
**IMPLICATIONS OF INFORMATION VULNERABILITIES
FOR MILITARY OPERATIONS**

Glenn C. Buchan

Can more effective use of information provide the leverage necessary to offset reductions in military force structure? Can new information systems lead to fundamental changes in the ways the United States uses force or otherwise coerces adversaries? These possibilities, which RAND and others have been analyzing for several years, are certainly extremely attractive, particularly for the United States, which seems to be well-positioned to exploit the new technologies. However, success is by no means preordained. The force has a dark side. One of the potential problems is that relying on the new information-related technologies that appear so powerful could also introduce vulnerabilities an enemy could exploit, or that would allow Mother Nature—or plain bad luck—to render the systems impotent or seriously degrade them. This chapter focuses on these vulnerabilities and their operational consequences and explores possibilities for managing the associated risks.

Recent RAND research has tried to address some of those problems, particularly the problems confronting the Air Force.¹ Some of the problems are common to all of the services. Others are unique, at least to a degree, to particular services, based either on the specific kinds of operations that they conduct (e.g., land versus air, “tactical” versus “strategic”), the kind of equipment they use, and the opera-

¹This discussion is derived primarily from a “sanitized” version of the analysis presented in Buchan et al. (forthcoming a, b). The author gratefully acknowledges the work of all his colleagues that is reflected here. I want to thank Keith Henry, in particular, for producing more appropriate versions of several figures for use in this chapter.

tional and organizational culture that has evolved within each. Joint operations complicate matters even further. Thus, while our discussion and specific analysis focus on Air Force operations, some of the general findings are likely to be more broadly applicable, but the details could vary considerably.

AN OVERVIEW OF AIR FORCE OPERATIONS AND THEIR DEPENDENCE ON INFORMATION: PRESENT AND FUTURE

Our analysis has focused primarily on operations—war and other lesser operations—as opposed to day-to-day peacetime activities. That means our analysis did not pay much attention to casual or even malicious computer hacking attacks, say, on Air Force computers involved in routine, day-to-day support activities, even though those are by far the most prevalent kind of “computer attacks” that are known to have occurred. It is not that we consider such information vulnerabilities unimportant. Indeed, interference with personnel, medical, and payroll databases, for example, could have annoying—even serious—consequences even in peacetime. However, we believe that protecting information-related systems that support Air Force operations, which are its stock-in-trade, should receive first priority. Moreover, many of the actions required to protect Air Force information systems during operations would be applicable in peacetime as well, *but the converse is not necessarily true*.

Two major sets of systems and processes are central to the Air Force’s ability to conduct operations. The first includes all the systems that actually collect the basic intelligence data necessary to support operations, plan the operations, and execute them. Figure 10.1 shows some of the critical systems that the Air Force currently relies on and how they are wired together. The most important elements include the following:

- The whole array of intelligence-collection sensors, platforms, processors, and analysts that collect and analyze the information necessary to provide planners a sense of what is going on, warn them of attacks, allow them to target weapons (if that is appropriate) or otherwise conduct operations, and allow them to assess the effects of earlier operations

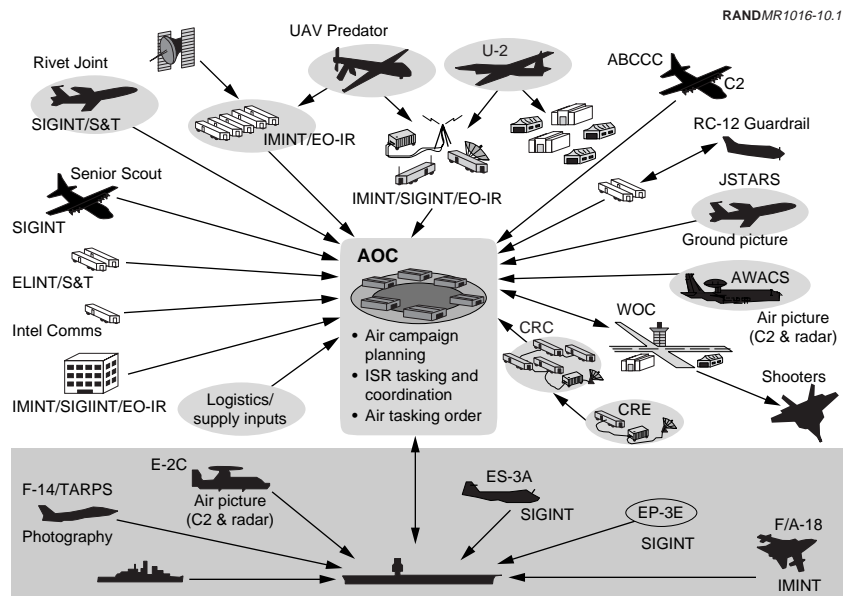


Figure 10.1—Air Force Combat Operations

- The planning and command center(s) where information is integrated, plans are constructed, orders are given, and progress of operations is monitored²
- The forces that execute the operations
- The communications systems that wire all of the critical systems together
- Systems that provide other critical information to planners and operators (e.g., Global Positioning Systems [GPS] satellites that provide navigational data and location information).

The details of future systems and architectures will change, of course, as technology evolves, operational procedures and organizational relationships change, and the new replaces the old. Physical and electronic “hubs” may not always coincide. Nevertheless, the

²Currently, the hub of Air Force planning activity is the Air Operations Center (AOC).

basic functional relationships are transcendent because, collectively, they represent the kinds of things the Air Force needs to do to do its job, whatever the specific details of that job may be.

The other critical part of the picture is the support infrastructure necessary to sustain operations. Figure 10.2 shows an airlift network centered at Scott AFB with tentacles reaching literally all over the world to deliver people, machines, munitions, and materiel of all sorts wherever they need to go. In combat operations, airlift supports the fighting forces. In other kinds of operations—delivery of humanitarian relief aid, for example—the airlift itself may be the focal point of the operation.

The information requirements for support and sustainability operations are similar to those of any shipping company. Airlift planners need to know who needs what material, in what quantities and by when, and where the goods need to be delivered. They also need to know what they have available to send, where it is stored, how to get it, and so on. Then, they have to allocate their airlift assets accordingly. Thus, if it were not for the possibility of getting shot at or hav-

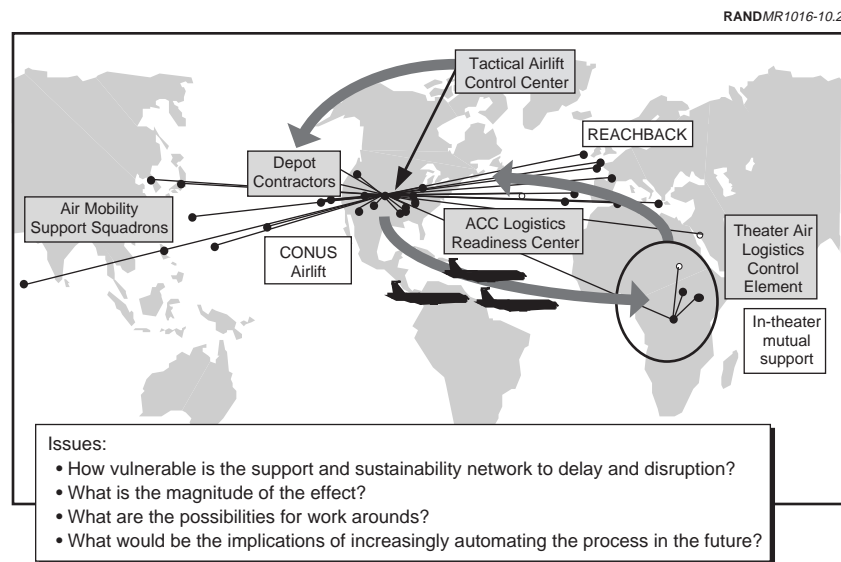


Figure 10.2—Supporting the Forces and Sustaining Operations

ing someone actively trying to disrupt their operations in other ways, their job would not be that different from that of Federal Express. In fact, current plans are to make military airlift operate more like Federal Express in the future.

An enemy might try to disrupt, distort, or destroy the information necessary to support the Air Force's ability to fight, to support and sustain its operations, or both. As we will show later in this chapter, the potential vulnerabilities of the information systems that support combat operations and sustainability efforts are quite different, as are the consequences of disrupting those systems.

DISRUPTING AIR FORCE OPERATIONS

Potential Threats

There are all manner of possibilities for disrupting information systems and information-related operations. Accordingly, we took a broad and comprehensive view of possible threats. Figure 10.3 shows some of those potential threats. They range from the sublime to the ridiculous, the well-understood to the ethereal, and the straightforward to the very challenging. For example, many critical information-related facilities remain vulnerable to direct attack by high explosives delivered any number of ways (e.g., by aircraft, missile, truck bomb, or command attack). Alternatively, an entire base could be cut off from landline communications for a time, or a key warning system could be disrupted deliberately or inadvertently if a critical cable were cut. Other familiar threats, such as jamming, spoofing, or deceiving information systems, could continue to be problems in the future. Futuristic weapons, such as high-power microwave (HPM) devices, could increase the vulnerability of some electronic systems unless they could be effectively shielded. Then, there is the master computer hacker (Kevin Mitnick, in the photo) who looks like—and might even be—the kid next door. Finally, there are natural events and even “Acts of God” (ask any computer user) that can disrupt information systems as thoroughly as any deliberate attack. Information systems have to be resilient to this kind of natural disruption regardless of any concern about “enemy action.” Thus, while most of the current topical interest has focused on the newer, trendier threats to information systems, particularly com-

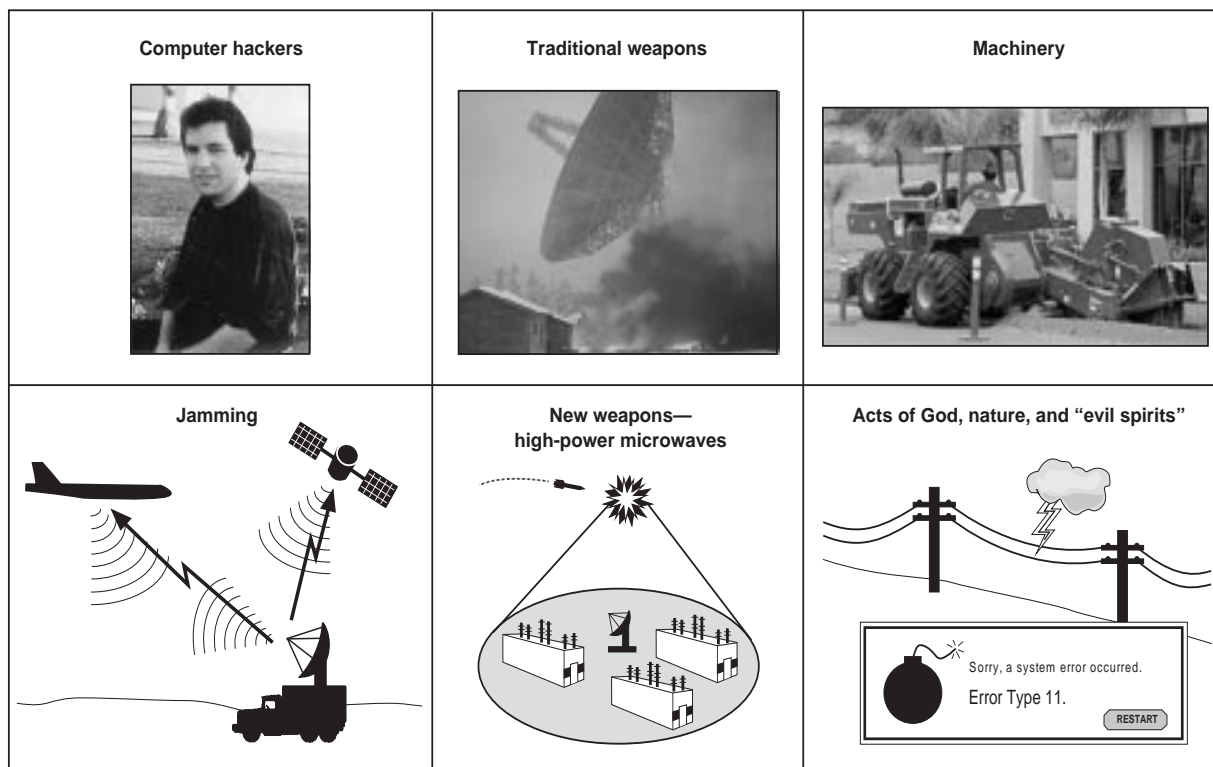


Figure 10.3—Potential Threats to Air Force Information Systems

puter hacking and associated information disruption and manipulation, the possible range of threats is much broader. Indeed, our analysis showed that some of the “old fashioned” threats appear to pose a greater danger to Air Force operations.

The character of the potential threats also has implications for the kinds of opponents that might be able to mount them and the prospects for the intelligence community’s being able to help in coping with them. In particular,

- At least some, even most, options for threatening Air Force information systems are within the capabilities of virtually any potential adversary, including non-nation-states. For example, physical attacks with high explosives against vulnerable facilities are within the capabilities of any attacker, although some will have more-effective delivery options available than others. As noted in the first part of this chapter, computer hacking skills are essentially universal. Similarly, effective jammers against unprotected communication systems and GPS satellites are cheap and readily available. Even “high end” futuristic weapons, such as HPM generators, are likely to be available on the international arms market to anyone with money once they become available at all. Thus, intelligence assessments may be of less use than usual in filtering the list of possible enemies who could interfere with U.S. information systems, and traditional notions of “strategic warning” of threats developing may be of little use, barring dumb luck in collecting intelligence.
- While the weapons to attack Air Force information systems appear to be cheap and readily available, *the requisite information to make those attacks effective may be difficult to obtain*. For example, many computer hacking attacks require knowledge that only insiders are likely to possess. Similarly, some physical vulnerabilities may be difficult to identify even if the basic information is unclassified.
- Because of the speed and ambiguity of computer hacking attacks, the prospects for receiving useful “tactical warning” in the traditional sense (i.e., receiving warning in time to respond, identifying the attacker) are remote.

This is going to complicate the defender’s problem in trying to protect against attacks on its key information systems.

Potential Vulnerabilities

The idea that the information systems on which the Air Force relies have numerous potential vulnerabilities is hardly a surprise. The issue is assessing the severity and possible operational impacts of those vulnerabilities.

Computer Vulnerabilities. The potential vulnerabilities of the computer networks directly involved in combat operations are strikingly different from those used for support and sustainability functions. Figures 10.4 and 10.5 illustrate the contrast.

Figure 10.4 shows the major groups of computer systems that are used in the AOC's planning process and indicates the critical information flows into and out of the AOC. Figure 10.4 shows the information flows in and out of the AOC and, as the shading in the figure suggests, we found that the computer systems used to plan and execute Air Force combat operations are relatively secure, absent a corrupted insider, in spite of the fact that they are UNIX-based systems that have well-known weaknesses. The intelligence-related systems, in particular, are as secure as technology and good operational procedures can make them. The reason is that the Air Force basically does everything right operationally:

- The databases and information flows among the various computers are encrypted.
- The computer networks are all isolated electronically from non-secure systems (e.g., none of these computers is connected to the Internet).
- All computer disks entering the AOC are checked for viruses.

Thus, there is basically no way to "hack" into the system from the outside if everyone does his job properly. Even a corrupted insider would have trouble because of a couple of artifacts of the design of the AOC. First, the AOC is not fully automated; as a result, information passes through several sets of hands and is scrutinized by many eyes, partly to catch innocent errors that occur routinely in inputting data to computers. Deliberate distortion of data is likely to be caught at roughly the same rate as innocent errors. Second, much planning is still done by hand, at least as a backup to the automated systems.

RANDMR1016-10.4

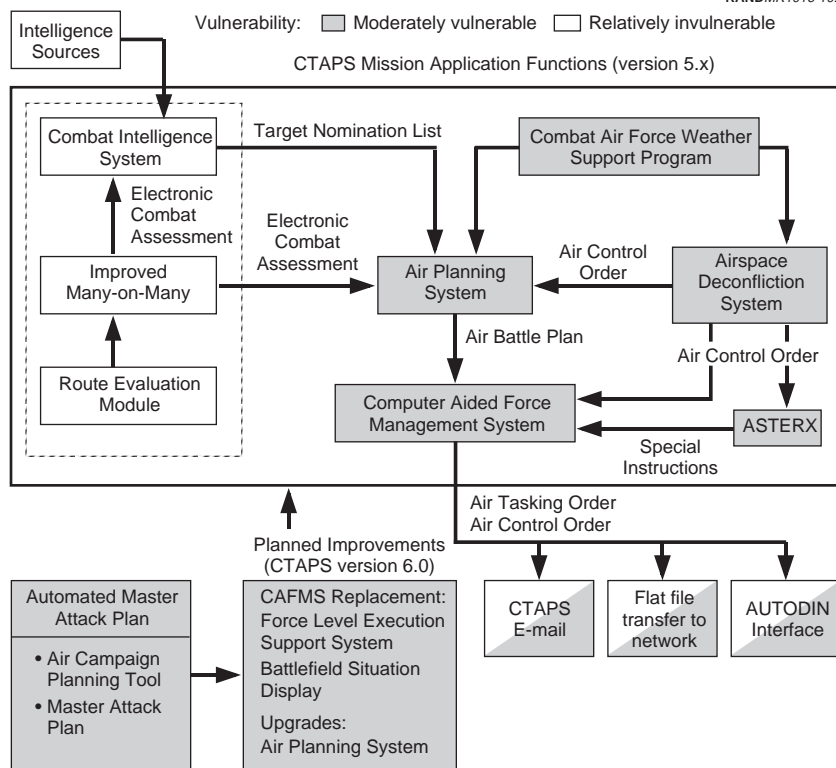


Figure 10.4—Potential Computer Vulnerabilities in the AOC

Ironically, the “inefficient” human involvement in the planning process provides an important hedge against computer hacking attacks, limiting the likely effect of such attacks to modest delays in generating and disseminating directions to the forces. Interestingly, maintaining enough skilled human planners to take over in an emergency would appear to be a prudent measure simply to protect against computers going down from natural causes.

If the AOC and similar military command centers evolve along the lines presently planned—the introduction of the Global Command and Control System and the Global Command and Support System, for example—the basic vulnerabilities could get somewhat worse. In

particular, the *consequences* of disrupting or corrupting computer networks could be more severe because the various command centers will rely on more-common software, and that software will allow integration across *applications*, not just databases. Thus, the effects of malicious code, perhaps triggered by a virus somehow introduced into the network, could have more far-reaching effects. Moreover, because the new systems will be standard commercial software, there is little chance of an independent check on the safety of the code. The burden will be on the software manufacturers to make sure the codes are “bug free.” On the other hand, the same sort of protections that we described earlier for the AOC still ought to work if they are applied properly (e.g., no connections with nonsecure communications or computer networks).

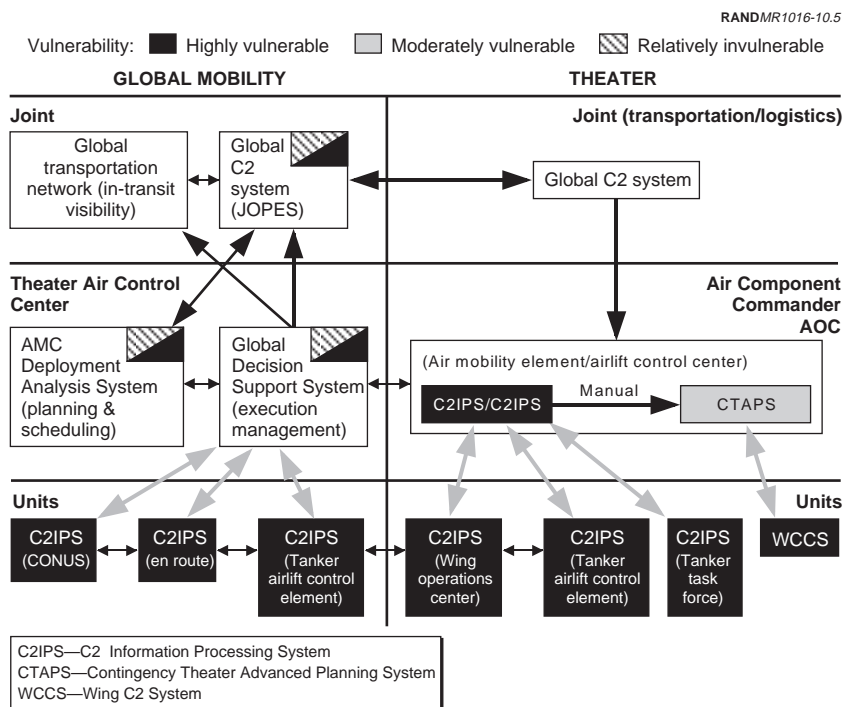


Figure 10.5—Potential Computer Vulnerabilities in the Support and Sustainability Network

If there is a danger from computer attacks, it is more likely to be at the Wing level, where controls could be looser. In the meantime, the best way to attack an AOC appears to be the direct way: Blow it up.

The story is quite different on the support and sustainability side. Figure 10.5 shows that some of the computers in that part of the system, particularly the Command and Control Information Processing System (C2IPS), which is widely used throughout the Air Force, are potentially very vulnerable to attack. The main difference is that the C2IPS computers are not always isolated electronically from outside nonsecure networks, and the data are not always encrypted. As a result, the system is potentially vulnerable to the whole array of hacker tricks. Even worse, other computer systems that would otherwise be considered secure are linked to C2IPS and could be corrupted accordingly. Thus, the entire computer network that services support and sustainability operations could be compromised, with key portions degraded or out of service.

However, that need not be as catastrophic as it sounds: In fact, it is not all that different from what actually occurred during Operation Desert Shield when Air Mobility Command's (AMC) computers went down for benign reasons. AMC planners and users in the field planned operations manually, working together closely, and made do. The operations were successful, and delays were minimal. Again, the key was having skilled human backups available. *Only if AMC goes to a highly automated, Federal Express-like system and drastically cuts manpower would computer vulnerabilities appear to pose a serious threat.*

Communication System Vulnerabilities. Future Air Force communication networks will be very different from those of the past (i.e., the Cold War years), when the Air Force and the Department of Defense in general invested heavily in dedicated, secure, resilient communications. In the future, while its demands for communication capacity are likely to increase dramatically, the Air Force will be obliged to rely primarily on commercial communication systems. The danger is that commercial systems are not typically configured to withstand jamming, physical attacks against critical facilities, or other standard tricks of the electronic warfare trade. Unless the collective set of future commercial systems can be configured into an adaptive network that is robust against most forms of interference,

the Air Force is likely to face critical shortfalls in communication capacity in all but the most benign environments.

Our analysis identified two major types of communication vulnerabilities. The first applies primarily to combat forces operating in a particular theater. Figure 10.6 shows the kinds of communication links used in current theater air operations. Some of the critical links are vulnerable to cheap, mobile, low-power jammers that would be easy for an enemy to obtain and use and difficult and expensive for the United States to suppress or otherwise counter. The result could be a substantial reduction in communication throughput rates. *Moreover, this problem is likely to get worse in the future.* The primary problem is *intratheater* communications because that is where mobile jammers are likely to be most effective. If that problem can be solved, more robust networks of commercial landlines and satellites can take over to move information over long distances if need be.

The second kind of problem relates primarily to the larger set of communication systems that the Air Force relies on to support sus-

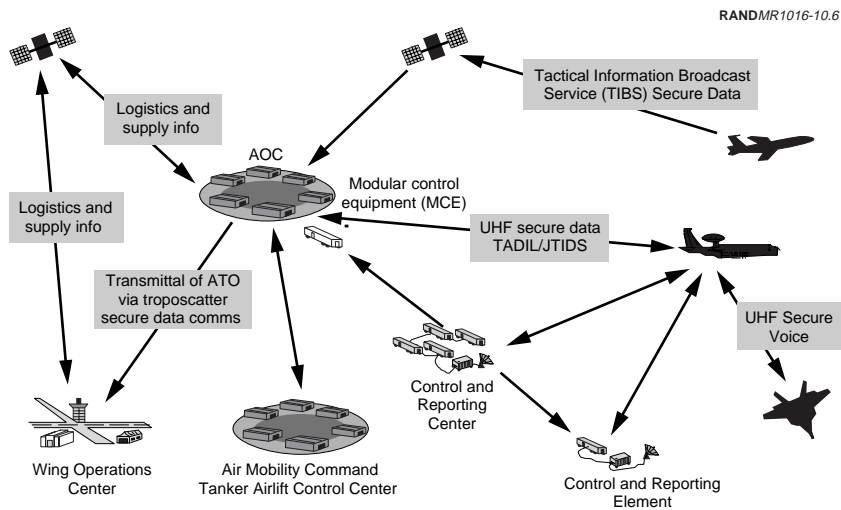


Figure 10.6—Some Typical Theater Air Communication Links

tainment operations. One key system is the Public Switched Network (PSN), which—as Figure 10.7 shows—is important to many other users as well. The PSN has a number of potential vulnerabilities.³ The two sorts of attacks that appear most threatening are physical attacks (e.g., high explosives) against the end office, trunk lines, or base point of presence for the PSN and computer hacking attacks on a switch or digital cross-connect. Of the two types of attacks, the physical attack appears easier to execute, harder to defend against, and more effective in a range of circumstances. The result could be a PSN communication outage for a particular military base or entire region of the country for some period of time.

Other Types of Vulnerabilities. Other types of systems are potentially vulnerable to attack as well. One of the most important is GPS. GPS, in its current form, is highly vulnerable to small, cheap, low-power jammers. Denying or degrading navigation data to various users could have diverse and wide-ranging effects. One of the most

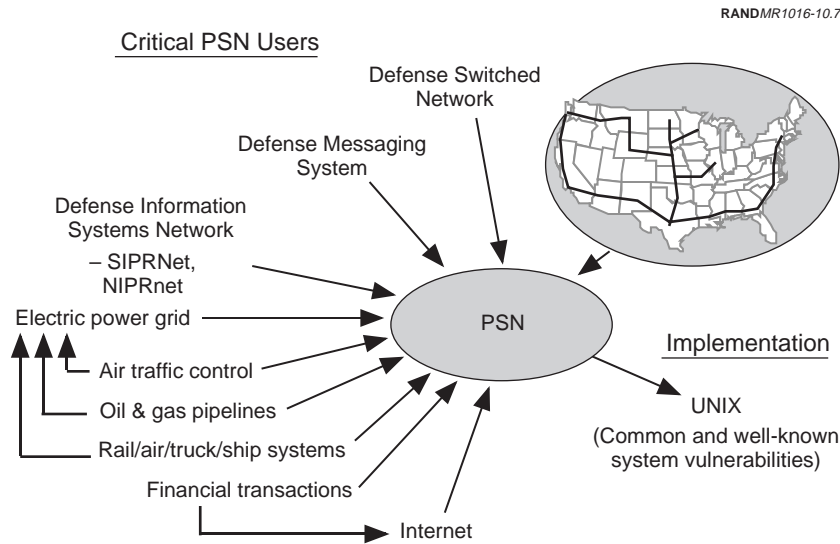


Figure 10.7—Air Force Systems Rely Heavily on Defense and Public Information Infrastructure

³See Feldman (1997) for a detailed discussion.

obvious and potentially important is degrading the accuracy of precision-guided weapons that rely on GPS. Figure 10.8 shows how GPS-guided weapon accuracy could degrade depending on the power of the jammer, the quality of the weapon's guidance system, and the quality of its GPS receiver. In the particular example highlighted, a jammer that could fit in the back of a jeep could reduce the accuracy of a missile equipped with a relatively high-quality GPS receiver and an affordable inertial measurement system by hundreds of meters, which would certainly remove it from the "precision-guided" category of weapons.

Identifying the most cost-effective solution to the GPS jamming problem involves exploring the trades that Figure 10.8 suggests in more detail. The issue, obviously, is balancing the effectiveness of better inertial systems and/or more jam-resistant GPS components against their cost. Intensive work on this problem is under way throughout the defense community. Resolving these issues is the reason that this study concluded, as others have, that determining how far it is practical to go in reducing the cost of high-quality all-inertial navigation systems should be one of the high-priority items for research and development funding.

Using countermeasures to try to defeat various types of sensors (e.g., surveillance and reconnaissance systems, weapon seekers) has been standard practice throughout the history of warfare, and the never-ending game of "hider versus finder" continues with even more vigor. Concealment and deception continue to be important arrows in the defender's quiver and are likely to become even more important as attackers seek increasingly detailed information to find targets and identify them accurately, locate critical aimpoints for precision-guided weapons to try to hit, and assess the damage of earlier attacks.

DIRECT IMPACTS OF INFORMATION DISRUPTION

If an enemy were to exploit these vulnerabilities, the effects could manifest themselves in a number of ways:

- loss or distortion of information
- delays of various sorts
- reduced weapon effectiveness

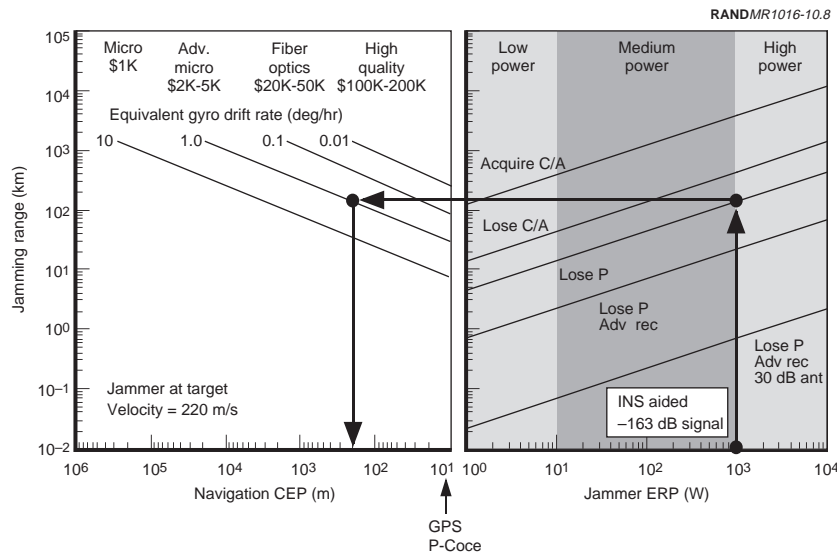


Figure 10.8—GPS Jamming Can Reduce Weapon Accuracy Substantially

- reduced sortie rates
- reduced target discrimination capability.

All aspects of air operations—force planning, force direction, force execution, and support and sustainability—could be affected.

Figure 10.9 briefly summarizes the immediate effects of the spectrum of possible attacks on information systems on the various processes involved in managing and conducting Air Force operations. The magnitudes of the effects are based on the detailed analysis presented in the RAND study described earlier (Buchan et al., forthcoming), and more-detailed results and the supporting analysis are available there. Note that these results assume that the Air Force continues to operate more or less the way it does today and is likely to in the reasonably near future. Some kinds of changes (e.g., drastic reductions in the number or skill levels of personnel in the AOC, logistics planning cells, or field stations) *could dramatically increase the magnitude of some of the adverse effects of information attacks* (e.g., some delays could be much longer because recovery would be much more difficult).

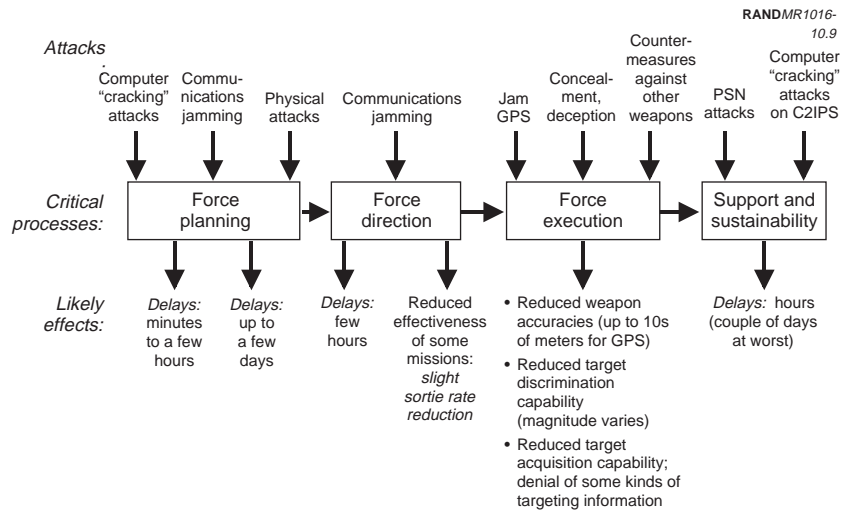


Figure 10.9—Potential Effects of Attacks on Information Systems

OPERATIONAL IMPLICATIONS

What really matters, though, is what effect this array of delays, disruptions, or outright loss of information might have on the outcome—success, failure, and cost—of a range of Air Force operations. In our analysis, the operational world appeared to divide into two major categories (excluding large-scale nuclear conflict): major conventional campaigns and everything else, where “everything else” includes a large spectrum of possibilities (e.g., peacekeeping, humanitarian assistance, hostage rescue). Interestingly, our analysis suggested that—unlike in the traditional force planning world, in which major campaigns are the stressing cases and other types of operations tend to be “lesser-included” cases, in terms of information vulnerabilities—*some kinds of lesser operations are actually more likely to be the stressing cases.*

Major Conflicts

The reason that the kinds of effects of information disruption described in Figure 10.9 have little impact on the outcome of major

campaigns is that, if one accepts the size, effectiveness, and deployment rates projected for future U.S. military forces, the U.S. should be able to bring so much high-quality firepower to bear quickly that its sheer mass simply overwhelms all other factors in the military equation. The delays and imprecision introduced by interfering with U.S. information-related systems generally appear to be mere “speed bumps”: They hardly even slow the U.S. forces down.

Figures 10.10 and 10.11 are typical of the results that we found and illustrate the insensitivity of campaign outcomes to even dramatic information disruptions. Figure 10.10 shows the effects of delays in introducing U.S. air forces into a major campaign and the reduced sortie rates that might result from delays in shipping spare parts to the theater. In this particular example, the U.S. objective is to prevent invading enemy forces from reaching a certain point on the ground. In the first case, even a two-week delay in introducing air forces would not have been sufficient to change the outcome, and the delays associated with information attacks are likely to be on the order of hours to a very few days at most. Similarly, sortie-rate reductions would have to be massive—much greater than disruption of the information systems supporting the logistics network would be likely to cause—to have much discernible effect on the overall campaign. The reason is that there is enough firepower available from other sources (e.g., Army forces, in this case) to take up the slack.⁴

Similarly, Figure 10.11 shows the effect of disrupting the planning process. It shows the number of targets killed in a specified amount of time as a function of how frequently a new targeting plan can be generated. We varied the Air Tasking Order generation rate from daily, which reflects current practice, to “infinite” (i.e., the “static” case in the figure), which essentially means that the United States begins the campaign with a single set of targets and a battle plan and never adjusts them over the course of the campaign. Note that, even

⁴That, of course, begs the question of what would happen if the Army forces were also delayed and/or disrupted by information attacks. The results then became very sensitive to metaphysics (e.g., How tough are the attackers and the indigenous defenders?) and model artifacts (e.g., How well does the model handle maneuver warfare? Answer: Not very).

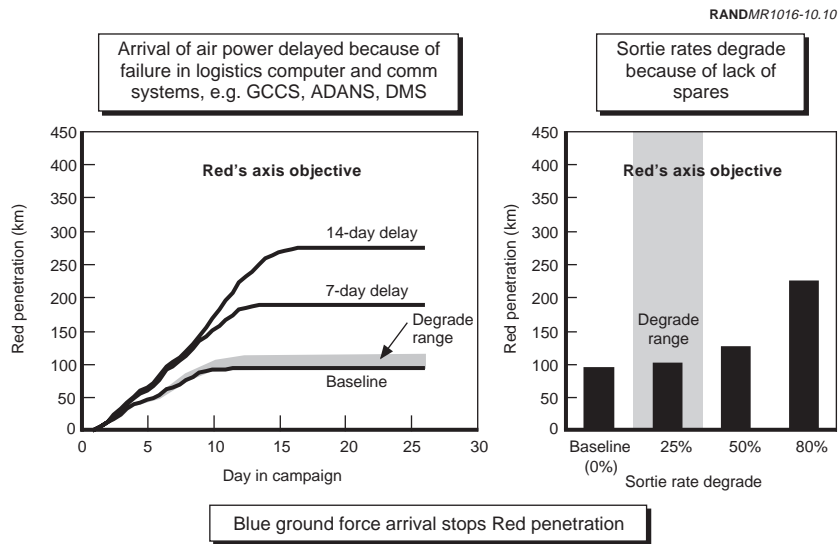


Figure 10.10—Arrival Delays Have Little Effect

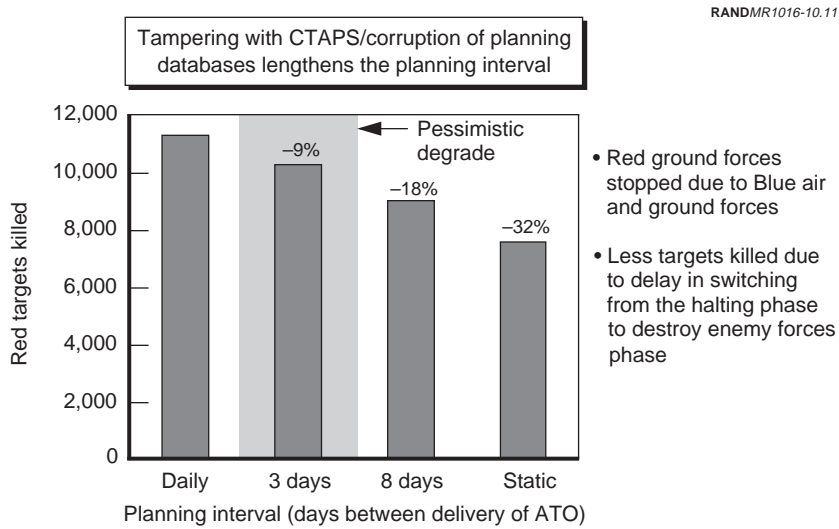


Figure 10.11—Planning Cycle Delays Have Only Minor Effect

in the latter extreme case, the number of targets killed in a fixed amount of time only drops by about 30 percent. In a less extreme but still pessimistic case, the reduction in targets killed is less than 10 percent.⁵ Thus, even severe degradation of the planning process would have only a modest impact on the outcome of the campaign. Examining why the effects of information disruption are no greater than they are provides useful insight into more general problems of the value of information in military campaigns and helps put the information vulnerability problem in perspective.

Interestingly, these results are probably “real” and *not simply model artifacts*. Instead, they are *consequences of the nature of large-scale campaigns* and, as noted earlier, *scenario assumptions* (e.g., weapon system effectiveness, force deployment rates, campaign objectives for both sides). In the first place, the postulated campaign is relatively straightforward (and typical). The aggressor’s objective is to seize territory in a neighboring country, so it launches an invasion. Accordingly, it needs to overcome the defender’s military forces and perhaps also be able to destroy or coerce its government by threatening selected national infrastructure or political leadership targets. The objective of the defenders (the victim country and its U.S. allies) is similarly straightforward: Halt the enemy invasion and prevent the aggressor from being able to damage or coerce its neighbors, preferably at minimum cost (i.e., in lost lives and equipment) to the United States and its allies. Thus, to win, the defenders basically have to destroy enough of the right kinds of targets in a timely manner.

That means that, if the defenders can bring enough effective firepower to bear against the right targets, they win, and that is exactly what is happening in these scenarios. Based on current Department of Defense planning guidance, the U.S. forces are assumed to be so capable and so large that they simply overwhelm the attackers. Moreover, assuming the United States has had the foresight to prepare for this potential conflict well enough in advance (a criterion that the United States barely met vis-à-vis Iraq in the Gulf War), it should have a reasonable list of the aggressor’s major fixed installa-

⁵In this example, the AOC is assumed to be destroyed on the first day of the war and reconstituted in three days. It then continues to operate at drastically reduced efficiency (or, conceivably, is periodically destroyed and reconstituted again) for the duration of the campaign.

tions, a pretty good picture of the enemy's military forces, and an *a priori* understanding of possible invasion routes at the start of the war. That should provide a major leg up on the targeting problem. Missing are likely to be

- individual mobile targets, particularly those that employ concealment and deception techniques⁶
- fixed targets whose function can be effectively disguised
- detailed knowledge of vulnerable points on some classes of targets.

Thus, the reason that the United States does so well in the cases shown in Figure 10.11 is that its forces are large and capable and already have most of the information that they need to conduct the campaign effectively. Delays in getting materiel to the theater do not matter much because there is so much materiel either available or on the way. Reducing sortie rates does not matter much for the same reason. Not even a failure to be able to adjust battle plays rapidly would have much effect as long as the initial plan was well-constructed. There is some lack of efficiency due to "overkilling" high-priority targets if the defenders cannot assess the effectiveness of their earlier attacks accurately and adjust the allocation of their forces accordingly. That is why the number of targets killed in Figure 10.11 can drop by 10 to 30 percent, depending on how frequently battle plans can be "tweaked." Thus, in this example, even massive interference with U.S. information systems can reduce the efficiency of the campaign, lengthen it somewhat, and raise its cost, but the final outcome is never in doubt.

Reassuring as that result might be from the U.S. point of view, even if the analysis is correct, it raises a couple of key questions:

- What if U.S. forces are not so large and robust?
- Could the cost of "victory" become excessive?

The first is likely to come about in any case as the defense budget continues to shrink but is particularly reasonable to consider if

⁶Note, however, that a massive mobile force, such as an invading armor force, is hard to conceal when it launches an attack. That is why the most effective countermeasure for an invading armored force is still likely to be the classical approach: Develop countermeasures to reduce the accuracy of the enemy's weapon guidance systems.

analyses continue to show that the services are buying more fire-power than they need. The second could occur not so much because the U.S. populace is perceived to be casualty-averse, which is probably a myth, but because, in the post-Cold War world, few potential quarrels are likely to be viewed as important enough to vital American interests to justify spilling much American blood.

To address these questions, we parametrically reduced both the size and complexity (i.e., the availability of alternative weapon systems using different technology to take up the slack if an enemy counters one type of system) of U.S. forces and assessed the cost of the campaign in terms of estimated U.S. casualties. To assess the likely impact of increases in U.S. casualties, we drew on the work of one of our colleagues (Larson, 1996) who had done a historical analysis of U.S. public support for past wars as a function of the level of U.S. casualties. We then tried to identify combinations of force reductions and changes in composition that could make them vulnerable enough in terms of increased U.S. casualties for information vulnerabilities to matter.

Figures 10.12 and 10.13 show some examples of the results of that analysis and suggest combinations of conditions under which information vulnerabilities could become important. Both cases show the effect of GPS jamming as forces are reduced. In the first case, alternative precision-guided weapons are available (e.g., laser-guided bombs in this particular case) that could partially replace GPS-guided weapons if someone were to jam GPS. In the second, there are not. Campaign duration is plotted as a surrogate for casualty levels. (We estimated casualties as a function of the length of the campaign to make the correlation). The shading on the figure is based on the casualty levels derived in the Larson analysis.

Figure 10.12 suggests that, absent interference with U.S. information systems, the war is unlikely to last long enough for casualties to become an issue until U.S. forces are reduced by at least 25 percent.⁷ In a severe GPS jamming environment (i.e., where GPS essentially

⁷For the purposes of this example, cuts were assumed to be uniform across all Air Force systems to get a rough idea of how large force cuts had to be (e.g., 1 percent versus 10 percent versus 50 percent) before they started to matter. In practice, of course, force cuts are likely to vary widely, some types of systems being largely untouched while others are eliminated entirely.

does nothing to improve the accuracy of weapons in the vicinity of the target), the forces could only shrink a few percent (10 percent) before casualties might become a matter of concern, and a 25 percent cut in forces could cause real problems.

The reason that the results shown in Figure 10.12 are not worse than they are is that other precision-guided weapons in the inventory based on different technology—and, therefore, not vulnerable to the same countermeasures—are partially offsetting the loss of the GPS-guided weapons. In the absence of these alternative weapons, the effects of the GPS degradation are much more severe, as Figure 10.13 shows. The force can tolerate only a slight degradation in GPS effectiveness before U.S. casualties could become a concern. In fact, while the analysis shows that a combination of force reductions and a less diverse weapons stockpile would have to occur before information vulnerabilities become a serious concern, comparing Figures 10.12 and 10.13 suggests that the results are more sensitive to the nature of the weapon inventory than to the size of the force. Thus, *maintaining a diverse inventory of weapons that rely on different technologies appears to be particularly important in reducing the impact of weapon vulnerabilities.*

Table 10.1 summarizes some of the impacts of several specific kinds of information vulnerabilities on large-scale campaigns. In general, in analyzing the possible effects of information vulnerabilities on major campaigns, we came to several general conclusions, some of which we were able to quantify to a degree and all of which seemed to pass the “common sense” test:

- If the U.S. maintains the kind of large, capable conventional forces that it currently plans and if they generally operate the way they are supposed to, the United States will have so much high-quality firepower available that potential information vulnerabilities will have little effect on a major conventional campaign.
- Only if U.S. forces are reduced substantially in size (i.e., more than 25 percent or so) and if technical diversity and U.S. policy-makers are particularly concerned about casualties will information vulnerabilities have a major impact on U.S. capability to fight and win major conventional wars.

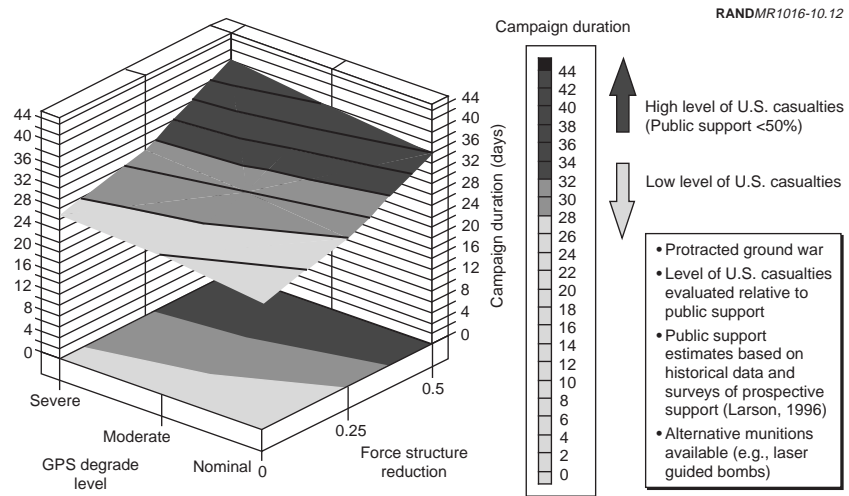


Figure 10.12—Maintaining Multiple Types of Munitions May Reduce the Impact of the Vulnerability of Specific Types of Systems

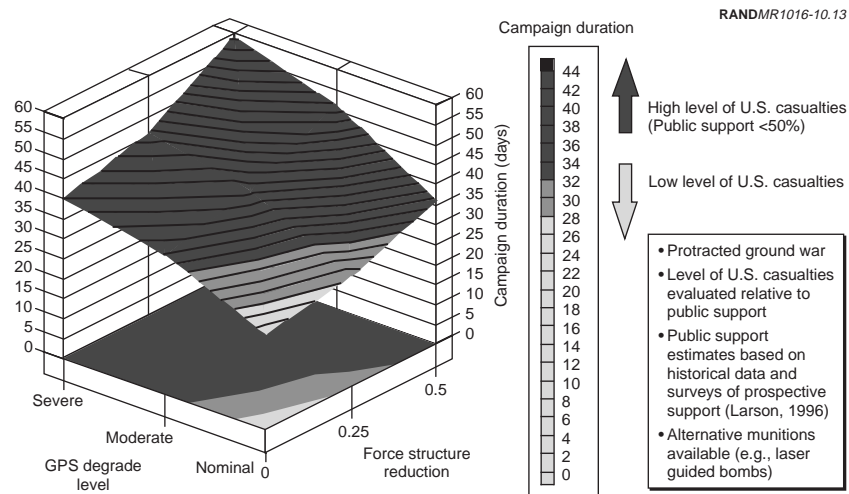


Figure 10.13—The Combination of Reduced Force Structure and Simplified Weapon Mix Can Substantially Increase the Impact of Information Vulnerabilities

Table 10.1
Summary of Information Vulnerabilities and Their Impact on the Outcome of Major Conventional Campaigns

Vulnerability	Impact
Air power deployment	U.S. objectives at risk if delay much greater than 2 weeks, if adversary's break rate high.
Ground power deployment	U.S. objectives at risk if delay greater than about 2 weeks, if adversary's break rate high.
Air Tasking Order planning	Reduces killing capability and slightly lengthens campaign, but does not put U.S. objectives at risk.
GPS jamming	May add high risk to operations unless alternative technologies are available.
Denial and deception (hindering battle damage assessment, target discrimination)	Waste resources (munitions and sorties) and may lengthen campaign.
Combined logistics delay and GPS jamming	No significant impact if alternatives to GPS munitions are available.
Combined force structure reduction with logistics delay	U.S. objectives at risk if force structure reduced by more than 25 percent.
Combined force structure reduction with GPS jamming	U.S. objectives at risk if force structure reduced by more than 25 percent, assuming alternatives to GPS munitions are available. Worse if no GPS alternatives.
Combined air power and ground power deployment delays, key technology failure (SFW), and break rate sensitivity	Objectives at risk if: 1. Both air and ground power delayed by more than about 7 days. OR 2. Low effectiveness of key technology (SFW) and either air or ground power delayed by a few days. OR 3. High break rate of enemy forces and either air or ground power delayed by a few days.

SOURCE: Buchan et al. (forthcoming b).

Among other things, these findings suggest that, while major conflicts are likely to remain the stressing cases for overall Air Force combat forces and, therefore, remain the basis for structuring the overall force, *other types of operations and situations may represent the stressing case for information-related systems.*

Lesser Operations

If information vulnerabilities are ever going to be critical, our analysis suggested that it is most likely to occur in some kinds of smaller-scale operations rather than all-out war. Large-scale conflict has never been the only function of the military or the only external security concern of major powers, but in the post-Cold War world, lower-level military operations have become both much more common and a more important part of U.S. foreign policy (e.g., Bosnia, Somalia, postwar Iraq). Moreover, since some of them can be relatively open-ended, and several may be going on simultaneously, they can collectively tax U.S. military resources considerably.

The problem with characterizing low-intensity conflicts and lesser operations is that they represent such a diverse set of possibilities, as Table 10.2 suggests. The possible problems to be solved are enormously diverse, as are the tasks that need to be performed to deal with them. Some are relatively straightforward. Others are extremely complex. Many are quite benign—unopposed humanitarian relief, for example—although even that is not a foregone conclusion. Still others, while not necessarily benign, are not terribly challenging either. However, as Table 10.2 suggests, some such “lesser” operations share common characteristics that could make them stressing cases from an information-planning point of view and, therefore, potentially sensitive to potential vulnerabilities in information-related systems:

- Sensitivities can be greater than in major campaigns:
 - Time delays sometimes matter more.
 - Political sensitivities are likely to be higher, so the consequences of any miscue are likely to be greater.
- There may be no analog to overwhelming force.
- Information demands are likely to be out of proportion to the other dimensions of the conflict:
 - A considerable amount of information is likely to be required even for a “small” operation.
 - Much of that information may be of an unusual nature (e.g., refugee numbers and locations), involve unfamiliar areas (e.g., Rwanda), and/or be hard to come by (e.g., which way doors open in a foreign embassy).

Table 10.2
Characteristics of Some Generic Types of Low-Intensity Conflicts and Lesser Operations—Implications for Information Sensitivities

Type of Operation	Examples	Characteristics
Moderate-scale direct action	Panama, Grenada, Haiti	<p>Involves a substantial force and at least some level of combat</p> <p>Has limited military operational objectives (e.g., capture Noriega; free “hostage” students and protect selected political figures), but may have broad political objectives (e.g., topple a government)</p> <p>Typically involves short time commitment for the bulk of U.S. forces</p>
Raids:		
Punitive	Libya, parts of Operation Southern Watch in Iraq	<ul style="list-style-type: none"> • Limited forces involved, but force is used • Timely information on targets and defenses required
Preemptive	Israeli attack on the Iraqi nuclear reactor at Osirak	Collateral damage and a spectrum of political sensitivities are typically involved (<i>potentially high cost of either military or political “failure”</i>)
Rescue missions:		
Hostages or prisoners	Iran, Entebbe, Son Tay	<ul style="list-style-type: none"> • Information usually at a premium • Time lines can be very tight • Rescuers probably “outgunned” • Reaching hostages and escaping likely to be difficult • Politics may be extremely delicate
Combat search and rescue	Gulf War search and rescue	Routine (and difficult) operations during combat—opposed, generally behind enemy lines, may or may not have good information on location of personnel to be rescued

Table 10.2—Continued

Type of Operation	Examples	Characteristics
U.S. personnel in combat zones or other dangerous situations	Liberia	<ul style="list-style-type: none"> • May or may not face opposition • Information is important and may be difficult to get • Usually relatively short duration; timeliness likely to be important
Noncombatants of various sorts (e.g., threatened indigenous populations)	Notable special operations during the Cold War	<p>Similar to the above:</p> <ul style="list-style-type: none"> • operation may be larger scale • politics likely to be more complicated
Disaster relief	Earthquakes in Soviet Union during later stages of Cold War	<ul style="list-style-type: none"> • Generally benign environment • Premium on information for efficiency
Humanitarian assistance		
Normal	Rwanda, early stages of Somalia operation	<ul style="list-style-type: none"> • Could be opposed (e.g., early days of Somalia) • Identifying, locating, and reaching those in need can be a challenge • Timeliness generally matters • Operation can be large scale • Politics can be complicated
With “mission creep”	Later stages of Somalia operation	<p>Can combine the most challenging features of humanitarian assistance and raids or hostage rescue</p> <ul style="list-style-type: none"> • environment, time-lines, and opposition all can be very demanding • premium on information • politics extremely delicate

Table 10.2—Continued

Type of Operation	Examples	Characteristics
Peacekeeping Normal “Information as a weapon”	Bosnia, post-war Iraq Bosnia	Combines complex and delicate politics with difficult military problems Information, implicitly backed by force, can provide powerful negotiating leverage
Peacemaking	Northern Ireland	<ul style="list-style-type: none"> • Peacekeeping with “attitude”; peacemaking is more proactive • Usually involves a heavier element of coercive military force
Insurgency	Kurdish areas of Northern Iraq, U.S. support of Afghan rebels, support for the Contras in Nicaragua	<ul style="list-style-type: none"> • Long-term commitment • Generally, militarily weaker than dominant force or government • Politics central • Information central
Counterinsurgency	Early operations in Vietnam and Laos	The flip side of insurgency; most of the same features except there is a presumption of superior forces available
Nation building	Haiti	Combines features of counterinsurgency, peacemaking, and peacekeeping
Counterterrorism	Continuing operations of various sorts	<ul style="list-style-type: none"> • Shares many of the characteristics of raids, hostage rescue, even counterinsurgency • Information critical and hard to collect • Force usually has to be measured • Legal and political constraints • Timeliness usually critical
Counternarcotics/ interdiction of contraband (e.g., nuclear materials or weapons)	Narcotics interdiction operations	Similar in many ways to counterterrorism; has similar sensitivities

Table 10.2—Continued

Type of Operation	Examples	Characteristics
Counternarcotics/ interdiction of contraband (e.g., nuclear materials or weapons)	Narcotics interdiction operations	Similar in many ways to counterterrorism; has similar sensitivities
	Hypothetical raids against the sources	Has both “offensive” and “defensive” components
Critical missions within larger campaigns	Scud hunting during Operation Desert Storm	<ul style="list-style-type: none">• Missions take on a life and importance of their own; separate “scorekeeping”• Timeliness is frequently important• Can be information intensive• Overwhelming force may not be an option• Frequently have political dimensions

SOURCE: Adapted from Buchan et al., forthcoming (b).

- As a result, for many classes of operations, success is likely to be extremely sensitive to the quality, quantity, and timeliness of information. Accordingly, enemy interference with information systems is likely to have a much greater impact than it would on large-scale conflicts.
- Defining and deciding what constitutes “victory” and how to measure success and failure can be much more difficult.

In large campaigns, the very scale of events tends to wash out nuances. In lesser operations, the reverse can be true: The smaller scale of events can *accentuate* nuances. Thus, even minor failures and modest casualties can take on disproportionate importance, and many of the problems that barely mattered in large-scale campaigns can be central to the success or failure of lesser operations. A useful analogy might be the comparison between mission-level and campaign-level analysis. Lesser operations frequently may be likened to missions; indeed, as Table 10.2 suggested, particular classes of missions within a larger campaign (e.g., Scud hunting in Desert Storm) may take on a life and political significance of their own independent of their contribution to the overall military campaign. In fact, the Scud example illustrates the larger point about information sensitivity. The failure of the Scud hunt had virtually no effect on the outcome of the military campaign but received considerable attention because of its political implications and, under other circumstances, *could* have been important. Thus, the Iraqis’ routine operational practices (e.g., mobility, concealment, deception) to deny the U.S. information about the locations of its mobile missiles was certainly successful.

Similar tactics or other countermeasures might be equally effective in the future, particularly since some of the tactical problems in Table 10.2 probably fall in the “too hard” category for purely technical solutions anyway (e.g., sorting out urban guerrillas from the rest of the population, locating concealed nuclear weapons, differentiating refugees from bandits). Accordingly, these kinds of situations might provide more stressing cases to test the effectiveness and robustness of U.S. information-related systems. Unfortunately, they are necessarily less tidy and well-defined than more traditional campaigns, but that is part of the challenge of planning in the post-Cold War world.

REDUCING VULNERABILITIES AND COPING WITH THEIR EFFECTS

Deciding what to do about all this is obviously a very complex, multi-faceted problem. To establish priorities in reducing or eliminating information vulnerabilities, one has to decide how serious the problems are, how severe the threats are likely to be, whether adequate technical and operational solutions are available, and whether those solutions are affordable. In examining the problem, we found several general trends that affected the way we approached choosing solutions:

- No single set of vulnerabilities was so overwhelmingly important that they demanded top priority, and no threats were so compelling that they dominated the analysis.
- Costs fell into three “bins”: cheap (and, therefore, potentially attractive enough on first principles to require little additional analysis), very expensive (and, as a result, probably too expensive in an austere fiscal environment absent a really compelling need), and somewhere in between (and perhaps worth a more detailed cost analysis for particular options that satisfied the other criteria).

More fundamentally, we found that traditional concepts of relying on intelligence to define threats and provide strategic and tactical warning of “information attacks” and then trying to deter or defeat such attacks by threats of retaliation are particularly inappropriate for coping with attacks on information systems. Thus, Cold War nuclear metaphors in particular do not apply to this sort of combat. Instead, we found that the most effective general approach to information attacks appears to be to *defend as well as one can afford to and be prepared to adapt and recover as quickly as possible if the defenses fail*.

Why Intelligence Assessments and Warning Concepts Are Largely Irrelevant

There are several reasons why intelligence assessments to identify potential threats to Air Force information systems and attempts to provide strategic or tactical warning of such attacks are likely to be inadequate and, therefore, why relying on such intelligence support

to protect operations would be very risky. Most of them fall into one of two general categories: *ambiguity* and *timeliness*.

Ambiguity. Capabilities to disrupt information systems are so widespread that virtually any potential enemy, be it a nation-state, a subnational group (e.g., a terrorist or criminal organization), or even an individual malcontent, could mount some kind of information attack. For example, computer hacking is virtually universal, particularly since there are no geographic limits to its “reach.” Moreover, there are undoubtedly “hackers for hire” on the world market who will work for anyone willing to pay for their services. Thus, threat assessments cannot narrow the field of potential enemies much. Neither can the actual source of an attack be identified with confidence, since the national origin, or even the actual identity, of an individual hacker might not tell much about who was behind the attack, and the attack itself could be launched from any geographic point that turned out to be convenient.

The same is true of other kinds of attacks as well. The ability to launch some kinds of physical attacks, either overt or covert, on critical information nodes is virtually universal. Similarly, access to jammers of various sorts is quite widespread. Even more-exotic weapons, such as HPM devices, may become widely available on the international arms market to “upscale” adversaries, once the weapons are available at all.

One of the reasons that the ability to attack information systems is so universal is that the tools are so cheap. Developing or employing a cadre of computer hackers or a commando squad capable of blowing up key installations is cheap. On the other hand, gathering the information to make such attacks truly effective is not necessarily either easy or cheap; indeed, it may be easy to overestimate the danger of really focused, militarily effective information attacks.

Complicating intelligence assessment and warning still further is the fact that both the capabilities and actual preparations to launch attacks on information systems are likely to be virtually invisible. There will probably be no visible indicators. There is no “information equivalent” to a buildup of missiles, for example, or specialized observable activity (e.g., the equivalent of a nuclear test) to observe. Thus, a competent adversary that was trying to be covert might be able to cover his tracks completely, particularly in view of

the competing demands on the U.S. intelligence community. As the cliché goes, “The absence of evidence is not evidence of absence.”

On the other hand, remaining covert does pose some risks for a potential attacker. It cannot really test its capability to disrupt U.S. information systems without risking tipping its hand and compromising its own capability. That is particularly true if its strategy relies, as it would have to if the United States is taking prudent protective measures, on “perishable” chinks in the U.S. armor, such as a corrupted insider or laxity in enforcing good security procedures. Ironically (and significantly), even a test of offensive capabilities that could be disguised to look like a natural failure is likely to prompt the victim to take corrective action. Even intelligence-collection efforts to identify exploitable weaknesses might get the U.S.’ attention and risk compromising future offensive operations against U.S. information systems. Such collection efforts can be difficult and expensive in any case, so the added risk of compromise just increases the burden on the attack planner. Ironically, the defense has an easier time in this regard. It really does not require a detailed assessment of who is threatening its systems or why. All it needs is a “wake-up call” to remind it that implementing reasonable protective measures for its information systems is a prudent thing to do in a hostile world. Even relatively imprecise intelligence is good enough to do that. Conversely, very detailed intelligence information would not provide that much more information that was operationally useful.

Timeliness. The time scale of attacks on information systems, particularly electronic attacks (e.g., computer hacking attacks), is another serious problem in developing a response strategy based on reacting to tactical warning. The attacks can simply happen too fast. The damage is done before the defense can react. Notice that that situation contrasts sharply with the Cold War nuclear standoff between the Soviet Union and the United States, in which either side might have as much as a half hour’s warning of a missile attack in which to launch its vulnerable intercontinental ballistic missiles, bombers, tankers, and mobile command and control assets. There is no analog for information attacks.

Time scale is also an issue for Air Force operations themselves. Depending on what kind of operation it is, times of hours, days, or weeks can be important even for operations that last much longer. That means that events can move rather rapidly, and responses to

information attacks must keep pace. That is why responses to information attacks that may be appropriate for peacetime are likely to be inadequate in an operational situation. For example, the Air Force and others currently place considerable emphasis on tracking down and arresting computer hackers who try to break into sensitive computer systems. That is perfectly appropriate for peacetime, when time and resources favor the victim of the attack, but is going to be of limited value in wartime. In the first place, any wartime hacker who is incompetent enough to get caught in spite of all his inherent advantages—e.g., mobility, anonymity, choice of geographic locations, resources at his disposal—deserves what he gets. Moreover, even in peacetime, tracking down highly skilled hackers has often taken months. That is too long to be useful in most operational situations. The same is true of other kinds of situations, such as fixing the blame for—or even determining the cause of—bombings and airline disasters. Thus, attackers are likely to be neither defeated nor deterred.

Implications. These factors all suggest several general conclusions about the role of intelligence and warning in defeating attacks on Air Force information systems:

- Neither intelligence threat assessments nor various warning concepts are likely to be of much use in defending against attacks on information systems if the opponent is competent.
- Because there is likely to be little or no useful warning of an attack on information systems, the first thing to do is protect important information systems as well as one can afford to.
- Because defenses are inherently imperfect and information systems are subject to various kinds of natural failures in any case, having the capacity to recover from an information system disruption is necessary *even in the absence of an information attack threat.* Thus, once a disruption occurs, the cause does not matter. Repairing the damage is what counts. Also, in most operations, except for relatively bizarre “catalytic war” scenarios,⁸ there is likely to be little ambiguity about the source of

⁸The “catalytic war” concept was discussed periodically during the early days of nuclear weapons and became a staple of Cold War melodramas. It involves a third

attacks on information systems, since these attacks are very unlikely to occur in a political and military vacuum.

The real test of intelligence and warning is identifying what investments in other types of systems and capabilities one can afford to forgo if one has good intelligence and warning. In the case of information system vulnerability, the answer is, “more.” The Air Force cannot afford *not* to defend its critical information systems and be prepared to recover from disruptions that do occur based on the possibility of getting more accurate threat assessment or warning information. Conversely, if it defends adequately and makes plans to recover from problems, better intelligence may not matter much.

In summary, the most reasonable view of the role for intelligence in reducing the vulnerability of Air Force information systems is probably something like the following. One should be prepared to make use of any intelligence about enemy information operations that one gets either routinely (e.g., the “luck of the draw”) on either human or communication intelligence, say, or relatively inexpensively by adjusting collection priorities. However, relying on getting this kind of intelligence is very risky, and significant investments in improved collection capability to protect against information attacks on Air Force systems are hard to justify.

How to Defend and Recover

That means the emphasis has to be on defense and recovery. Our analysis identified a number of potential steps that the Air Force could take to reduce the vulnerability of information systems on which it relies and to minimize the impact of problems that do occur. In prioritizing the protective measures, we concluded that various combinations of steps fit logically together into “packages” of options. The most attractive of those are discussed below. We also identified some areas where more analysis will be required to select the best option.

party—usually, but not necessarily, another country—trying to start a war between other countries by creating an incident of some sort and trying to place the blame on others. The reason this subject has come up again recently in the information war context is that it could be much easier to disguise the true source of a computer hacking attack, say, than to disguise more traditional kinds of military attacks.

The Basic Options. We derived two basic sets of options that together appeared to represent the basic minimum package necessary to keep the risks associated with Air Force information vulnerabilities within tolerable bounds. The details of the options are described in Buchan, et al. (forthcoming) and summarized below.

The “No Brainer.” The first package includes a set of options that appear to be relatively cheap and easy to implement, effective for reducing some obvious vulnerabilities, and logical in combination against modest threats. The details are summarized in Table 10.3. This package emphasizes protecting computers against hacking attacks, reducing the vulnerability of the PSN, and taking some basic steps to protect key installations against physical attack. A couple of noteworthy items include improving the career paths of Air Force computer system administrators, either by enhancing the career field inside the Air Force or by contracting out these services, and making much broader use of software encryption on a variety of Air Force computer systems. The second point is particularly important. Very secure Air Force classified computers already use high-quality encryption. However, many sensitive, but unclassified, computers that might be targets for hackers do not. Cheap, effective, readily

Table 10.3
Low-Cost Package to Reduce Obvious Vulnerabilities

Problem	Security Measures
Vulnerability of computer networks to “cracking” attacks	<ul style="list-style-type: none"> • Fix AFCERT-identified holes • Use software encryption • Isolate critical systems and eliminate unencrypted links into secure computers • Improve career paths for system administrators • Monitor network activity • Map all U.S. Air Force computers
Vulnerability of PSN	<ul style="list-style-type: none"> • Maximizing the effectiveness of the Telecommunications Service Priority program • Increased physical diversity in military leased-line networks • Better protection for connections between bases and end offices
Vulnerability to physical attack	<ul style="list-style-type: none"> • Extended defensive perimeters around key installations

available commercial encryption software could give those computers a considerable degree of protection. Implementing this package is an admission price to get “into the game.” Thus, we consider adopting it to be a “no brainer.”

A More Expensive Package. The second package involves a more serious, although probably modest, investment. Table 10.4 describes individual items in more detail. This set of options takes steps to begin to deal with the communication jamming problem, includes exercising seriously with degraded information systems, adds some more-expensive fixes to computer and communication vulnerability problems, and limits reductions in force size and complexity that could exacerbate information vulnerability problems. This package offers significant operational payoffs. It does come at a cost, however. Some of the technical improvements will require making a modest investment. Exercise costs could increase as well. The more serious costs, though, are the opportunity costs associated with having to forgo some of the options for cost savings associated with dramatic force and manpower reductions. That is the real essence of the problem: the trade between achieving possibly dramatic cost reductions by cutting forces and manpower substantially and the attendant risks of substantially increasing the vulnerability of Air Force operations to attacks on or simple failure of major elements of its information support network.

The combination of these two packages of defensive options appears adequate to reduce the overall risk associated with potential vulnerabilities of Air Force information systems to attack or disruption to a manageable level. Moreover, many of these measures would be needed to cope with normal equipment failures, even absent a direct enemy threat.

Some Unresolved Issues. There are several problems that are important to solve and for which technical solutions are available but that require more analysis to select the best solution. Reducing GPS vulnerability is an example of such a problem. A number of solutions are available. Identifying the most cost-effective approach will require more-detailed analysis. There are other problems, such as the potential vulnerability of various U.S. systems to HPM, that require more research to resolve. Other problems—the physical vulnerability of command centers, for example—will have to be

Table 10.4
Supplementary Package to Enhance Security Against All Levels of Threats Substantially

Problem	Security Measures
Vulnerability of computer networks to “cracking” attacks	<ul style="list-style-type: none"> • Enhance user identification • Alternative communication access • Maintain skilled “backup” personnel • Exercise seriously with degraded systems
Vulnerability of tactical communication systems to jamming	<ul style="list-style-type: none"> • Transition from FLTSATCOM to either MILSTAR or DSCS for Rivet Joint–TIBS Link • Increase AWACS output power and available bandwidth for JTIDS/TADIL–J link • Solve the problems of some existing systems • Retain the option for theater line-of-sight links in GBS and theater-based processing and analysis capability • Develop adaptive networks of redundant components that are collectively resistant to jamming^a
Vulnerability of PSN	<ul style="list-style-type: none"> • More-extensive implementation of automatic reconfiguration procedures
Vulnerability to physical attack	<ul style="list-style-type: none"> • Expanded ground security forces, perhaps enhanced by additional sensors of various sorts
Vulnerability of communication systems to HPM weapons	<ul style="list-style-type: none"> • Installation of fast-response limiters • Proper shielding during manufacture
Vulnerability of GPS to jamming	<ul style="list-style-type: none"> • Development of high-quality, low-cost IMUs for weapons • Maintenance of alternative approaches to achieving weapon accuracy
Sensitivity of force effectiveness to combined vulnerability effects	<ul style="list-style-type: none"> • Avoiding excessive additional force reductions (>25 percent) in the cases we examined, particularly if the forces are simplified as well

^aWe have analyzed this possibility for several years. So far, the results are not encouraging, but the final chapter has yet to be written, so the work continues.

addressed in a larger context with information vulnerability as only one element of the problem. Still other problems appear to have no good solutions. One of these is providing assured jam resistant, high-bandwidth communications. Well-known technical solutions are available, but they tend to be overly expensive in the current cli-

mate (e.g., MILSTAR-like communication satellites). Finding cheaper alternatives is extremely important. Failing that, the services will have to make operational adjustments (e.g., not rely on operational concepts that require such “heroic” communications capability). *That could have major implications for the viability of many of the heavily information-dependent “Third Wave” military operational concepts currently being discussed.*

CONCLUSIONS

We found that most vulnerabilities of U.S. Air Force information-related systems appear to be more nuisances than serious problems at present and are likely to stay that way in the future if the United States takes prudent measures to manage the risks. Particularly important is resisting the urge to reduce force levels or technical diversity too much in an attempt to save money. Equally important is maintaining sufficient skilled manpower as “backups” to automated systems if they should fail and exercising with degraded systems to allow operators to maintain their skills.

The value of information—and the effects of information vulnerabilities—could be much more pronounced in some kinds of lesser operations than in major conflicts because the outcomes of lesser operations might be more sensitive to information-related factors (e.g., time delays, collateral damage). As a result, major conflicts may no longer be the appropriate paradigms to emphasize for planning purposes where information-related systems are concerned.

Detailed threat assessments are not going to be of much use as a practical matter in preparing to deal with attacks on critical information systems, because the capabilities to conduct such attacks are so widespread. Similarly, traditional notions of strategic and tactical warning of “information attacks” are likely to be of little use because the attacks can be so ambiguous and occur so rapidly. That means the most effective way to deal with attacks on information systems is (1) *defend* important systems as well as one can afford to, and (2) be prepared to *adapt* and *recover* as quickly as possible from attacks that initially succeed. Ironically, that general approach is necessary even absent an external threat, just to deal with natural failures of information systems. Thus, having to defend against deliberate attacks may not impose much of an added burden.

Relatively straightforward technical and operational solutions appear to be available for most information vulnerability problems to at least allow the United States to manage the risks, if not eliminate the problems entirely. A package of options to address many of the problems appears to be both practical and affordable. However, choosing the most cost-effective solutions to some problems will require more-detailed analysis, and some problems may not have good solutions. Some of those problems could be serious enough to call into question the feasibility of more advanced information-intensive operational concepts.

There is a broader aspect to this problem that we have not considered in this chapter. An enemy might be able to disrupt U.S. military operations indirectly by attacking the U.S. civilian information infrastructure and making enough mischief to divert the U.S. public's and political elites' attention away from overseas operations. Thus, there might be a way to "end run" the relatively invulnerable military information systems. These "strategic" information attacks are considered elsewhere in this volume.

REFERENCES

- Buchan, G. C., *One-and-a-Half Cheers for the Revolution in Military Affairs*, Santa Monica, Calif.: RAND, P-8015-AF, 1997.
- Buchan, G. C., et al., *Potential Vulnerabilities of U.S. Air Force Information Systems: An Overview Briefing* (U), Santa Monica, Calif.: RAND, DB-227-AF, forthcoming (a). Classified publication; not cleared for public release.
- _____, *Potential Vulnerabilities of U.S. Air Force Information Systems: Final Report*, Santa Monica, Calif.: RAND, MR-816-AF, forthcoming (b). Classified publication; not cleared for public release.
- Cheswick, W. R., and S. M. Bellovin, *Firewalls and Internet Security: Repelling the Wily Hacker*, Addison-Wesley, 1994.
- Defense Science Board, "Report of the Defense Science Board Task Force on Information Warfare-Defense (IW-D)," Office of the Under Secretary of Defense for Acquisition & Technology, Washington, D.C., 1996.

- Denning, P. J., *Computers Under Attack: Intruders, Worms, and Viruses*, Addison-Wesley, 1990.
- Feldman, P. M., *Vulnerabilities of the Public Switched Network: Potential Implications for the Air Force*, Santa Monica, Calif.: RAND, MR-869-AF, 1997.
- Hoffman, L. J. ed., *Rogue Programs: Viruses, Worms, and Trojan Horses*, Van Nostrand Reinhold, 1990.
- Hura, M., G. McLeod, K. O'Connell, P.S. Sauer, "Challenges and Issues in Formulating Defensive Information Warfare Policy: Intelligence Community Perspective," Santa Monica, Calif.: RAND, DB-179-CMS, 1996. Distribution limited to U.S. Government agencies and their contractors.
- Larson, E., *Casualties and Consensus*, Santa Monica, Calif.: RAND, MR-726-RC, 1996.
- Neumann, P., *Computer Related Risks*, New York: Addison-Wesley, 1994.
- Wilson, E., "The Information Revolution and National Security," Draft, Center for International Development and Conflict Management, College Park, Md.: University of Maryland, October 31, 1995.