune reactions.

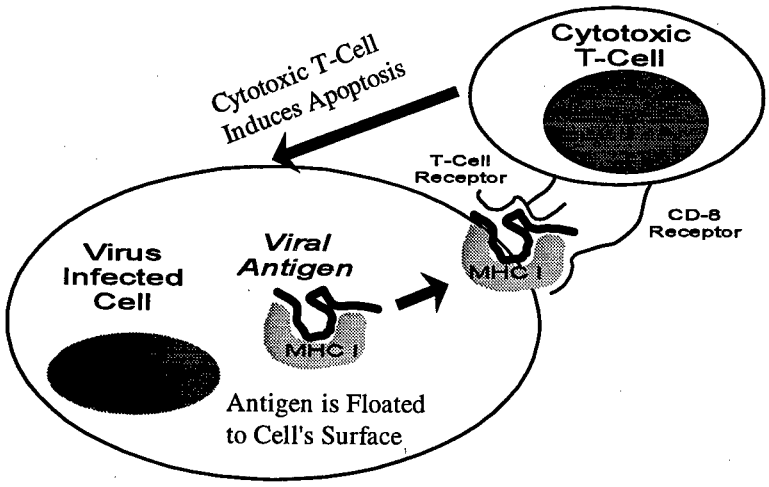
As Figure 7 illustrates, if an antigen brought by a MHC class I molecule encounters a cytotoxic T-cell with the right receptors, the T-cell will inject chemicals into infected cells, which inhibit viral replication and induce apoptosis. Cytotoxic T-cells generally have to be turned on by cytokines; the reaction of a helper T-cell in the neighborhood increases the likelihood that enough cytokines are present to stimulate the cytotoxic T-cell.

---

[96]A cascade usually begins with a reaction between one antigen and either two IgG molecules or an IgM molecule.

[97]Tumors, as opposed to antigens, tend to have less access to B7 proteins and therefore do not elicit so strong an immune response.

Figure 7
Cytotoxic T-Cells



The Immune System as an Analog Complex System

Clausewitz observed that "Everything in war is simple, but the simplest thing is difficult."[98] Similarly, distinguishing between self and nonself is unambiguous but making the distinction in practice is difficult.[99]

The immune system is not perfect. It arose through slow, uncertain, and random processes of evolution.[100] Evolved

---

[98]Carl von Clausewitz, *On War* (Princeton: Princeton University Press, 1976 [originally published in 1832]), 119.

[99]By contrast, computers can differentiate long strings of characters by a difference in one bit; yet imagine the human lifespan were the immune system to crash as often as Windows does.

[100]The passing of genes to the next generation rather than the survival of the organism that carries them is what makes traits survive evolution. Traits that ensure survival are important only insofar as they keep an organism alive long enough for it to have and rear children. After that, additional years offer little gene-passing advantage. The immune system has correspondingly selected for

systems tend to be robust and well tested, but they do not start from scratch. New structures and chemical pathways are usually variations on earlier ones; traits are not discarded but written around or over (so that a feature that no longer makes sense but is seldom harmful is likely to stay in the gene pool). Biochemical mechanisms may be efficient but hardly precise or deterministic information processors; they depend on the statistical mechanics that result from the random peregrinations of molecules. The human immune system must be sufficiently redundant to withstand most genetic errors and be able hold its own against pathogens, whose survival depends on outwitting immune systems.

It important for the human immune system to turn itself off as well as on. Anyone who has suffered from swelling (tumor), redness (rubor), heat (calor), and pain (dolor) intuitively understands why the immune system cannot be kept on all the time. As noted, complement reactions, macrophages, and PMNs tend to attack everything in their immediate vicinity. Every new year brings further evidence that autoimmune disorders are more common than earlier believed, as in lupus, multiple sclerosis, and rheumatoid arthritis. Diabetes and Alzheimer's disease may also have autoimmune components.

How does the immune system turn itself off? To start with, most of its active components have lifespans measured in weeks; thereafter, memory cells alone persist in semi-active state. The protein *fas* is used to deactivate and retire mature T-cells. Small resting B-cells may limit T-cell activation by presenting antigens to them but without the B7 molecule.[101] IL-16, secreted by

---

traits that fight diseases of childhood and early adulthood, rather than against geriatric afflictions.

[101]Once T-cells are activated, they have CTLA-4 rather than CD-28 receptors; a reaction which pairs the B7 molecule with the CTLA-4 receptor turns off the synthesis of IL-2 and induces the production of memory cells.

cytotoxic T-cells, may help get rid of infected helper T-cells.[102] Some research suggests the existence of "veto" cells capable of turning off or deleting T cells that recognize antigens on the "veto" cell surface.

Good and bad are closely interwoven in the immune system. A mast cell attached to the stem of an IgE molecule with an antigen in its grip will release tumor necrosis factor alpha, and histamines, both thought to be important in fighting protozoa. Histamines accelerate the entry of immune cells into the bloodstream and attract PMNs, which also attack invaders. Yet excess histamine production can induce allergic reactions, sometimes leading to anaphylaxis, which can be fatal. Some superantigens are believed to be able to overstimulate T-cells, that is, to produce IL-2 in amounts that can disable or kill.[103] Toxic-shock syndrome and septic-shock syndrome are related to excess cytokine production.

One source of complexity is that pathogens practice, what is in effect, information warfare. Viruses often change protein coats to become unrecognizable to activated immune cells primed for the original signature. The strategy of the AIDS virus is to attack the immune system directly, by targeting the helper T-cell as its host. Rapid mutation allows the AIDS virus to present the slowly declining population of helper T-cells with one random antigen after another, until one evokes only a weak immune response. Other viruses inhibit MHC I molecules and keep them from appearing, antigen in grip, on the surface of the cell. A pathogen can inhibit an immune system reaction by releasing a chemical that fits a key receptor in the immune process in such a way that the cell fails to turn on; if enough receptors are occupied the

---

[102]IL-16 and IL-12 (which may retard tumor growth by inhibiting the development of blood vessels) are being investigated for use in the treatment of AIDS.

[103]See Howard M. Johnson, Jeffrey K. Russell, and Carol H. Pontzer, "Superantigens in Human Disease," *Scientific American* **266**, 4 (April 1992), 92-101.

immune reaction is minimized—a form of deception. Other viruses capture and thus turn on genes that produce the proteins that inhibit certain cytokine cascades that would otherwise lead to cell activation.

Some Lessons for Warfare

The problems of immunological defense and national defense differ of course. Nevertheless, it may be instructive to speculate (within limits[104]) on lessons the former might hold for the latter *if* they were sufficiently similar.

March to the Sound of Guns. Chemotaxis is the method by which components of the innate immune system make their way to the invasion site and thereby respond within minutes and seconds. It holds the fort, so to speak, until the acquired immune system can be brought up to speed.

But Shape the Battlefield Soon Thereafter: The acquired immune system follows a day or two behind; it shapes the immune response to the type of invader encountered by insuring that specific antibodies are produced.

Mobilize Resources Rapidly: T- and B-cells are the ultimate specialists; only one in perhaps ten thousand can tackle any specific foe. Once activated, these specialists are capable of multiplying rapidly to meet the challenge. Other elements of the immune system (e.g., macrophages) need not multiply to be effective.

Exploit Redundancy: The immune system is highly differentiated and robust against a bewildering array of

[104]Several features of the immune system tend to be Stalinist: attacking everything it does not recognize, inducing infected cells to commit suicide, "retiring" warriors who have had close contact with the enemy, and eliminating all stray substances that the attacker may feed on.

pathogens. Pathogens, which attack cells and organs throughout the body, come in all shapes and sizes. Some linger in the bloodstream; others dive for a friendly cellular host at the first opportunity. A robust immune system must take care of all of them, which is one reason that immunoglobulins come in five primary (and many more secondary) flavors, each suited to a particular assignment. The various MHC molecules that grip antigens for presentation to the immune cell must sport a variety of holds to match the profusion of potential attackers and their various peptide sequences.

Learn to Act with Minimal Command and Control: The immune system is the epitome of one designed to give actors mission responsibilities to each other, but which thereafter do their job without any further top-down command. It lacks real-time command-and-control. Functionality is built into design rather than into an explicit signalling mechanism even though the body cannot anticipate where the next invasion will come from. As with Admiral Nelson's Band of Brothers who intuit their commander's general intent, architecture (and training), rather than fingertip crisis management, is decisive.

Learn to Act with Minimal Information: The immune system operates on a severe economy of inputs. An immune response does not recognize an entire antigen but rather is triggered by individual epitopes[105].

Balance Reaction and Inaction: An immune system which is on all the time is untenable. Even if it has the energy to sustain itself, constant activation risks auto-immune reactions in which too many self proteins are erroneously recognized as antigens. A

[105]Designers of the Army's All-Source Assessment System have recognized that a phenomenon (e.g., a platoon preparing for a hostile operation) need not be recognized in its entirety in order to trigger a conclusion; a sufficiently good template can be constructed by considering only a fraction of all the relevant attributes.

targeting system must maintain a balance between tolerating false negative targets (the enemy slips through) or tolerating false positive targets (friends and neutrals are hit); the same holds for winnowing trustworthy from misleading information. The immune system suggests that a gradation among alert states may be useful for information warfare, so that periods of increasing stress, triggered by suspicious events or other nonself activities, are associated with finely calibrated and multidimensional filters, validation tests, and other protections.

Learn from both Historic and Recent Experience: The innate immune system's reaction to certain proteins and the evolution of MHC cells against specific antigens is akin to learning from history. The presence of memory cells, and retaining APCs to regenerate them is akin to learning from one's own experiences. The combination is analogous to doctrine that incorporates past lessons but can accept innovation to respond to unforeseen threats.

Balance Concentration and Dispersion: The opposed principles of concentration (the need to couple specific T-cells and B-cells in a cognate reaction in the lymphatic system) and patrol or dispersion (T-cells wandering through the bloodstream) are both essential to the immune system.

Remember that Information Warfare Pervades Combat: Much of the human immune system is designed to pass and process information, rather than to apply force. APCs and MHC molecules emulate networks, presenting this or that antigen for inspection by one or another T-cell. Helper T-cells function as indications-and-warning systems. Immunoglobulins tag antigens for subsequent destruction. All (but two) of the molecules in the complement chain exist to turn another molecule on. The macrophage has two missions, to eat pathogens and to act as fine-grained molecular sensors. Killer T-cells, which come closest to resembling autonomous warriors, can be activated only by a complex series of checkpoints.

Combining the importance of information warfare with the ability to mobilize suggests that an armed forces composed of specialist corps can be effective—if methods exist to expand and amplify the core of specialists whose doctrine and capabilities are best suited to defeat a specific foe.

Implications for Information Systems

The immune system may also hold lessons for DOD when it comes time to integrate its various information systems into an overarching network-based framework. Two in particular are knowledge processing and systematic security.

Knowledge Processing: A key component of intelligence-based warfare is the ability to take a heterogenous mass of data and pound some useful conclusions from this. Tomorrow's emerging system of systems may be likened to an enormous inference engine, mobilizing chains of facts to trigger rules which create more facts (e.g., through syllogism, or induction). The immune system, in a sense, is a distributed computer for solving some very complex problems, which (in common with many other biochemical processes) works through a series of pathways in which one reaction causes the emission of chemicals (and the multiplication of the specifically triggered cell) that spur other reactions. In a system of systems, chaining can be applied to requests for information and the discovery of this information or sources for similar information. If the various agents in a system have receptors for each other, a certain level of random mixing and matching can provide a robust and rapid series of responses to events introduced into the system. In immune systems, successful reactions often spur replication of the reaction's results; perhaps problems in knowledge representation can benefit by giving disproportionate weight to rules which have worked well in a specific situation.

Systemic Security: Can studying human defenses against biology's viruses teach analysts anything about defenses against computer viruses? Most antivirus software depends on an

inventory of known viruses to prevent their attack but is helpless against newly invented ones it does not recognize. Computer researchers have looked at the human immune system to learn how to handle unknown viruses.[106] One approach sets up a dummy program for the virus to infect while a second program analyzes the infected dummy program to locate a characteristic signature of the virus and to communicate this signature throughout the network. Thus the virus can be identified and eradicated. Alternatively, native bit strings can be characterized as self proteins, which are then eliminated from the program's search repertoire.[107]

Another approach to securing complex networks is to develop security agents continually testing computers for the presence of potential antigens—like the (unproven) theory of immune surveillance, according to which immune cells detect and destroy emerging neoplasms.

At the present stage of computer science, large systems tend to be fragile. If the network immune system were, for example, to locate and destroy code that later turned out to be a functioning part of itself, the effect would be more serious than the small size of the deleted code might suggest. It is worth noting that those organs of the human body which can least afford bit errors—brains, eyes, and testicles—are kept isolated from the human immune system. The brain's immune system does not work on self/nonself distinctions; instead, diseased cells are isolated and disposed of.[108] The analog immune system has

---

[106]See Jeffrey Kephart, "A Biologically Inspired Immune System for Computers," in *Artificial Life IV*, edited by R. Brooks and P. Maes (Cambridge, Mass.: Massachusetts Institute of Technology Press, 1994).

[107]See S. Forrest, A. S. Perelson, L. Allen, and R. Cherukuri, "Self-Nonself Discrimination in a Computer," in *Proc. IEEE Symp. Res. Security and Privacy* (Los Alamitos, Cal.: IEEE Comp. Soc. Press, 1994), 202-212.

[108]Woflgang J. Streit and Carol A. Kincaid-Colton, "The Brain's Immune System," *Scientific American*, **273**, 5 (November 1995), 54-61.

built into itself various complex mechanisms to control autoimmune responses, which the digital computer systems lack.

Conclusions

Sufficient appreciation of how the immune system works ought to introduce many useful ways to examine military concepts in a new light. The immune systems works as it does because it must respond to particular problems posed in a particular environment—one that is analog, low-bandwidth, and fuzzy. Overall, it seems to be a better metaphor for guiding the use of force in the information fog and the action friction of war; it seems less suited to the digital, high-bandwidth, and mathematical world of cyberspace.

Essay Six

Point, Counterpoint, and Counter-Counterpoint

One problem with applying metaphors from conventional warfare to information warfare may be that these metaphors are growing obsolete. Classical warfare is dominated by lines, which are one dimensional. In a densely populated battlefield, "front lines" separate opposing military forces; in local engagements, the advantage goes to the side that can break or outflank the other's "line." An aggressor seeks to develop "lines of attack," which usually run orthogonally to the front; in a large battlefield, various echelons are separated by "fire-control lines."

Today's patterns of conflict may be better characterized by points, blots as counterpoints, and gated fences as counter-counterpoints. A point represents *precision warfare*; precision allows advanced militaries such as the United States's to attack and destroy only the few targets critical to an enemy's center of gravity, saving time and material as well as minimizing unnecessary damage. A blot represents *pollution warfare*, which entails inhibiting or preventing the use of media common to enemy populations, causing them various levels of pain. It is becoming the weapon of choice for those too poor, weak, or small to attack militaries directly. Modern societies can respond to blots with gated fences, which are enclosures around (with gates or other tightly monitored openings for pass-through control). This is *partition warfare*, often used to restrain and enclose (perhaps isolate, prefatory to the later destruction of) foes.

The shift from the one-dimensional line to a collection of points, blots, and gated fences is a feature of a period uniquely lacking serious tensions between major powers. Today's security

nightmares feature malevolent individuals and groups (some with tacit state support), many armed with weapons of mass destruction. Such warfare is highly asymmetric.

Conflict in the Physical Realm

How might point, blot, and gated fence be applied to physical conflict?

Precision Warfare: Until roughly the 1960s, the goal of weapons development was to achieve the most bang for the buck. Since then, refining weapons to hit their target but leave as much of everything else intact as possible has become more important. Nuclear weapons development, for instance, has featured methods to select the explosive yield in the field. The development of low-radioactivity weapons has enabled specifically military targets to be taken out with less collateral damage than its predecessors offered. Both kill fewer people, and each could reduce the risk of uncontrollable escalation driven by revenge.

For conventional weapons, the need to hit a specific point in order to kill a target has become mantra, partly because of expensive and vulnerable logistics arrangements associated with heavy ordnance use. As earlier noted, in World War II, bombers required several thousand bombs to take out a point target; in Vietnam, F-4 Phantoms still needed more than a hundred. In 1972, one Walleye bomb took out the Ganh Hoa bridge in North Vietnam, which had withstood larger raids with dumb bombs. Twenty years later, during the Gulf War, the U.S. Air Force proved it could pick and choose exactly in which building—even in which window—it wanted laser-guided bombs to land. Both Russian theorists of war and the authors of *Discriminate*

Deterrence[109] have argued that in some instances precision weapons can substitute for nuclear weapons, offering power without the obloquy.

The point destroyed and the neighborhood left intact are the dream of the modern military. The extent to which that dream can be realized is debatable. Technology makes things more visible and promotes the efficiency of their destruction, but the ability to collect and sort through intelligence to identify the correct point may be elusive.

Pollution Warfare: As precision was being developed by the United States, those left behind seem to be moving in the opposite direction, toward warfare as pollution: nuclear effects, poisoned air and water or direct environmental damage, land mines, space dust, and terrorism.

The purpose of polluting a medium—in the military sense: ground, sea, air, space, the infosphere or the biosphere—is to make its use more difficult and hazardous, even impossible. Such warfare is attractive to the weak because of its low cost and the probability that the poor and weak are less likely than the rich to care about the airlines, space, biosphere (agricultural uses aside), and the electromagnetic spectrum.

Is pollution a form of warfare in the Clausewitzian sense? *No*, insofar as a nation polluted is not a nation disarmed. *Yes*, if a nation's internal security is its center of gravity and thus a fulcrum of its policies.

Among potential examples of pollution warfare, consider nuclear pollution. To construct a usable nuclear device requires considerable nuclear material as well as clever engineering. Far less plutonium and sophistication are needed to scatter

---

[109]Fred Iklé and Albert Wohlstetter, *Discriminate Deterrence: Report of the Commission on Integrated Long-Term Strategy* (Washington, D.C.: U.S. Gov't Printing Office, 1988).

radioactive poison over a business district and render it unusable for years. Chemical weapons delivered directly (by artillery shell) have a local impact, while chemicals placed in reservoirs can mortally pollute the drinking supply of an entire metropolitan area. Agricultural pests introduced where they had been tightly controlled can do terrible, long-lasting damage to a local agricultural economy. Airborne biological agents offer a deadly form of air pollution.

Widespread random and pointless crime can be considered a way to pollute public spaces and can inhibit their use. Bombs in jets can, in effect, pollute a nation's airways, rendering them unusable except by those with a high tolerance for risk.

In the Third World, cheap land mines have become an insidious blot on the landscape, one that persists even after fighting ends. Roughly a hundred million land mines have been sown, with Kampuchea and Bosnia two now familiar sites. Land thus riddled is unusable except at risk to life and limb; mines account for a disproportionate percentage of all civilians killed indirectly from war. As of November 1996, land mines accounted for most of the (few) fatalities suffered by NATO peace forces in Bosnia after the Dayton accords. International calls for assistance in clearing these mines offer many parallels to calls to clean up superfund sites.

Even conventional air and water pollution have become part of conflict. Toward the end of the Gulf War, Saddam Hussein opened up oil pipeline valves to create a giant oil slick floating toward Saudi Arabia. On retreating from Kuwait, Iraqi troops set oil fields on fire, blackening the skies for months afterward. Had it been possible, Saddam Hussein might have used pollution to interfere with the United States's space capability. Pellets scattered in low-earth orbit can dramatically shorten the lives of

satellites that perform military and commercial surveillance.[110] Similarly, a nuclear electromagnetic pulse (EMP) explosion in a carefully chosen stratospheric point can create enough electronic flux (or scintillation) to disable electronics.

Partition Warfare: With or without state support, a few determined people can do enormous damage by polluting shared media. Given the difficulty of maintaining media unpolluted in the face of a determined adversary, an alternative strategy is to control access to such media. Partition, aimed at separating clean worlds from potential polluters, may be a way to avoid violence while also protecting common media.

A simple version is to isolate an entire country or area. Terrorist incidents by Hamas invariably lead Israel to shut off access to Gaza and the West Bank. Their bombings in March 1996 led Israel to use high-technology devices designed to look for illicit border crossings and individuals carrying explosives. Well before entering World War II, President Roosevelt appropriated the medical term for separation, quarantine, to characterize the posture of the United States toward the Axis powers.

Economic embargo is a form of putting up fences and has been used against the white regimes of Rhodesia and South Africa as well as against Iraq and Serbia. Does it succeed? Given correlated factors, such as internal political trends or military defeat, an economic embargo probably could have some effect, but only slowly and rarely by itself.

The U.S. court system can be considered a partitioning element, separating criminals from the population after due process has identified them as guilty. Immigration control, notwithstanding economic rationalizations, contains elements of partition. One

---

[110]Most surveillance satellites fly a polar orbit in a band 200 to 400 kilometers high. A population of several hundred million pellets scattered across the equator in that altitude band would hit such a satellite with a cross section of four square meters once every five years—halving its normal ten-year lifespan.

response to violence by immigrants—whether by supposed anarchists of the early twentieth century or today's terrorists—has been to limit immigration from certain regions. U.S. law can deny entry to specific individuals with criminal records or unwanted characteristics (e.g., diseases). In theory, barring specific individuals would be easier when personal files become globalized and easily forwarded across borders, but not everyone to be kept out has a well-documented past.

At a military level, partition warfare was carried out by the British in suppressing the Boer rebellion. The British used a dense network of barbed wire and armed watchtowers which sharply reduced the mobility of the Boers and allowed them to be checked by conventional army forces. In the Gulf War, General Colin Powell predicted that U.S. forces would first cut the Iraqi army off (from Iraq), then kill it.

As Applied to Information Warfare

How might these topological constructs apply to information warfare?

Precision Warfare: The promise of information warfare is that it will carry precision further than even one target, one shot, one hit. During Operation Desert Storm, the coalition's destruction of key Iraqi communications and headquarters facilities essentially blinded Iraq's military, reducing their capability substantially, perhaps even determining the outcome before too many shots were fired. In Desert Storm the Sequel, soft-kill mechanisms—perhaps electromagnetic pulses or malevolent computer code inserted over the wire—might achieve the same effect without violence, hence without collateral damage.

The reduction from 2,500 bombs to one could be reduced further by a form of command-and-control warfare. Knowing in which of fifty tanks a commander sits could mean that destroying the one tank may be sufficient, because it would leave an enemy

leaderless, thus easy prey. But finding one tank in fifty is more easily said than done. If signal intelligence becomes more difficult to acquire (e.g., thanks to encryption and fiber optics) and human intelligence gets no better, the ability to determine which tank has the commander may not improve. Nor may a determined enemy be stopped when its commanders or computers are disabled.

Pollution Warfare: The Internet is becoming the commons of cyberspace, but its usefulness depends on its users observing rules of decorum. Spamming (widespread electronic junk mail) makes the Internet less usable. Hacker activity can complicate the blithe downloading of unsigned computer files (even e-mail cannot be read without risk, because it may contain viruses built into macros), discourage the use of software agents and Java-like active code, and force users to implement security measures, raising costs and inhibiting casual, free use of cyberspace. Hacker attacks are like crime waves, which force people to lock their doors at night.

Electronic media can be polluted. Dropping an enormous number of cheap jammers into congested areas, such as large cities, can interfere with communications but are extremely difficult to disable fully or quickly.

Psychological uses of information warfare can be regarded as pollution. People watch TV, listen to radio, or read newspapers in the expectation that most of what they hear is accurate (if often biased). Technology can now be used to make images look real and construct artificial sentences using a speaker's recorded voice. Lies or, worse, the clandestine replacement of real with false messages, pollute trusted media just as chemicals pollute waterways.

Partition Warfare: Information warfare can involve partition techniques. One aim of command-and-control warfare, for example, is to divide an army's body from its head without immediately disabling either. Air defense systems are disabled by

disconnecting radars from one another and depriving them of air tracks that cue each radar for air threats. Air control along with continuous observation—intelligence-based warfare—may permit tomorrow's version of the McNamara line proposed across Vietnam's Demilitarized Zone (DMZ) to work better than it would have in the 1960s. Armies are particularly vulnerable to attempts to cross imposed or natural barriers (e.g., ridges or rivers). When armies concentrate to cross at an obvious gating point (passes, bridges), they can be surveilled intensely, and if they cross at a less advantageous place, their passage may be slowed or they may stick out from surrounding terrain (e.g., by crossing a ridgeline).

Partition is also a way of responding to information warfare. A nation whose citizens, with state complicity, have abused connections to the Internet or the international telephone system to damage the infrastructures of other nations may find as a result that their own external connections are constrained.

In cyberspace, both the use of firewalls and the formation of trusted networks among cooperating institutions follow the strategy of warding off the evil outside by ensuring that one's own systems are effectively and cleanly fenced in and communications must pass through increasingly sophisticated gates.

In the realm of cultural warfare partition can be seen in the growing number of Western electorates that have adopted anti-immigrant themes, who fear their own culture being swamped by "others." Many Third World nations fear cultural pollution (e.g., free speech, pornography) from the West, just as some Western nations disdain cultural pollution (e.g., fast food) from the United States.

Conclusions

The trio of precision, pollution, and partition warfare will probably continue in restless coevolution, growing increasingly

sophisticated and information-hungry as they compete with one another. These constructs, as the above examples suggest, seem to have especial relevance for the contemplation of information warfare—but they also illustrate the traps to which metaphor is heir. Precision, after all, is often oversold, pollution is often used as an ascription of the "other" and too easily suggests "ethnic cleansing," and partition has formed the core of some very ugly deeds (e.g., Jim Crow, and concentration camps). Topological metaphors, like any other, must be used with care.

Metaphor

Because we live in an information age, information warfare, it would seem, must also rise to ascendancy. Information warfare may have old components, but, as an aggregate, it is new and thus without precedent. Metaphor, in turn, is how new things are framed so that they can be discussed in terms of the familiar.

Metaphors, like loaded weapons, should be used cautiously. As the first two essays suggest, the notion of defending a nation's cyberspace begs the question of whether cyberspace is a defensible space per se. Such poor ascription may come to distort government's proper role in promoting security. The third essay sketched the potential chasm between the reality and perception of information warfare, derived, as it is, from the wizardry of computation. The fourth essay examines how information warfare may revive metaphors that supposedly fell with the Berlin Wall. The fifth essay asked whether the immune system is a good metaphor for defenses against information warfare (e.g., organic viruses as analogs to computer viruses) and found that the question is complex, because the boundary between self and nonself, while in theory sharp, is fuzzy in practice. The sixth essay tried out a few metaphors from topology and found them worth playing with.

Ultimately, one hopes, information warfare will be understood for what it is, rather than for what it resembles. Defensive information warfare, in particular, needs to evolve from a strategy to a profession. If information warfare is not to be driven into some third-wave cul-de-sac, it must shed its overwrought metaphor of twenty-first century strategic warfare and acquire instead the pedestrian status of safety

engineering.[111] The art of working with dangerous machines and chemicals without taking casualties has long been studied in militaries. Operators are inculcated with its dicta and forced to relearn them continually. Safety officers have enormous influence over day-to-day operations. Entire Services have stood down when an accident level is found unacceptable. Defensive information warfare must similarly be taken seriously when institutions rely on information systems.

Information warriors may see this new identity as a comedown in much the same way that economists used to bridle at the suggestion of John Maynard Keynes that, "If economists could manage to get themselves thought of as humble, competent people on a level with dentists, that would be splendid."[112] If understood correctly, information warfare would loses its sex appeal or media attention; and it would disappear from Presidential Decision Documents and grand national strategy. But it would grow up and go to work.

---

[111]Perhaps the most useful on the subject of how to secure computer systems (even though computer security, itself, gets scant mention) is Nancy Leveson's *Safeware: System Safety and Computers* (Reading, MA: Addison-Wesley, 1995). The habits and practices required to secure systems against accident and error carry over very nicely to securing them against deliberate attack.

[112]From Chapter Five of *Essays in Persuasion* (New York, W. W. Norton, 1963 [originally published in 1926]).

Acronyms

APC	antigen-presenting cell
ATM	automated teller machines
CERT	Computer Emergency Response Team
CNN	Cable News Network
DARPA	Defense Advanced Research Projects Agency
DEFCON	defense conditions
DISA	Defense Information Systems Administration
DOD	Department of Defense
EMP	electromagnetic pulse
FAA	Federal Aviation Administration
FBI	Federal Bureau of Investigation
GAO	U.S. General Accounting Office
Ig	immuno-globulin
KGB	former Soviet secret police
MEII	minimum essential information infrastructure
MHC	major histocompatibility complex
MILSPEC	military specification
NDU	National Defense University
NII	national information infrastructure
NK	natural killer (cell)
OODA	observation-orientation-decision-and-action
OSD	Office of the Secretary of Defense
PBX	private branch exchange
PC	personal computer

PMN	polymorphonuclear (cell)
R&D	research and development
SCADA	supervisory control and data acquisition
SDI	Strategic Defense Initiative
STP	signal transfer point
TCO	transnational criminal organization

*U.S. G.P.O.:1997-418-297:60003