Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
2000		**00-00-2000 to 00-00-2000**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Cyber Warfare: Protecting Military Systems	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Air Force Material Command (AFMC),Wright Patterson AFB,OH,45433**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES
Acquisition Review Quarterly, Spring 2000

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**Same as Report (SAR)**	**22**	

CYBER WARFARE: *PROTECTING MILITARY SYSTEMS*

Lt Col Lionel D. Alford, Jr., USAF

Software is a key component in nearly every critical system used by the Department of Defense. Attacking the software in a system—cyber warfare—is a revolutionary method of pursuing war. This article describes various cyber warfare approaches and suggests methods to counter them.

Karl von Clausewitz (1996) defined war as "…an act of violence intended to compel our opponent to fulfill our will… In order to attain this object fully, the enemy must be disarmed, and disarmament becomes therefore the immediate object of hostilities…." At the end of the second millennium, this definition no longer describes the full spectrum of modern warfare. In the future, we will have the potential to make war without the use of violence and fulfill the second half of von Clausewitz's definition—with software alone. Today's software-intensive systems make this possible.

"Cyber" describes systems that use mechanical or electronic systems to replace human control. In this article the term includes systems that incorporate software as a key control element. Cyber warfare can be executed without violence, and therefore the dependence on software-intensive systems—cyber systems—can make nations vulnerable to warfare without violence.

FROM PROTECTING INFORMATION TO PROTECTING SOFTWARE-CONTROLLED SYSTEMS

Cyber warfare is the conduct of military operations according to information-related principles (Arquilla and Ronfeldt, 1992). This does not define the full degree of capabilities now possible in cyber warfare. Limiting the scope of cyber warfare to "information-related principles" does not describe what happens when an enemy disrupts the electrical power grid of a nation by hacking into the controlling software (Figure 1). Information is not only

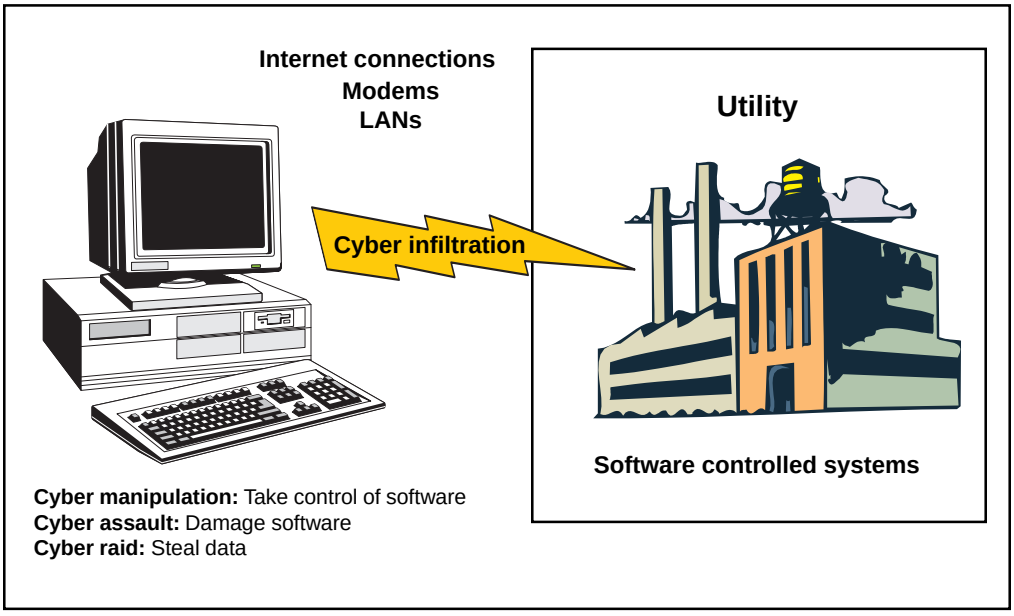

Figure 1. Infiltration of a Utility

at risk—the fundamental control of the civilization is. As technology pro-gresses, this "fundamental control" will devolve into networks and software-controlled electronics (Vatis, 1998).

This transition has already occurred in aviation. In the past, 100 percent of an aircraft's performance and capabilities were defined by hardware—the physical makeup of the aircraft. Today in the most advanced aircraft, 75 percent or more of the aircraft's performance and capability is absolutely dependent upon the software (U.S. Air Force, 1992). Without software, aircraft would not be controllable or reach the desired performance capabilities.[1] In some cases, through software, aircraft performance is gaining limited independence from physical configuration.[2]

Software dependence and hardware independence are growing. For example, modern aircraft fly by wire, their engines are controlled by wire, and their weapons are fired and dropped by wire. Systems that in the past were entirely hardware with mechanical control are being replaced by software with software control. Software defines the strength of modern systems, and provides a basis for the integration of many disparate items through networking. These networked software systems are under attack today, and the attacks are increasing (Figure 2).

Current Department of Defense (DoD) doctrines and instructions do not adequately cover the scope of cyber warfare (Stein, 1995). The following all handle information warfare as a discrete part of a military system: Joint Publication (JP) 3-13, "Joint Doctrine for Information Operations"; JP 3-13.1, "Joint Doctrine for Command and Control Warfare"; and instructions such as DoD 5000.2-R, "Mandatory Procedures for Major

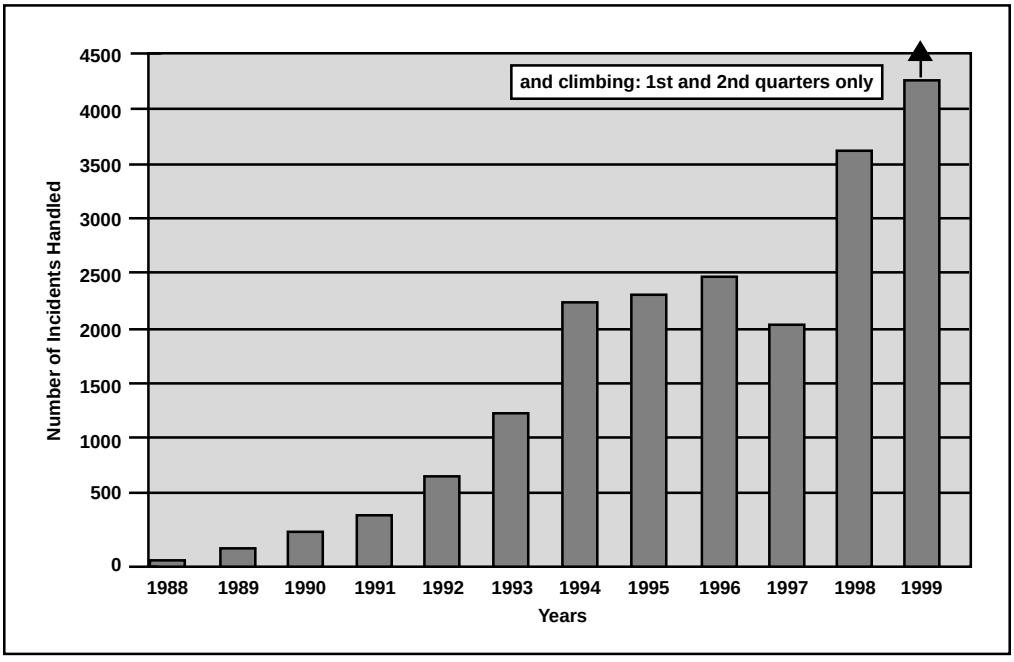

Figure 2. Number of CERT Incidents Handled

Defense Acquisition Programs (MDAPs) and Major Automated Information System (MAIS) Acquisition Programs." Current doctrine does not address software as the major element of a military fighting system; yet as the above discussion shows, many software and software-controlled systems cannot be separated from the system being developed.

The F–22 weapon system is an example of a software-controlled aircraft system that contains and communicates with integrated information systems (Figure 3). The F–22 is not a closed system; external information systems update and integrate F–22 combat operations during flight. Through these external connections, not just the information systems but the basic software systems of the F–22 can be attacked. Current information warfare doctrine in the Joint Pubs is mainly concerned with security of external C^4I (command, control, communications, computers, and intelligence) systems integrated on the F–22, but software-intensive systems make internal systems of the F–22 vulnerable to cyber warfare attack. Our doctrine must account for these vulnerabilities and provide methods of offense and defense. Definitions for building future weapon systems and in cyber forces doctrine and recommended methods to incorporate them follow.

CYBER WARFARE DEFINITIONS

JP 3-13, JP 3-13.1, and DoD 5000.2-R focus on information systems and not software-controlled systems; definitions these documents provide are not sufficient to describe the full range of cyber warfare.

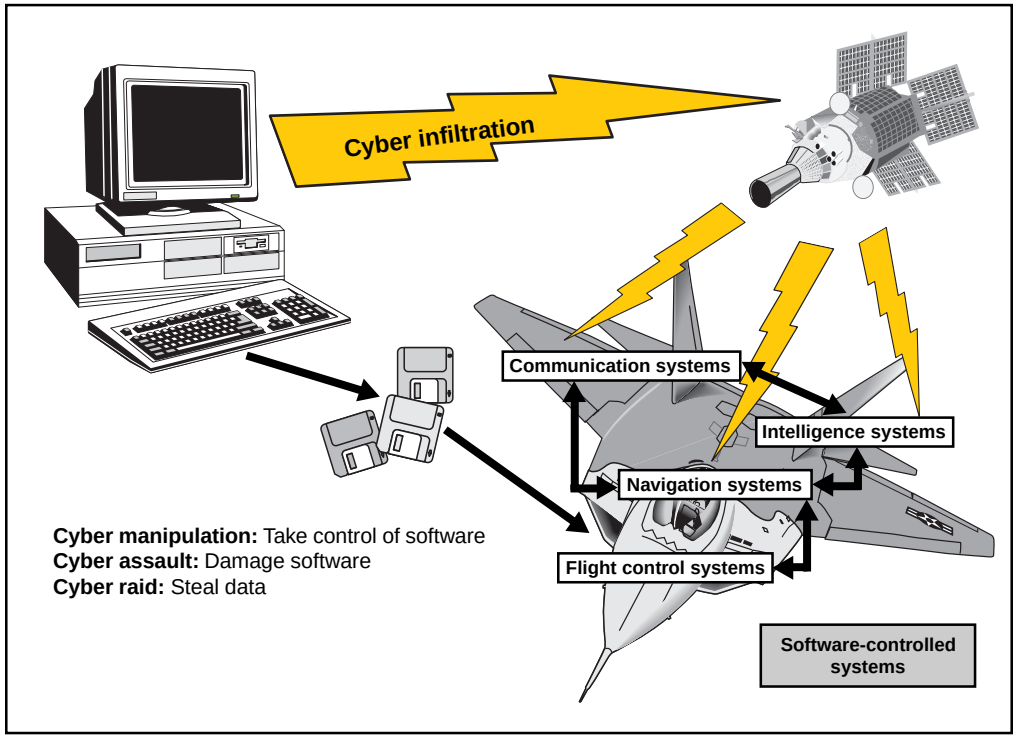

Figure 3. Infiltration of an Aircraft

The CERT® Coordination Center does provide a strong set of common terms to define cyber system security for the DoD (Carnegie Mellon, 1997), but these terms do not discuss military doctrine or national security. Furthermore, these terms focus on current methods of defense against infiltration and attack; they do not focus on future cyber force capabilities. We need a new taxonomy that includes the full range of cyber operations, and aids the development of a national cyber warfare doctrine (see adjacent box).

Military Cyber Warfare Targets

Any military system controlled by software is vulnerable to cyber attack. The first step in any attack is cyber infiltration; all systems that incorporate software are vulnerable to cyber infiltration.[4] Actions following cyber infiltration can affect organizations via the transfer, destruction, and altering of records—cyber raid. Software within systems can be manipulated—cyber manipulation. Systems controlled by that software can be damaged or controlled—cyber manipulation. The software itself can be copied, damaged, or rewritten—cyber assault.

Military C4I

Military C4I systems are particularly vulnerable, and are the primary focus of DoD cyber-related doctrine. JP 3-13 and JP 3-13.1 both provide doctrine for information-related warfare. C4I systems are a

A New Taxonony of Cyber Terms

Cyber warfare (CyW). Any act intended to compel an opponent to fulfill our national will, executed against the software controlling processes within an opponent's system. CyW includes the following modes of cyber attack: cyber infiltration, cyber manipulation, cyber assault, and cyber raid.

Cyber infiltration (CyI). Penetration of the defenses of a software-controlled system such that the system can be manipulated, assaulted, or raided.

Cyber manipulation (CyM). Following infiltration, the control of a system via its software which leaves the system intact, then uses the capabilities of the system to do damage. For example, using an electric utility's software to turn off power.

Cyber assault (CyA). Following infiltration, the destruction of software and data in the system, or attack on a system that damages the system capabilities. Includes viruses and overload of systems through e-mail (e-mail overflow).

Cyber raid (CyR). Following infiltration, the manipulation or acquisition of data within the system, which leaves the system intact, results in transfer, destruction, or alteration of data. For example, stealing e-mail or taking password lists from a mail server.

Cyber attack. See CyI, CyM, CyA, or CyR.

Cyber crime (CyC). Cyber attacks without the intent to affect national security or to further operations against national security.

Intentional cyber warfare attack (IA). any attack through cyber-means to intentionally affect national security (cyber warfare) or to further operations against national security. Includes cyber attacks by unintentional actors prompted by intentional actors. (Also see "unintentional cyber warfare attack.")

IA can be equated to warfare; it is national policy at the level of warfare. Unintentional attack is basically crime. UA may be committed by a bungling hacker or a professional cyber criminal, but the intent is self-serving and not to further any specific national objective. This does not mean unintentional attacks cannot affect policy or have devastating effects (Vatis, 1998).

Intentional cyber actors (I-actors). Individuals intentionally prosecuting cyber warfare (cyber operators, cyber troops, cyber warriors, cyber forces).

Unintentional cyber actors (U-actors). Individuals who unintentionally attack but affect national security and are largely unaware of the international ramifications of their actions. Unintentional actors may be influenced by I-actors but are unaware they are being manipulated to participate in cyber operations. U-actors include anyone who commits CyI, CyM, CyA, and CyR without the intent to affect national security or to further operations against national security. This group also includes individuals involved in CyC, journalists, and industrial spies.[3] The threat of journalists and industrial spies against systems including unintentional attacks caused by their CyI efforts should be considered high.

Unintentional cyber warfare attack (UA). Any attack through cyber-means, without the intent to affect national security (cyber crime).

very complex mix—from radios to radars, mainframes to personal computers. Military C4I uses interfaces through the Internet, base and organizational local area networks (LAN), modems, civilian and military communication systems, navigation systems, and radios in all frequency ranges.

Military C4I systems are extremely vulnerable because they interconnect. Cyber infiltration can enter at many points and potentially affect a myriad of systems. These systems and their interactions are so complex that any modern military organization is unlikely to trace the full potential of any single cyber infiltration. The possibility exists for cyber attacks of every type, and the results can be catastrophic. For instance, nuclear weapon control systems are incorporated into military C4I. As demonstrated by recent incursions in DoD networks, databases, and Web sites (Lemos, 1998), almost any dedicated foe can engage in cyber attacks against military computer systems (Vatis, 1998). Since military computers are the core of national C4I, successful IA and UA against such targets pose a national security peril.

"The possibility exists for cyber attacks of every type, and the results can be catastrophic."

Weapon Systems

No current DoD doctrine adequately covers cyber attacks on military hardware systems such as aircraft and vehicles that require software to operate (JP 3-13, 1998; JP 3-13.3, 1996; and DoD 5000.4-R, 1998). As noted previously, the F–22 is a cyber-controlled aircraft (Figure 3). Infiltration and degradation of the aircraft's systems directly or via its C4I connections can be as devastating as shooting it out of the sky.

Cyber infiltration of the C4I system providing data to modern aircraft allows an avenue for cyber raid, manipulation, and assault. Because many systems like the Global Positioning System (GPS) automatically update aircraft information and intelligence, they can allow undetected infiltration of the aircraft. Intelligence, navigation, and communication systems are integrated to each other and input and output to a host of other aircraft systems—the flight control system (through the auto pilot), propulsion system (through the auto throttles), radar system, master warning system, and environmental control system. Using the correct control sequences, inputs, or reprogramming, an infiltrator could produce any level of systems damage, from driving the aircraft off course to overwriting the flight control software.

Identifying Cyber Warfare Vulnerabilities

The first rule in identifying cyber warfare vulnerabilities is that any software-controlled system that can accept an input can theoretically be infiltrated and attacked! This means all systems that accept inputs are vulnerable. Fundamentally, cyber systems can be infiltrated in two ways—by physical and signal inputs.

Physical Infiltration

Physical infiltration is made through the system hardware. For example, the on/off switch, keyboard, mouse, cockpit controls, flight controls, and removable

The F–22 is a cyber-controlled aircraft

media provide physical inputs into a system. The first line of defense for a software-based system is to secure the physical inputs and outputs of the system. If these are not secure, the system is not secure. Any system can be compromised if a cyber attacker can enter the facility, aircraft, or vehicle and directly infiltrate the system. The cyber infiltration can be maintained afterwards by the installation of repeaters and remote input devices on the hardware. For example, electronic bugs on phone lines are a common method of surreptitious surveillance; modem and LAN lines are equally vulnerable.

An easy method of physical infiltration is to use a spare LAN connection on a hub or route. Using common network parts, a connection can be made directly, or through a Radio Frequency (RF) transmitter (wireless connection) from the LAN to an infiltrator's computer. These infiltration methods are only discovered by careful system audits or visual inspection (Marshall, 1991).

SIGNAL INFILTRATION

Signal infiltration comes through existing indirect or direct connections to a system. These connections are typically LANs, infrared (IR) devices, RF connections (radios), and modems (phone lines). Any system with an external connection can theoretically be infiltrated. The number of potential entry points is limited only by the number of direct and indirect connections into the system. For instance, a system with an Internet server is vulnerable to cyber infiltration from any computer connected to the Internet. An isolated network with a modem is vulnerable to any computer that can call

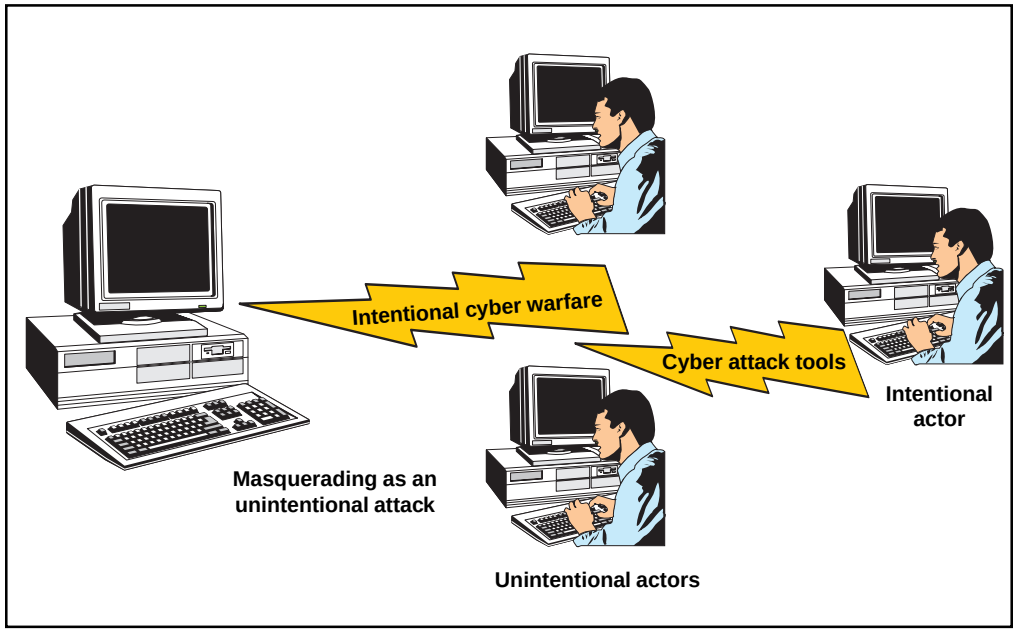

Figure 4. Cyber Warfare Method using UA and IA

into it. These input paths are used to infiltrate the system and then assault, manipulate, or raid it.

Physical infiltration may be protected by physical security: walls, fences, restricted areas, identification, guards, etc. Signal infiltration has similar defenses, but these are incorporated within the software or hardware itself (for instance, passwords, coded signals, firewalls, terminal identification, isolation, and system monitors).

The second rule of identifying CyW vulnerabilities is to expect every software-controlled system to be the objective of an attempted cyber infiltration. Even isolated systems can experience cyber assault through a computer virus brought in on a contaminated floppy disk. Because cyber attacks are largely unpredictable, all systems must have some degree of protection, and the level of protection must be commensurate with the likelihood and consequences of expected attack. Every vulnerable system needs proactive and effective virus-protection in place.

Assume U-actors will be influenced by I-actors. The anonymity of the Internet makes it possible for a cyber operative to pass on information about password-cracking, system phone numbers, infiltration techniques, and programs to U-actors (Figure 4). Many U-actors are young, immature, and unsophisticated. They don't understand the ramifications of their actions. However, some attacks that appear unintentional may be made by I-actors, operating through U-actors on the Internet. The recent cyber infiltration of information systems by California teens trained by the Israeli hacker "Analyzer" is an example of this mentoring relationship (Cole, 1998).

I-actors can easily influence the direction of attacks by providing system access

numbers and system passwords. Trojan horse programs written and passed to U-actors achieve an entirely different result than the U-actor intended. The outcome, from the perspective of the I-actor, is the same as if the attack had been made directly. Because passwords and infiltration data are shared by U-actors across the net, the I-actor's mission package is likely farmed out to more than one U-actor, or data may be passed through multiple U-actors. This ensures many attacks on the same target and further muddies the trail back to the source. This also means organizations that detect attacks and neutralize them should be prepared to receive the same attack over and over again. In addition, organizations that detect attacks must share data on the attacks immediately with other organizations (Howard, 1997).

Defense Against Cyber Warfare

The exploitation of system weaknesses and social engineering[5] are the primary avenues of attack against cyber systems (Howard, 1997). System weaknesses and social engineering techniques take advantage of computer and human limitations to steal and bypass signal and physical defenses, mainly passwords and machine-to-machine authentication. Unfortunately, the largest part of signal and physical defenses is based on identification and authentication codes—passwords. Passwords can be stolen, bypassed, or obtained by deception (and in theory, any password or authentication can be cracked). Until a different method of protection is invented, dependency on password identification and authentication guarantees that all systems will be in some degree vulnerable to cyber infiltration.

Use dedicated and redundant security to protect cyber systems. Twenty-two security methods are compiled below. Each method is described, along with some specific examples to accomplish it. This list is intended to provide a starting point for decision making and risk analysis; in some cases, especially systems integration and offensive methods, these suggestions run counter to current DoD policy and practice.

"Passwords can be stolen, bypassed, or obtained by deception (and in theory, any password or authentication can be cracked)."

These methods are intended to provoke thoughtful examination of all cyber security options to allow a tailored approach to military cyber systems development. To provide the best defense, these techniques must be customized, combined, and layered with one another. In every case, cyber systems should be set up so U- and I-actors can get into decoy sections[6] of the security network. This allows identification and containment of the infiltrator. Only when infiltration is identified can it be solved.

Inactive Defense Methods

Physical security is the primary means of cyber system protection. Without some degree of physical security, all of the defenses mentioned below will fail.

Isolate all critical systems. Provide no system inputs outside of a physically

secure area. Many agencies handle classified systems this way (Federal Information Processing Standards [FIPS] Publication 112, 1985); the systems themselves are physically isolated from any other inputs or systems. Isolation of critical systems also reduces damage caused by cyber infiltration.

Put critical operations under manual control. Critical functions should not be controlled directly by software. For example, an electrical power system should not be turned on or off through software. To be effective, the capability must be entirely eliminated from software control. For example, in a water utility, any setting that could cause water contamination should be manual so the system cannot be breached electronically. MIL-STD-882, "System Safety Program Requirements," is used by the military to classify critical functions. A basic rule for all critical cyber systems is that systems should be manual, when possible, so critical functions cannot be addressed by software. With industries such as nuclear power this is impossible; with military systems, this can be achieved by hardwiring critical functions—such as missile launches.

"All connections into a system must be physically controlled and monitored to prevent cyber infiltration."

Reduce integration. Integration increases cyber warfare risk because there are more avenues for cyber infiltration (and all system interconnections may not be known). To reduce cyber warfare vulnerability, integration should be limited as much as possible, and all system inputs and outputs must be fully defined. Critical cyber functions should be isolated physically so there are no inputs from outside. This type of compartmentalization should be considered when the use of cyber systems to control critical operations is necessary or desirable.

Keep the human element in the loop when integrating systems. Many software-controlled systems are integrated to reduce human workload. Although some systems require cyber integration to operate, many do not. When it is possible to keep a person in the loop or when a person can monitor or control a critical system, it is better to increase necessary monitoring and provide human interaction rather than automate the process. This is another way to isolate a system.

For instance, a request to shut down electrical power may generate a system message to tell a human operator to flip a switch. Only after the switch is moved can the automatic shutdown take place. An even safer setup would direct the operator through the shutdown sequence, instead of automating any of it. These methods may seem like we are turning back the technological clock, but protecting essential systems in this manner is necessary.

Inherent breach-points. Communication connections into the system are inherent, potential breaches of security. All connections into a system must be physically controlled and monitored to prevent cyber infiltration. The strongest breach-point occurs where the system is physically connected to an outside input. This part is also the most vulnerable to physical infiltration. Security must patrol, track, and control these inherent breach-points to prevent physical infiltration.

ACTIVE DEFENSE METHODS

These methods make up the software programming that protects the system from unauthorized use.

Passwords and authentications. Passwords and authentications are necessary parts of system security to allow authorized human and other cyber system input. Because personal passwords are not usually very long (10 digits is the standard maximum [FIPS Publication 112, 1985]), they are relatively easy to decode or predict. The longer the password, the better. Long passwords (32 characters or more) make code-breaking theoretically impossible, but codes that length are not commonly used and require other computers or hardware code devices such as tokens. Short passwords (eight characters or less) should be mixed into unpredictable, alphanumeric combinations and with other methods to provide an assured level of security. FIPS Publication 112, "Standard for Password Usage," provides specific information on the use of short passwords. Nicknames, popular words, and street names are easily predicted by some hacker programs.

Anthropomorphic measures. These measurements and data use a person's physical features—fingerprints, retinal scans, or face. These are better than passwords and can provide a much longer code, but are still relatively easy to break. Due to daily human physical changes, anthropomorphic measures cannot produce a large enough number to give a super-long password. For instance, if your face has swollen 0.001 of an inch during the night and the measure is to 0.0001 inch, you would not be able to log on your computer. However, anthropomorphic measures provide good security when combined with other methods such as passwords.

Tokens. These include magnetic cards or other code modules. They contain passwords and are read mechanically or electronically. Cards, modules, and other devices enable the use of very long codes and provide excellent security. Future encryption methods that use devices containing extremely long codes have the potential to make code-breaking almost impossible. A major drawback is that they must be kept physically secure because they can be lost or stolen. Tokens should be combined with anthropomorphic passwords to provide the best security.

"The first line of defense for a software-based system is to secure the physical inputs and outputs of the system."

Multiple authentications or log-ons. More than one interrogation is required to get into the system. For instance, log-on may require a basic password followed by an anthropomorphic measure (fingerprint, for example), or a password followed by a token. Figure 5 shows an example of this type of authentication scheme. The first layer should be a decoy layer and should be easy to crack but difficult to reprogram and disconnect. The second password layer should be very secure. Intrusions are recorded for investigation when the first layer is passed but the second layer is not. An infiltrator will invade the first layer, but not pass the second: then hopefully the infiltrator can be identified. In addition, the decoy layer can be filled with various offensive

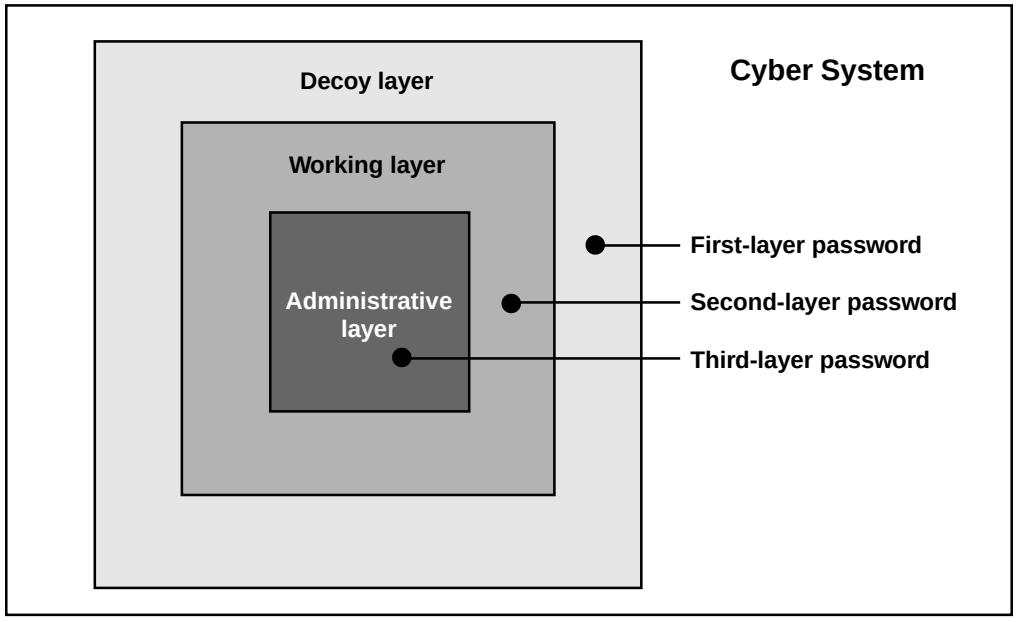

Figure 5. An Example of Different Security Layers on a Cyber System

programs that allow the identification and neutralization of the infiltrator. This type of log-on should be required for all vulnerable systems and especially for systems that interface with and support software-controlled aircraft and vehicles.

Multiple connection log-ons. More than one log-on over different addresses or lines is required for system entry. For instance, a log-on may be required at one phone number that activates a second, actual communication line. Another method is the call-back system. Using call-back, the user calls the computer and logs on, then the computer hangs up and calls back to the number authorized for the user. The user completes the sequence by logging on again with a second password. This method of log-on can also be used for Internet and LAN addresses.

Multiple log-on addresses. This requires either a call over two separate phone lines or two separate addresses at the same time. The signal is resolved in the user's computer only when both signals are received and the security authentication is passed on both lines. Multiple methods make it easy to detect cyber infiltration. Infiltrators who log-on in the initial layer, but whose second log-on fails, are instantly identified.

Monitoring software (Marshall, 1991). At the lowest level, this software records the user's activities on the system. In many systems, this software limits the user's access based on a security level. More complex systems monitor activity and alert the system or people monitoring when a user attempts to access resources not authorized at the user's security level. These programs provide audit trails and system logs that are a primary means of tracking unauthorized access and operations. This kind of software also detects multiple attempts at system log-on.

ACTIVE OFFENSIVE METHODS

These methods include software programming and cyber operations that identify, attack, disable, tag, and capture I- and U-actors and their equipment. The chief problem to gaining the offensive is the detection of cyber infiltration. At least 75 percent or more cyber infiltrations are not detected (Howard, 1997). To an unsophisticated security system, cyber infiltration appears to be a normal connection. The security itself needs a footprint that is unpredictable to the infiltrator—that separates authorized from unauthorized operators. The techniques described in the previous Active Defense Methods section give some ideas how this can be accomplished.

This section provides methods that can be used against infiltrators after they are detected. Some of these techniques are theoretical and based on extrapolations of current program capabilities. Simple active programs (e.g., Microsoft macro viruses) and passive programs can be used against unsophisticated computer security and systems with crippling results. Commercially available system monitoring software can be used to accomplish cyber infiltration, assault, raid, and manipulation; to cyber infiltrate password-secured LANs requires only a rewrite of commercially available software.

Highly proficient programmers can write machine code programs that can be sent across a data stream into a Web browser or other communications program. For example, "Back Orifice" is a Trojan horse program that surreptitiously sends information through the Internet back to its originator. Most I-actors are not proficient enough to write these advanced programs, but simple offensive programs are available now on the Internet. Advanced programs can be written to do almost anything to a computer. They can tag a computer for identification (cookies), operate the different components of the computer, and rewrite programs in the computer.

Password-cracking programs. These were the first programs used for cyber infiltration. Password-cracking programs, at their simplest, repeatedly try different codes until they get a log-on. The main method of protecting against these simple programs is automatic monitoring that cuts off users who attempt multiple unsuccessful log-ons. Complex password cracking programs can potentially disable monitoring and other security methods. Super-long passwords and the defensive methods mentioned above protect against password cracking.

> "Advanced programs can be written to do almost anything to a computer."

Identification, location, sniffer, spoofing, and watcher programs. Identification and location programs identify computers and users in a system. Sniffer and watcher programs glean passwords and other information from the system. Many of these programs are passive—that is, they are used by LANs to keep track of which computers and users are logged on. Some are active spoofers, actually asking for information from the user or the system.

The most widespread software-based method of obtaining passwords and other confidential information is through sniffer and watcher programs that monitor

network traffic. These are commonly deployed using Trojan horse programs such as "Back Orifice." Defeat these programs by applying the password encryption methods delineated in FIPS Pub 112 (1985). Sophisticated identification programs can make undetectable queries to the user's computer and even allow the cyber raid of data. The main line of protection from these programs is active-defense methods. Cyber protection systems should use covert identification programs to discover information about an infiltrator.

"As experiments, failure is not only allowed, it is a key aspect of success in allowing the system to be refined in the same environment it will ultimately be used."

Attack programs. An attack program is any program used to cripple or destroy a computer or computer system. These programs are complex and uncommon. They are like viruses, but are directed and singular, instead of random and replicating. Attack programs can be developed to impair the target's software, writable system basic input/output systems (BIOS),[7] and disks. When employed in defense, these programs should be used by cyber forces to immediately stop any cyber attack-in-progress, to prevent the infiltrator from continuing operations from the attacking computer. Any cyber attack should tag the system for identification.

Protection against direct attacks is best accomplished by defensive methods. However, because all parts of a network or the Internet may not be secure, each individual computer must have some way of independently identifying attacks and rejecting them. Similar methods are used extensively now to protect against viruses and reject cookies.

Tagging programs. These programs insert data on a computer for later identification and cyber infiltration. These programs can be as simple as a "cookie"[8] or as complex as a BIOS tag. Some versions write data to the boot sector on the hard drive; the drive must be low-level reformatted to remove it. Cyber forces should be able to tag a computer for later criminal investigation. Methods of defense from tagging are similar to those from attack programs.

Viruses. These are programs that replicate themselves by attaching their codes to other programs, disk boot sectors, and writable-system BIOSs. Viruses can be used both for malicious terrorism and cyber warfare (Symantic Antivirus Research Center, 1994). This capability can be added to any offensive program. It attacks computers in the opponent's system except for the primary infiltrator's computer. Virus capabilities can be added to tagging programs when there is a threat that the infiltrator will destroy the system or hard drives attacked, and thus attempt to prevent later identification. Because of their ability to get into nonopponent computer systems, viruses should be used cautiously by cyber forces. Viruses can be written with checks that only target specific systems.

Methods of defense from viruses are:

- programs that scan for identified viruses and virus-like code (virus scanners),

- inoculation of systems by identification of authorized programs and data (Cyclic Redundancy Code [CRC] records; many virus checkers provide this capability), and

- personnel training.

Unfortunately, by 1997 as many as 15,500 viruses were identified and an estimated 400 new ones are reported each month (Dr. Solomon Company, 1997). This makes absolute protection from viruses and viruslike programs impossible without the use of the defensive methods enumerated previously.

Trojan horses. These programs are the most common method of cyber infiltration (Howard, 1997). These are programs that perform like any other program a user may wish to run, but they execute unauthorized operations (Carnegie Mellon, 1997). A common example of a Trojan horse program is a Microsoft macro virus. Trojan horses can be defeated by the same methods used against viruses.

System overflows. One method of cyber infiltration and cyber assault is the use of large amounts of data to cause a system overflow or "crash." The typical e-mail pyramid letter is a crude example of e-mail overflow. This kind of letter can accumulate an address tail that will choke any e-mail system. A cyber attacker can also be attacked and infiltrated in this manner.

Overflows are most effective when the overflow is not detected immediately. This can be achieved when the infiltrator has a very fast connection or when there is a second signal input line to the attacking computer. Data overflows are also an excellent method to mask the transmission of offensive programs. Methods of defense from overflows are e-mail scanners that check for very large e-mail files, and personnel training. For instance, all personnel must be taught not to pass on dubious e-mail warnings, chain e-mails, and massive official e-mail. In addition, all employees should never open files from questionable sources or unofficial files.

Direct manipulation. When a computer is connected to another computer, current software makes it relatively easy to take control of many of the basic functions of the computer. Machine code and operating systems address codes can be used to turn on peer-to-peer sharing or to directly manipulate devices controlled through the operating system and BIOS. Cyber forces should develop programs that will allow this kind of manipulation of infiltrator computers. Cyber systems must lock out unauthorized system requests at all levels.

"One method of cyber infiltration and cyber assault is the use of large amounts of data to cause a system overflow or 'crash.'"

Logic bombs. Some code sequences in data files manipulate both the programs using the data files and the address codes of the BIOS and operating system. This is evident in macro viruses found in document files and files that result in program and operating system crashes. These kinds of programs can be written to achieve even more pointed results: for example, tagging or systems impairment. Logic bombs can also be used against infiltrators when they are attached to password data bases, classified data files, or to other files that might be downloaded following cyber infiltration.

Statutory action (legal actions). Cyber forces cannot be fully effective without capturing and prosecuting both U- and I-actors. The primary goal of offensive cyber operations must be to identify and tag infiltrating systems. These actions allow prosecution as well as confirmation of the infiltration. Because it is relatively simple to back up systems and replace damaged computer components, the infiltrator will not be out of action for long unless legal action is taken. When it is not possible to extradite and prosecute U- or I-actors outside the United States, national policy must determine the extent of the cyber operations to be undertaken against the shielding foreign nation.

"The primary goal of offensive cyber operations must be to identify and tag infiltrating systems."

Measuring the Effectiveness of Cyber Defenses and Operations

The effectiveness of cyber forces cannot be measured by a lack of detected cyber infiltration against targets This is because undetected cyber infiltration is certainly taking place (Lee, 1998), and most cyber infiltrations and attacks go undetected (Howard, 1997). The only reasonable measure of effectiveness is detecting cyber infiltration when it happens. This is why a multilayered approach to cyber system defenses is necessary. If the policy of the United States regarding CyW is wholly one of defense, the absolutely perfect measure of defense effectiveness is that every cyber infiltration is identified and the U- or I-actor neutralized.

The success of cyber operations against and in support of the U.S. government must be classified. As mentioned previously, when a cyber attack occurs, with due regard for active cyber operations, the detecting agency should immediately inform all possible targets (Howard, 1997). But, when an agent of the government is the victim of successful cyber infiltration or attack, that agency should not release the degree or effects of any cyber operation against it. Acknowledging the results would be similar to acknowledging the classification of publicly published materials. It would tell the enemy they are successful and provide information so the next attack might be even more effective.

The best approach is for the agency to make no comment at all and provide immediate recovery and cleanup as part of its cyber operations. This keeps the I- and U-actors guessing and allows the effective use of the offensive and defensive methods outlined above. This is not to say the agency should not report the attack to proper authorities and provide suggested methods of protection.

New Doctrine

The first step to develop a strong doctrine that includes all the dimensions of current and future cyber warfare threats. Taxonomy and cataloged security methods go a long way to build a framework for this doctrine. The challenge is to put the required effort and funding forward to ensure a strong level of security for all software-controlled systems.

CONCLUSION

Cyber operations have the potential to overcome any system controlled by software. The military systems we are developing today depend on software and software-controlled components to operate. Cyber warfare defenses must be incorporated into all of these military systems. The future of warfare makes it imperative that cyber warfare concerns become the interest of every software and hardware developer—not only of military systems but civilian systems as well.

Cyber warfare may be the greatest threat that nations have ever faced. Never before has it been possible for one person to potentially affect an entire nation's security. And never before has one person had the ability to cause such widespread harm as is possible in cyber warfare. Like radioactive fallout, the affects of cyber warfare can devastate economies and civilizations long after the shooting war is over.

This genie can' t be put back into the bottle; societies will not want to give up the manifold prosperity brought about by cyber systems. But a nation must ensure that it maintains the upper hand in cyber warfare. If our nation can' t, then even with the most powerful military and defense economy in the world, we face an insurmountable threat to our future prosperity and security.

Lt Col Lionel D. Alford, Jr., U.S. Air Force, is an aeronautical test policy manager for the Headquarters Air Force Materiel Command, Wright-Patterson Air Force Base, OH. He is an Air Force experimental test pilot with more than 3,600 hours in more than 40 different kinds of aircraft and is a member of the Society of Experimental Test Pilots. He is a graduate of the Air Ground Operations School, the Combat Aircrew Training School, the All Weather Aerial Delivery Training School, Defense Systems Management College, and the U.S. Air Force Test Pilot School. He has a master's degree in mechanical engineering from Boston University and a bachelor's degree in chemistry from Pacific Lutheran University.
(E-mail address: Pilotlion@aol.com)

REFERENCES

Arquilla, J., & Ronfeldt, D. (1992). Emergent modes of conflict. In *Cyberwar is coming.* Santa Monica, CA. The RAND Corporation.

Carnegie Mellon. (1997). *Glossary of terms.* Software Engineering Institute, CERT® Coordination Center. http://www.cert.org/research/JHThesis/appendix_html/Glossary.html

Cole, R. (1998). FBI hunts "master hacker." ABC News: High Technology, The Associated Press.

DoD 5000.2-R. (1998, February 27). Mandatory procedures for major defense acquisition programs (MDAPs) and major automated information system (MAIS) acquisition programs.

DoD Joint Publication (JP) 3-13. (1998, October 9). *Joint doctrine for information operations.*

DoD Joint Publication (JP) 3-13.1. (1996, February 7). *Joint doctrine for command and control warfare.*

Dr. Solomon Company. (1997). The future impact of viruses. *Dr. Solomon's Virus Central.* http:/www.drsolomon.com/vircen/vanalyse/future.html

Federal Information Processing Standards (FIPS) Publication 112. (1985). Standard for password usage.

Hafner, K. (1998, July 23). Chiquita case illustrates vulnerability of voice mail. *New York Times.* http://www.nytimes.com/library/tech/98/07/circuits/articles/23voic.html

Howard, J. D. (1997). *An analysis of security incidents in the Internet 1989–1995.* Carnegie Mellon University. http://www.cert.org/research/JHThesis/Start.html

Lee, S. (1998). Most computer hackers go unnoticed. *South China Morning Post*.http://www.infowar.com/HACKER/hack_030198s_b.html-ssi

Lemos, R. (1998). DoD confirms hacker boast. *ZDNN*. http://www.zdnet.com/zdnn/content/zdnn/0421/309056.html

Marshall, V. H. (1991). Intrusion detection in computers. *Summary of the Trusted Information Systems (TIS) report on intrusion detection systems.* http://csrc.nist.gov/secpubs/auditool.txt

Stein, G. J. (1995, Spring). Information warfare. *Airpower Journal, IX*(1).

Symantic Antivirus Research Center. (1994). *Computer viruses—An executive brief.* http://www.symantec.com/avcenter/reference/corpst.html

Vatis, M. A. (1998). *Cybercrime, transnational crime, and intellectual property theft. Statement for the record before the Congressional Joint Economic Committee.* http://www.ilspi.com/vatis.htm

von Clausewitz, K. (1976). In M. Howard & P. Paret (Trans.), *On War* (Book I). Princeton, NJ: Princeton University Press.

U.S. Air Force (1992). Bold stroke. Executive Software Course.

ENDNOTES

1. The F-16 is unstable below Mach 1, and uncontrollable without its software-based flight control system. The Boeing 777 and the Airbus 330 have software flight control systems without any manual backup; the performance of these aircraft is dependent on their digital flight control systems.

2. The F–22 in high angle of attack flight uses software-controlled vectored thrust and flight controls to maneuver the aircraft.

3. As seen in allegations that a *Cincinnati Enquirer* reporter stole voice mail messages from Chiquita Brands International (Hafner, 1998), CyR is becoming a common method to take information from cyber systems.

4. The "hacker" is a U-actor commonly characterized as affecting cyber infiltration without further damage to a computer system.

5. Social engineering refers here to both the process of gaining privileged information, such as passwords, by deception (3) and the use of Trojan horse programs.

6. A decoy section is a first layer area of a cyber system that appears to provide access to the system but in fact only simulates the inner layers.

7. A basic input/output system is a set of instructions stored on a ROM chip inside IBM PCs and PC-compatibles, which handles all input-output functions.

8. A cookie is a set of data that a Web site server gives to a browser the first time the user visits the site, that is updated with each return visit. The remote server saves the information the cookie contains about the user and the user's browser does the same, as a text file stored in the Netscape or Explorer system folder. Not all browsers support cookies.