Cyber Warfare: A New Doctrine and Taxonomy

Lt. Col. Lionel D. Alford Jr.
U.S. Air Force

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 paper discusses the limitations of current doctrine and suggests new cyber warfare taxonomy.

Karl von Clausewitz 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 … [1]." At the end of the second millennium, this definition no longer describes the full spectrum of modern warfare. In the near future, – with software alone – we will have the potential to make war without the use of violence and fulfill the second half of von Clauswitz's definition. Today's software-intensive systems make this possible.

Cyber describes systems that use mechanical or electronic systems to replace human control. In this paper 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.

Full-Circle Protection Required

Cyber warfare is the conduct of military operations according to information-related principles [2]. However, 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 the controlling software (Figure 1). Information is not only at risk – so is the fundamental control of civilization. As technology progresses, this fundamental control will continue to devolve into networks and software-controlled electronics [3].

This transition has already occurred in aviation. Previously, 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 on the software [4]. 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: modern aircraft fly-by-wire, their engines are controlled-by-wire, 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 through networking provides a basis for the integration of many disparate items. These networked software systems are under attack today, and the attacks are increasing (Figure 2).

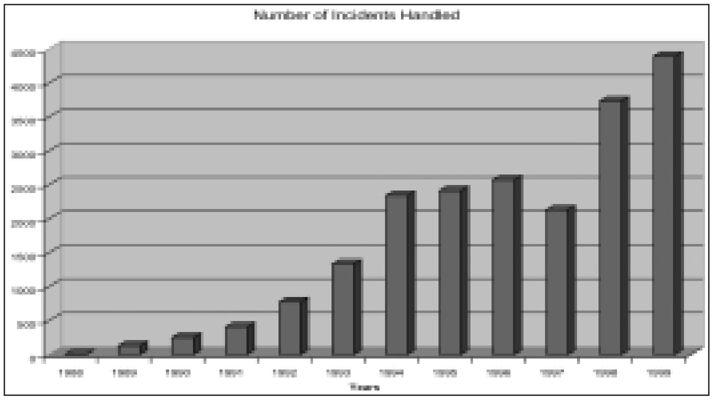


Figure 2. Number of CERT Incidents Handled (3)

Unfortunately current Department of Defense (DoD) doctrines and instructions do not adequately cover the scope of cyber warfare [5]. Several handle information warfare as a discrete part of a military system. These include Joint Publication 3-13 Joint Doctrine for Information Operations (JP3-13), Joint Publication 3-13.1 Joint Doctrine for Command and Control Warfare (JP3-13.1), and instructions such as DoD 5000.2-R Mandatory Procedures for Major Defense Acquisition Programs, and Major Automated Information System 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 soft-

Figure 1. Infiltration of a Utility

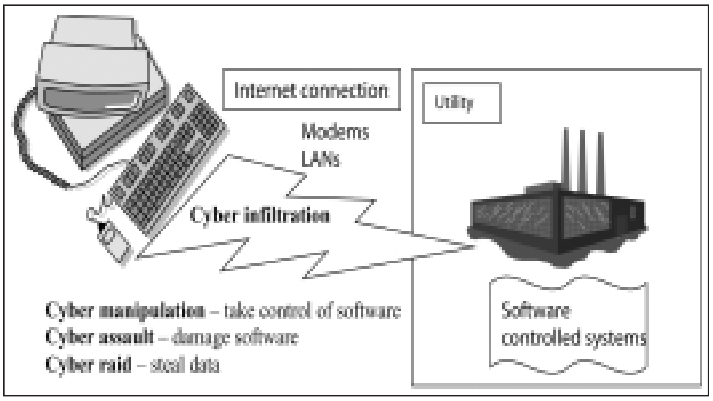
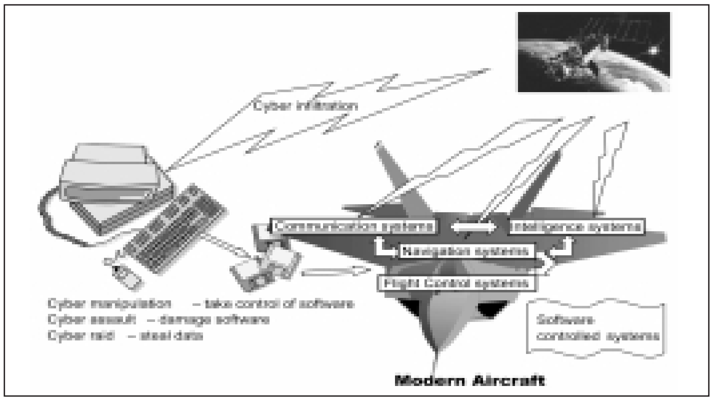

Internet connection
Modems
LANs
Utility
Cyber infiltration
Cyber manipulation – take control of software
Cyber assault – damage software
Cyber raid – steal data
Software controlled systems

Figure 3. Infiltration of an Aircraft



ware-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, page 27). The F-22 is not a closed system; external information systems update and integrate F-22 combat operations during flight. Through these external connections, both the information systems and 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 C4I 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 cyber forces doctrine and recommended methods to incorporate them follow.

Cyber Warfare Definitions

Joint Pub 3-13, Joint Pub 3-13.1, and DoD 5000.2-R focus on information systems but not software controlled systems; these documents' definitions are not sufficient to describe the full range of cyber warfare. The Computer Emergency Response Team® coordination center does provide a strong set of common terms to define cyber system security for the DoD [6], 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 accompanying sidebar).

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 or systems controlled by that software can be damaged or controlled – cyber manipulation. The software itself can be copied, damaged, or rewritten – cyber assault.

Military Command, Control, Communications, Computers, and Intelligence (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 very complex mix – from radios to radars, mainframes to PCs. 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 [7], almost any dedicated foe can engage in cyber attacks against military computer systems [3]. Since military computers are the cores of national C4I, successful intentional and unintentional cyber warfare attack against such targets pose a national security peril.

A New Taxonomy 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 that 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, overload of systems through e-mail (e-mail overflow), etc.

Cyber raid (CyR) - Following infiltration, the manipulation or acquisition of data within the system that leaves the system intact and 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 (UA).)

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

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

Weapon systems are cyber attack targets, but current DoD doctrine adequately covers cyber attacks on military hardware systems such as aircraft, vehicles, etc. that require software to operate [8, 9, 10]. As noted previously, the F-22 is a cyber-controlled aircraft (Figure 3). Infiltrating and degrading 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 and future intelligence systems automatically update aircraft information and intelligence, they can allow undetected aircraft infiltration. Intelligence, navigation, and communication systems are integrated with each other and to a host of other aircraft systems – the flight control system (through the autopilot), propulsion system (through the autothrottles), radar system, master warning system, and environmental control system. Using the correct control 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 (CyW) vulnerabilities is that any software-controlled system that can accept input can theoretically be infiltrated and attacked. This means all systems that accept input are vulnerable. Fundamentally, there are two ways to infiltrate cyber systems: physical and signal inputs.

•**Physical infiltration** is made through the system hardware. For example, the on/off switch, keyboard, mouse, cockpit controls, flight controls, and removable 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/vehicle and directly infiltrate the system. The cyber infiltration can be maintained afterwards by installing 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 router. 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 [11].

•**Signal infiltration** comes through existing indirect/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; only the number of direct and indirect connections into the system limits the number of potential entry points. 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 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/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.

All infiltration's should be assumed to be cyber attacks, until proven otherwise. Unintentional actors (U-actors) will be influenced by intentional actors (I-actors). The anonymity of the Internet makes it possible for a cyber operative to pass information on password-cracking, system phone numbers, infiltration techniques, and programs to U-actors. Many U-actors are young, immature, and unsophisticated. However, I-actors, operating through U-actors on the Internet may make some attacks that appear unintentional. The recent cyber infiltration of information systems by California teens trained by the Israeli hacker "Analyzer" is an example of this mentoring relationship [12].

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 [13].

Measuring Cyber Defense Effectiveness

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 [14], and most cyber infiltration's and attacks go undetected [13]. The only reasonable measure of effectiveness is detecting cyber infiltration when it happens. This is why a multi-layered 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 [13]. 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 above. This is not to say the agency should not report the attack to proper authorities and provide suggested methods of protection.

In light of today's cyber warfare, the first proactive step is 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 could one person 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 cannot, then even with the most powerful military and defense economy in the world, we face an insurmountable threat to our future prosperity and security[5].◆

References

1. von Clausewitz, Karl, *On War*, Book I, translated by Michael Howard and Peter Paret, Princeton University Press, 1976.
2. Arquilla, John and David, Ronfeldt, *Emergent Modes of Conflict*, *Cyberwar is Coming*, The RAND Corporation, 1992.
3. Vatis, Michael A., Cybercrime, Transnational Crime, and Intellectual Property Theft, Statement for the record before the Congressional Joint Economic Committee, 1998, www.ilspi.com/vatis.htm
4. U.S. Air Force, Bold Stroke, Executive Software Course, 1992.
5. Stein, George J., Information Warfare, *Airpower Journal*, Vol. IX, No. 1 Spring 1995.
6. Carnegie Mellon, Software Engineering Institute, CERT® Coordination Center, Glossary of Terms, 1997, www.cert.org/research/JHThesis/appendix_html/Glossary.html
7. Lemos, Robert, DoD Confirms Hacker Boast, ZDNN, 1998, www.zdnet.com/zdnn/content/zdnn/0421/309056.html
8. Joint Publication 3-13, Joint Doctrine for Information Operations, 9 Oct. 1998.
9. Joint Publication 3-13.1, Joint Doctrine for Command and Control Warfare, 7 Feb. 1996.
10. DoD 5000.2-R, Mandatory Procedures for Major Defense Acquisition Programs and Major Automated Information System Acquisition Programs, 27 Feb 1998.
11. Marshall, Victor H., Intrusion Detection in Computers, Summary of the Trusted Information Systems (TIS) Report on Intrusion Detection Systems, 1991.
12. Cole, Richard, FBI Hunts Master Hacker, ABC News: High Technology, *The Associated Press*, 1998.
13. Howard, John D., *An Analysis Of Security Incidents On The Internet 1989 - 1995,* Carnegie Mellon University, 1997. http://www.cert.org/research/JHThesis/Start.html
14. Lee, Stella, Most Computer Hackers Go Unnoticed, *South China Morning Post*, 1998. www.infowar.com/HACKER/hack_030198s_b.html-ssi

Notes

1. The F-16 is unstable below Mach one, 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 air craft 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 [7], 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 sys tem.
5. The views expressed in this paper represent the personal views of the author and are not necessarily the views of the Department of Defense or of the Department of the Air Force.

About the Author

Lt. Col. Lionel D. Alford Jr is an aeronautical test policy manager for the Headquarters Air Force Materiel Command, Wright-Patterson Air Force Base, Dayton, Ohio. He is an Air Force experimental test pilot with more than 3,600 hours flying more than 40 different types of aircraft. He is a member of the Society of Experimental Test Pilots. Lt. Col. Alford has served in worldwide military operations as a member of three different operational combat squadrons. 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 USAF Test Pilot School. He was an instructor for three Air Force aircraft and a senior Air Force evaluator. He has a master's degree in mechanical engineering from Boston University and a bachelor's degree in chemistry from Pacific Lutheran University. Lt. Col. Alford is a computer experimenter and programmer, and is currently working on certification as a Microsoft system engineer.

Lionel D. Alford Jr.
HQ AFMC/DOP
4375 Chidlaw Road, Room S143
Wright-Patterson AFB, OH 45433-5006
Phone: 937-257-8496
Lionel.alford@wpafb.af.mil