
**CONCLUSION: THE CHANGING ROLE OF
INFORMATION IN WARFARE**

Martin Libicki and Jeremy Shapiro

Information achieves value by improving decisions. Thus, the role of information in warfare must be to affect strategic or tactical decisions in one's favor. This role is as old as warfare itself; indeed, it might be said to be the very purpose of warfare. So what is new, or, more precisely, why does information seem to be becoming more important now? In a word: technology. New machines and new processes have recently become integral to collection, processing, and dissemination of information. An increasing percentage of decisionmaking and decision support has been transferred from people to machines. People operate under familiar physical and psychological parameters. Machines operate under unfamiliar and increasingly complex parameters. They and their logical processes are subject to attacks and manipulations that are both novel and difficult to understand intuitively.

In evaluating the effects of these new machines and new processes, the chapters in this volume have covered an extremely diverse set of topics and viewpoints, ranging from the sources of national power and the possibilities for psychological operations to the rise of arcane techniques as the new arm of military decision. These topics are ultimately linked only by their information and national security components. The influence of information in and on warfare appears so pervasive that one may reasonably wonder how "information warfare" differs from warfare itself. Information warfare in this sense is less a distinct topic than an approach—a way of bringing to the fore an aspect of warfare that has always been critical but that we sense is becoming still more important.

At the same time, dramatic changes in the ways we communicate, organize, and work will inevitably mean that wars may be fought for entirely new motives and even by new actors. David Gompert sees the new technologies as creating a world far more favorable to U.S. interests in which peer competitors and even major theater wars will cease to plague the United States. By contrast, John Arquilla, David Ronfeldt, and Michele Zanini see a world of new threats, stemming primarily from nonstate actors that may create a very unstable environment and severely tax U.S. defense resources. Finally, Jeremy Shapiro cautions against accepting either of these claims of wholesale transformation. Yet, all three contributions warn that those who see only direct military effects may miss the greater change. According to Carl Builder, the U.S. military has tended to see new technologies in terms of how they can improve mission capabilities, rather than anticipating how their missions will change.

If the future looks foggy, a wait-and-see attitude is easiest to justify. But the Department of Defense (DoD) must be aware of the context in which it operates and know that this context is subject to change by technological and other influences—even if it cannot help but react to changes that it cannot influence. Inevitably, an awareness of the possibility of a radical social transformation means that the military must strive to maintain both its flexibility and its link to civil society. A military cut off from civilian influences in a time of social transformation risks becoming dangerously out of touch with the polity it is supposed to protect.

The purpose of this volume has been to prepare the United States for these transformations by revisiting old questions with a new attention to information and emerging information technology. The chapters probably raise more questions than they answer, but in their diversity they serve to highlight the important areas for attention. This final chapter will point to several such areas and the implications of all this for the nation and for the U.S. Air Force.

TREND OR FAD?

One theme that runs through nearly all of the chapters in this volume is the idea that the new technologies herald a new age of warfare. Nonetheless, many maintain that less has changed than we might think. They hold that the nature of war; the admixture of fear, glory,

and survival instincts; the transcendent qualities of leadership (or its failures); and Clausewitzian fog and friction are both persistent and dominant; “information warfare” is just another in a series of failed technological solutions to this permanent feature of war.

Their millenarian counterparts aver that people war as they work. Just as the transition from agriculture to industry was correlated with the industrialization of warfare, so too will the transition from industry to information-based services be correlated with the “informating” of warfare. War waged in cyberspace might be bloodless and even clean, a possibility that has led one high-ranking military officer to see information technology as “America’s gift to warfare.” (Owens, 1995.) Sun Tzu is an icon in this pantheon, with his observation that the “acme of skill” consists in winning without fighting.

This war of words between those who see war as hopelessly messy and violent and those who foresee bloodless battles belies an important change. For the United States and its allies, people are expensive; stuff is cheap. Silicon is getting cheaper, and casualties are growing prohibitively expensive. Thus, as any economist would argue, it makes sense to substitute what is getting cheaper for what is getting more expensive—that is, to substitute as much silicon for casualties as one can. Throughout the U.S. military, precision weapons are being substituted for simple shot and shell (precision weapons accounted for over 99 percent of all North Atlantic Treaty Organization ordnance dropped in Bosnia in 1995), and networked sensors are illuminating the battlespace to generate aimpoints that give these precision weapons somewhere to go. Information technology is changing the U.S. military, whether it creates a new age of warfare or not. It is changing others as well, albeit more slowly and less completely so far.

No sooner, however, does a military adopt a certain functional architecture than the core of that architecture becomes its center of gravity, the logical target for the enemy, and thus what must be most vigilantly protected. Just as no one today would build a car without brakes and bumpers, so should no one design an information system without due attention to its fault modes, whether accidental or deliberately induced. Deception (dummies, decoys, and ghosts) represents a time-honored way of inducing failure in both man and machine-based information systems. Electronic warriors have

thought through the interplay of measure, countermeasure, counter-countermeasure, and so on for years, in part because radar and radio-electronic communications are meant to work “outdoors” where the enemy may lurk. System architects have been somewhat slower to catch on, in large part because computers were designed for indoor work. Only recently, with ubiquitous networking, have they been transformed, with little forethought, into outdoor systems.

The sudden understanding that critical systems are vulnerable to someone operating from a phone booth anywhere in the world has led, and properly so, to great concern. Information security is increasingly a cost of doing business—especially in war, an endeavor whose purpose is to foil others.

PERFECT SECURITY?

Is perfect information security possible? This issue is probably the most vexing of any in the science of computer security; its answer rests, in large part, on which metaphor we use to describe information warfare: engineering, combat, or disease.

In theory, perfect security is possible. There is no such thing as forced entry in cyberspace. If someone enters a system without authorization, it can only be through a door inadvertently left open. Information security is therefore an engineering problem, akin to making a ship watertight. In that case, it may be misleading to think in terms of “information-warfare weapons” or in terms of second-order considerations, such as arms control or deterrence. Insofar as information weapons exist, their design follows directly from the features and flaws of the system being attacked. Focusing on the weapons rather than on the security flaws has the unfortunate effect of centralizing a problem best dealt with at the local level.

In practice, however, pessimists argue that, as systems grow more complex and continue to evolve rapidly, what is theoretically possible becomes practically impossible. Determining all fault modes with security implications simply cannot be done in any feasible time period. In the real world, then, information security may, like combat, be a continual race between offensive measure and defensive countermeasure.

Combat is marked by a conceptual parity between offense and defense. No wall, however thick, can withstand a battering ram of

sufficient size; no battering ram, however large, can knock down a wall of sufficient thickness. It may be thus with information security. One side builds defenses; the other side builds weapons; and the race is never ending. This metaphor implies that invulnerability from information attack is impossible or is at least fleeting. This is the premise that led Zalmay Khalilzad to think beyond local measures of information security to national strategies.

Information-warfare hawks go further by invoking the metaphor of disease. They see a world of big organisms at risk from small germs. Offensive information warfare is cheap; for most tasks, a laptop and a phone line suffice. Not everyone can be a good hacker, but rogue hackers can peddle their expertise worldwide. Disposable jammers can wreak havoc on communication systems. Viruses can propagate endlessly from one machine to another. Tools of intrusion and cover-up flow freely on the Internet. Cyberspace is becoming increasingly plague-ridden, and ever-larger percentages of computer investment must be devoted to protection. In this view, information security is a crisis that threatens us all and demands a centralized public response, much as the urbanization of the 19th century created a requirement for public health.

But the disease metaphor also speaks to a growing facet of information warfare: complexity. On the one hand, the more complex a system is, the harder it is to ensure its integrity. On the other hand, people—the world's most complex information-processing systems—are generally immune to the sorts of attacks that keep system administrators up nights.

A normal person told by a stranger that the world would be a better place when he or she is dead is unlikely to take that information to its logical conclusion. The information makes no sense; there is little a stranger can do to make one believe in such nonsense; and, anyway, such strangers have no authority to so command you. The last two barriers to doing stupid things have analogies in computer security: virus protection (lack of trust in outside sources) and authentication (verifying that a person is known to you). But the first notion of "common sense" is far less effective in securing computers. We expect our machines to do what they are told, but such expectations leave them prey to low-level, but insidious, information-warfare attacks.

With the inevitable (if oft-delayed) advent of artificial intelligence, the practice of generating general mission orders and having the machine determine how and when to carry them out may become more common. Heuristics may prevent them from doing stupid things. Yet, such technologies as knowledge engineering, rule-based logic, and neural nets, while making machines more sophisticated, leave them harder to predict and understand. The price of preventing obvious failure may leave them heir to the subtle manipulations that humans have long been exposed to. (See, for instance, MacKay, 1841.)

NATIONAL POLICY ISSUES

The policy issues that information warfare raises are, in a sense, a subset of the policy issues that are raised by the entire field of information technology. Some come under the rubric of national public information policy—a shadowy area that often mixes truth and propaganda. Other issues are raised by the increasing importance of network systems to the U.S. economy and the consequent desirability of their protection.

It is only somewhat of an oversimplification to reduce the issue of national public information policy to the blunt question: Should it be the official policy of the U.S. government to lie? Of course not, John Arquilla suggests. Yet, as Brian Nichiporuk argues, DoD may at times want to insert false messages into another nation's communication systems. Moral difficulties aside, as long as the United States is not directly threatened (a condition that, by and large, obtains today), its primary national security strategy consists of inducing other nations to adopt what are considered good and universal norms of conduct. Among them are democracy, rule of law, and freedom of expression. All three must rest on a foundation of truth. If that foundation erodes, the norms get shaky. In any case, as society becomes increasingly networked and as electronic surveillance makes the world increasingly transparent, the art of lying becomes harder and harder.

The issues that relate to protecting the national information infrastructure, as Roger Molander, Peter Wilson, and Robert Anderson outlined, are dense and intertwined. In theory, the government's right and responsibility to protect cyberspace are straightforward,

perhaps even more obvious than a comparable aegis over protecting the nation's ships, aircraft, and space satellites. In practice, the government may wish to approach this new task gingerly.

The justifications for the government's diffidence stem from technology. By and large, people play havoc with networks by attacking systems attached to them. Each system has its owner, and each owner is the one to choose the hardware and software, as well as set the parameters and policies that collectively determine how easily an attack takes place. The government can facilitate good choices with both carrots and sticks. It can also prosecute malefactors and seek to dissuade their sponsors—although, as Glenn Buchan points out, this may be very difficult to do. What the government cannot do is to erect a barrier through which bad bytes cannot flow, a continental firewall as it were.

If the government cannot reliably protect systems, should it nevertheless accept the responsibility to do so? The answer is not obvious (replace "systems" with "borders" and most people would answer "yes"). Popular sentiment may leave the government little choice in the matter, especially after the first disaster. Yet accepting such responsibility for itself has a tendency to reduce the responsibility of others, notably system owners—and the latter have the means and tools to protect themselves. Roger Molander et al. speak of a "loss of confidence" in national institutions as a result of strategic information warfare. Would accepting responsibility create a linkage whereby loss of confidence in, say, the telephone system also erodes the confidence that people feel in the government?

As both the Gompert and the Arquilla, Ronfeldt, and Zanini contributions emphasized, realizing the true potential of information technology requires a decentralized market economy and the motivated actions of each of its citizens. Except for providing common infrastructures, the logic of centralization is absent. Indeed, centralization and hierarchy may limit the advantages one can draw from the new technologies.

Not only are owners of the information infrastructure desirous of defending their own systems, but most do not answer to the federal government, and some are highly suspicious of any unsolicited "help" they may get from such quarters. Many suspect that bureaucrats are incapable of understanding or keeping pace with emerging

technology. An overemphasis on security at the expense of other features and the bureaucracy's natural tendency to emphasize procedures over outcomes may yield no better security and far less innovation. If nothing else, there is a perceived contradiction between the government's offer of help to the owners of private systems, and its continuing efforts against the market for encryption products, which are one of the better defenses.

If owners bear *all* the costs (including third-party costs) of their own negligence, there is no reason they cannot provide optimal levels of protection in this field as in others. True, some aspects of information security are best done collectively because of economies of scale (e.g., research and development, indicators and warning). Others are inherently matters of state (e.g., criminal prosecution, military retaliation). Nonetheless, they hardly constitute, even collectively, all the tasks necessary for a complete defense of the nation against information warfare. The burden is therefore on the government to demonstrate that the protection of commercial information infrastructure is a national security concern that cannot be discharged any other way. Convincing a population wary of government intervention of the need for such intrusive government action may require a crisis.

Turning from the general to the more specific, the federal government can do many useful things to help matters when the only interesting question is not "whether" but "how much":

- *Protect Its Own Systems:* Not only are national systems of national importance, but the federal government has declared that the security of its information systems would set a standard for the rest of the nation.
- *Enforce the Law:* A thicket of laws already exists against computer hacking, abuse of spectrum (e.g., jamming radio signals), and microwave weapons (as a category of weapons in general). In enforcing such laws, the federal performance has been very efficient, and an unexpectedly high percentage of high-profile attacks has resulted in successful prosecutions.
- *Promote Standards:* Standards are important for interoperability, security, and creating a performance level against which existing systems can be judged.

- *Invest in Research and Development:* The level of federally sponsored research and development in information security has risen at a good clip from the \$100 million-per-year level of several years ago (a lightweight secure network operating system remains one crying need). Although the scarcity of skilled researchers puts an upper bound on any funding trajectory, R&D funding today means more graduate students tomorrow and more professionals the day after.
- *Establish an Incident Clearinghouse:* The Computer Emergency Response Team is a well-established clearinghouse for collecting information on Internet security incidents, disseminating warnings, and generating countermeasures for novel attacks. Other industries and the military are starting similar clearinghouses for their own sectors. The Computer Emergency Response Team model represents a compromise between centralized and decentralized control that combines the best features of both. It preserves local responsibility but provides a central repository of expertise that can acquire a global view of any emerging threat.

Some policy instruments are worthwhile, but have some potential for backfiring if broader ramifications are not kept in mind:

- *Generating Indications and Warnings:* In theory, premonitions of an information attack could be broadcast so that system owners can ratchet up their monitoring and review their access procedures. In practice, as Glenn Buchan points out, premonitions may be hard to come by, and establishing the credibility of such indications and warnings may raise difficult issues about sources and methods.
- *Fostering International Norms and Cooperation:* Progress has been made in fostering international cooperation among law enforcement agencies and in persuading other countries to make computer hacking a criminal offense. As Lynn Davis warns, however, beyond some point, other nations will demand that the United States pay comparable heed to violations of what they consider norms in the information age (e.g., violation of data privacy—a nascent issue in Europe). If U.S. military policy is to maintain “information dominance,” emerging norms against the use of information weapons may limit the utility of that capability.

Still other policy instruments seem attractive but require a good deal of thought prior to their implementation:

- *Determining a Minimum Essential Information Infrastructure (MEII):* Research to determine candidate members in a national MEII is all well and good, but should policy actually be based on the findings? Two troubling questions present themselves: “essential” for what end, and “essential” for how long (in the face of furious technological change)? An MEII for the military (or the broader national security community) raises fewer difficult issues. DoD’s various operational plans answer the question of ends, and its acquisition policies inform near- and medium-term changes in its own MEII. Once the elements of a defense MEII are determined, DoD can use several specific tools (e.g., through clauses in defense contracts) to bolster the security of networks essential to its own missions. Nonetheless, the increasing interconnection of civilian systems with the DoD information infrastructure complicates even this simpler task.
- *Protecting Auditing and Testing:* Honest third-party audits may become more frequent if the auditors can be shielded from having to testify in civil suits about what they find. Red-team testing of critical systems may become more common if owners could be covered from some legal liabilities that accidentally result from such tests. Yet, there is no legal protection that cannot be abused, and extensions of long-standing claims to one area give rise to demands for protection in others (e.g., if computer security specialists, why not safety engineers?).
- *Limiting Legal Indemnity for the Consequences of Attack:* If an attack on a network (e.g., one that controls electrical distribution) causes harm to third parties, can third parties sue network owners and collect damages against them? If the answer is *no*, network owners will underinvest in security (and demand the government step in to cover their failures). A *yes* answer, however, adds one more basis for lawsuits in a very litigious society.
- *Declaring a Retaliatory Policy on Information Attack:* Can the United States deter a strategic information attack by declaring it tantamount to a physical attack (e.g., mass disruption as a subspecies of mass destruction)? Were such a thing possible, deterrence might obtain, but as Zalmay Khalilzad enumerates, practi-

cal difficulties abound: setting a threshold for response, determining the perpetrator, and forcing the United States to react in predetermined ways where wisdom might suggest otherwise.

- *Declaring a No-First-Use Policy on Information Warfare:* It makes sense for residents of glass houses to look askance at stones. Nevertheless, the case that information warfare has a bad reputation morally that shell and shot lack may be hard to make. Again, practical difficulties matter. In nuclear warfare, the event is unmistakable; the perpetrator can often be identified reliably; and the requisite equipment can be placed under secure command and control. None of this applies to information warfare.

AIR FORCE POLICY ISSUES

At one level, information warfare presents fewer troubling policy issues for the Air Force than for the nation as a whole. Understood broadly, information warfare is a collection of operational techniques that are used with greater or lesser efficacy as circumstances and capabilities warrant. At another level, however, as the Air Force redefines and reorganizes itself, it must necessarily ask whether information warfare is at the heart of its mission or whether it is one of several adjunct competencies necessary to promote the main task of aerospace superiority.

Most of what falls under information warfare, with its many historic components (e.g., command-center targeting, psychological operations, electronic combat, signals intelligence), has been parceled out for action long ago. However, to many, the mechanization of the world's decision processes has introduced a new medium of warfare, cyberspace. Conflict in cyberspace, like conflict in predecessor media, must be dealt with in its own terms and may justify entirely new missions and organizations.

The concept of cyberspace as a new medium, of course, cannot help but resonate with the U.S. Air Force. Air forces spent most of the first half of the 20th century arguing that their medium was fundamentally different from those before it. Mastering the medium of air, they claimed, required new doctrine, new culture, and new people and, as a result, a new home for its masters. Having won the argu-

ment for air, the U.S. Air Force makes a similar argument for space: It too is a new medium, with its own doctrine, culture, and people. However, the argument continues, the link between air and space is strong (e.g., the natural complementarity between space assets and high stratospheric unmanned aerial vehicles to support surveillance; reconnaissance; and, perhaps soon, communications). Thus, those who pioneered the first should be asked to master the second. In its 1996 Corona conference, the Air Force hierarchy concluded that the Air Force should see itself as an Air and Space Force today and perhaps a Space and Air Force in the future.

Airmen have been arguing since Douhet that air operations could, in and of themselves, be an arm of decision. Both the Six-Day War and Desert Storm indicate that, under certain circumstances, winning the air campaign makes the land campaign very easy. Information warfighters, using Desert Storm as an example, now make similar claims for information warfare. Achieving information superiority will make winning the air and land wars much simpler.

Warfare in cyberspace fits a service that has been quick to convert new technological possibilities into new forms of power and quick to see that new media have new rules. The great majority of U.S. "military opportunities" that David Ochmanek and Ted Harshberger document would appear to accrue to the Air Force. But history also suggests that institutions that have mastered one new medium are not automatically assigned the next. After all, the U.S. space program grew out of work undertaken by the *Army* at Redstone Arsenal.

More fundamentally, integrating cyberspace warfare will perhaps, as Carl Builder's contribution suggests, require the Air Force to address "the enterprise question." What are the Air Force's objective, purpose, and comparative advantage as a service? This is the question that bedeviled the *Army* during the interwar period and, after much acrimony, eventually led to an independent air force. If the Air Force wishes to absorb the cyberspace mission as warfare in a new medium, it must be prepared for the creation of new constituency in its midst, one that will seek its own identity and perhaps independence from the Air Force's pilot culture. This much may be seen from its experience with integrating space operations and the consequent struggles over space assets, people, and organizations. Nevertheless, it is quite likely that the issue of whether to absorb

cyberspace as a single medium into the Air Force is less likely to be as defining as were similar issues in earlier media.

First, post-Goldwater Nichols, the various commanders in chief (CINCs) have increasing say and discretion over how they put force packages together—and with ever finer granularity. The Air Force may argue that information operations are so uniquely integral to air and space operations that they belong in the same service. Come wartime, however, a CINC will likely build a force by picking up a squadron here, a vessel there, and a battalion somewhere else based on the logic of time and place. Information operations will need to function in this joint, CINC-determined environment.

Second, once the issue of constructing coherent force packages is left to the CINCs, the service slice of information warfare will consist of training and equipping information warriors. The Air Force may be able to make a case for training information warriors (a subject that the military has only started to come to grips with), but, in contrast with aerospace warfare, equipping them is usually a trivial undertaking that need not be limited to one service.

Third, as widely noted, information warfare spans considerable terrain, whose boundaries are very difficult to distinguish. For this reason, in asking about the relevance and wisdom of making information warfare an Air Force mission, it may be worthwhile to look at individual chunks as Table 15.1 subdivides them.

Information assurance is a broad function with many responsibilities. Intrusion detection and thwarting of attacks on systems is the focus of the Air Force’s 609th squadron at Shaw Air Force Base and the impetus for intense activity at the Joint Information Warfare Center at Kelly Air Force Base. But real-time cybercombat is just one

Table 15.1
Information-Warfare Matrix

	Unit Level	Systemic
Defense	Information assurance	System of systems
Offense	Hacker attacks, electronic warfare	Command-and- control warfare

aspect of information assurance. Vigilance, sound engineering choices, and internal controls are of comparable importance. Responsibility for these functions is best pushed down the hierarchy. Defending networks should be the primary responsibility of those who run them. Complexity and the need to integrate information about attacks offer the counterarguments. The more one must know to defend a network, the more it pays to concentrate the expertise and information within a few people as opposed to forcing everyone to learn everything.

Tactical offensive information warfare (see the contribution by Brian Nichiporuk) has two components: intelligence and operations. If existing intelligence and information functions are a clue, the civilian leadership is not predisposed to assign primary responsibility for information warfare to any one service. A large and growing share of DoD's information functions reside in defense agencies and joint commands, even if Air Force personnel and facilities provide more than proportional support for these missions. Offensive information warfare, especially, is likely to be the province of intelligence agencies because of its elite and clandestine nature.

Offensive electronic warfare, however, is an enterprise that is disproportionately Air Force today (although the Navy has comparable responsibilities in the fleet, and the Army conducts similar operations). Indeed, the mission to suppress enemy air defenses is critical to successful air operations. Extending this mission to encompass information warfare offensive techniques would seem an easy fit for the Air Force.

At the systemic level, information warfare is the organization of information to provide warfighters with what has been termed "dominant battlespace knowledge," an important component of which is the DoD's nascent "system of systems." Insofar as the ability to kill what can be seen makes seeing (locating, identifying, and tracking) the key to war, seeing is increasingly best done by networking sensors and human observers to create a shared ground truth that forms the basis of command, control, and operations. This evolution can be seen in the widely heralded transition from platform-centric warfare (wherein networks exist to enhance platform performance) to network-centric warfare (wherein platforms are the eyes, ears, and fists of a broader entity). If there is to be an entity in

charge of building and maintaining this shared ground truth, the Air Force, with its air and space intelligence, surveillance, and reconnaissance assets, is as good a candidate as any. Indeed, some in the Air Force have concluded that the first assets the United States should deploy into a combat zone are not the folks who are “First to Fight” but the illuminators. With today’s technology, these illuminators may be represented by a package of the Joint Surveillance and Target Attack Radar System; the Airborne Warning and Control System; Rivet Joint; and, soon, long-range unmanned aerial vehicles. (See Fulghum, 1998.)

Finally, systemic information warfare is a matter of determining how an adversary uses information to inform decisions and then using this knowledge to disrupt or corrupt their decisionmaking processes. Of course, some attack methods may be attacks on information systems themselves, but if critical nodes of an adversary can be discovered, iron bombs are another feasible approach, as Glenn Buchan argues.

Based on what is admittedly an initial assessment of various aspects of information warfare, the best places for the Air Force to build up and defend unique core competencies lie in the area of unit-level operations against enemy information systems and in the care and maintenance of the top-level system of systems. By contrast, the case for centralizing tactical systems defense and understanding adversary decision processes under Air Force control will be harder to make.

A TIMELESS LESSON OF INFORMATION WARFARE

Deeper consideration of this area, however, suggests that information warfare, in the end, may be less about a discrete set of activities or responsibilities than about a way of thinking about conflict. It forces warfighters to ponder not just each side’s physical capabilities, but also the decision processes that govern when, where, and with what effect these physical capabilities are used. These are habits of mind that all warfighters, at all times, should adopt and not simply those of any one service or nation. That new technologies have made us reconsider this timeless piece of wisdom does not mean that everything has changed suddenly. To the contrary, we may simply be rediscovering what we have really known all along.

REFERENCES

Fulghum, David A., "Info War Fleet Tapped for Fast Deployment," *Aviation Week & Space Technology*, February 9, 1998, pp. 90–91.

MacKay, Charles, *Extraordinarily Popular Delusions and the Madness of Crowds*, New York: Crown Trade Paperbacks, 1995 [1841].

Owens, Admiral William, quoted in Douglas Waller, "Onward Cyber Soldiers," *Time*, Vol. 146, No. 8, August 21, 1995.