3. Information Systems Security

Draft of Chapter 3 of *Realizing the Potential of C4I: Fundamental Challenges*, National Academy Press, 1999.
Written mainly by T. Berson, R. Kemmerer, and B. Lampson

Security section of Executive Summary

Goal: C4I systems that remain operationally secure and available for U.S. forces in the face of attacks by adversaries.

The greater the military leverage that C4I systems provide for U.S. forces, the larger the incentives are for an opponent to attack those systems. Indeed, it makes little sense for an opponent to challenge the U.S. “symmetrically”, i.e., force-on-force. More likely avenues of challenge are “asymmetric”, i.e., avenues that exploit potential U.S. vulnerabilities. Attacking U.S. C4I systems – whether directly or indirectly (e.g., through the U.S. civilian information infrastructure on which DOD C4I systems often depend)—is only one of many asymmetric attacks, but such an attack is one for which the U.S. must be adequately prepared.

Principles

- *Information systems security begins at the top and concerns everyone*. Security is all too often regarded as an afterthought in the design and implementation of C4I systems. In fact, the importance of information systems security must be felt and understood at all levels of command and throughout the DOD.
- *Cyber-attack is easier than cyber-defense. A*n effective defense must be successful against all attacks while an attacker need only succeed once,. Cyber-attack is easier, faster, and cheaper than cyber-defense. Paradoxically, cyber-attack is also more highly rewarded in U.S. military culture. Consequently, those expert in cyber-attack are more numerous than those skilled in cyber-defense. Today, the need for cyber-defenders far outstrips the supply, and defenders must be allocated wisely and encouraged in their efforts.
- *Cyber-attackers attack the weakest points in a defense*. (“An army is like water it avoids obstacles and flows through low places.”) Thus, the security of a system—any system—can never been guaranteed. Any system is always compromised to some extent, and a basic design goal of any system should be that it can continue to operate appropriately in the presence of a penetration. Vulnerabilities include fraudulent identification and authorization, abuse of access privileges, compromises in the integrity of data, and artificially induced disruptions or delays of service.

  Implementation of good system security depends on several principles:
- *A culture of information security is required throughout the organization*. The culture of any organization establishes the degree to which members of that organization take their security responsibilities seriously. Organizational policies and practices are at least as important as technical mechanisms in providing information assurance. Policies specify the formal structures, ensure responsibility and accountability, establish procedures for deploying and using technical means of protection and assigning access privileges, create sanctions for breaches of security at any level of the organization, and require training in the privacy and security practices of an organization. Furthermore, senior leadership must take the lead to promote information assurance as an important cultural value for the organization. Top-level commitment is not sufficient for good security

practices to be put into place, but without it, organizations will drift to do other things that appear more directly related to their core missions.

- *Defend in depth*. Defense in depth is a sound countermeasure against security failures at a single point and also against security failures which share a common mode. Furthermore, an attacker that faces multiple defenses must have the expertise to overcome all of them (rather than just one) and must also expend the time required to overcome all of them.
- *Degrade gracefully*. Prudence thus requires C4I developers and operators to assume some non-zero probability that any system will be successfully attacked, that some DOD systems have been successfully attacked, and that some C4I systems are compromised at any given moment. Nevertheless, most of the C4I systems connected to compromised components (and the organization that relies on these systems) should be able to function effectively despite local security failures.
- *Manage the tension between security and other desirable C4I attributes*, including user convenience, interoperability, and standardization. This tension is unavoidable. It is not appropriate to use the need for any of these attributes as an excuse for not working on security, and vice versa.
- *Do what is possible, not what is perfect*. Insistence on “perfect” security solutions for C4I systems means that as a practical matter, C4I systems will be deployed without much security functionality. By contrast, a pragmatic approach (e.g., one that makes significant use of commercial information security products) that provides moderate protection is much better than nothing.
- *Recognize the inherent weaknesses in passive defense*. Because passive defense techniques are used to provide security, an unsuccessful attack on a C4I system usually does not result in a penalty for the attacker. Thus, a persistent attacker willing to expend the time to find weaknesses in system security will eventually be successful. Cyber-defenders of C4I systems must anticipate facing persistent attackers.

Findings

Finding S-1: Protection of information and information systems is a pressing national security issue.

DOD is in an increasingly compromised position. The rate at which information systems are being relied upon outstrips the rate at which they are being protected. Also, the time needed to develop and deploy effective defenses in cyberspace is much longer than the time required to develop and mount an attack. The result is vulnerability: a gap between exposure and defense on the one hand and attack on the other. This gap is growing wider over time, and it leaves DOD a likely target for disruption or pin-down via information attack.

Finding S-2: The DOD response to the information systems security challenge has been inadequate.

In the last few years, a number of reports, incidents, and exercises have documented significant security vulnerabilities in DOD C4I systems. Despite such evidence, the committee’s site visits revealed that DOD’s words regarding the importance of information systems security have not been matched by comparable action. Troops in the field do not appear to take the protection of their C4I systems nearly as seriously as they do other aspects of defense. Furthermore, in many cases, DOD is legally constrained from taking retaliatory action against a cyber-attacker that might deter future cyber-attacks.

On the technology side, information systems security has been hampered by a failure to recognize fully that C4I systems are today heavily dependent on commercial components that often do not provide high levels of security. Thus, while the most secure systems may be those that are built from scratch with attention from the start paid to security, real-world military C4I systems built on commercial components have very little effective security and low assurance they will work under real attacks. By contrast, the commercial sector has taken a largely pragmatic approach to the problem of information systems security. While acknowledging that security in the commercial sector is on average not particularly good, the best commercial practices for security are in general far in advance of what the committee has observed with fielded C4I systems.

Recommendations

The committee believes that operational dimensions of information systems security have received far less attention and focus than the subject deserves in light of a growing U.S. military dependence on information dominance as a pillar of its warfighting capabilities. Furthermore, it believes that *DOD must greatly improve the execution of its information systems security responsibilities*.

One critical aspect of improving information systems security is changing the DOD culture, especially within the uniformed military, to place a high value on it. With a culture that values the taking of the offensive in military operations, the military may well have difficulty in realizing that defense against information attack is a more critical function than being able to conduct similar operations against an adversary, and indeed is more difficult and requires greater skill and experience than offensive information operations. Senior DOD leadership must therefore take the lead to promote information systems security as an important cultural value for DOD. The committee is encouraged by conversations with senior defense officials, both civilian and military, who appear to take information systems security quite seriously. Nevertheless, these officials have a limited tenure, and the issue of high-level attention is a continuing one.

A second obstacle to an information systems security culture is that good security from an operational perspective often conflicts with doing and getting things done. And because good information systems security results in nothing (bad) happening, it is easy to see how the can-do culture of DOD might tend to devalue it.

Recommendation S.1: The Secretary of Defense, through the ASD/C3I and the CJCS, should designate an organization responsible for providing direct defensive operational support to commanders.

Recommendation S.2: The Secretary of Defense should direct that all DOD civilian and military personnel receive appropriate training in the use of adequate information security tools, ensure that these tools are made available to all appropriate personnel, and hold both civilian and military personnel accountable for their information security practices.

Recommendation S.3: The ASD/C3I and the Chairman of the Joint Chiefs of Staff should support and fund a program to conduct frequent, unannounced penetration testing of deployed C4I systems.

Recommendation S.4: The ASD/C3I should mandate the department-wide use of currently available network/configuration management tools and strong authentication mechanisms immediately.

Recommendation S.5: The Undersecretary of Defense for Acquisition and Technology and ASD/C3I should direct the appropriate defense agencies to develop new tools for information security.

Recommendation S.6: The Chairman of the Joint Chiefs of Staff and the Service secretaries should direct that all tests and exercises involving DOD C4I systems be conducted under the routine assumption that they are connected to a compromised network.

Recommendation S.7: The Secretary of Defense should take the lead in explaining the severe consequences for its military capabilities that arise from a purely passive defense of its C4I infrastructure and exploring policy options to respond to these challenges.

Contents

Introduction

DOD's increasing reliance on information technology in military operations increases the value of DOD's information infrastructure and information systems as a military target. Thus, for the U.S. to realize the benefits of increased use of C4I in the face of a clever and determined opponent, it must secure its C4I systems against attack.

As noted in Chapter 2, the maximum benefit of C4I systems is derived from their interoperability and integration. That is, to operate effectively, C4I systems must be interconnected so that they can function as part of a larger "system-of-systems". These electronic interconnections multiply many-fold the opportunities for an adversary to attack them.

Maintaining the security of C4I systems is a problem with two dimensions. The first dimension is physical, that of protecting the computers and communications links as well as command and control facilities from being physically destroyed or jammed. For this task, the military has a great deal of relevant experience that it applies to systems in the field. Thus, the military knows to place key C4I nodes in well-protected areas, to place guards and other access control mechanisms in place to prevent sabotage, and so on. The military also knows how to design and use wireless communications links so that enemy jamming is less of a threat.

Information systems security is a much more challenging task. Information systems security -- the task of protecting the C4I systems connected to the communications network against an adversary's information attack against those systems -- is a much more poorly understood area than physical security.[1] Indeed, DOD systems are regularly attacked and penetrated,[2] though most of these attacks fail to do damage. Recent exercises such as Eligible Receiver (Box 0.1) have demonstrated real and

[1] Within the information technology industry, the term "information security" encompasses technical and procedural measures providing for confidentiality, authentication, data integrity, and non-repudiation, as well as for resistance to denial-of-service attacks. The committee understands that within many parts of DOD, the term "information security" does not have such broad connotations. Nevertheless, it believes that lack of a broad interpretation for the term creates problems for DOD because it focuses DOD on too narrow a set of issues. Note that information systems security does not address issues related to the quality of data before it is entered into the C4I system. Obviously, such issues are important to the achievement of information superiority, but they are not the focus of this chapter.

[2] It is reported that [in 1997?] DOD systems were attacked at a rate of [25,000?] known attacks per day [ref.].

significant vulnerabilities in DOD C4I systems, calling into question their ability to survive any serious attach by a determined and skilled adversary.

---- Insert Box 0.1 about here ----

Such observations are unfortunately not new. A series of earlier reports have noted a history of insufficient or ineffective attention to C4I information systems security (Box 0.2).

---- Insert Box 0.2 about here ----

The problem of protecting DOD C4I systems against attack is enormously complicated by the fact that DOD C4I systems and the networks to which they are connected are not independent of the U.S. national information infrastructure.[3] Indeed, the line between the two is quite blurred because many military systems make use of the civilian information infrastructure,[4] and because military and civilian systems are often interconnected. DOD is thus faced with the problem of relying on components of the infrastructure over which it does not have control. While the general principles of protecting networks as described below apply to military C4I systems, both those connected to civilian components and those that are not, the policy issues related to DOD reliance on the national information infrastructure are not addressed in this report. Lastly, C4I systems are increasingly built upon commercial technologies, and thus are coming to suffer from the same set of vulnerabilities than is observed in the commercial sector.

Vulnerabilities in Information Systems and Networks[5]

Information systems and networks can be subject to four generic vulnerabilities. The first is *unauthorized access to data.* By surreptitiously obtaining the sensitive data (whether classified or unclassified) or by browsing a sensitive file stored on a C4I computer, an adversary might obtain information that could be used against the national security interests of the U.S. Moreover, even more damage could occur if the fact of unauthorized access to data has gone unnoticed, because it would be impossible to take remedial action.

The second generic vulnerability is *clandestine alteration of data*. By altering data clandestinely, an adversary could destroy the confidence of a military planner or disrupt the execution of a plan. For example, alteration of logistics information could significantly disrupt deployments if troops or supplies were re-routed to the wrong destinations or supply requests were deleted.

A third generic vulnerability is *identity fraud*. By illicitly posing as a legitimate user, an adversary could issue false orders, make unauthorized commitments to military commanders seeking resources, or alter the situational awareness databases to his advantage. For example, an adversary who obtained access to military payroll processing systems could have a profound effect on military morale.

A fourth generic vulnerability is *denial of service*. By denying or delaying access to electronic services, an adversary could compromise operational planning and execution, especially for time-critical tasks. For example, attacks that resulted in the unavailability of weather information systems could delay planning for military operations. Denial of service is, in the view of many, the most serious vulnerability, because denial-of-service attacks are relatively easy to do and often require relatively little technical sophistication.

Also, it is worth noting that many compromises of security result not from a successful direct attack on a particular security feature intended to guard against one of these vulnerabilities. Rather, they involve the “legitimate” use of designed-in features in ways that were not initially anticipated by the designers of that feature.

Lastly, non-technical vulnerabilities – such as the intentional misuse of privileges by authorized users – must be considered. For example, even perfect access controls and unbreakable encryption will not prevent a trusted insider from revealing the contents of a classified memorandum to unauthorized parties.

[3] The U.S. national information infrastructure includes those information systems and networks that are used for all purposes, both military and civilian, while DOD’s C4I systems are by definition used for military purposes.

[4] Over 90% of DOD communications are transmitted over the public switched telecommunications network. (Cite..)

[5] Adapted from *Cryptography’s Role In Securing the Information Society,* Box 1.3

The types of attack faced by DOD C4I systems are much broader and potentially much more serious and intense than those usually faced by commercial (non-military) networked information systems. The reason is that attacks on DOD C4I systems that are part of an attack sponsored or instigated by a foreign government can have virtually unlimited resources devoted to those attacks. Furthermore, perpetrators sponsored or supported by a foreign government are largely immune to retaliation or punishment through law enforcement channels, and are thus free to act virtually without constraint.

Security Requirements

Needs for information systems security and trust can be formulated in terms of several major requirements:

- **Data confidentiality** - controlling who gets to read information in order to keep sensitive information from being disclosed to unauthorized recipients - e.g., preventing the disclosure of classified information to an adversary
- **Data integrity** - assuring that information and programs are changed, altered, or modified only in a specified and authorized manner - e.g., preventing an adversary from modifying orders given to combat units so as to shape battlefield events to his advantage
- **System availability** - assuring that authorized users have continued and timely access to information and resources - e.g., preventing an adversary from flooding a network with bogus traffic that delays legitimate traffic such as that containing new orders from being transmitted
- **System configuration**- assuring that the configuration of a system or a network is changed only in accordance with established security guidelines and only by authorized users - e.g., detecting and reporting to higher authority the improper installation of a modem that can be used for remote access.

In addition, there is a requirement that cuts across these three for **accountability** - knowing who has had access to information or resources.

It is apparent from this listing that security means more than protecting information from disclosure (e.g., classified information). In the DOD context, much of the information on which military operations depend (for example, personnel, payroll, logistics and weather) is not classified. While its *disclosure* might not harm national security, alteration or delay certainly could.[6] In other cases, access to unclassified information can present a threat (e.g., access to personnel medical records used to enable blackmail attempts).

Satisfying these security requirements requires a range of security services, including:

- **Authentication** - ascertaining that the identity claimed by a party is indeed the identity of that party. Authentication is generally based on what a party knows (e.g., a password), what a party has (e.g., a hardware computer-readable token), or what a party is (e.g., a fingerprint).
- **Authorization** - granting of permission to a party to perform a given action (or set of actions)
- **Auditing** - recording each operation that is invoked along with the identity of the subject performing it and the object acted upon (as well as later examining these records)
- **non-repudiation** - the use of a digital signature procedure affirming both the integrity of a given message and the identity of its creator to protect against a subseqeuent attempt to deny authenticity.

Role of cryptography

It is important to understand what role the tool of cryptography plays in information system security, and what aspects of security are not provided by cryptography. Cryptography provides a number of useful capabilities:

[6] Statements typically issued by DOD in the aftermath of an identified attack on its systems assure Congress and the public that "no classified information was disclosed." These may be technically correct, but they do not address the important questions of whether military capabilities were compromised, or more broadly, if a similar incident would have adverse implications in future, purposeful attach situations.

- **Confidentiality -** the characteristic that information is protected from disclosure, in transit during communications (so-called link encryption) and/or when stored in an information system. The security requirement of confidentiality is the one most directly met by cryptography.
- **Authentication -** cryptographically based assurance that an asserted identity is valid for a given person or computer system
- **Integrity check -** cryptographically based assurance that a message or file has not been tampered with or altered
- **Digital signature -** assurance that a message or file was sent or created by a given person, based on the capabilities provided by mechanisms for authentication and integrity checks

Cryptographic devices are important, for they can protect information in transit against unauthorized disclosure, but this is only a piece of the information systems security problem. The DOD mission also requires that information be protected while in storage and while being processed, and that the information be protected not only against unauthorized disclosure, but also against unauthorized modification and against attacks that seek to deny authorized users timely access to the information.

Cryptography is a valuable tool for authentication as well as verifying the integrity of information or programs.[7] Cryptography alone does not provide availability (though because its use is fundamental to many information security measures, its widespread application can contribute to greated assurance of availability[8]). Nor does cryptography directly provide auditing services, though it can serve a useful role in authenticating the users whose actions are logged and in verifying the integrity of audit records.

Cryptography does not address vulnerabilities due to bugs in the system, including configuration bugs and bugs in cryptographic programs. It does not address the many vulnerabilities in operating systems and applications.[9] It certainly does not provide a solution to such problems as poor management and operational procedures or dishonest or suborned personnel.

In summary, cryptography may well be an necessary component of these latter protections, but cryptography alone is not sufficient.[10]

Major Challenges to Information Systems Security

Networked Systems

The utility of an information or C4I system generally increases as the number of others systems to which it is connected increases. On the other hand, increasing the number of connections of a system to other systems also increases its vulnerability to attacks routed through those connections.

The use of the Internet to connect C4I systems poses special vulnerabilities. It is desirable to use the Internet because the Internet provides lower information transport costs compard to the public switched telephone network or dedicated systems. But the Internet provides neither quality-of-service guarantees nor good isolation from potentially hostile parties.

[7] Cryptography can be used to generate digital signatures of messages, enabling the recipient of a message to assure himself that the message has not been altered (i.e., an after-the-fact check of message integrity that does not protect against modification itself). However, in the larger view, a properly encrypted communications channel is difficult to compromise in the first place, and in that sense cryptography can also help to prevent (rather than just to detect) improper modifications of messages.

[8] Widespread use of encryption (vs. cryptography) can also result in reduced availability, as it hinders existing fault isolation and monitoring techniques. It is for this reason that today's network managers are often not enthusiastic about deployment of encryption.

[9] Recent analysis of CERT reports suggests that fewer than 50% of the bugs reported in the last 8 years would be ameliorated by the use of cryptography. Source???? ASK REVIEWER W.

[10] It is worth noting that cryptography is often the *source* of failures of C4I systems to interoperate. That is, two C4I systems often fail to exchange data operating in secure encrypted mode.

The Asymmetry Between Defense and Offense

Information systems security is fundamentally a defensive function, and as such suffers from an inherent asymmetry. A successful defender must be successful against all attacks, regardless of where the attack occurs, the modality of the attack, or the time of the attack. A successful attacker has only to succeed in one place at one time with one technique. Furthermore, information systems security has several interrelated dimensions that make it particularly difficult.

Ease-of-use compromises

Compromises arise because information systems security measures ideally make the system impossible to use by someone who is not authorized to use it while considerations of system functionality require that the system be easy to use by authorized users. From the perspective of an authorized user, a system with information systems security features should look like the same system without those features. In other words, security features provide no direct functional benefit to the authorized user. At the same time, measures taken to increase the information security a system almost always make using that system more difficult or cumbersome. The result in practice is that all too often (from a security standpoint) security features are simply omitted (or not turned on) to preserve the ease-of-use goal.

Perimeter defense

Today's commercially available operating systems and networks offer only weak defensive mechanisms, and thus the components that make up a system are both vulnerable and hard to protect. One approach to protecting a network is then to allow systems on the network to communicate freely (i.e., without the benefit of security mechanisms protecting each individual network transaction) while allowing connection to the larger world outside the network only through carefully defined and well-protected "gateways". The result is an arrangement that is "hard on the outside" against attack but "soft on the inside." Thus, it is today very common to see "enclaves" hiding from the Internet behind firewalls, but few defensive measures within the enclaves themselves.

A perimeter strategy is less expensive than an approach in which every system on a network is protected (a "defense-in-depth" strategy) because defensive efforts can be concentrated on just a few nodes (the gateways). But the major risk is that a single success in penetrating the perimeter compromises everything on the inside, and a perimeter can be compromised by the addition of a single unauthorized modem connected to the network inside the perimeter. Once the perimeter is breached, the attacker need not expend additional effort to increase the number of targets that he may attack. The limitations of a perimeter defense are issues that should be redressed by C4I architecture – the paradigm of perimeter defense is an implicit element of today's C4I architecture that needs to be made explicit and changed.

One alternative to perimeter defenses is defense-in-depth, a strategy that requires the adversary to penetrate multiple independently-vulnerable obstacles to have access to all of his targets.The property of "independent vulnerabilities" is key; if the different mechanisms of defense share common-mode vulnerabilities, e.g., all use an operating system with easily exploited vulnerabilities, even mutiple mechanisms of defense will be easily compromised. When the mechanisms are independently vulnerable and deployed, the number of accessible targets becomes a strong function of the effort expended by the attacker. The problem of perimeter defense is made worse by the tendency to let one's guard down within the protection of the firewall (believing that the inside is secure) and thus to not take full advantage of even the (relatively weak) protections afforded by the security built into the network components.

The Use of COTS Components[11]

For reasons of economy, time to completion, and interoperability, networked information systems, including many DOD C4I systems, are increasingly built out of COTS components. But the use of COTS components, especially COTS software (including operating systems, network management packages, e-mail programs, web browsers, and word processors, among others), can lead to security problems for a number of reasons:

- Increasing functionality and decreasing time-to-market characterize the COTS software market today—often at the expense of security. The reason is simple -- security features and functionality do not usually play a large role in buyer decisions.
- The increased functionality of COTS software is generally associated with high complexity and a large number of bugs. The high complexity means that specifications for COTS components are likely to be incomplete and consequently, system architects may be unaware of some of the vulnerabilities in the building-block components.
- The developers of COTS software rely on customer feedback as a significant, or even primary, quality assurance mechanism, which can lead to uneven quality levels within the different subsystems or functionality in a COTS product. Even worse, security problems in COTS products may not even be known to the customer.
- The use of COTS components implies a dependence on the vendor for decisions about the component's evolution and the engineering processes used in its construction (notably regarding security). Similarly, the security mechanisms available in a COTS product, if any are present at all, are dictated by the developers of COTS products. Because COTS software is developed for a range of application domains, their security mechanisms are usually not tailored to the specific needs of any particular application area.
- The growing use of COTS components, from a small set of vendors, throughout all segments of the IT industry suggests a continuing decrease in heterogeneity in the coming years. Thus, the similarity intrinsic in the component systems of a homogeneous collection implies that these systems will share vulnerabilities. A successful attack on one system is then likely to succeed on other systems as well.

These factors do not argue that COTS components should not be used to develop networked information systems, only that such use should be undertaken with care. For example, wise developers learn to avoid the more complex features of COTS software because these are the most likely to exhibit surprising behavior and such behavior is least likely to remain stable across releases. When these features cannot be avoided, encapsulating components with wrappers, effectively narrowing their interfaces, can protect against some undesirable behaviors.

Still, in an overall sense, the relationship between the use of COTS software and system security is unclear. Research is needed to improve our understanding of this relationship, and how to use COTS components to build secure systems.

Threats posed by insiders

Insiders are those authorized to access some part or parts of a network. When security depends on the defenses built into the perimeter, the coercion or subornation of a single individual on the inside leaves the entire network open to attack to the extent that internal protections are lacking. Controlling the privileges of authorized individuals more finely (i.e., enabling such an individual to use some system resources or capabilities but not others) is only a partial solution, because abuse of the enabled resources is possible.

[11] The discussion of this section is based largely on *Trust in Cyberspace*.

Passive defense

Legal and technical constraints preclude retaliation against the perpetrator of an information systems attack (a cyber attack). Thus, the attacker pays no penalty for failed attacks. He or she can therefore continue attacking unpunished until he or she succeeds or quits.

The following example from physical space illustrates the futility of passive defense. Imagine a situation in which truck bombers in a red truck attempt entry to a military base. The bomb is discovered and they are turned away at the front gate of a military base, but allowed to go away in peace to refine their attack. They return later that day with a bomb in a yellow truck, are again turned away, and again go away in peace to refine their attack. They return still later with a stolen military truck. This time the bomb is undetected, they penetrate the defenses, and they succeed in their attack. A base commander taking this approach to security would be justly criticized and held accountable for the penetration.

Yet in cyberspace passive defense is standard operating procedure. For example, an attacker can use an automatic telephone dialer to dial every number on a military post's telephone exchange looking for modem tones. An attacker probing the defenses of a computer system in which an IP connection can test one port number after another without penalty. In a phone probe looking for modem tones, all 10,000 phone numbers may be tested. No sane commander would allow a truck bomber 10,000 unchallenged, penalty-free attempts to drive on base. But the same commander today is constrained to routinely allow 10,000 unchallenged, penalty-free attempts to find modems attached to base systems. Passive defense in cyberspace represents both the tradition and the standard operating practice. But it is a losing proposition, and inadequate for protection of military operations in cyberspace.

Defensive functions

Effective information systems security is based on a number of functions described below. This list of functions is not complete; nevertheless, evidence that all these functions are being performed in an effective and coordinated fashion will be evidence that information systems security is being taken seriously and conducted effectively.

Some of these functions were also noted in the military context by the Defense Science Board, and some by the President's Commission on Critical Infrastructure Protection in its report.[12] [ref.]. These functions are listed here because they are important, and because the committee feels that they have not yet been addressed by the DOD in an effective fashion (as described in the committee's findings below).

Function 1. Collect, analyze, and disseminate strategic intelligence about threats to systems.

Any good defense attempts to learn as much as possible about the threats that it may face, both the tools that an adversary may use and the identity and motivations of likely attackers. In the information systems security world, it is difficult to collect information about attackers (though such intelligence information should be sought). It is however much easier to collect and analyze information on technical and procedural vulnerabilities, both to characterize the nature of these vulnerabilities and their frequency at different installations. Dissemination of information about these vulnerabilities enables administrators of the information systems that may be affected to take remedial action.

Function 2. Monitor indications and warnings

All defenses -- physical and cyber -- rely to some extent on indications and warning of impending attack. The reason is that if it is known that attack is impending, the defense can take actions to reduce its vulnerability and to increase the effectiveness of its response. This function calls for:

- **Monitoring of threat indicators**. For example, near-simultaneous penetration attempts on hundreds of military information systems might reasonably be considered an indication of an orchestrated attack. Mobilization of a foreign nation's key personnel known to have responsibility for information attacks might be another indicator. The notion of an "information condition" or

[12] [ref. DSB-IW and PCCIP report

“infocon”, analogous to the DEFCON (defense condition) indicator, would be a useful summary device to indicate to commanders the state of the cyber-threat at any given time (Box 0.3). This concept is being developed by various DoD elements but is yet immature.

---- Insert Box 0.3 about here ----

- **Assessment and characterization of the information attack (if any)**. Knowledge of the techniques used in an attack on one information system may facilitate a judgment of the seriousness of the attack. For example, an attack that involves techniques that are not widely known may indicate that the perpetrators have a high degree of technical sophistication.
- **Dissemination of information about the target(s) of threat**. Knowledge of the techniques used in an attack on one information system may enable administrators responsible for other systems to take preventive actions tailored to that type of attack. This is true even if the first attack is unsuccessful, because security features that may have thwarted the first attack may not necessarily be installed or operational on other systems.

Note that dissemination of information about attacks and their targets is required on two distinct time scales. The first time scale is seconds or minutes after the attack is known; such knowledge enables operators of other systems not (yet) under attack to take immediate preventive action (such as severing some network connections). In this instance, alternative means of secure communication may be necessary to disseminate such information. The second time scale is days after the attack is understood; such knowledge allows operators throughout the entire system-of-systems to implement fixes and patches that they may not yet have fixed, and to request fixes that are needed but not yet developed.

A DOD example of monitoring is the AFIWC element that monitors and responds to penetrations at Air Force installations world-wide from San Antonio, TX.

Function 3. Be able to identify intruders

Electronic intruders into a system are admittedly hard to identify. Attacks are conducted remotely, and a chain of linkages from the attacker’s system to an intermediate node to another to another to the attacked system can easily obscure the identity of the intruder. Nevertheless, certain types of information -- if collected -- may shed some light on the intruder’s identity. For example, some attackers may preferentially use certain tools or techniques (e.g., the same dictionary to test for passwords), or use certain sites to gain access. Attacks that go on over an extended period of time may provide further opportunities to trace the origin of the attack.

Function 4. Test for security weaknesses in fielded and operational systems

An essential part of a security program is searching for technical and operational/procedural vulnerabilities. Ongoing tests (conducted by groups often known as “red teams” or “tiger teams”) are essential for several reasons:

- Recognized vulnerabilities are not always corrected and known fixes are frequently found not to have been applied as a result of poor configuration management.
- Security features are often turned off in an effort to improve operational efficiency. Such actions may improve operational efficiency, but at the potentially high cost of compromising security, sometimes with the primary damage occurring in a some distant part of the system.
- Some security measures rely on procedural measures and thus depend on proper training and ongoing vigilance on the part of commanders and system managers
- Security flaws that are not apparent to the defender undergoing an inspection may be uncovered by a committed attacker (as they would be uncovered in an actual attack)

Thus, it is essential to use available tools and conduct “red team” or “tiger team” probes often and without warning to test security defenses. In order to maximize the impact of these tests, reports should be disseminated widely. Release of such information may risk embarrassment of certain parties or possible release of information that can be used by adversaries to attack, but especially in the case of vulnerabilities uncovered for which fixes are available, the benefits of releasing such information -- allowing others to learn from it and motivating fixes to be installed -- outweigh these costs.

Tiger team attacks launched without the knowledge of the attacked systems also allow estimates to be made of the frequency of attacks. Specifically, the fraction of tiger team attacks that are detected is a reasonable estimate of the fraction of adversary attacks that are made. Thus, the frequency of adversary attacks can be estimated from the number of adversary attacks that are detected.

Function 5. Plan a range of responses

Any organization relying upon information systems should have a number of routine information systems security activities (e.g., security features that are turned on, security procedures that are followed). But when attack is imminent (or in process), an organization could prudently adopt additional security measures that during times of non-attack might not be in effect because of their negative impact on operations. Tailoring in advance a range of information systems security actions to be taken under different threat conditions would help an organization plan its response to any given attack.

For example, a common response under attack is to drop non-essential functions from a system connected to the network so as to reduce the number of routes for penetration. A determination in advance of what functions count as non-essential and under what circumstances such a determination is valid would help facilitate an orderly transition to different threat conditions, and would be much better than an approach that calls for dropping all functionality and restoring only those functions that people using the system at the time complain about losing. Note that such determinations can be made only from an operational perspective rather than a technical one, a fact that points to the essential need for an operational architecture in the design of C4I systems.

The principle underlying response planning should be that of “graceful degradation”, that is -- the system or network should lose functionality gradually, as a function of the severity of the attack compared to its ability to defend against it.[13] This principle stands in contrast to a different principle that might call for the maintenance of all functionality until the attack simply overwhelms the defense and the system or network collapses. The latter principle is tempting because reductions in functionality necessitated for security reasons may interfere with operational ease-of-use, but its adoption risks catastrophic failure.

It is particularly important to note that designing a system for graceful degradation depends on system architects who take into account the needs of security (and more generally, the needs of coping with possible component failures) from the start For example, the principle would forbid a system whose continued operation depended entirely on a single component remaining functional, or on the absence of a security threat. This principle was apparently violated in the design of the SmartShip architecture being prototyped on the USS Yorktown.[14]

This principle is often violated in the development of prototypes. It is often said that “it is necessary for one to crawl before one can run”, i.e., that it is acceptable to ignore security or reliability considerations when one is attempting to demonstrate the feasibility of a particular concept. This argument is superficially plausible, but in practice it does not hold water. It is reasonable for a prototype to focus only on concept feasibility, ignoring considerations of reliability or security, only if the prototype will be thrown away and a new architecture is designed and developed from scratch to implement the concept. Budget and schedule constraints usually prevent such new beginnings, and so in practice, the prototype’s architecture is never abandoned, and security or reliability considerations must be addressed in the face of an architecture that was never designed or intended to support them.

[13] Of course, graceful degradation assumes an ability to detect an attack and make adjustments to system operation and configuration in near real-time. It is possible that in preparation of an attack, a clever opponent will be able to plant initially undetected “trojan horses” that can be activated when the attack begins in earnest, or other programs that can operate covertly, making it hard for the defender to respond to an attack that is ongoing. This fact does not negate the utility of the design philosophy, but it does point out that graceful degradation cannot solve all security problems.

[14] Published reports indicate that the U.S.S. Yorktown suffered a major propulsion systems failure as the result of entering bad data into a ship-wide network that was also controlling its engines. See....

Function 6. Coordinate defensive activities throughout the enterprise

Any large, distributed organization has many information systems and subnetworks that must be defended. The activities taken to defend each of these systems and networks must be coordinated because the distributed parts have interconnections and the security of the whole organization depends on the weakest link. Furthermore, it is important for different parts of organizations to be able to learn from each other about vulnerabilities, threats, and effective countermeasures.

Function 7. Ensure adequacy/availability/functioning of public infrastructure used in systems (will require cooperation with commercial providers and civilian authorities)

Few networks are built entirely using systems controlled by the organization that relies upon them. Therefore organizations (including DOD) are required to work cooperatively with the owners of the infrastructure they rely upon and relevant authorities to protect them.

Function 8. Include security requirements in any specification of system or network requirements that is used in the acquisition process.

Providing information systems security for a network or system that has not had security features built into it is enormously problematic. Retrofits of security features into systems not designed for security invariably leave security holes, and procedural fixes to inherent technical vulnerabilities only go so far.

Perhaps more importantly, security requirements must be given prominence from the beginning in any system conceptualization. The reason is that security considerations may affect the design of a system in quite fundamental ways, and a designer that decides upon a design that works against security should at least be cognizant of the implications of such a choice. This function thus calls for information systems security expertise to be integrally represented on design teams, rather than added later.

Note that specification of the “Orange Book” security criteria would be an insufficient response to this function. “Orange Book” criteria typically drive up development times significantly, and more importantly, are not inherently part of an initial requirements process and do not address the security of networked or distributed systems.

Function 9. Monitor/assess/understand offensive and defensive information technology.

Good information systems security requires an understanding of the types of threats and defenses that might be relevant. Thus, those responsible for information systems security need a vigorous ongoing program to monitor, assess, and understand offensive and defensive information technologies. Such a program would address both the technical details of these technologies, their capability to threaten or protect friendly systems, and their availability.

Function 10. Advance the state-of-the-art in defensive information technology (and processes) with research.

While much can usually be done to improve information systems security simply through the use of known and available technologies, bug fixes, and procedures, better tools to support the information systems security mission are always needed. In general, such improvements fall into two classes (which may overlap). One class consists of improvements so that tools can deal more effectively with a broader threat spectrum. A second class, equally important, provides tools that provide better automation and thus can solve problems at lower costs (costs that include direct outlays for personnel and equipment and operational burdens resulting from the hassle imposed by providing security).

Similar considerations apply to processes for security as well. It is reasonable to conduct organizational research into better processes and organizations that provide more effective support against information attacks and/or reduce the impediments into using or implementing good security practices.

Function 11. Promote information systems security awareness

Just as it is dangerous to rely upon a defensive system or network architecture that is hard on the outside and soft on the inside, it is also dangerous if any member of an organization fails to take information systems security seriously. Because the carelessness of a single individual can seriously compromise the security of the entire organization, education and training for information systems security must be required for all members of the organization. Moreover, such education and training must be systematic, regarded as important by the organization (and demonstrated with proper support for such education and training), and undertaken on a regular basis (both to remind people of its importance and to update their knowledge in light of new developments in the area).

Function 12. Set security standards (both technical and procedural)

Security standards should articulate in well-defined and actionable terms what the organization expects to do in the area of security. They are therefore prescriptive. For example, a technical standard might be "all passwords must be 8 or more characters long, contain both alphabetics and numerics, be pronounceable, and not contained in any dictionary", or "all electronic communications containing classified information must be encrypted with a certain algorithm and key length." A standard involving both technical and procedural measures might specify how cryptographic keys known to be compromised are revoked. Furthermore, security standards should be expected to apply to all those within the organization. (For example, generals should not be allowed to exercise poorer information systems security discipline than captains, as they might be tempted to do in order to make their use of C4I systems easier.)

Function 13. Develop and use criteria for assessing security status

Information security is not a one-shot problem, but a continuing one. Threats, technology, and organizations are constantly changing in a spiral of measures and counter measures. Organizations must have ways of measuring and evaluating whether they have effective defensive measures in place. Thus, once standards are set in place, the organization must periodically assess the extent to which members of the organization comply with those standards (and characterize the nature of the compliance that does exist).

Metrics for security could include number and characterizations of attacks, fraction of attacks detected, fraction of attacks repelled, damages incurred, and time needed to detect and respond to attacks. Note that making measurements on such parameters depends on understanding the attacks that do occur -- because many attacks are today not detected, continual penetration testing is required to establish such a baseline.

One example of such monitoring is the efforts NSA makes to ensure that cryptographic devices are being used. NSA can detect if any U.S. military communicators shut off cryptographic COMSEC devices, and provides appropriate feedback to the relevant commands.

Responsibility for Information Systems Security in DoD

The responsibility of information systems security within the Department of Defense is distributed through the entire organization, including both civilian and military components. The Assistant Secretary of Defense for Command, Control, Communications and Intelligence (ASD(C3I)) is the principal staff assistant to the Secretary of Defense for C3I and information management and information warfare matters and as the Chief Information Officer for the DOD. Other OSD components with some connection to information systems security include the Defense Information Systems Agency, the Defense Advanced Projects Research Agency, the National Security Agency, the Defense Intelligence Agency, and DOD's federally funded research and development centers, such as MITRE, the Institute for Defense Analyses, and RAND. Each of the military services and the combatant commands have one or more activities focusing on information systems security, as does the Joint Staff.

Of particular relevance to the DOD-wide issues related to information systems security are:

- the Defense-wide Information Assurance Program (DIAP), established in January 1998 to provide a "common framework and central oversight necessary to ensure the protection and reliability of the DII."[15] The DIAP goal is to change the way DOD and its various agents look at information assurance, from a technical issue to an operational readiness issue. It will look at new tools (e.g., better systems) and techniques (e.g., vulnerability assessments, read team testing) to monitor and deter attacks on defense information systems.
- the Defense Advanced Research Projects Agency, which has a large part of the DoD effort in basic R&D for information security. DARPA's efforts are located in its Information Technology Office (Information Survivability) and in the Information Systems Office (Information Assurance), and its efforts are coordinated with NSA and DISA through a memorandum of understanding. The mission of the Information Assurance Program is to "develop security and survivability solutions for the Next Generation Information Infrastructure that will reduce vulnerability and allow increased interoperability and functionality."[16] The program's objectives include architecture and infrastructure issues, preventing, deterring, and responding to attacks, and managing security systems. Its goal is to "create the security foundation" for the DII and future military C4I information systems.
- the National Security Agency (NSA), which develops cryptographic and other information systems security techniques to protect sensitive (classified and unclassified) U.S. communications and computer systems associated with national security. For many years, NSA produced link encryptors that were used to protect data during communications. As the boundary between communications and computing has blurred, however, NSA has broadened its protect mission on information assurance rather than just the more narrow communications security; today, information protection activities are found within the activities the Information Systems Security Organization (ISSO). This component of NSA houses considerable INFOSEC expertise, but the bulk of the NSA budget and human resources is devoted to the intelligence component of NSA's mission.
- the Defense Information Systems Agency, which serves as the manager for the Defense Information Infrastructure. In this role, it helps to "protect against, detect and react to threats to" the DII and DOD information sources.[17] The INFOSEC Program Management Office coordinates all INFOSEC activities for DISA by providing technical and product support as well as INFOSEC education throughout the DOD. In addition, the DISA Chief Information Officer's Information Assurance Division focuses on the implementation of information assurance by developing effective security policy and processes and establishing training and awareness program.[18]
- the Joint Command and Control Warfare Center (JC2WC), charged with providing direct tactical and technical analytical support for command and control warfare to operational commanders. The JC2WC supports the integration of Operations Security, Psychological Operations, military deception, Electronic Warfare (EW) and destruction throughout the planning and execution phases of operations. Direct support is provided to unified commands, joint task forces, functional and service components, and subordinate combat commanders. Support is also provided to OSD, the Joint Staff, the services and other government agencies. The JC2WC maintains specialized expertise in C2W systems engineering, operational applications, capabilities and vulnerabilities.

The Information Systems Security Threat

[15] Remarks made by the Deputy Secretary of Defense, John J. Hamre, in his "Statement Before The Senate Armed Services Committee Information Systems: Y2K & Frequency Spectrum Reallocation," June 4, 1998.

[16] See the DARPA Information Assurance home page at <http://web-ext2.darpa.mil/iso/ia/>.

[17] For future information, see the DISA home page at <http://www.disa.mil>.

[18] For additional information, see the DISA INFOSEC Program Management Office home page at <http://www.disa.mil/infosec/index.html>

Reliable threat estimates of national-level threats to DOD C4I systems are hard to obtain, even in the classified literature. Unlike more traditional threats (where vehicles and weapons platforms could be counted and exercises observed), the information security threat requires capital resources that are few in number and easily concealed and expertise that has both civilian and military applications and is thus difficult to control. Thus, threat estimates in this domain are necessarily more dependent on human judgment, with all of the subjectivity and uncertainty thereby implied.

That said, essentially all nations with hostile intent towards the U.S. have the financial resources and the technological capability to threaten U.S. C4I systems. Because the equipment budgets to threaten U.S. C4I systems are small, and the knowledge available world-wide, non-state groups (e.g., terrorist groups or domestic hackers) can also pose a threat.

For these reasons, prudent planning dictates a serious DOD response to such potential threats, even if they have not yet been part of a concerted national attack on the U.S.

Technical Assessment of C4I System Security

The available evidence from exercises which the committee observed (e.g., Blue Flag 98-2) or have received briefings (e.g., Eligible Receiver) show that security at all levels, from the national down to the platform level command in today's fielded systems is insufficient. The security in today's fielded military systems is weak, and weaker than it need be, as illustrated by the following examples of behavior and practices that the committee observed or heard:

- Individual nodes are running commercial software with many known security problems. Operators use little in the way of tools for finding these problems, to say nothing of fixing them.
- Computers attached to sensitive C2 systems are also used by personnel to surf Web sites worldwide, raising the possibility that rogue applets and the like could be introduced into the system.
- Units are being blinded by denial of service attacks, made possible because individual nodes were running commercial software with many known security problems.
- IP addresses and other important data about C2 systems can be found on POST-IT notes attached to computers in unsecured areas, making denial of service and other attacks much easier.
- Some of the networks used by DOD to carry classified information are protected by a perimeter defense. As a result, they exhibit all of the vulnerabilities that characterize networks protected by perimeter defenses.[19]

FINDINGS

Finding S-1: Protection of information and information systems is a pressing national security issue.

DOD is in an increasingly compromised position. The rate at which information systems are being relied upon outstrips the rate at which they are being protected. Also, the time needed to develop and deploy effective defenses in cyberspace is much longer than the time required to develop and mount an attack. The result is vulnerability: a gap between exposure and defense on the one hand and attack on the other. This gap is growing wider over time, and it leaves DOD a likely target for disruption or pin-down via information attack.

Finding S-2: The DOD response to the information systems security challenge has been inadequate.

[19] It is ironic that the use of a perimeter defense for a C4I network is inconsistent with the more stringent rules for protecting classified data in physical environments. For example, the storage of classified documents requires a safe in a room that is alarmed.

As noted in Section 0, the committee observed a variety of inadequate responses to the security problem in its field visits. Within the DOD, NSA is the primary repository of expertise with respect to information systems security, and this repository is arguably the largest and best in the world. Nevertheless, DOD has been unable to translate this expertise into adequate information assurance defenses except in limited areas (primarily the supply of cryptographic devices). For example, the committee observed in one exercise NSA personnel working in intelligence roles and in support of an information warfare attack cell. The information warfare defensive cell was not using NSA-supplied tools and was not directly supported by NSA personnel.

Many field commanders have told the committee that “Cyberspace is part of the battlespace”, and several organizations within the DOD assert that they are training “C2/Cyber warriors”. But good intentions have not been matched by serious attention to cyberspace protection. Soldiers in the field do not take the protection of their C4I systems nearly as seriously as they do other aspects of defense. For example, information attack red teams were a part of some exercises observed by the committee, but their efforts were usually highly constrained for fear that unconstrained efforts would bring the exercise to a complete halt. Granted that all red teams operate under certain rules of engagement established by the “white team”, but the information attack red teams appeared to the committee to be much more constrained than appropriate. In one exercise, personnel in an operations center laughed and mistakenly took as a joke a graphic demonstration by the red team that their operations center systems had been penetrated.

One particularly problematic aspect of the DOD response to information systems security is its reliance on passive defense. As noted above, passive defense does not impose a meaningful penalty against an opponent, and thus the opponent is free to probe until he or she finds a weak spot in the defense. This reliance upon passive defense is not a criticism of DOD, but rather an unavoidable consequence of a high-level policy decision made by the U.S. government that retaliation against cyber-attackers is not to be controlled or initiated by DOD; nevertheless, the committee is compelled to point out that this policy decision has a distinctly negative consequence for the security of DOD C4I systems.

On the technology side, the development of appropriate information systems security tools has suffered from a mindset that fails to recognize that C4I systems are today heavily dependent on commercial components that often do not provide high levels of security. It may be true that the most secure systems are those that are built from scratch with attention from the start paid to security; in essence, this is the philosophy on which NSA’s Trusted Computer Security Evaluation Criteria are based.[20] But in practice, system builders must obtain security from whatever is provided by COTS products, security which is admittedly inadequate against the best efforts of world-class adversaries but which would improve security against less sophisticated threats. Because NSA has focused its efforts to date with the “build from scratch” philosophy, real-world military C4I systems built on commercial components have very little effective security and low assurance they will work under real attacks.

DOD efforts in information systems security have also focused a great deal of attention on high-assurance multi-level security (MLS). MLS security mechanisms seek to prevent a hostile piece of software from leaking high-level (e.g. secret) information to low-level (e.g. uncleared) users. While hostile “Trojan horse” software is certainly a real and important threat, it is far from the most serious problem facing command and control systems today. For example, denial-of-service attacks represent a serious threat, not least because such attacks may be the easiest to conduct. Moreover, the U.S. computer industry has not found sufficient demand, either from the DOD or elsewhere, for MLS-qualified systems.[21] MLS may still be needed for certain specialized C4I applications, but from the standpoint of meeting the broad demands for security it is not a commercially viable approach.

[20] (The Orange Book) [ref.]

[21] At one time, the U.S. computer industry was preparing at its own expense high-assurance MLS systems for use by DOD. These systems failed to make the transition from development project to commercial product. Perhaps the best example of such a system is Digital Equipment Corporation’s VAX Virtual Machine Monitor security kernel. [ref. IEEE S&P 1990] This project was canceled, apparently for commercial reasons, in 1991 [check date]. The committee is aware of no similar systems on the horizon today. One major reason for the lack of demand for such

By contrast, the commercial sector has taken a largely pragmatic approach to the problem of information systems security. While acknowledging that security in the commercial sector is on average not particularly good, the best commercial practices for security are in general far in advance of what the committee has observed with fielded C4I systems. As noted above, the committee observed a number of instances were C4I security was inadequate but where adoption of existing good technologies and practices would greatly improve information systems security. Because these best practices have not been adopted for military use, the protection of C4I cyberspace is worse than it need be, and there is a large gap between the security that is reasonably possible today and the security that is actually in place.

An example of a more pragmatic approach might be to view the threat as a pyramid. A large percentage of the low-level threats at the base of the pyramid can be handled with readily available tools. This keeps the "ankle biters" out. The apex of the pyramid represents that small percentage of "professionals" that, given time, will penetrate any defense. The middle levels then are the ones that benefit most from concentrated system design work.

RECOMMENDATIONS

The committee believes that information systems security -- especially in its operational dimensions -- has received far less attention and focus than the subject deserves in light of a growing U.S. military dependence on information dominance as a pillar of its warfighting capabilities.

At the highest level of abstraction, the committee believes that *DOD must greatly improve the execution of its information systems security responsibilities*. The same military diligence and wisdom that the U.S. military uses to defend physical space can and must be applied to defend the “cyberspace” in which C4I systems operate. For example, the principle of defense-in-depth is a time-honored one, whose violation has often led to military disaster (e.g., the Maginot line).

This is easier said than done. The defense of physical spaces and facilities has a long history, while cyberspace is a new area of military operations. In cyberspace, boundaries are fluid, control is distributed and diffuse, and most of what occurs is invisible to the defender’s five senses without appropriate augmentation. As a result, analogies between physical space and cyberspace cannot be perfect, and may even be misleading. Nevertheless, a goal of achieving “cybersecurity” for C4I systems comparable to what can be achieved with physical security for physical facilities and spaces is a reasonable one that the DOD should strive to meet.

One critical aspect of improving information systems security is changing the DOD culture, especially within the uniformed military, to promote an information systems security culture. Organizational policies and practices are at least as important as technical mechanisms in providing information systems security. Policies specify the formal structures, ensure responsibility and accountability, establish procedures for deploying and using technical means of protection and assigning access privileges, create sanctions for breaches of security at any level of the organization, and require training in the privacy and security practices of an organization. Thus, the organizational issues relating to how to ensure the appropriate use of information systems security technologies are critical.

The culture of any organization establishes the degree to which members of that organization take their security responsibilities seriously. With a culture that values the taking of the offensive in military operations, the military may well have difficulty in realizing that defense against information attack is a more critical function than being able to conduct similar operations against an adversary, and indeed is more difficult and requires greater skill and experience than offensive information operations.

For example, the committee observed the 609th IW Squadron in action during the Blue Flag 98 exercise. The 609th Squadron had split responsibilities, responsible for both red team (attacking) and blue team (defending) information activities. The defensive cell performed its duties admirably, yet was

systems is that the time-to-market of MLS-qualified systems is so long that the functional capabilities of these systems have been superseded many times by other non-MLS systems over by the time they are available.

overwhelmed by its red team counterpart. (For example, the red team was able to download the Air Tasking Order before it was transmitted.) In asking about the composition of the two teams, committee members were told that that blue-team defensive duty and experience was a pre-requisite for participation on the red team.[22]

The notion that less experienced personnel first perform the defensive function and more experienced ones perform the offensive function is counter to normal practice in other settings. For example, NSA requires code-breaking experience before an analyst can begin to develop encryption algorithms. In general, the rule of good practice in information systems security is that the most experienced people serve the vital protection function.

In all instances of which the committee is aware, large organizations that take information systems security seriously have leadership that emphasizes its importance. Top-level commitment is not sufficient for good security practices to be put into place, but without it, organizations will drift to do other things that appear more directly related to their core missions. Thus, senior DOD leadership must take the lead to promote information systems security as an important cultural value for DOD.

Senior leadership is responsible for two tasks: the articulation of policy for the department as a whole, and oversight to ensure that policy is being properly implemented.

In this regard, the committee is encouraged by conversations with senior defense officials, both civilian and military, who appear to take information systems security quite seriously. Nevertheless, these officials have a limited tenure, and the issue of high-level attention is a continuing one.

A second obstacle to the promulgation of an information systems security culture is that good security from an operational perspective often conflicts with doing and getting things done. And because good information systems security results in nothing (bad) happening, it is easy to see how the can-do culture of DOD might tend to devalue it.

Finally, it is important to note that DOD must protect both classified and unclassified information. While DOD has a clear legislative mandate to protect both types of information, DOD treats the protection of classified information much more seriously than the protection of unclassified information. For example, DOD often responds to reports of hacker penetration by asserting that “no classified information was revealed.” Such assertions may be true, but they are also misleading, in that hostile adversary penetration of systems that process unclassified information (e.g., the schedules of transportation systems, the flow of logistics) may also result in serious harm to national security.

The first step is to take action now. Exercises such as Eligible Receiver have served as a “wake-up” call for many senior DOD leaders, both civilian and military. The perception at the highest levels of leadership that the information systems security problem is big, urgent, and real must translate quickly into actions that can be observed in the field.

One way of characterizing the committee’s recommendations is that the DOD should adopt as quickly as is possible best commercial practices, which are in general far in advance of what the committee has observed with fielded C4I systems. It is essential that security requirements be considered from the very beginning of each program and not postponed until later which inevitably causes either major cost increases or the requirements to be diluted or eliminated. As a next goal DOD must then attempt to advance the state of the art in each of these areas.

Finally, in an organization as large as DOD, recommendations must refer to concrete actions and to specific action offices responsible for their execution. On the other hand, given an ongoing restructuring and streamlining within DOD, especially within the Office of the Secretary of Defense and

[22] It can be argued that it is desirable to train against the most experienced adversaries. Indeed, experience at the National Training Center in which units in training are routinely overwhelmed by an experienced and superbly trained opposing force is based on this point. But for operational purposes, the commander must decide where to deploy his best personnel -- and the committee believes cyber-defense warrants the very best. Because units fight as they train, the committee believes that the most experienced personnel should be involved as defenders in exercises too. (An additional point is that the red-team threat so far overmatched the defense that red-team sophistication was never required.)

the Joint Chiefs of Staff, the committee is reluctant to specify action offices with too much confidence or precision. Thus, its recommendations are cast in terms of *what* the committee believes should be done, rather than specifying an action office. The argumentation for each recommendation contains, where appropriate, a paragraph regarding a *possible* action office or offices for that recommendation representing the committee's best judgment in that area. However, this action office (or offices) should be regarded as provisional, and DOD may well decide that a different action office is more appropriate given its organizational structure.

Recommendation S-1: The Secretary of Defense, through the ASD/C3I and the CJCS, should designate an organization responsible for providing direct defensive operational support to commanders.

As noted earlier, defensive information operations require specialized expertise that may take years to develop. Thus, it is in the short run unrealistic to expect operational units to develop their own organic capabilities in this area. Because the committee believes that all operators and commanders during exercises and operations must be supported in the C4I defensive role by specialized experts serving in operations centers, it makes sense to organize units that can be deployed with forces that are dedicated to providing operational support. Providing such support also reinforces the commitment of DOD to this mission.

In its site visits, the committee has observed limited resources devoted to providing operational support for the information systems security mission in some instances, such as the 609th IW Squadron at Blue Flag 98. But even in these instances (and they were not frequent), the defensive resources and efforts have been paltry compared to the magnitude and severity of the threat. NSA provides invaluable technical support, but for the most part does not appear to provide direct operational support to deployed units (or those on exercise). The services are beginning to pay more attention to the requirements of information systems security, and each has established an IW component, another promising development. But until the operators are brought into the picture in a central and visible manner, the security of fielded systems will remain inadequate.[23]

Only the Secretary of Defense has the necessary defense-wide purview of authority to designate and properly fund an appropriate organization to perform this function. The committee is silent on the appropriate executing organization, but notes that today. The JC2WC is charged with providing direct tactical and technical analytical support for command and control warfare to operational commanders, and it supports the integration of Operations Security (OPSEC), Psychological Operations (PSYOP), military deception, Electronic Warfare (EW) and destruction throughout the planning and execution phases of operations. Direct support is provided to unified commands, joint task forces, functional and service components, and subordinate combat commanders. Support is also provided to OSD, the Joint Staff, the services and other government agencies. The JC2WC maintains specialized expertise in C2W systems engineering, operational applications, capabilities and vulnerabilities. The JC2WC does do some of the things that the committee believes should be done in providing direct defensive support to commanders, but not on the scale that the committee believes is necessary.

Recommendation S-2: The Secretary of Defense should direct that all DOD civilian and military personnel receive appropriate training in the use of adequate information security tools, ensure that these tools are made available to all appropriate personnel, and hold both civilian and military personnel accountable for their information security practices.

[23] Today, NSA does provide significant SIGINT support to field commanders. Whether or not it is NSA that is tasked with providing defensive support to operational commanders, this NSA role with respect to SIGINT suggests the feasibility of such a role for some organization.

Accountability for upholding the values of an organization is an essential element of promulgating a culture. Once senior leaders have articulated a department-wide policy for information systems security and provided personnel with appropriate tools, training, and resources, it is necessary to develop well-defined structures with clear lines of responsibility.

Policies require procedures to translate their intent and goals into everyday practices, which may vary somewhat across departments. The most important aspect of such procedures is that authority and responsibility for implementation must be clearly assigned and audited by higher authority. In addition, units within the organization need procedures that to determine the proper access privileges to an information system for individuals. Furthermore, privileges once determined must be established responsively (e.g., a new user needs certain privileges granted quickly in order to perform his or her job, and users who have been compromised must have their privileges revoked quickly).

In addition to the necessary policies and procedures, accountability within DOD rests on several pillars, including:

- education and training. All users of information and C4I systems receive some minimum level of training in relevant security practices *before* being granted access to these systems. Refresher courses are also necessary to remind long-time users about existing practices and to update them on changes to the threat. Note also that training activities for information systems security can be seen as a disruptive and unnecessary intrusion into the already busy schedule of personnel.
- incentives, rewards, and opportunities for professional advancement. For security to be taken seriously, people within the organization must see the benefits and costs of compliance with good security practices. For example, promotions and an upward career path should be possible for specialists in information systems security, understanding that unless pay scales are changed, the lure of the private sector may prove irresistible for many individuals. Personnel who demonstrate extraordinary diligence or performance under information attack should be eligible for special recognition (e.g., cash awards, medals).
- individual and unit-based measures of performance. Military and civilian personnel should have an information security component as part of their performance ratings. Units should be rated with respect to their information security practices in exercises.
- sanctions. The other side of rewards is sanctions. Sanctions for violations of good information systems security practice must be applied uniformly to all violators. Experience in other organizations indicates that if security practices are violated and no response follows, or if sanctions are applied, but only irregularly, after a long delay, or with little impact on perpetrators, the policy regime promoting security is severely undermined, and its legitimacy is suspect. Commanders and high-ranking officials in particular are often willing to compromise security practices for their own convenience and ease-of-use, and may not give the subject due attention in their oversight roles. It is thus not unreasonable that system administrators and their commanders, given the necessary tools, training, and resources be held accountable or keeping systems configured securely and maintaining good operational security practices with respect to information systems security.[24]

Because this recommendation calls for an across-the-board cultural change within DOD, many different offices must be involved. The senior leadership within the department – the Secretary of Defense – must take responsibility for a department-wide policy on information systems security. The Service Secretaries and their military Chiefs of Staff must develop policies that tie performance on information systems security issues to appropriate sanctions and rewards. Given NSA's traditional role in providing tools for information security, NSA is probably the most appropriate agency to identify available tools that are practically usable by DOD personnel at all levels of seniority and irrespective of specialized expertise (i.e., they should be usable by tank commanders as well as C4I specialists).

[24] For example, the Army has explored the possibility of security regulations that would make base commanders and systems operators liable for information systems intrusions under the military's Uniform Code of Military Justice. See "Army to hold commanders and sysops liable for hacks", Elana Varon, *Federal Computer Week*, February 2, 1998, Volume 12(3).

Military departments and the OSD must take steps to instruct military and civilian personnel respectively in the use of these tools.

Recommendation S-3: The Secretary of Defense, through the ASD/C3I, the CJCS, and the CINCs should support and fund a program to conduct frequent, unannounced penetration testing of deployed C4I systems.

As noted above, a continuing search for technical and operational/procedural vulnerabilities in a network or system is essential, especially for those that are operating in an exercise or in an actual deployment. (An example of such a search is the COMSEC monitoring undertaken by NSA. In other domains such as base security, unscheduled red-team visits are not uncommon) Such tests should be conducted at a level consistent with a high-grade threat, and must be conducted against different C4I assets. These “red team” or “tiger team” probes would be unscheduled and conducted without the knowledge of the installation being probed; furthermore, the teams conducting would report to and be under the direction of parties that are separate from those of the installation being tested. Information gleaned from these probes should be passed to cognizant authorities within the DOD and the administrator of the network penetrated; if a penetration is successful where the implementation of a known fix would have stopped the penetration, the commander of the installation and the administrator should be sanctioned. Note the critical focus on C4I systems operating in a “full-up” mode, rather than on individual C4I components.

A second important element of penetration testing is for the installation itself -- probably under the technical direction of the on-site system administrator -- to conduct or request its own penetration testing. Information on successful penetrations conducted under these auspices should still be shared with cognizant DOD authorities, but in order to encourage installation commanders to conduct such testing on their own, sanctions should not be applied to vulnerabilities that are discovered.

In the area of DOD-wide penetration testing, the ASD/C3I has the authority to direct such testing. The CINCs, especially ACOM as the force provider, have operational responsiblities, and JCS must cooperate in the promulgation of policy in this area because such testing has a direct impact on operational matters. The committee also notes that the Information Warfare Red Team (IWRT) of the Joint Command and Control Warfare Center (JC2WC) in San Antonio, Texas[25], was created to improve the readiness posture of the DoD by identifying vulnerabilities in information systems and vulnerabilities caused by use of these information systems and then demonstrating these vulnerabilities to operators and developers (sometimes as part of the opposition force in exercises. The IWRT was initiated in 1995 and is sponsored jointly by the DUSD(AT), the Office of the Assistant Secretary of Defense (Command, Control, Communications and Intelligence (OASD (C3I)) and the Joint Staff (J-3). Establishing the IWRT is an important step in the right direction to support the intent of this recommendation, but the scale of the activities undertaken by the IWRT is incommensurate with the much larger need for such testing.

Recommendation S-4: The ASD/C3I should mandate the department-wide use of currently available system/network management tools and strong authentication mechanisms immediately.

Many information vulnerabilities arise from improper system or network configuration.[26] For example, a given system on a network may have a modem improperly attached to it that is not known to the network administrator. It may be attached for the most benign of reasons, such as a programmer or an applications developer who needs off-hours access to the system to complete work on an application on time. But the very presence of such a device introduces a security hole through which penetrations

[25] See http://www.aia.af.mil/aialink/homepages/pa/bios/jc2wc.html

[26] [note: not source code configuration management]

may occur. Or, a firewall may be improperly configured to allow Web access for a certain system when in fact the system should only be able to transmit/receive e-mail. Default passwords and accounts may still be active on a given system, allowing adversaries inappropriate access. Foreign software may have been downloaded inadvertently for use on some system, software whose purpose is hostile.

A network/system administrator should know the configuration of the network/systems for which he is responsible. He or she should be able to find unauthorized modems, poor passwords, factory settings, unpatched holes in operating systems. But because checking an operational configuration is very labor-intensive if done manually, configuration management and network assessment tools must be able to run under automated control on a continuous basis, alerting the administrator when variances from the known configuration are detected. Some tools are available to do configuration management and network assessment, as well as inspection tools that allow correct configurations to be inspected. These tools are not perfect, but their widespread use would be a significant improvement over current DOD practice.

A second aspect of configuration control is more difficult to achieve. Good configuration control also requires that every piece of executable code on every machine carry a digital signature that is checked as a part of configuration monitoring. Furthermore, code that cannot be signed (for example, macros in a word processor) must be disabled until development indicates a way to sign it. Today, it is quite feasible to require the installation of virus-checking programs on all servers and to limit the ability of users to download or install their own software (though Java and Active-X applets do complicate matters to some extent). Census software or regular audits can be used to ensure compliance with such policies. However, no tool known to the committee and available today undertakes this task systematically. Tools for systematic code verification are an area in which DOD-sponsored R&D could have high payoff in both the military and civilian worlds, as organizations in both worlds face the same problem of hostile code.

Note that it is not practical to secure every system in the current inventory. It is probably unrealistic to develop and maintain tools that do thorough monitoring of the security configuration for more than two or three platforms (e.g., Windows NT and Sun Unix). Over the long run, it may well be be necessary to remove other systems from operational use, depending on the trade-offs between lower costs associated with maintaining fewer systems and greater security vulnerabilities arising from less diversity in the operating systems base.

Authentication of human users is a second area in which DOD practices do not match the best practices found in the private sector.   Passwords -- ubiquitously used within the DOD as an authentication device -- have many well-known weaknesses. An adversary can guess passwords, or re-use a compromised password (e.g., one found in transit on a network by a “sniffer”), and can compromise a password without the knowledge of its legitimate user without his or her knowledge.

A hardware-based authentication mechanism suffers from these weaknesses to a much lesser extent.[27] Because the mechanism is based on a physical piece of hardware, it cannot be duplicated freely (whereas passwords are duplicated when one person tells another a password). The hardware can be designed to be tamper-resistant, which increases the difficulty of duplicating it.   Furthermore, because persistent (i.e., long-lasting) identifying information is never transmitted outside the piece of hardware, attacks to which password authentication is vulnerable (e.g., sniffing and playback attack) are essentially impossible. Hardware-based authentication is a highly effective method for authenticating communications originating from individuals. It also has particular value in the protection of remote access points (Box 0.4).

---- Insert Box 0.4 about here ----

[27] The device (e.g., a PC card) is enabled by a short password, usually called a PIN, entered by the user directly into the device. The device then engages in a secure and unforgeable cyrptographic protocol with the system demanding the authentication; this protocol is much stronger than any password could be. The use of passwords is strictly local to the device and does not suffer from the well-known problems of passwords on networks, for example sniffing and playback attacks. This authentication depends on what you have (the device) together with that you know (the PIN).

Biometric identifiers complement hardware-based authentication devices. Because biometric information is closely tied to the user, biometric identifiers serve a function similar to that of the PIN that is used to activate the device. Biometric identifiers are based on some distinctive physical characteristics of an individual (e.g., a fingerprint, a voiceprint, a retinal scan); biometric authentication works by comparing a real-time reading of some biometric signature to a previously stored signature. Biometric authentication is a newer technology than that of hardware-based authentication; as such it is less well-developed (e.g., slower, less accurate) and more expensive even as it promises to make PINs entirely obsolete.

Hardware-based authentication can also be used to authenticate all computer-to computer communication (e.g., those using security protocols such as Secure Sockets Layer (SSL) or IPsec). In this way, all communications carried in the network can be authenticated, not just those from outside a security perimeter. "Mutual suspicion" requiring mutual authentication among peers is an important security measure in any network.

The potential value of strong authentication mechanisms is more fully exploited when the authentication is combined with mechanisms such as IPSec or TCP wrappers that protect the host machines against suspicious external connections[28] and a fine-grained authorization for resource usage. For example, a given user may be allowed to read and write to some databases, but only to read others. Access privileges may be limited in time as well (e.g., a person brought in on a temporary basis to work a particular issue may have privileges revoked when he or she stops working on that issue.) In addition (or in other words?), the network administrator should be able to establish groups of users that are authorized to participate in a particular missions and the network configured to allow only such interactions as necessary to accomplish those missions. Similarly, the network administrator should be able to place restrictions on the kinds of machine-to-machine interactions allowable on the network. This requires that the administrator has tools for the establishment of groups of machines allowed to interact in certain ways.

Some network management/configuration systems allow configuration control that would support fine-grained access controls. But most do not make it easy for a network administrator to quickly establish and revoke these controls.

Finally, the trend of today towards "single login" presents a dangerous vulnerability. When a perimeter defense is breached, an adversary can roam the entire network without ever being challenged again to authenticate himself. A more secure arrangement would be for the network to support remote interrogation of the hardware authentication device by every system the user attempts to access, even though the user need only enter the PIN once to activate the device. In this way, every request to a computer, no matter where it is located on the network, is properly supported by strong evidence of the machine and the individual that is responsible for the request, allowing this evidence to be checked against the rules for that determine who is allowed access to what resources.

Implementing this recommendation is not easy, but is well within the state of the art. A reader for a hardware authentication device in every keyboard and in every laptop (via PC-card slots) is very practical today.[29] In principle, even smart "dog tags" could be used as the platform for a hardware

[28] TCP wrappers protect individual server machines, whereas firewalls protect entire networks and groups of machines. Wrappers are programs that intercept communications from a client to a server and perform a function on the service request before passing it on to the service program. Such functions can include security checking. For example, an organization may install a wrapper around the patient record server physicians use to access patient information from home. The wrapper could be configured to check connecting IP addresses against a predefined approved list and to record the date and time of the connection for later auditing. Use of wrapper programs in place of firewalls means that all accessible server machines must be configured with wrapper(s) in front of network services, and they must be properly maintained, monitored, and managed. See Venema, Wietse. 1992. "TCP WRAPPER: Network Monitoring, Access Control and Booby Traps," pp. 85-92 in *Proceedings of the Third Usenix UNIX Security Symposium,* Baltimore, Md., September.

[29] The Fortezza card was an attempt by the DOD in the mid-1990's to promote hardware-based authentication. While the Fortezza program itself has not enjoyed the success that was once hoped for it, the fact remains that one of

authentication device. However, the most difficult issue is likely to be the establishment of the public key infrastructure for DOD upon which these authentication devices will depend. Biometric authentication devices are not practical for universal deployment (e.g., for soldiers in the field), but they may be useful in more office-like environments (e.g., command centers).

Since DOD increasingly relies on commercial technology for the components of C4I systems, engagement of commercial support for authentication is important to making this affordable. It should be possible to enlist strong industry support for this technology program if it is properly conceived and marketed. Many commercial customers have very similar requirements, which are poorly met by existing security products. If the DOD can field systems containing security that is as good as what these customers want, it will be better than it is today. Therefore, from a practical standpoint, the DOD's needs with respect to authentication are very similar to commercial needs.

Because this recommendation calls for DOD-wide action with respect to C4I systems, the ASD/C3I must promulgate appropriate policy for the department. The information security policy is within the purview of the DOD's Chief Information Officer, who today is also the ASD/C3I. Finally, given its history of involvement with information systems security, NSA is probably the appropriate body to identify the best available authentication mechanisms and configuration tools.

Recommendation S-5: The Undersecretary of Defense for Acquisition and Technology and ASD/C3I should direct the appropriate defense agencies to develop new tools for information security.

Aligning DOD information security practice with the best practices found in industry today would be a major step forward in the DOD information security posture, but it will not be sufficient. Given the stakes of national security, DOD should feel an obligation to go further still. Going further will require research and development in many areas.

For example, good configuration control requires that every piece of executable code on every machine carry a digital signature that is checked as a part of configuration monitoring. Furthermore, code that cannot be signed (for example, macros in a word processor) must be disabled until development indicates a way to sign it. Tools for systematic code verification are an area in which DOD-sponsored R&D could have high payoff in both the military and civilian worlds, as organizations in both worlds face the same problem of hostile code.

A second example involves fine-grained authorization for resource usage. Some network management/configuration systems allow configuration control that would support fine-grained access controls. But most do not make it easy for a network administrator to quickly establish and revoke these controls, and DOD-sponsored R&D in this area could have high payoff as well.

A third area for R&D is tools that can be used in an adaptive defense of its C4I systems. Adaptive defenses change the configuration of the defense in response to particular types of attack. In much the same way that an automatic teller machine eats your ATM card if the wrong PIN is entered more than three times, an "adaptive" defense that detects an attack being undertaken through a given channel can deny access to that channel for the attacker, thus forcing him to expend the time and resources to find a different channel. More sophisticated forms of adaptive defense might call for "luring" the attacker into a safe area of the system and manipulating his cyber-environment to waste his time and to feed him misleading information.

A fourth area for R&D is biometrics. The basic technology and underlying premises of biometrics have been validated, but biometric authentication mechanisms are still sometimes too slow and too inaccurate for convenient use. (For example, they often take longer to operate than typing a password, and they sometimes result in false negatives (that is, they reject a valid user fingerprint or retinal scan).) Broad user acceptance will depend both on more convenient-to-use mechanisms and the

the capabilities that Fortezza provides —widespread use of hardware-based authentication—is likely to prove a valuable security tool.

integration of biometrics into the man machine interface such as a fingerprint reader in a mouse or keyboard.

Finally, R&D on active defenses is needed. Active defenses make attackers pay a price for attacking (whether or not successful), thus dissuading a potential attacker, and offering deterrence to attack in the first place (an idea that raises important policy issues as Recommendation 3.7 (below). Passive information systems security is extremely important but against a determined opponent with the time and resources to conduct an unlimited number of penetration attempts against a passive non-responding target, the attacker will inevitably succeed. This area for R&D raises important policy issues that are discussed below. But the fact remains that even if policy allowed the possibility of retaliation, the tools to support such retaliation are wholly inadequate. Instruments to support a policy-authorized retaliation are needed in two areas:

- <u>Identification of an attacker</u>. Before any retaliatory action can be undertaken, the attacker must be identified in a reasonable time scale with a degree of confidence commensurate with the severity of that action. Today, the identification of an attacker is an enormously time-consuming task -- even if the identification task is successful, it can take weeks to identify an attacker. And, it is often that considerable uncertainty remains about the actual identity of the attacker, who may be an individual using an institution's computer without the knowledge or permission of that institution. Note also that better tools for the accurate and rapid location of cyber-attackers would greatly assist law enforcement authorities in apprehending and prosecuting them.
- <u>Striking back against an attacker</u>. Once the attacker is identified, tools are needed to attack him. Many of the techniques employed against friendly systems can be used against an attacker as well, but all of these techniques are directed against computer systems rather than individual perpetrators. Furthermore, using these techniques may well be quite cumbersome for friendly forces (just as they are for attackers). However, the most basic problem in striking back is that from a technical perspective, not enough is known about what retaliation and active defenses might be.

Other possible R&D areas include: secure composition of secure systems and components to support ad hoc (e.g. coalition) activities; better ways to configure and manage security features; generation of useful security specifications from programs; more robust and secure architectures for networking (e.g., requiring trackable, certificated authentication on each packet, along with a network fabric that denies transit to unauthenticatable packets); and automatic determination of classification from content.

Many agencies within DOD can conduct research and development for better information security tools, but a high-level mandate for such activity would help increase the priority of work in this area for such agencies. NSA and DARPA are the most likely agencies to develop better tools for information systems security. As noted in Chapter 3, better tools developed for DOD use are also likely have considerable application in the commercial sector, a fact that places a high premium on conducting R&D in this area in an unclassified manner. Note that *Trust in Cyberspace* also outlines a closely related research agenda.

Recommendation S-6: The Chairman of the Joint Chiefs of Staff and the Service secretaries should direct that all tests and exercises involving DOD C4I systems be conducted under the routine assumption that they are connected to a compromised network.

Because both threat and technology evolve rapidly, perfect information systems security will never be achieved. Prudence thus requires C4I developers and operators to assume some non-zero probability that any system will be successfully attacked, that some DOD systems have been successfully attacked, and that some C4I systems are compromised at any given moment. (A "compromised" system or network is one that an adversary has penetrated or disrupted in some way, so that it is to some extent no longer capable of serving all of the functions that it could serve when it was not compromised.). This pessimistic assumption guards against the hubris of assumed perfection. However, despite this assumption, most of the C4I systems connected to the compromised components should be able to function effectively despite local security failures.

C4I systems should be designed and developed so that their functions and connectivity are easy to reconfigure under different levels of information threat. Critical functions must be identified in advance for different levels of threat (at different “infocons”) so that responses can occur promptly in a planned and orderly fashion. Note also that the nature of a mission-critical function may vary during the course of a battle.

C4I systems should be tested and exercised routinely under the assumption that they are connected to compromised systems. Doctrine should account for this possibility as well. Commanders must have a range of useful responses when they detect an information attack. This premise differs from today’s operational choices, which are either to stay connected to everything or to disconnect and have nothing, with added exhortations to “be careful” when intrusions are detected. Finally, units must know how they will function when the only C4I available to them is unsecured voice communications.

Because this recommendation affects all operational deployments and exercises, both service and joint, a number of offices must take action. The CJCS should promulgate a directive that calls for such a policy in all joint exercises and operational deployments. And, because many C4I systems are owned and operated and controlled by the services, the Services – perhaps through their training and doctrine commands -- should establish doctrinal precepts for commanders to follow in implementing this policy.

Recommendation S-7: The Secretary of Defense and the Chairman of the Joint Chiefs of Staff should take the lead in explaining the severe consequences for its military capabilities that arise from a purely passive defense of its C4I infrastructure and exploring policy options to respond to these challenges.

Because a purely passive defense will ultimately fail against a determined attacker does not pay a price for unsuccessful attacks, a defensive posture that allows for the possibility of inflicting pain on the attacker would bolster the security of U.S. C4I systems.[30] Today, a cyber-attack on U.S. C4I systems is regarded primarily as a matter for law enforcement, which has the lead responsibility for apprehending and prosecuting the attacker. DOD personnel may provide technical assistance in locating and identifying the attacker, but normally DOD has no role beyond that.

If an attack is known with certainty to emanate from a foreign power (a very difficult task, to be sure) and to be undertaken by that foreign power, the act can be regarded as a matter of national security. If so, then a right to self-defense provides legal justification for retaliation. If the National Command Authorities (i.e., the President) decides that retaliation is appropriate, the remaining questions are those of form (e.g., physical or cyber) and severity (how hard to hit back). Under such circumstances, DOD would obviously play a role. However, DOD is legally prohibited from taking action beyond identification of a cyber-attacker on its own initiative, even though the ability of the U.S. to defend itself against external threats is compromised by attacks on its C4I infrastructure, a compromise whose severity will only grow as the U.S. military becomes more dependent on the leverage provided by C4I.

From a national security perspective, the geographical origin of the attack matters far less than the fact that it is military C4I assets that are being attacked. Thus, the military desirability of cyber-retaliation to protect the nation’s ability to defend itself should be clear. But the notion of cyber-retaliation raises many legal and policy issues, including issues related to Constitutional law, law enforcement, and civil liberties.

[30] DOD is not alone in having to deal with the difficulties of a purely passive defense. But given the consequences for the national security, the inevitable consequences of passive defense have immense significance for DOD.

As a first step, DOD should review the legal limits on its ability to defend itself and its C4I infrastructure against information attack.[31] After such a review, DOD should take the lead in advocating changes in national policy (including legislation, if necessary) that change the current "rules of engagement" specifying the circumstances under which force is an appropriate response to a cyber-attack against its C4I infrastructure. These rules of engagement would explicitly specify the nature of the force that could be committed to retaliation (e.g., physical force, cyber-attack), the damage that such force should seek to inflict, the authorizations needed for various types of response, the degrees of certainty needed for various levels of attack, the issues that would need to be considered in any response (e.g., do the benefits of exploiting the source of an attack outweigh the costs of allowing that attack to continue), and the oversight necessary to ensure that any retaliation falls within all the parameters specified in the relevant legal authorizations.

The committee is not advocating a change in national policy with respect to cyber-retaliation. Indeed, it was not constituted to address the larger questions of national policy, i.e., whether other national goals do or do not outweigh the narrower national security interest in protecting its military information infrastructure, and the committee is explicitly silent on the question of whether DOD should be given the authority (even if constrained and limited to specific types and circumstances) to allow it to retaliate against attackers of its C4I infrastructure. But it does believe that DOD should take the lead in explaining the severe consequences for its military capabilities that arise from a purely passive defense, that DOD should support changes in policy that might enable it, perhaps in concert with law enforcement agencies, to take a less passive stance, and that a national debate should begin about the pros and cons of passive vs active defense.

The public policy implications of the recommendation profound enough that they call for involvement at the highest levels of the DOD – the active involvement of the secretary of defense is necessary to credibly describe the implications of passive defense for C4I systems in cyberspace.

To whom should DOD explain these matters? Apart from the interested public, the Congress plays a special role. The reason is that actual changes in national policy in this area that enable a less passive role for DOD will certainly require legislation. Such legislation would be highly controversial, have many stakeholders, and would be reasonable to consider (let alone adopt) only after a thorough national debate on the subject.

[31] Press reports indicate that DOD authorities are "struggling to define new rules for deciding when to launch cyber attacks, who should authorize and conduct them and where they fit into an overall defense strategy." See Bradley Graham, "Authorities Struggle With Cyberwar Rules", *Washington Post,* July 8, 1998; Page A1.

Box 0.1: Eligible Receiver

Conducted in the summer of 1997 and directed by the Chairman of the Joint Chiefs of Staff, Eligible Receiver 97 was the first large-scale no-notice DOD exercise (a real, not table-top, exercise) designed to test the ability of the U.S. to respond to an attack on the DOD and U.S. national infrastructure. This exercise involved a simulated attack against components of the national infrastructure (e.g., power and communications systems) and an actual "Red Team" attack against key Defense information systems at the Pentagon, Defense Support Agencies, and in Combatant Commands.

The attack on the national infrastructure was based on potential vulnerabilities, while the actual attack on defense systems exploited both actual and potential vulnerabilities. (The vulnerabilities exploited were common ones, including bad or easily guessed passwords, operating system deficiencies, and improper system configuration control, sensitive site-related information posted on open web pages, inadequate user awareness of operational security, and poor operator training.) All Red Team attacks were based on information and techniques derived from open non-classified research, and no insider information was provided to the Red Team. Furthermore, the Red Team conduced extensive "electronic reconnaissance" before it executed its attacks.

The exercise demonstrated a high degree of interdependence between the Defense and National Information Infrastructures. For example, the defense information infrastructure is extremely reliant on commercial computer/communication networks, and the public and private sectors often share common commercial software/systems. As a result, vulnerabilities demonstrated in DOD systems and procedures may be shared by others, and vulnerabilities in one area may allow exploitation in other areas.

The exercise revealed vulnerabilities in DOD information systems and deficiencies in the ability of the U.S. to respond effectively to a coordinated attack on the national infrastructure and infromation systems. Poor operations and information security practices provided many Red Team opportunities. In short, the exercise provided real evidence of network vulnerabilities.

Box 0.2: Some related studies on information security

Computers at Risk

Computers at Risk: Safe computing in the information age (CSTB, 1991) focused approaches for "raising the bar" of computer and communications security so that all users – both civilian and military – would benefit, rather than just those users and handlers of classified government information. The report responded to prevailing conditions of limited awareness by the public, system developers, system operators, and policymakers. To help set and raise expectations about system security, the study recommended the following:

- Development and promulgation of a comprehensive set of generally accepted security system principles (GSSP);
- Creation of a repository of data about incidents;
- Education in practice, ethics, and engineering of secure systems; and
- Establishment of a new institution to implement these recommendations.

Computers at Risk also analyzed and suggested remedies for the failure of the marketplace to substantially increase the supply of security technology; export control criteria and procedures were named as one of many contributing factors. Observing that university-based research in computer security was at a "dangerously low level," the report mentioned broad areas where research should be pursued.

Report of the Defense Science Board Task Force on Information Warfare Defense (IW-D)

In 1996, a Defense Science Board task force focused on defending against cyber-threats and information warfare. The task force documented an increasing military dependence on networked information infrastructures, analyzed vulnerabilities of the current networked information infrastructure, discussed actual attacks on that infrastructure, and formulated a list of threats that has been discussed broadly within the Department of Defense (DOD) and elsewhere. The task force concluded that "there is a need for extraordinary action to deal with the present and emerging challenges of defending against possible information warfare attacks on facilities, information, information systems, and networks of the United States which [sic] would seriously affect the ability of the Department of Defense to carry out its assigned missions and functions."

Some of the task force recommendations answered organizational questions, e.g., where within DOD various IW-D functions might be placed, how to educate senior-level government and industry leaders about vulnerabilities and their implications, how to determine current infrastructure dependencies and vulnerabilities. Other recommendations addressed short-and longer-term technical means for repelling attacks. The task force urged greater use of existing security technology, certain controversial encryption technology, and the construction of a minimum essential information infrastructure (MEII). The task force noted the low levels of activity concerning computer security and survivable systems at universities, and also suggested a research program for furthering the development of:

- System architectures that degrade gracefully and are resilient to failures or attacks directed at single components;
- Methods for modeling, monitoring, and managing large-scale distributed systems; and
- Tools and techniques for automated detection and analysis of localized or coordinated large-scale attacks, and tools and methods for predicting anticipated performance of survivable distributed systems.

Trust in Cyberspace

Trust in Cyberspace (CSTB, 1998) proposed a research agenda for building networked systems that are more robust, reducing software design problems, and developing mechanisms to protect against new types of attacks from unauthorized users, criminals, or terrorists. The report noted that much of the today’s security technology for operating systems is based on a model of computing centered on mainframe computers.   Today, different security mechanisms are needed to protect against the new classes of attacks that become possible because of computer networks, the distribution of software using the Internet, and the significant use of commercial, off-the-shelf software.   Furthermore, the report recommended a more pragmatic approach to security that incorporates add-on technologies, such as firewalls, and utilizes the concept of "defense in depth," which requires independent mechanisms to isolate failures so that they don't cascade from one area of the system to another.

In the area of network design, the report noted a need for research to better understand how networked information systems operate, how their components work together, and how changes occur over time. Since a typical computer network is large and complex, few engineers are likely to understand the entire system. Better conceptual models of such systems will help operators grasp the structure of these networks and better understand the effects of actions they may take to fix problems. Approaches to designing secure networks built from commercially available software warrant attention. Improvements in testing techniques and other methods for determining errors also are likely to have considerable payoffs for enhancing assurance in networked systems.

Finally, research is needed to deal with the major challenges for network software developers that arise because COTS components are used in the creation of most networked information systems. Indeed, today’s networked information systems must be developed with limited access to significant pieces of the system and virtually no knowledge of how those pieces were developed.

The first two summaries stolen from Trust in Cyberspace.

Box 0.3: Information Operations Conditions (INFOCONs)

One implementation of INFOCONs is defined by the U.S. Strategic Command. Beginning with the Defense Science Board report of 1996 identifying a need for structured response to attacks on the nation's information infrastructure, the Information Assurance division of Stratcom drafted operating instructions that became the INFOCON program. INFOCONs "provide a set of pre-established measures to assess threats against the Command's information systems and defines graduated actions to be taken in response to those threats." On a day-to-day basis, the INFOCON is set at "normal", and only routine security measures are taken. If increased hostile actions are detected, INFOCONs are increased to raise information assurance awareness, with higher INFOCONs representing more intense hostile activity and more rigorous response actions.

INFOCONs are roughly analogous to DEFCON and Terrorist THREATCON levels. The decision to change the INFOCON is based on the assessed threat, the capability to implement the required protective measures, and the overall impact the action will have on USSTRATCOM's capability to perform its mission. INFOCONs define appropriate information operations measures to be taken. Each INFOCON is designed to produce detection, assessment and response measures commensurate with the existing threat. Escalating INFOCONs enhance Information operations capabilities and send a clear signal of increased readiness. Different INFOCONs are not necessarily linear in nature as an organized malicious information attack could immediately require higher INFOCONs to be set and appropriate measures taken.

INFOCON procedures received their first full scale workout during USSTRATCOM's annual readiness exercise Global Guardian '98. Stratcom officials believe that exercise results demonstrated the ability of INFOCONs to raise security awareness and to counter hostile actions. For example, based on independent monitoring of communications during Global Guardian, Stratcom officials believe that improved operations security practices were demonstrated as compared to previous exercises-an improvement attributed in part to the new INFOCONs.

Source: Adapted from Intercom on-line, January 1998...........Vol. 4, No. 1
(http://infosphere.safb.af.mil/~rmip/98jan/intercom.htm)

Box 0.4: Protection of Remote Access Points

Remote access points pose particular vulnerabilities. A hostile user attempting to gain access to a computer on the premises of a U.S. command post, for example, must first gain physical entry to the facility. He also runs the risk of being challenged face-to-face in his use of the system. Thus, it makes far more sense for an adversary to seek access remotely, where the risk of physical challenge is essentially zero.

Strong authentication -- whether hardware-based or biometric -- is thus particularly important for protecting remote access points that might be used by individuals with home or portable computers. Some organizations (not necessarily within the DOD) protect their remote access points by using dial-back procedures[32] or by embedding the remote access telephone number in the software employed by remote users to establish a connection. Neither approach is adequate for protecting remote access points (e.g., dial-back security is significantly weakened in the face of a threat who is capable of penetrating a phone switch, such as a competent military IW group) and their use does not substitute for strong authentication techniques.

[32] In a dial-back procedure, a remote user dials a specified telephone number to access the system. The system then hangs up and checks the caller's number against a directory of approved remote access telephone numbers. If the number matches an approved number, the system dials the user back and restores the connection.