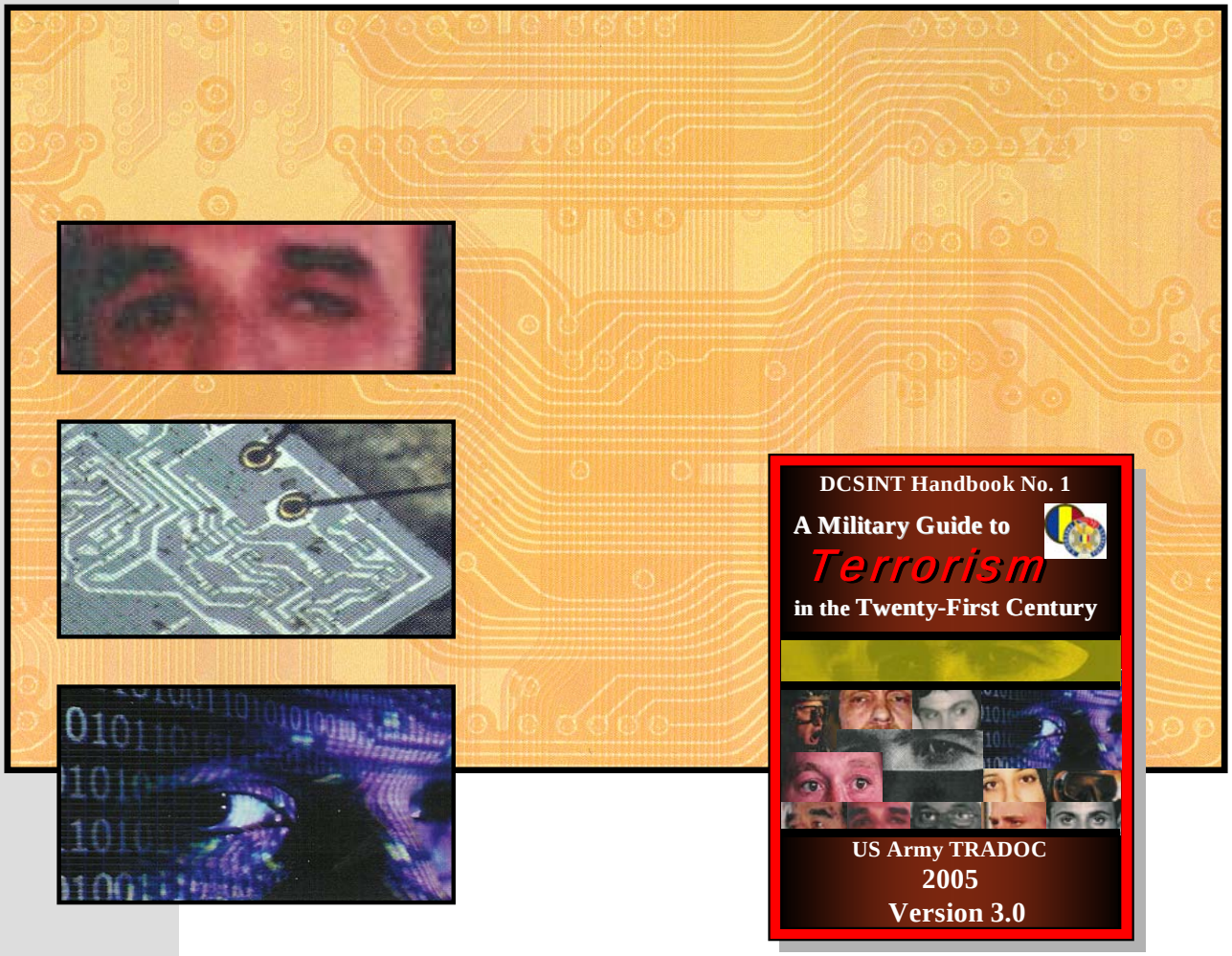
DCSINT Handbook No. 1.02

Cyber Operations and Cyber Terrorism



US Army Training and Doctrine Command
Deputy Chief of Staff for Intelligence
Assistant Deputy Chief of Staff for Intelligence - Threats
Fort Leavenworth, Kansas

15 August 2005

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
15 AUG 2005	**N/A**	**-**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Cyber Operations and Cyber Terrorism, Handbook No. 1.02	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) **US Army Training and Doctrine Command, Dep Chief of Staff for Intelligence, Asst Deputy Chief of Staff for Intelligence - Threats, Fort Leavenworth, KS 66027**	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
The original document contains color images.

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**	**UU**	**46**	

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std Z39-18

Page Intentionally Blank

Preface

This handbook is one in a series of supplements to TRADOC DCSINT Handbook No. 1, ***A Military Guide to Terrorism in the Twenty-First Century,*** which is a basic terrorism primer prepared under the direction of the U.S. Army Training and Doctrine Command, Assistant Deputy Chief of Staff for Intelligence-Threats. The terrorist threat confronting our military spans foreign and domestic threats of nation-states, rogue states with international or transnational agent demonstrations, and actors with specific strategies, tactics, and targets. A major tactic used by many terrorist groups is Cyber Terrorism. Although Cyber Terrorism is covered in the capstone terrorism handbook, this supplement provides more detail and insight.

Purpose. This informational document supplements the basic terrorism handbook and supports operational missions, institutional training, and professional military education for U.S. military forces in the Global War on Terrorism (GWOT). This document provides an introduction to Cyber Terrorism, and addresses the history of the phenomena, how terrorist organizations recruit, the motivations behind use of the tactic, characteristics of Cyber Terrorism, and the types of attacks against networks. Finally, the handbook addresses specific threats to military forces.

Intended Audience. This document exists primarily for U.S. military forces, however, other applicable groups include interagency; intergovernmental; civilian contractor; and, non-governmental, private volunteer, and humanitarian relief organizations. Compiled from open source materials, this supplement promotes a "Threats" perspective of suicide terrorism. Neither a counter-terrorism directive nor anti-terrorism manual, the supplement complements but does not replace training and intelligence products on terrorism.

Handbook Use. Study of contemporary terrorist behavior and motivation, terrorist goals and objectives, and a composite of probable terrorist tactics, techniques, and procedures (TTP) improves readiness of U.S. military forces. As a living document, this supplement will be updated as necessary to ensure a current and relevant resource. A selected bibliography presents citations for detailed study of the topic. Unless stated otherwise, masculine nouns or pronouns do not refer exclusively to men.

Proponent Statement. Headquarters, U.S. Army Training and Doctrine Command (TRADOC) is the proponent for this publication. Periodic updates will accommodate emergent user requirements on terrorism. Send comments and recommendations on DA Form 2028 directly to TRADOC Assistant Deputy Chief of Staff for Intelligence – Threats at the following address: Director, TRADOC ADCSINT – Threats, ATTN: ATIN-L-T (Bldg 53), 700 Scott Avenue, Fort Leavenworth, Kansas 66027-1323. This handbook will be available at Army Knowledge Online (**www.us.army.mil**). Additionally, the General Dennis J. Reimer Training and Doctrine Digital Library (www.adtdl.army.mil) list the handbook as a special text.

This Page Intentionally Blank

ACKNOWLEDGEMENTS
Threats Terrorism Team (T3) Network

The Deputy Chief of Staff for Intelligence at U.S. Army Training and Doctrine Command extends special appreciation to the many stakeholders who were invited to contribute information, subject matter expertise, and insight into the update of this 2005 unclassified terrorism handbook, *A Military Guide to Terrorism in the Twenty-First Century.*

This expanding partnership of the Threats Terrorism Team (T3) Network in conjunction with the Assistant Deputy Chief of Staff for Intelligence-Threats includes:

U.S. Northern Command, J2 Combined Intelligence and Fusion Center (CIFC)
U.S. Northern Command, Director of Operations, J3
U.S. Northern Command, J34, Force Protection and Risk Management Branch
U.S. Northern Command, J35
U.S. Northern Command, JTF-Civil Support, J5 Plans, CBRNE Consequence Management
U.S. European Command, Plans and Operations Center
U.S. Pacific Command, Antiterrorism and Training Branch, J34
U.S. Pacific Command, U.S. Marine Forces Pacific, G5
U.S. Central Command, J2
U.S. Special Operations Command, Center for Special Operations, J23
U.S. Southern Command, J2
U.S. Strategic Command, Joint Intelligence Center, J2201
U.S. Joint Forces Command, J9
U.S. Joint Forces Command, J34
Joint Staff, J34 Deputy Directorate for Antiterrorism/Homeland Defense
Joint Staff, J5 War on Terrorism Directorate, Strategic Planning Division
Joint Military Intelligence Training Center (JMITC)
State Department, Bureau of Diplomatic Security, Intelligence-Threats Analysis Directorate
Office of the Assistant Secretary of Defense for Homeland Defense
Department of Energy, Office of Headquarters Security Operations
Department of Homeland Security, Director Preparedness Division, Operational Integration Staff
Department of Homeland Security, Federal Emergency Management Agency, Region VII
Department of Homeland Security, Citizen Corps FEMA Region VII Program Manager
Department of Homeland Security, Transportation Security Administration, KCI Airport
Federal Bureau of Investigation (FBI) Terrorism Watch and Warning Unit
FBI, National Joint Terrorism Task Force (NJTTF)
FBI, Counterterrorism Division, Military Liaison and Detainee Unit
U.S. First Army Headquarters, Military Support Division, G3
U.S. Fifth Army Headquarters, G3
U.S. Navy Center for Antiterrorism and Navy Security Forces
U.S. Navy, Naval War College
U.S. Navy, Navy Command and Staff College
U.S. Marine Corps Training and Education Command, G3 Training Readiness, Plans and Policy
U.S. Marine Corps, Marine War College
U.S. Marine Corps, Marine Corps Command and Staff College
U.S. Air Force Security Forces Center
U.S. Air Force, National Air and Space Intelligence Center, Behavioral Influences Analysis Division
U.S. Air Force, Air War College
U.S. Air Force, Air Command and Staff College
U.S. Army Office of Deputy Chief of Staff G2, for Counterintelligence, HUMINT, and Security
U.S. Army Office of the Chief Information Officer (CIO)/G6

U.S. Army Network Enterprise Technology Command, 9th ASC, G2
U.S. Army Network Enterprise Technology Command, Office of Information Assurance
U.S. Military Academy (West Point), Combating Terrorism Center (CTC)
U.S. Army Combined Arms Center (CAC)
U.S. Army Maneuver Support Center (MANSCEN)
U.S. Army Combined Arms Support Command (CASCOM)
U.S. Army Combined Arms Center-Training (CAC-T)
U.S. Army Battle Command Training Program (BCTP)
National Defense University
U.S. Army TRADOC Centers and Schools, including:
U.S. Army, Army War College
U.S. Army Command and General Staff College (CGSC)
U.S. Army Logistics Management College (ALMC)
U.S. Army Aviation Logistics Center
U.S. Army Management Staff College
U.S. Army School of Information Technology
U.S. Army Leader College for Information Technology
U.S. Army Fort Eustis, Directorate of Plans, Training, Mobilization, and Security
U.S. Army Command and General Staff School (CGSS)
U.S. Army School for Command Preparation (SCP)
U.S. Army School for Advanced Military Studies (SAMS)
U.S. Army Center for Army Leadership (CAL)
U.S. Army Infantry Center, G2 Director of Intelligence and Security
U.S. Army Intelligence Center, Futures Development and Integration Center
U.S. Army Warrant Officer Career Center
U.S. Army Sergeants Major Academy
U.S. Army Soldier Support Institute
U.S. Army Academy of Health Sciences, Medical Department Center and School
U.S. Army Nuclear and Chemical Agency
U.S. Northern Command, Homeland Security/Defense Education Consortium (HSDEC)
U.S. Army TRADOC, Assistant Deputy Chief of Staff for Intelligence-Threats

Cyber Terrorism

Contents

This Page Intentionally Blank

Introduction

Information technology (IT) and digitization are integral elements woven into the virtual fabric of today's society. Whether in our personal or professional lives, the cyber world has become a dominant factor in everyday life. The CIA pointed out in a statement for the Joint Economic Committee in 2001, "Most experts agree that the IT revolution represents the most significant global transformation since the Industrial Revolution beginning in the mid-eighteenth century."[1] The increasingly indispensable nature of information technology, however, has transformed these systems into high value targets of cyber terrorists and presents a significant threat to the military, our economy and national security.

To highlight the importance of this technology to the U.S. military, in July 2003, DOD had more than 3 million individual computers on 12,000 local area networks (LANs). [2] These interconnected systems and LANs are part of what is known as the Global Information Grid (GIG), which is the globally interconnected set of information capabilities, processes, and personnel for collecting, processing, storing, disseminating, and managing information on demand to warfighters, policymakers, and support personnel. The GIG includes all owned and leased communications and computing systems and services, software, data, security services, and other associated services necessary to achieve information superiority.[3]

The GIG supports all DOD, National Security, and related intelligence community missions and functions in both peace and war that span the strategic, operational, tactical, and business arenas. The GIG provides capabilities from all operating locations, including bases, facilities, mobile platforms, and deployed sites; and provides interface to coalition, allied, and non-DOD users and systems.[4]

A portion of the GIG, the Defense Information System Network (DISN), is the global, end-to-end information transfer infrastructure of DOD. It provides long haul data, voice, video, and transport networks and services needed for national defense command, control, communication, and intelligence requirements, as well as corporate defense

---

[1] Director of Central Intelligence, *Cyber Threat Trends and U.S. Network Security*, Statement for the Record for the Joint Economic Committee by Lawrence K. Gershwin, National Intelligence Officer for Science and Technology, (Washington, D.C., 21 June 2001), 1; available from http://www.cia.gov/cia/public_affairs/speeches/2001/gershwin_speech_06222001.html; Internet; accessed 14 April 2004.

[2] Congress, House, Armed Services Subcommittee on Terrorism, Unconventional Threats and Capabilities, *Cyber-Terrorism*, Statement by Major General James D. Bryan, U.S. Army Commander, Joint Task Force-Computer Network Operations, U.S. Strategic Command and Vice Director, Defense Information Systems Agency, (Washington, D.C., 24 July 2003), 3; available from http://www.defenselink.mil/search97/s97is.vts?Action=FilterSearch&Filter=dl.hts&query=cyber-terrorism; Internet; accessed 6 April 2004.

[3] "Global Information Grid," Defense Information Systems Agency, Network Services (Website on line, n.d.); available from http://www.disa.mil/ns/gig.html; Internet; accessed 7 April 2004.

[4] Ibid.

requirements.[5] Examples of the services include video teleconferencing, the Defense Switched Network (DSN), the uNclassified IP Router NETwork (NIPRNET), and the Secret IP Router NETwork (SIPRNET).

Figure Intro-1. The Global Information Grid
(Source: Defense Information Systems Agency)

Just as the United States has capitalized on the use of computer technology, our enemies have not overlooked the fact that they must also operate in the computer age. As briefed to Congress in July 2003 by the Commander, Joint Task Force-Computer Network Operations, U.S. Strategic Command/Vice Director, Defense Information Systems Agency, the sophisticated threat to our Global Information Grid is extensive and presents a real danger to our national security. This threat includes more than 40 nation-states that have openly declared their intent to develop cyber warfare capabilities. Additionally, it includes transnational and domestic criminal organizations, hacker groups who sympathize with our [U.S.] enemies, terrorist organizations (evidenced by forensic analysis of captured computers) and "insiders" who support our enemies.[6]

Terrorists realize the benefits they can reap from using this technology. Equipped with a personal computer and an Internet connection, small players can somewhat level the playing field with their larger opponents in this "cyber arena." Terrorists do not have to

[5] "Defense Information System Network," Defense Information Systems Agency, Network Services (Website on line, n.d.); available from http://www.disa.mil/ns/gig.html; Internet; accessed 7 April 2004.
[6] Congress, House, Armed Services Subcommittee on Terrorism, Unconventional Threats and Capabilities, *Cyber-Terrorism*, Statement by Major General James D. Bryan, U.S. Army Commander, Joint Task Force-Computer Network Operations, U.S. Strategic Command and Vice Director, Defense Information Systems Agency, (Washington, D.C., 24 July 2003), 3-4; available from http://www.defenselink.mil/search97/s97is.vts?Action=FilterSearch&Filter=dl.hts&query=cyber-terrorism; Internet; accessed 6 April 2004.

expend large resources on a global intelligence collection organization or match the United States weapon-for-weapon on the battlefield to execute an operation. Terrorist groups can use cyber capabilities to assist them in planning and conducting their operations, and also to create destruction and turmoil by attacking our GIG systems and our critical infrastructures. Although many people believe terrorists only operate in the world of physical violence, many terrorist groups have well educated people and modern computer equipment to compete in cyberspace. Consequently, to fully understand the threat, we need to be aware of both sides of cyber operations, cyber support to terrorist operations and cyber-terrorism.

Page Intentionally Blank

.

Section I: Cyber Support to Terrorist Operations

Al-Qaeda "was using the Internet to do at least reconnaissance of American utilities and American facilities. If you put all the unclassified information together, sometimes it adds up to something that ought to be classified."

Richard Clark, Former Chairman, President's Critical Infrastructure Protection Board, February 13, 2002

Terrorists recognize the benefit of cyber operations and continue to exploit information technology in every function of their operations. Macro-functions include:

Planning

Terrorists use the cyber infrastructure to plan attacks, communicate with each other, and posture for future exploitation. Employing easy-to-use encryption programs that they can easily download from the Internet, terrorists are able to communicate in a secure environment. Using steganography, they hide instructions, plans and pictures for their attacks in pictures and posted comments in chat rooms. The images and instructions can only be opened using a "private key" or code known only to the recipients. In fact, reports that use encryption are a common tool of Muslim extremists and is being taught in their training camps.[7] Additionally, these encryption programs can scramble telephone conversations when the phones are plugged into a computer.[8]

Recruitment

Recruitment is the life-blood of a terrorist organization and they use multiple methods to entice new members. In addition to traditional methods, such as written publications, local prayer leaders, audio-video cassettes and CDs promoting their cause; terrorist groups also use their own websites to recruit new members. This is accomplished by providing their view of the history of their organization, its cause, and additional information to encourage potential members to join. Additionally, they often have hyperlinks to other material to encourage membership. They also use these sites to collect "donations" for their cause. Good examples of these websites include HAMAS, http://www.hamasonline.com/; Hizballah, http://www.hizbollah.org/; Revolutionary Armed Forces of Colombia (FARC), http://www.farcep.org/pagina_ingles/; and the Earth Liberation Front (ELF), http://www.earthliberationfront.com/main.shtml.

[7] Jack Kelley, "Terror Groups Hide Behind Web Encryption," *USA Today*, 5 February 2001; available from http://www.usatoday.com/tech/news/2001-02-05-binladen.htm; Internet; accessed 6 April 2004.
[8] Ibid.

Research

Using the Internet, terrorists can tap into thousands of databases, libraries and newsgroups around the world to gather information on any subjects that they need to research. The information can be in the form of text, maps, satellite images, pictures or even video material. The use of search engines, such as Google, have made searching the Internet very easy and allows terrorists to obtain critical information located in the public domain using very simple resources. For example, by typing "Bombs" in the Google search engine, 2,870,000 references were found in 0.17 seconds. To narrow this list, typing "Bombs AND Homemade," resulted in 47,200 references being found in 0.08 seconds. Although most of these are harmless references that may just refer to news articles, many provide detailed information on how to manufacture bombs. One site not only provided information on bombs, but also provided additional references on subjects such as drugs, fake IDs, fraud, lock picking, and weapons.

To highlight the importance terrorists place on research over the Internet, an al Qaeda training manual recovered in Afghanistan states: "Using public sources openly and without resorting to illegal means, it is possible to gather at least 80% of information about the enemy." After finding this manual, Secretary of Defense Donald Rumsfeld disseminated a memo to the armed services stating: "One must conclude our enemies access DoD Web sites on a regular basis."[9] The memo directed the military to purge their websites of information that could benefit our potential enemies.

Although the military has tightened up security on their sites, terrorists can still conduct research on military units. Using a search engine, they simply type in a specific organization and the search engine will provide the links if they exist. For example, typing in "Army AND Fort Hood" resulted in the Fort Hood home page being displayed. This site provided the entire list of units assigned to III Corps simply by opening the web page. Looking at a Fort Bragg web site, available references included a map of the installation, the schedule for the installation shuttle bus, and a copy of the official telephone directory, which provides all of the units on the installation. Other critical information is available on the military, such as every Army and Air Force airfield in the United States, and the location of military ammunition depots throughout CONUS.

Terrorists can also use the Internet to research information on the critical infrastructure of the United States. In the fall of 2001, police found a pattern of surveillance by Middle East and South Asia unknown browsers against Silicon Valley computers used to manage Bay Area utilities and government offices. As the FBI became involved, the trail revealed even broader surveillance, casing sites nationwide. Routed through telecommunication switches in Saudi Arabia, Indonesia, and Pakistan, surveillance was conducted on emergency telephone systems, electrical generation and transmission

[9] Kevin Poulsen, "Rumsfeld Orders .mil Web Lockdown," *The Register*, 17 January 2003; available from http://www.theregister.co.uk/2003/01/17/rumsfeld_orders_mil_web_lockdown; Internet; accessed 8 April 2004.

facilities, water storage and distribution systems, nuclear power plants, and gas facilities.[10]

Unfortunately, using the convenience of the Internet, terrorists can virtually research any subject, to include information on potential targets, without ever leaving the safety of their locales overseas or within the United States.

Propaganda

As Christopher Harmon states in his book, *Terrorism Today*, "Propaganda is a veritable terror group standard."[11] Terrorist organizations depend on the backing of a broad base of support for both recruiting and funding. They use propaganda to discredit their enemy while making themselves look good. Earlier terrorist groups published newspapers and leaflets to spread their propaganda. Although this form of media is still widely used, terrorist groups are now using the Internet.

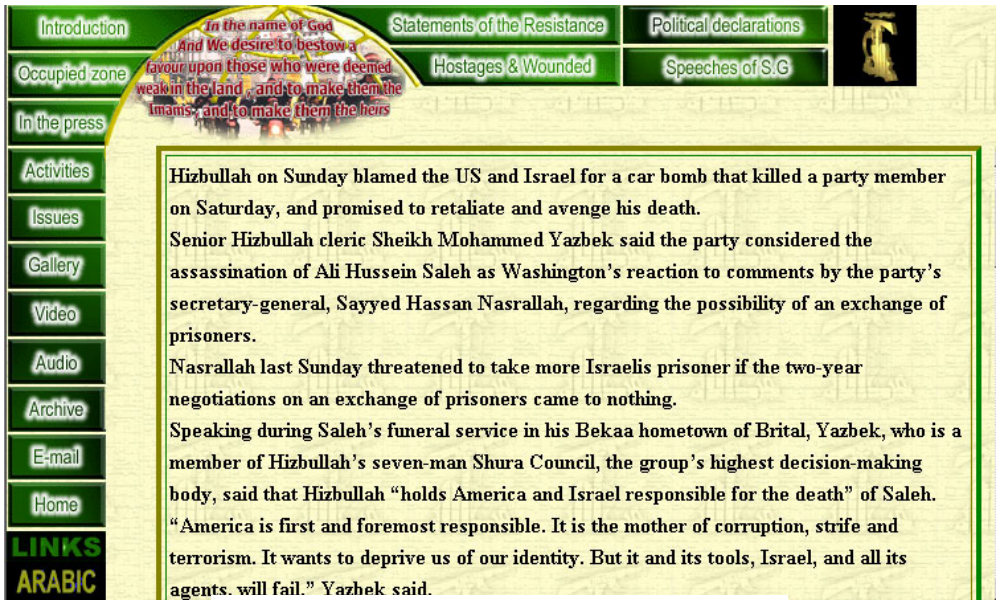


Figure I-1. Hizballah Website Example

Most radical groups of international significance operate Internet sites. These groups post articles supporting their agendas on these sites, which make them instantly available to the worldwide cyber community. Radical Islam in particular makes use of propaganda to enlist the support of their own public for jihad and to demoralize the enemy. The statement from the Hizballah website is an example of some of their propaganda.

[10] Bartom Gellman, "Cyber-Attacks by Al Qaeda Feared," *Washingtonpost.com*, 27 June 2002; available from http://www.washingtonpost.com/ac2/wp-dyn/A50765-2002Jun26; Internet; accessed 12 April 2004.
[11] Christopher C. Harmon, *Terrorism Today* (London: Frank Cass Publishers, 2000; reprint, Portland: Frank Cass Publishers, 2001), 55.

Section II: Cyber-Terrorism

Cyber-terrorism is a development of terrorist capabilities provided by new technologies and networked organizations, which allows terrorists to conduct their operations with little or no physical risk to themselves. Cyber-terrorism is a new and somewhat nebulous concept, with debate as to whether it is a separate phenomenon, or just a facet of information warfare practiced by terrorists. Even for those that believe cyber-terrorism is a separate phenomenon; the boundaries often become blurred between information warfare, computer crime, online social activism, and cyber-terrorism.

Cyber-terrorism differs from other improvements in terrorist technology because it involves offensive information technology capabilities, either alone or in combination with other forms of attack. Some examinations of cyber-terrorism focus on the physical destruction of information hardware and software, or physical damage to personnel or equipment using information technology as the medium. Examples of this approach would include the chaos and destruction caused by disrupting a nation's air traffic control system, crashing two trains together by overriding the railroad signal and switching system, interfering with the control systems for water or electricity, or blocking and falsifying commercial communications to cause economic disruption.

One common aspect is that organizations trying to attack using information technology will more than likely want to keep the information network up, or at least limit their destruction or disruptions to discrete portions of the network. For a true "cyber-terrorist," the network is the method of attack. It is the weapon, or at the least, the medium through which an attack is delivered. Information warfare of this sort requires that messages and computer commands are transmitted, programs and malicious software be emplaced, fraudulent transactions take place, and information be available for exploitation. Defacing websites, crashing portions of a target network, accessing enemy information, denying network access to other groups, manipulating financial confidence and causing panic exemplify this warfare. Still, they require that the target network remain more or less intact. A terrorist group could crash a network through physical destruction or technological attack, but only a group whose perceived gains would offset their loss of information, communication, and other capabilities would do this.[12]

Outside of computer networks, communications networks can also be targeted for destruction, disruption, or hijacking. This has a direct impact on the military and the government since a large percentage of the GIG is dependent on commercial telephone links and the Internet. Destructive and disruptive attacks upon communication networks would likely be supporting operations designed to increase the effectiveness of physical attacks. Hijacking, or taking control of a communication network might support another operation, or be attempted for it's own impact. Dissident factions have already substituted their own satellite TV signals for state controlled broadcasting.[13] Terrorists could exploit

[12] John Arquilla and David Ronfeldt, ed., *Networks and Netwars* (Santa Monica: RAND, 2001): 5.
[13] "Chinese Satellite TV Hijacked by Falun Gong Cult," *People's Daily Online,* 9 July 2002; available from http://english.peopledaily.com.cn/200207/08/eng20020708_99347.shtml; Internet; accessed 27 November 2002.

such capabilities to bypass mainstream media restraint in covering particularly shocking actions, or to demonstrate their power and capability to challenge their enemies.

Other views of cyber terror stress the manipulation, modification, and destruction of non-physical items such as data, websites, or the perceptions and attitudes this information can influence. Attacks that would destroy electronic records of financial transactions, or permit large-scale electronic theft would cause significant economic damage to a country, but not truly "exist" in the physical world. Changing the information or appearance of an enemy's official web page allows the terrorist to spread negative perceptions or false information without physical intrusion.

Currently, DOD does not have a definition of cyber-terrorism, but does define cyberspace as: "The notional environment in which digitized information is communicated over computer networks."[14] In the Federal Government, the FBI describes cyber-terrorism as: "Cyber-terrorism is a criminal act perpetrated by the use of computers and telecommunications capabilities, resulting in violence, destruction and/or disruption of services to create fear by causing confusion and uncertainty within a given population, with the goal of influencing a government or population to conform to a particular political, social, or ideological agenda."[15] Another definition by Kevin Coleman, a former chief strategist at Netscape who writes a Homeland Security focused column for *Directions* magazine is: "The premeditated use of disruptive activities, or the threat thereof, against computers and/or networks, with the intention to cause harm or further social, ideological, religious, political or similar objectives. Or to intimidate any person in furtherance of such objectives."[16]

These definitions spotlight the fact that cyber-terrorism is a serious threat. In the first half of 2002, there were more than 180,000 Internet based attacks on business and these attacks are increasing at an annual rate above 60%. Additionally, it is estimated that the reported incidents may represent only 10% of the actual total. A research study conducted by the Computer Crime Research Center in 2002 reported that 90% of respondents detected computer security breaches within the previous twelve months.[17] In the Department of Defense, the speed and complexity of attacks are increasing. The Defense Information Systems Agency estimated in 1996 that DOD IT systems were attacked about 250,000 times per year and the Government Auditing Office (GAO) reported in the same year that only about 1 in 500 attacks were detected and reported.[18]

---

[14] Joint Publication 1-02, *DOD Dictionary of Military and Associated Terms*, 12 April 2001, as amended through 17 December 2003.
[15] Harold M. Hendershot, "CyberCrime 2003 – Terrorists' Activity in Cyberspace" (Briefing slides from the Cyber Division, Federal Bureau of Investigation, Washington, D.C.): 12; available from http://www.4law.co.il/L373.pdf; Internet; accessed 6 April 2004.
[16] Kevin Coleman, "Cyber Terrorism," *Directions Magazine*, 10 October 2003, 1; available from http://www.directionsmag.com/article.php?article_id=432; Internet; accessed 15 March 2004.
[17] Ibid., 2-3.
[18] General Accounting Office, *Information Security: Computer Attacks at Department of Defense Pose Increasing Risks*, Report AIMD-96-84, (Washington, D.C., 22 May 1996), 1; available from http://www.fas.org/irp/gao/aim96084.htm; Internet; accessed 12 April 2004.

In 2002, DOD successfully defended against 50,000 intrusion attempts to gain root access to the GIG. By June 2003, there were over 21,000 attempts.[19]

Objectives of Cyber Attack

When analyzing the objectives of a cyber attack and the ultimate outcome the attack may have, the effects of cyber attack align generally into four areas. The first three effects listed below address the impact on the actual IT systems themselves, [20] whereas the last effect addresses the impact of using the IT system for physical destructive purposes.

- Loss of Integrity. System and data integrity refers to the requirement that information be protected from improper modification. Integrity is lost if unauthorized changes are made to the data or IT system by either intentional or accidental acts. If the loss of system or data integrity is not corrected, continued use of the contaminated system or corrupted data could result in inaccuracy, fraud, or erroneous decisions. Also, violation of integrity may be the first step in a successful attack against system availability or confidentiality. For all these reasons, loss of integrity reduces the assurance of an IT system.

- Loss of Availability. If a mission-critical IT system is attacked and rendered unavailable to its end users, the organization's mission will most likely be affected. Loss of system functionality and operational effectiveness, for example, may result in loss of productive time, thus impeding the end users' performance of their functions in supporting the organization's mission.

- Loss of Confidentiality. System and data confidentiality refers to the protection of information from unauthorized disclosure. The impact of unauthorized disclosure of confidential information can range from the jeopardizing of national security to the disclosure of Privacy Act data. Unauthorized, unanticipated, or unintentional disclosure could result in loss of public confidence, embarrassment, or legal action against the organization.

- Physical Destruction. Physical destruction refers to the ability to create actual physical harm or destruction through the use of IT systems. Much of our critical infrastructure, such as transportation, power, and water companies are operated with networks of computer-controlled devices known as supervisory control and data acquisition (SCADA) systems. These systems can be attacked and used to cause

[19] Congress, House, Armed Services Subcommittee on Terrorism, Unconventional Threats and Capabilities, *Cyber-Terrorism*, Statement by Major General James D. Bryan, U.S. Army Commander, Joint Task Force-Computer Network Operations, U.S. Strategic Command and Vice Director, Defense Information Systems Agency, (Washington, D.C., 24 July 2003), 9; available from http://www.defenselink.mil/search97/s97is.vts?Action=FilterSearch&Filter=dl.hts&query=cyber-terrorism; Internet; accessed 6 April 2004.

[20] Department of Commerce, National Institute of Standards and Technology, *Risk Management Guide for Information Technology Systems*, NIST Special Publication 800-30, by Gary Stoneburner, Alice Goguen, and Alexis Feringa, (Washington, D.C., 2001): 22; available from http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf; Internet; accessed 12 April 2004.

operations to malfunction, such as the release of water from a dam or switching the tracks on a railroad to create a collision. There have also been concerns that a terrorist could take control of the air traffic control system and cause aircraft to crash. Fortunately these specific scenarios have not occurred, and there are normally sufficient manual checks and overrides that help prevent this type of failure. However, the possibility of taking over a SCADA system is real. There was a case in 2001 where an individual used the Internet, a wireless radio, and stolen control software to release up to 1 million liters of sewage into the river and coastal waters of Queensland, Australia. The individual had attempted to access the system 44 times, prior to being successful in his 45th attempt, without being detected.[21] This example does indicate that individuals with the proper tools and knowledge can bypass security in public utilities or other organizations using SCADA systems.

Actors

Not every individual or group who uses information technology to further their agenda or attack their opponents are necessarily cyber terrorists. However, it can often be difficult to determine if an attack is originating from terrorists or from high school students with the technical expertise to access your system. It often becomes a judgment call on what is truly cyber-terrorism and what is just hacking. There are various categories of attackers that the military may be faced with in the cyber arena.

- Hackers: These are advanced computer users who spend a lot of time on or with computers and work hard to find vulnerabilities in IT systems. Some hackers, known as Whitehat Hackers, look for vulnerabilities and then work with the vendor of the affected system to fix the problem. The typical hacker, though, is often referred to as a Blackhat Hacker. They are the individuals who illegally break into other computer systems to damage the system or data, steal information, or cause disruption of networks for personal motivations, such as monetary gain or status. However, they generally lack the motivation to cause violence or severe economic or social harm.

  An example of the systems hackers can access was demonstrated in 1998. Two teenage hackers accessed computers at Lawrence Livermore National Laboratory, the U.S. Air Force, and other organizations. After being caught by the FBI, the teenagers pleaded guilty to illegally accessing restricted computers, using "sniffer" programs to intercept computer passwords, and reprogramming computers to allow complete access to all of their files. They also inserted "backdoor" programs in the computers to allow themselves to re-enter at will.[22]

  A concern beyond just gaining access to a system is what hackers may do with information that they steal from the military. In November 1998, the Detroit News

[21] Robert Lemos, "What are the Real Risks of Cyberterrorism?" *ZDNet*, 26 August 2002, 4; available from http://zdnet.com.com/2102-1105_2-955293.html; Internet; accessed 6 April 2004.
[22] Andrew Quinn, "Teen Hackers Plead Guilty to Stunning Pentagon Attacks," Reuters, 31 July 1998, 1; available from http://www.geocities.com/Area51/Shadowlands/6583/project395.html; Internet; accessed 14 April 2004.

reported that a member of Harkat-ul-Ansar, a militant Pakistani group, tried to buy military software from hackers who had stolen it from DOD computers.[23]

- "Hactivists:" These are combinations of hackers and activists. They usually have a political motive for their activities, and identify that motivation by their actions, such as defacing opponents' websites with counter-information or disinformation. Alone, these actions bear the same relation to cyber-terrorism that theft, vandalism, or graffiti do to mundane physical terrorism; they may be an unrelated activity, or a supporting piece of a terrorist campaign.

  An example of this type activity occurred following the inadvertent bombing of the Chinese embassy in Belgrade during the 1999 NATO bombing campaign in Yugoslavia when pro-Beijing Chinese hackers conducted mass cyber protests against U.S. government Web sites in response to this accident. This type activity occurred again in May 2001 when Chinese protesters defaced or closed over 100 sites in the U.S., after a Chinese fighter jet collided with a U.S. reconnaissance plane off the Chinese coast.

- Computer Criminals: Criminals have discovered they can exploit computer systems, primarily for financial gain. Computer extortion is a form of this type crime. An example is the case of media titan Michael Bloomberg. His corporation was hacked into by two suspects who demanded two hundred thousand dollars from Bloomberg in "consulting fees" in order for them to keep quiet on how they compromised Bloomberg's computer system.

  Another example deals with gaining unauthorized access to government computers and obtaining information for financial gain. In September 2003, an individual was in a conspiracy to access military, government and private sector computers. The indictment alleged that the defendant was the president of a computer security company and he was trying to gain unauthorized access to government and military computers, copy computer files and take these files to the media in order to generate public visibility for his company. He thought this would lead to new clients and increased profits. According to the indictment, the conspirators possessed government files belonging to the National Aeronautics and Space Administration (NASA), United States Army, United States Navy, Department of Energy and National Institutes of Health.[24]

- Industrial Espionage: Industrial espionage has a long history in our industrialized society and there is no question that with today's reliance on computer systems and

---

[23] Congress, House, Armed Services Special Oversight Panel on Terrorism, *Cyberterrorism*, Testimony by Dorothy E. Denning, Georgetown University, (Washington, D.C., 23 May 2000): 3; available from http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html; Internet; accessed 9 April 2004.

[24] Department of Justice, U.S. Attorney Southern District of California, Press Release, *President of San Diego Computer Security Company Indicted in Conspiracy to Gain Unauthorized Access into Government Computers*, (San Diego, CA, 29 September 2003): 1; available from http://www.usdoj.gov/criminal/cybercrime/okeefeArrest.htm; Internet; accessed 12 April 2004.

networks to plan, document, and store research data; industrial espionage has added the electronic medium to its list of methods of operation. These industrial spies may be government sponsored or affiliated, from commercial organizations, or private individuals. Their purpose may be to discover proprietary information on financial or contractual issues, or to acquire classified information on sensitive research and development efforts.

Although industrial espionage is normally associated with civilian corporations, it can have a direct impact on the military as well. As stated by the Defense Security Service (DSS) in a 2002 report, U.S. military critical technologies are the most sought after in the world.[25] The espionage may be directed against a defense contractor; against DOD's military research, development, test, and evaluations community; or against DOD's acquisition program offices. To demonstrate the assault against military technology, DSS received reports of suspicious activities concerning defense technology from sources in 75 countries in 2001. This activity covered every militarily critical technology category, with the highest interest being information systems, sensors and lasers, armaments and energetic materials, aeronautic systems, and electronics.[26]

- Insiders: Although IT professionals do everything possible to secure their systems from outsiders; there is always the threat of an insider with authorized access to a system conducting an attack. These insiders may be disgruntled employees working alone, or they may be working in concert with other terrorists to use their access to help compromise the system.

  An example occurred in July 1997, when a U.S. Coast Guard employee used her insider knowledge and another employee's password and logon identification to delete data from a U.S. Coast Guard personnel database system. It took 115 agency employees over 1800 hours to recover and reenter the lost data.

- Consultants/contractors: Another concern is the practice by many organizations to use outside contractors to develop software systems. This often provides these contractors with the access required to engage in cyber-terrorism.

  In March 2000, Japan's Metropolitan Police Department reported that they had procured a software system to track police vehicles that had been developed by Aum Shinryko. This is the cult that released sarin gas in the Tokyo subway in 1995. The police discovered that the cult had received classified tracking data on 115 of the vehicles. Additionally, the cult had developed software for 80 Japanese firms and 10 government agencies. One of several concerns is that they had installed a Trojan horse in the systems to launch or facilitate cyber terrorist attacks at a later date.[27]

---

[25] Department of Defense, Defense Security Service, *Technology Collection Trends in the U.S. Defense Industry 2002* (Alexandria, VA, n.d.), 1; available from http://www.wright.edu/rsp/Security/TechTrends.pdf; Internet; accessed 19 April 2004.
[26] Ibid., 2-3.
[27] Ibid., 3.

- Terrorists: Although there have been no major cyber attacks caused by terrorist groups that have taken lives or caused severe physical destruction, some government experts believe that terrorists are at the point where they may be able to use the Internet as a direct instrument to cause casualties, either alone or in conjunction with a physical attack. In fact, the FBI's director of the National Infrastructure Protection Center stated in 2002, "The event I fear most is a physical attack in conjunction with a successful cyber-attack on the responders' 911 system or on the power grid."[28]

  The Cyber Division of the FBI states that in the future, cyber-terrorism may become a viable option to traditional physical acts of violence due to:[29]

  - Anonymity
  - Diverse targets
  - Low risk of detection
  - Low risk of personal injury
  - Low investment
  - Operate from nearly any location
  - Few resources are needed

The following table from the National Institute of Standards and Technology summarizes threats to IT systems, including the source, their motivation, and actions.[30]

Threat-Source	*Motivation*	*Threat Actions*
Hacker, cracker	Challenge Ego Rebellion	. Hacking . Social engineering . System intrusion, break-ins . Unauthorized system access
Computer criminal	Destruction of information Illegal information disclosure Monetary gain Unauthorized data alteration	. Computer crime (e.g., cyber stalking) . Fraudulent act (e.g., replay, impersonation, interception) . Information bribery . Spoofing . System intrusion

[28] Bartom Gellman, "Cyber-Attacks by Al Qaeda Feared," *Washingtonpost.com*, 27 June 2002; available from http://www.washingtonpost.com/ac2/wp-dyn/A50765-2002Jun26; Internet; accessed 12 April 2004.
[29] Harold M. Hendershot, "CyberCrime 2003 – Terrorists' Activity in Cyberspace" (Briefing slides from the Cyber Division, Federal Bureau of Investigation, Washington, D.C.): 7; available from http://www.4law.co.il/L373.pdf; Internet; accessed 6 April 2004.
[30] Department of Commerce, National Institute of Standards and Technology, *Risk Management Guide for Information Technology Systems*, NIST Special Publication 800-30, by Gary Stoneburner, Alice Goguen, and Alexis Feringa, (Washington, D.C., 2001): 14; available from http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf; Internet; accessed 12 April 2004.

Terrorist	Blackmail Destruction Exploitation Revenge	. Bomb/Terrorism . Information warfare . System attack (e.g., distributed denial of service) . System penetration . System tampering
Industrial espionage (companies, foreign governments, other government interests)	Competitive advantage Economic espionage	. Economic exploitation . Information theft . Intrusion on personal privacy . Social engineering . System penetration . Unauthorized system access (access to classified, proprietary, and/or technology-related information)
Insiders (poorly trained, disgruntled, malicious, negligent, dishonest, or terminated employees)	Curiosity Ego Intelligence Monetary gain Revenge Unintentional errors and omissions (e.g., data entry error, programming error)	. Assault on an employee . Blackmail . Browsing of proprietary information . Computer abuse . Fraud and theft . Information bribery . Input of falsified, corrupted data . Interception . Malicious code (e.g., virus, logic bomb, Trojan horse) . Sale of personal information . System bugs . System intrusion . System sabotage . Unauthorized system access

Table II-1. Human Threats – Threat-Source, Motivation, and Threat Actions

Tools of Cyber Attacks

There are a myriad of tools that cyber terrorists will use to accomplish their objectives. Some of these are:

- Backdoor: This is used to describe a back way, hidden method, or other type of method of by passing normal security in order to obtain access to a secure area. It is also referred to as a trapdoor. Sometimes backdoors are surreptitiously planted on a network element; however, there are some cases where they are purposely installed on a system. An example of this is the craft interface. This interface is on network elements and is designed to facilitate system management, maintenance, and troubleshooting operations by technicians, called craft personnel. The craft interface

allows the technician to access the equipment on site, or in many cases, access it via remote terminal. Actions they can conduct include: [31]

- Initial turn–up of network elements and/or systems
- Trouble verification
- Repair verification
- Monitor network element (NE) performance
- Update NE software and hardware
- Manual control of NE
- Remote inventory

Security for these interfaces is normally via userids and passwords. Unfortunately, passwords are often the weakest link in a computer security scheme because password cracking tools continue to improve and the computers used to crack passwords are more powerful than ever. Network passwords that once took weeks to crack can now be cracked in hours.

Although the craft interface allows the service provider access to conduct maintenance on the equipment, many vendors build back doors to have access to these interfaces so they can also remotely troubleshoot equipment. Unfortunately, this means a technician from outside the organization is able to gain access to the system and could facilitate cyber terrorist activities.

- Denial of Service Attacks (DOS): A DOS attack is designed to disrupt network service, typically by overwhelming the system with millions of requests every second causing the network to slow down or crash. An even more effective DOS is the distributed denial of service attack (DDOS). This involves the use of numerous computers flooding the target simultaneously. Not only does this overload the target with more requests, but having the DOS from multiple paths makes backtracking the attack extremely difficult, if not impossible. Many times worms are planted on computers to create zombies that allow the attacker to use these machines as unknowing participants in the attack. To highlight the impact of these type attacks, in February 2000, DOS attacks against Yahoo, CNN, eBay and other e-commerce sites were estimated to have caused over a billion dollars in losses.[32] DOS attacks have also been directed against the military. In 1999, NATO computers were hit with DOS attacks by hactivists protesting the NATO bombing in Kosovo.

- E-mail Spoofing: E-mail spoofing is a method of sending e-mail to a user that appears to have originated from one source when it actually was sent from another source. This method is often an attempt to trick the user into making a damaging statement or

[31] "NE-NE Remote Login Initial Solution Evaluation Criteria," *SONET Interoperability Forum* Document Number SIF-RL-9605-043-R4, (12 June 1996): 4; available from http://www.atis.org/pub/sif/approved/sif96008.pdf; Internet; accessed 9 April 2004.
[32] Congress, House, Armed Services Special Oversight Panel on Terrorism, *Cyberterrorism*, Testimony by Dorothy E. Denning, Georgetown University, (Washington, D.C., 23 May 2000), 1; available from http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html; Internet; accessed 9 April 2004.

releasing sensitive information (such as passwords). For example, e-mail could be sent claiming to be from a person in authority requesting users to send them a copy of a password file or other sensitive information.

- IP Address Spoofing: A method that creates Transmission Control Protocol/Internet Protocol (TCP/IP) packets using somebody else's IP address. Routers use the "destination IP" address to forward packets through the Internet, but ignore the "source IP" address. This method is often used in DDOS attacks in order to hide the true identity of the attacker.

- Keylogger: A software program or hardware device that is used to monitor and log each of the keys a user types into a computer keyboard. The user who installed the program or hardware device can then view all keys typed in by that user. Because these programs and hardware devices monitor the actual keys being typed, a user can easily obtain passwords and other information the computer operator may not wish others to know.

- Logic bomb: A program routine that destroys data by reformatting the hard disk or randomly inserting garbage into data files. It may be brought into a computer by downloading a public-domain program that has been tampered with. Once it is executed, it does its damage immediately, whereas a virus keeps on destroying.

- Physical Attacks: This involves the actual physical destruction of a computer system and/or network. This includes destroying transport networks as well as the terminal equipment.

- Sniffer: A program and/or device that monitors data traveling over a network. Although sniffers are used for legitimate network management functions, they also are used during cyber attacks for stealing information, including passwords, off a network. Once emplaced, they are very difficult to detect and can be inserted almost anywhere through different means.

- Trojan Horse: A program or utility that falsely appears to be a useful program or utility such as a screen saver. However, once installed performs a function in the background such as allowing other users to have access to your computer or sending information from your computer to other computers.

- Viruses: A software program, script, or macro that has been designed to infect, destroy, modify, or cause other problems with a computer or software program. There are different types of viruses. Some of these are:

    - Boot Sector Virus: Infects the first or first few sectors of a computer hard drive or diskette drive allowing the virus to activate as the drive or diskette boots.
    - Companion Virus: Stores itself in a file that is named similar to another program file that is commonly executed. When that file is executed the virus

will infect the computer and/or perform malicious steps such as deleting your computer hard disk drive.

- Executable Virus: Stores itself in an executable file and infects other files each time the file is run. The majority of all computer viruses are spread when a file is executed or opened.
- Overwrite Virus: Overwrites a file with its own code, helping spread the virus to other files and computers.
- Polymorphic Virus: Has the capability of changing its own code allowing the virus to have hundreds or thousands of different variants making it much more difficult to notice and/or detect.
- Resident Virus: Stores itself within memory allowing it to infect files instantaneously and does not require the user to run the "execute a file" to infect files.
- Stealth Virus: Hides its tracks after infecting the computer. Once the computer has been infected the virus can make modifications to allow the computer to appear that it has not lost any memory and or that the file size has not changed.

- Worms: A destructive software program containing code capable of gaining access to computers or networks and once within the computer or network causing that computer or network harm by deleting, modifying, distributing, or otherwise manipulating the data.

- Zombie: A computer or server that has been basically hijacked using some form of malicious software to help a hacker perform a Distributed Denial Of Service attack (DDOS).

Section III: Cyber Threat to U.S. Critical Infrastructures

Today, the cyber economy is the economy. Corrupt those networks and you disrupt this nation.

Condoleezza Rice, National Security Advisor to President George W. Bush, March 22, 2001

Several studies examining the cyber threat have shown that critical infrastructures are potential targets of cyber terrorists. These infrastructures make extensive use of computer hardware, software, and communications systems. However, the same systems that have enhanced their performance potentially make them more vulnerable to disruption by both physical and cyber attacks to these IT systems. These infrastructures include: [33]

- Energy systems
- Emergency services
- Telecommunication
- Banking and finance
- Transportation
- Water system

A quick review of the automation used in the electric power industry demonstrates the potential vulnerabilities to our critical infrastructures. The electrical industry has capitalized on computer technology for improved communication and automation of control centers, substations and remote protection equipment. They use a host of computer-based equipment including SCADA systems; substation controllers consisting of programmable logic controllers, remote terminal units, data processing units and communication processors; and intelligent electronic devices consisting of microprocessor-controlled meters, relays, circuit breakers, and circuit reclosers. If unauthorized personnel gain cyber access to these systems, any alterations to settings or data can have disastrous consequences similar to physical sabotage, resulting in widespread blackouts.[34]

There have been many documented attacks against this infrastructure from hackers and criminals. As an example, FBI agents arrested a Louisiana man in February 2004 for sending an e-mail to certain users of a WebTV service that, once opened, reprogrammed

[33] Department of the Treasury, Office of the Comptroller of the Currency, *Infrastructure Threats from Cyber-Terrorists*, OCC Bulletin 99-9, (Washington, D.C., 5 March 1999), 2; available from http://www.occ.treas.gov/ftp/bulletin/99-9.txt; Internet; accessed 6 April 2004.
[34] Paul Oman, Edmund Schweitzer, and Jeff Roberts, "Protecting the Grid from Cyber Attack Part I: Recognizing Our Vulnerabilities," *Utility Automation and Engineering T&D*, November 2001; available from http://uaelp.pennnet.com; Internet; accessed 24 June 2004.

their computers to dial "9-1-1" instead of a local Internet access telephone number. The 9-1-1 calls caused by the e-mail resulted in the dispatch of police in locations from New York to California.[35]

Another example occurred in New York in 1997. A juvenile accessed the components of the phone system operated by NYNEX. Several commands were sent that disrupted the telephone service to the Federal Aviation Administration tower at the Worcester Airport, to the Worcester Airport Fire Department, and to other related entities such as airport security, the weather service, and various private airfreight companies. As a result of this disruption, the main radio transmitter and the circuit, which enabled aircraft to send an electronic signal to activate the runway lights on approach, were disabled. This same individual then accessed the loop carrier system for customers in and around Rutland, Massachusetts and sent commands that disabled the telephone service, including the 911 service, throughout the Rutland area.[36]

Although there have been no major terrorist attacks to these critical infrastructure systems to date, there is evidence that terrorist groups have been conducting surveillance on them. As stated earlier in this section under “Research,” police have found a pattern of surveillance by unknown browsers located in the Middle East and South Asia against emergency telephone systems, electrical generation and transmission facilities, water storage and distribution systems, nuclear power plants, and gas facilities.

Although these systems fall within the civilian sector, the military is highly dependent on all of these critical functions and would be directly impacted if they were successfully attacked. Consider the impact on unit deployment if a successful cyber attack, or a combination of cyber and physical attack, is conducted against our critical infrastructure during movement—

- Disruption of the rail system could severely impact movement of equipment to a port of embarkation.
- A successful attack against a power substation could halt loading operations at the port.
- A successful attack against the telecommunications systems would directly impact the command and control of the operations.

[35] Department of Justice, U.S. Attorney, Northern District of California, Press Release, *Louisiana Man Arrested for Releasing 911 Worm to WebTV Users*, (San Francisco, CA, 19 February 2004), 1; available from http://www.usdoj.gov/criminal/cybercrime/jeansonneArrest.htm; Internet; accessed 12 April 2004.
[36] Congress, Senate, Judiciary Subcommittee on Terrorism, Technology, and Homeland Security, *Cyber Terrorism*, Testimony of Keith Lourdeau, Deputy Assistant Director, Cyber Division, FBI, (Washington, D.C., 24 February 2004), 3; available from http://www.fbi.gov/congress/congress04/lourdeau022404.htm; Internet; accessed 15 April 2004.

Section IV: Cyber Threat to the Military

Peace really does not exist in the Information Age.

Air Force Lt. Gen. Kenneth Minihan,
Director, National Security Agency,
June 4, 1998

As discussed at the beginning of this sub handbook, the military is linked together through the Global Information Grid, and the computers and computer networks comprising the GIG are likely targets for cyber terror. Although many people may think that the military's only vulnerability is to command and control systems, it is important to realize that the Department of Defense uses IT systems for a number of functions, in both peace and war. These include:[37]

- Commercial transactions
- Payrolls
- Sensitive research data
- Intelligence
- Operational plans
- Procurement sensitive source selection data
- Health records
- Personnel records
- Weapons systems maintenance records
- Logistics operations

In addition to the day-to-day operations in DOD that encompass the above functions, a current operational example of the military's reliance on the GIG is Operation Iraqi Freedom. In 2003, unclassified testimony to the House Armed Services Subcommittee on Terrorism, Unconventional Threats, and Capabilities by the Commander, Joint Task Force-Computer Network Operations, U.S. Strategic Command/Vice Director, Defense Information Systems Agency stated that deployed forces used 50 times more bandwidth per person during Operation Iraqi Freedom than during Operation Desert Storm. The GIG was used for collaborative command and control across the globe, and concurrent planning was used extensively to execute missions. Additionally, Predator aircraft used

[37] General Accounting Office, *Information Security: Computer Attacks at Department of Defense Pose Increasing Risks*, Report AIMD-96-84, (Washington, D.C., 22 May 1996), 7; available from http://www.fas.org/irp/gao/aim96084.htm; Internet; accessed 12 April 2004.

in theater to collect intelligence were controlled remotely from CONUS and the collected intelligence was analyzed in real-time.[38]

For U.S. military forces, likely "cyber terror" threats include attempts to overload data transmission and information processing capabilities. Physical destruction of some communications nodes, combined with decoys, false chatter, and deception to overload the remainder could significantly slow the ability to assess and respond to threats. Another threat is the use of unsecured personal information to target service members or their families for physical and electronic harassment campaigns. This technique has found widespread use amongst single-issue terrorists. These terrorists make phone numbers, addresses, and any other available personal information public via the Internet; and urge sympathizers or proxies to threaten and harass service members, their families, and associates, vandalize their property, or steal their identity. This could easily erode morale and inflict uncertainty and fear throughout the military community. The Provisional Irish Republican Army, who employed contract hackers to obtain home addresses of law enforcement and intelligence officers, has demonstrated this tactic. This information was used to develop plans to kill the officers if the British government did not meet terms for a cease-fire.[39]

A major threat to the military deals with the fact that a large percentage of the Global Information Grid is dependent upon commercial telecommunications links and the Internet, which are not controlled by DOD.[40] For instance, Sprint is one of the many carriers that provides the communications backbone to transport DOD data. Sprint must develop software systems to manage their network infrastructure; however, they do not have total control of who develops this software. In September 2003, Sprint announced that they were outsourcing software development, computer coding, and other related tasks to EDS and IBM.[41] A March 2004 report in *BusinessWeek online*; however, shows that these two companies are hiring offshore programmers to complete their work.[42] The

---

[38] Congress, House, Armed Services Subcommittee on Terrorism, Unconventional Threats and Capabilities, *Cyber-Terrorism*, Statement by Major General James D. Bryan, U.S. Army Commander, Joint Task Force-Computer Network Operations, U.S. Strategic Command and Vice Director, Defense Information Systems Agency, (Washington, D.C., 24 July 2003), 7-8; available from http://www.defenselink.mil/search97/s97is.vts?Action=FilterSearch&Filter=dl.hts&query=cyber-terrorism; Internet; accessed 6 April 2004.

[39] Congress, House, Armed Services Special Oversight Panel on Terrorism, *Cyberterrorism*, Testimony by Dorothy E. Denning, Georgetown University, (Washington, D.C., 23 May 2000), 3; available from http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html; Internet; accessed 9 April 2004.

[40] Congress, House, Armed Services Subcommittee on Terrorism, Unconventional Threats and Capabilities, *Cyber-Terrorism*, Statement by Major General James D. Bryan, U.S. Army Commander, Joint Task Force-Computer Network Operations, U.S. Strategic Command and Vice Director, Defense Information Systems Agency, (Washington, D.C., 24 July 2003), 5; available from http://www.defenselink.mil/search97/s97is.vts?Action=FilterSearch&Filter=dl.hts&query=cyber-terrorism; Internet; accessed 6 April 2004.

[41] "Sprint Inks Outsouring Pacts with EDS, IBM," *Dallas Business Journal*, (16 September 2003); available from http://www.bizjournals.com/dallas/stories/2003/09/15/daily21.html; Internet; accessed 9 April 2004.

[42] "Software - Programming Jobs are Heading Overseas by the Thousands. Is there a Way for the U.S. to Stay on Top?" *BusinessWeek online*, 1 March 2004; available from http://businessweek.com/magazine/content/04_09/b3872001_mz001.htm; Internet; accessed 9 April 2004.

question that arises is who is developing the software for them? Reviews of the companies that provide offshore development indicates over 40 countries provide this service, to include numerous Eastern European countries, China, Pakistan, and Russia. India is by far, though, the country that provides the majority of this work. One concern is how tight is their security and how well do they conduct background investigations of personnel working on products that will eventually support DOD systems? Similar to the case in Japan where Aum Shinryko developed software for the police department, it is not unreasonable to assume that malicious software or backdoors could be planted into Sprint's systems that could ultimately impact the military.

There have been many examples of attacks on the Defense Department's IT systems. Between April 1990 and May 1991, hackers from the Netherlands penetrated computer systems at 34 Defense sites. The hackers were able to access directories, read e-mail, and modify systems to obtain full privileges allowing them future access to the systems. Investigation into the unauthorized access indicated the hackers were searching the messages for key words, such as nuclear, weapons, missile, Desert Shield, and Desert Storm. The hackers also copied and stored military data on various systems at several major U.S. universities.[43]

More recently, an unemployed computer system administrator living in London, England hacked into nearly 100 different systems belonging to the U.S. Army, U.S. Navy, U.S. Air Force, the Pentagon, and NASA over a year period ending in March 2002. After gaining access to the various systems, he deleted user accounts and critical system files, copied files containing usernames and encrypted passwords, and installed tools used for obtaining unauthorized access to computers.[44] In one of these attacks, a network of 300 computers at a Naval weapons station was shut down for a week.[45]

The Department of Defense (DOD) has recognized the cyber threat to its systems for years. However, in 1998 DOD formally established Joint Task Force-Computer Network Defense to combat these threats and develop security procedures. This was a result of two key factors. First, National Security Agency personnel were able to inflict, through simulation, a significant amount of damage to Defense networks during Exercise Eligible Receiver '97. This exercise involved DOD, Joint Staff, all the Armed Forces, the Defense and Central Intelligence Agencies, various combatant commands, and the Departments of State, Justice, and Transportation.[46]

---

[43] General Accounting Office, *Information Security: Computer Attacks at Department of Defense Pose Increasing Risks*, Report AIMD-96-84, (Washington, D.C., 22 May 1996), 16-17; available from http://www.fas.org/irp/gao/aim96084.htm; Internet; accessed 12 April 2004.

[44] Department of Justice, U.S. District Court for the Eastern District of Virginia, Alexandria Division, Indictment, *United States of America v. Gary McKinnon*, (Alexandria, VA, November 2002), 2-3; available from http://news.findlaw.com/hdocs/docs/cyberlaw/usmck1102vaind.pdf; Internet; accessed 16 April 2004.

[45] "U.S. Officials Charge Briton for Hacking Pentagon," *Asian School of Cyber Laws*, November 2002, 1; available from http://www.asianlaws.org/cyberlaw/archives/11_02_penta.htm; Internet; accessed 16 April 2004.

[46] "Eligible Receiver," *Global Security.org*, 9 June 2002; available from http://www.globalsecurity.org/military/ops/eligible-receiver.htm; Internet; accessed 24 June 2004.

The second factor occurred in February 1998, when a number of computer attacks were detected which targeted U.S. military computers worldwide. These attacks appeared to be originating from the Middle East and were initiated as the U.S. was preparing for possible military action against Iraq. The concern was that the attacks were being conducted by Iraq. An interagency investigation was quickly conducted and found that the attackers were two California teenagers and an 18-year old Israeli mentor. Although no classified systems were compromised, the security breaches could have been used to disrupt DOD information flow during possible combat operations in the Middle East. [47]

In October 2002, Joint Task Force-Computer Network Defense was re-designated Joint Task Force-Computer Network Operations (JTF-CNO) and was assigned to the U.S. Strategic Command. It includes components from all four Armed Services and the Defense Information System Agency's Computer Emergency Response Team. The task force has two missions: Computer Network Defense (CND) and Computer Network Attack (CNA). The CND mission is to defend DOD computer networks and systems from any unauthorized event, such as probes, scans, virus incidents, or intrusions. The CNA mission is to coordinate, support, and conduct computer network attack operations, at the direction of the President, in support of regional and national objectives.[48]

[47] Colin Robinson, *Military and Cyber-Defense: Reactions to the Threat* (Washington: Center for Defense Information Terrorism Project, 2002), 1-2; available from http://www.cdi.org/terrorism/cyberdefense-pr.cfm; Internet; accessed 24 June 2004.

[48] "Joint Task Force-Computer Network Operations," (Offutt Air Force Base: U.S. Strategic Command Fact Sheet, 2003); available from http://www.stratcomaf.mil/factsheetshtml/jtf-cno.htm; Internet; accessed 25 June 2004.

Conclusion

Although many of the current weaknesses in IT systems can be fixed, ever-evolving IT capabilities will continue to challenge cyber security and information assurance. Additionally, as one system is fixed, other vulnerabilities are often found. Even if the actual technology used in a system has excellent security, the system is often configured or used in ways that open it up for attack. Additionally, insiders can use their access to support the cyber terrorists to bypass security.[49]

As an example of how fast the cyber threat changes, the Melissa virus that infected networks in 1999 took weeks to have an effect. However, the Code Red worm that infected the Internet in July 2001 took only hours to flood the airways, while the Slammer worm that appeared in January 2003 took only minutes to infect thousands of hosts throughout the world. To further demonstrate the complexity of attacks, it took Code Red 37 minutes to double in size, but only took Slammer 8.5 seconds to do the same. In fact it took the Slammer worm only 10 minutes to infect 90 percent of vulnerable hosts.[50]

Clearly, attacks in cyberspace will continue in the future. Cyber terrorists will try to capitalize on known weaknesses and continue dedicated research and mining to discover new vulnerabilities in our systems. As stated in an al Qaeda article in February 2002, "Despite the fact that the jihadi movements prefer at this time to resort to conventional military operations, jihad on the Internet from the American perspective is a serious option for the movements in the future for the following reasons:

- First: Remote attacks on Internet networks are possible in complete anonymity.
- Second: The needed equipment to conduct attacks on the Internet does not cost much.
- Third: The attacks do not require extraordinary skill.
- Fourth: The jihadi attacks on the Internet do not require large numbers [of people] to participate in them."[51]

[49] Ibid., 3.
[50] Congress, House, Armed Services Subcommittee on Terrorism, Unconventional Threats and Capabilities, *Cyber-Terrorism*, Statement by Major General James D. Bryan, U.S. Army Commander, Joint Task Force-Computer Network Operations, U.S. Strategic Command and Vice Director, Defense Information Systems Agency, (Washington, D.C., 24 July 2003), 9; available from http://www.defenselink.mil/search97/s97is.vts?Action=FilterSearch&Filter=dl.hts&query=cyber-terrorism; Internet; accessed 6 April 2004.
[51] Ben Venzke and Aimee Ibrahim, *The al-Qaeda Threat: An Analytical Guide to al-Qaeda's Tactics and Targets* (Alexandria: Tempest Publishing, LLC, 2003), 36, quoting Abu 'Ubeid al-Qurashi, "The Nightmares of America, 13 February 2002.

Page Intentionally Blank

Glossary

adware (see also spyware): **Any** software application in which advertising banners are displayed while the program is running. The authors of these applications include additional code that delivers the ads, which can be viewed through pop-up windows or through a bar that appears on a computer screen. The justification for adware is that it helps recover programming development cost and helps to hold down the cost for the user.

Note - Adware has been criticized because it usually includes code that tracks a user's personal information and passes it on to third parties, without the user's authorization or knowledge. This practice is called **spyware**.

anti-terrorism: (AT) (JP 1-02) — Defensive measures used to reduce the vulnerability of individuals and property to terrorist acts, to include limited response and containment by local military forces.

AOR: Area of responsibility

asset (terrorist): A resource — person, group, relationship, instrument, installation, or supply — at the disposition of a terrorist organization for use in an operational or support role. Often used with a qualifying term such as suicide asset or surveillance asset. Based upon JP 1-02 asset (intelligence).

cyber crisis action team: (C-CAT) – A group formed by the National Infrastructure Protection Center (NIPC) to assist government agencies in handling a cyber crisis.

cyber-terrorism: (FBI) — A criminal act perpetrated by the use of computers and telecommunications capabilities, resulting in violence, destruction and/or disruption of services to create fear by causing confusion and uncertainty within a given population, with the goal of influencing a government or population to conform to a particular political, social, or ideological agenda.

data mining: A method of using computers to sift through personal data, backgrounds to identify certain actions or requested items. A technique used by the Total Information Awareness (TIA) program.

Defense Advanced Research Projects Agency: (DARPA) – The Defense Advanced Research Projects Agency (DARPA) is the central research and development organization for the Department of Defense (DoD). It manages and directs selected basic and applied research and development projects for DoD, and pursues research and technology where risk and payoff are both very high and where success may provide dramatic advances for traditional military roles and missions.

Defense Information Systems Agency: (DISA) – The Defense Information Systems Agency is a combat support agency responsible for planning, engineering, acquiring, fielding, and supporting global net-centric solutions to serve the needs of the President, Vice President, the Secretary of Defense, and other DoD Components, under all conditions of peace and war.

denial of service attack: (DOS) An attack designed to disrupt network service, typically by overwhelming the system with millions of requests every second causing the network to slow down or crash.

distributed denial of service attack: (DDOS) Similar to a denial of service attack, but involves the use of numerous computers to simultaneously flood the target.

e-mail spoofing: A method of sending e-mail to a user that appears to have originated from one source when it actually was sent from another source.

electro-magnetic-pulse: (EMP) – high-intensity electromagnetic radiation most likely generated by a nuclear blast that may couple with electrical or electronic systems to produce damaging current and voltage surges (DOD).

firewall: A barrier to keep destructive forces away from your property.

force protection: Security program designed to protect Service members, civilian employees, family members, facilities, and equipment, in all locations and situations, accomplished through planned and integrated application of combating terrorism, physical security, operations security, personal protective services, and supported by intelligence, counterintelligence, and other security programs.

force protection condition (FPCON): There is a graduated series of Force Protection Conditions ranging from Force Protection Conditions Normal to Force Protection Conditions Delta. There is a process by which commanders at all levels can raise or lower the Force Protection Conditions based on local conditions, specific threat information and/or guidance from higher headquarters. The four Force Protection Conditions above normal are:

Force Protection Condition ALPHA--This condition applies when there is a general threat of possible terrorist activity against personnel and facilities, the nature and extent of which are unpredictable, and circumstances do not justify full implementation of Force Protection Conditions BRAVO measures. The measures in this Force Protection Conditions must be capable of being maintained indefinitely.

Force Protection Condition BRAVO--This condition applies when an increased and more predictable threat of terrorist activity exists. The measures in this Force Protection Conditions must be capable of being maintained for weeks without causing undue hardship, affecting operational capability, and aggravating relations with local authorities.

Force Protection Condition CHARLIE--This condition applies when an incident occurs or intelligence is received indicating some form of terrorist action against personnel and facilities is imminent. Implementation of measures in this Force Protection Conditions for more than a short period probably will create hardship and affect the peacetime activities of the unit and its personnel.

Force Protection Condition DELTA--This condition applies in the immediate area where a terrorist attack has occurred or when intelligence has been received that terrorist action against a specific location or person is likely. Normally, this Force Protection Conditions is declared as a localized condition.

Global Information Grid: (GIG) DOD's globally interconnected set of information capabilities, processes, and personnel for collecting, processing, storing, disseminating, and managing information on demand to warfighters, policymakers, and support personnel.

hacker: Advanced computer users who spend a lot of time on or with computers and work hard to find vulnerabilities in IT systems.

hactivist: These are combinations of hackers and activists. They usually have a political motive for their activities, and identify that motivation by their actions, such as defacing opponents' websites with counter-information or disinformation.

Homeland Security Advisory System (HSAS): The advisory system provides measures to remain vigilant, prepared, and ready to deter terrorist attacks. The following Threat Conditions each represent an increasing risk of terrorist attacks. Beneath each Threat Condition are suggested protective measures, recognizing that the heads of Federal departments and agencies are responsible for developing and implementing appropriate agency-specific protective measures:

- **Low Condition (Green)**. This condition is declared when there is a low risk of terrorist attacks. Federal departments and agencies should consider the following general measures in addition to the agency-specific Protective Measures they develop and implement: refining and exercising as appropriate preplanned Protective Measures; ensuring personnel receive proper training on the Homeland Security Advisory System and specific preplanned department or agency Protective Measures; and institutionalizing a process to assure that all facilities and regulated sectors are regularly assessed for vulnerabilities to terrorist attacks, and all reasonable measures are taken to mitigate these vulnerabilities.

- **Guarded Condition (Blue)**. This condition is declared when there is a general risk of terrorist attacks. In addition to the Protective Measures taken in the previous Threat Condition, Federal departments and agencies should consider the following general measures in addition to the agency-specific Protective Measures that they will develop and implement: checking communications with designated emergency response or command locations; reviewing and updating emergency response procedures; and providing the public with any information that would strengthen its ability to act appropriately.

- **Elevated Condition (Yellow)**. An Elevated Condition is declared when there is a significant risk of terrorist attacks. In addition to the Protective Measures taken in the previous Threat Conditions, Federal departments and agencies should consider the following general measures in addition to the Protective Measures that they will develop and implement: increasing surveillance of critical locations; coordinating emergency plans as appropriate with nearby jurisdictions; assessing whether the precise characteristics of the threat require the further refinement of preplanned Protective Measures; and implementing, as appropriate, contingency and emergency response plans.

- **High Condition (Orange)**. A High Condition is declared when there is a high risk of terrorist attacks. In addition to the Protective Measures taken in the previous Threat Conditions, Federal departments and agencies should consider the following general measures in addition to the agency-specific Protective Measures that they will develop and implement: coordinating necessary security efforts with Federal, State, and local law enforcement agencies or any National Guard or other appropriate armed forces organizations; taking additional precautions at public events and possibly considering alternative venues or even cancellation; preparing to execute contingency procedures, such as moving to an alternate site or dispersing their workforce; and restricting threatened facility access to essential personnel only.

- **Severe Condition (Red)**. A Severe Condition reflects a severe risk of terrorist attacks. Under most circumstances, the Protective Measures for a Severe Condition are not intended to be sustained for substantial periods of time. In addition to the Protective Measures in the previous Threat Conditions, Federal departments and agencies also should consider the following general measures in addition to the agency-specific Protective Measures that they will develop and implement: increasing or redirecting personnel to address critical emergency needs; signing emergency response personnel and pre-positioning and mobilizing specially trained teams or resources; monitoring, redirecting, or constraining transportation systems; and closing public and government facilities.

HUMINT: Human intelligence

Incident Command System (ICS): A standardized on-scene emergency management concept specifically designed to allow its user(s) to adopt an integrated organizational structure equal to the complexity and demands of single or multiple incidents without being hindered by jurisdictional boundaries. The national standard for ICS is provided by NIMS.

keylogger: A software program or hardware device that is used to monitor and log each of the keys a user types into a computer keyboard.

logic bomb: A program routine that destroys data by reformatting the hard disk or randomly inserting garbage into data files.

malware: (short for **mal**icious soft**ware**) software designed specifically to damage or disrupt a system, such as a virus or a Trojan Horse.

millenarian: Apocalyptic; forecasting the ultimate destiny of the world; foreboding imminent disaster or final doom; wildly unrestrained; ultimately decisive. (Merriam –Webster's)

National Incident Management System: (NIMS). See *National Incident Management System* published by the Department of Homeland Security, 1 March 2004. The NIMS represents a core set of doctrine, concepts,

principles, technology and organizational processes to enable effective, efficient, and collaborative incident management. Nationwide context is an all-hazards, all jurisdictional levels, and multi-disciplines approach to incident management.

National Information Protection Center: (NIPC) – Serves as a national critical infrastructure threat assessment, warning, vulnerability, and law enforcement investigation and response entity. The NIPC provides timely warnings of international threats, comprehensive analysis and law enforcement investigation and response.

Non-Secure Internet Protocol Router Network: (NIPRNET) – The network used Department of Defense.

operations security: (OPSEC) A process of identifying critical information and subsequently analyzing friendly actions attendant to military operations and other activities to: a. Identify those actions that can be observed by adversary intelligence systems. b. Determine indicators hostile intelligence systems might obtain that could be interpreted or pieced together to derive critical information in time to be useful to adversaries. c. Select and execute measures that eliminate or reduce to an acceptable level the vulnerabilities of friendly actions to adversary exploitation. Also called OPSEC. (Joint Pub 1-02)

phreaks: A term used to describe telephone hackers

physical security: That part of security concerned with physical measures designed to safeguard personnel; to prevent unauthorized access to equipment, installations, material and documents; and to safeguard them against espionage, sabotage, damage, and theft. (Joint Pub1-02)

Secret Internet Protocol Routing Network: (SIPRNET) – The secure network used by the Department of Defense and intelligence communities to share data.

Security Administrator's Tools for Analyzing Networks: (SATAN) – A free scanning tool to help systems administrators, it recognizes common network related security problems, and reports them.

Sniffers: A program designed to assist hackers/and or administrators in obtaining information from other computers or monitoring a network. The program looks for certain information and can either store it for later retrieval or pass it to the user.

Spam: The unsolicited advertisements for products and services over the internet, which experts estimate to comprise roughly 50 percent of the e-mail.

Spyware (see also adware): Any technology that gathers information about a person or organization without their knowledge. Spyware can get into a computer as a software virus or as the result of installing a new program.
Software designed for advertising purposes, known as adware, can usually be thought of as spyware as well because it invariably includes components for tracking and reporting user information.

steganography: The process of hiding information by embedding messages within other, seemingly harmless messages. The process works by replacing bits of useless or unused data in regular computer files (such as graphics, sound, text) with bits of different, invisible information. This hidden information can be plain text, cipher text, or even images.

terror tactics: Given that the Army defines tactics as **"**the art and science of employing available means to win battles and engagements," then terror tactics should be considered "the art and science of employing violence, terror and intimidation to inculcate fear in the pursuit of political, religious, or ideological goals."

terrorism: (JP 1-02) — The calculated use of violence or threat of violence to inculcate fear; intended to coerce or to intimidate governments or societies in the pursuit of goals that are generally political, religious, or ideological.

terrorist: (JP 1-02) — An individual who uses violence, terror, and intimidation to achieve a result.

terrorist goals: The term *goals* will refer to the strategic end or end state that the terrorist objectives are intended to obtain. Terrorist organization goals equate to the strategic level of war as described in FM 101-5-1.

terrorist group: Any group practicing, or that has significant subgroups that practice, international terrorism (U.S. Dept of State)

terrorist objectives: The standard definition of *objective* is – "The clearly defined, decisive, and attainable aims which every military operation should be directed towards" (JP 1-02). For the purposes of this work, terrorist objectives will refer to the intended outcome or result of one or a series of terrorist operations or actions. It is analogous to the tactical or operational levels of war as described in FM 101-5-1.

transnational: Extending or going beyond national boundaries (Webster's). In this context, not limited to or centered within a single nation.

trojan horse: A program or utility that falsely appears to be a useful program or utility such as a screen saver. However, once installed performs a function in the background such as allowing other users to have access to your computer or sending information from your computer to other computers.

virus: A software program, script, or macro that has been designed to infect, destroy, modify, or cause other problems with a computer or software program.

unified command: As a term in the Federal application of the Incident Command System (ICS), defines agencies working together through their designated Incident Commanders at a single Incident Command Post (ICP) to establish a common set of objectives and strategies, and a single Incident Action Plan. This is NOT "unified command" as defined by the Department of Defense.

WEG: Worldwide Equipment Guide. A document produced by the TRADOC ADCSINT – Threats that provides the basic characteristics of selected equipment and weapons systems readily available for use by the OPFOR.

worm: A destructive software program containing code capable of gaining access to computers or networks and once within the computer or network causing that computer or network harm by deleting, modifying, distributing, or otherwise manipulating the data.

zombie: A computer or server that has been basically hijacked using some form of malicious software to help a hacker perform a Distributed Denial Of Service attack (DDOS).

Page Intentionally Blank

Selected Bibliography

Anderson, Sean K., and Stephen Sloan. *Historical Dictionary of Terrorism.* Lanham, MD: Scarecrow Press, Inc, 2002.

AR 190-52. *Countering Terrorism and Other Major Disruptions on Military Installations*. 1978.

Arquilla, John and David Ronfeldt, ed. *Networks and Netwars*. Santa Monica: RAND, 2001.

Axtman, Kris. "The Terror Threat At Home, Often Overlooked." *Christian Science Monitor*, 29 December 2003. Available at http://ebird.afis.osd.mil/ebfiles/s20031229244982.html; Internet; Accessed 29 December 2003.

The Basics of Terrorism: Parts 1-6. The Terrorism Research Center, 97. Available from http://www.terrorism.com/terrorism/bpart1.html through /bpart6.html; Internet; Accessed 29 Aug 02.

Blythe, Will. "A Weatherman in Autumn." *Newsweek: Arts & Opinion*, 12 June 2003. Available from http://msnbc.msn.com/id/3069267/; Internet; Accessed 12 February 2004.

Bowman, Steve. *Homeland Security: The Department of Defense's Role.* Congressional Research Service Report for Congress, Order Code RL 31615, 7, 14 May 2003.

Central Intelligence Agency. Director of Central Intelligence. *Cyber Threat Trends and U.S. Network Security.*` Statement for the Record for the Joint Economic Committee by Lawrence K. Gershwin, National Intelligence Officer for Science and Technology. (Washington, D.C., 21 June 2001), 1. Available from http://www.cia.gov/cia/public_affairs/speeches/2001/gershwin_speech_06222001.html; Internet; Accessed 14 April 2004.

"Chinese Satellite TV Hijacked by Falun Gong Cult." *People's Daily Online*, 9 July 2002. Available from http://english.peopledaily.com.cn/200207/08/eng20020708_99347.shtml; Internet; Accessed 27 Nov 2002.

Coleman, Kevin. "Cyber Terrorism," *Directions Magazine*, 10 October 2003. Available from http://www.directionsmag.com/article.php?article_id=432; Internet; Accessed 15 March 2004.

Corpus, Victor N. "The Invisible Army." Briefing presented at Fort Leavenworth, KS, 5 November 2002. TRADOC ADCSINT-Threats Files, Fort Leavenworth, KS.

Cyber-Terrorism. Statement by Major General James D. Bryan, U.S. Army Commander, Joint task Force-Computer Network Operations, U.S. Strategic Command and Vice Director, Defense Information Systems Agency. Washington, D.C., 24 July 2003, 5. Available from http://www.defenselink.mil/search97/s97is.vts?Action=FilterSearch&Filter=dl.hts&query=cyber-terrorism; Internet; Accessed 6 April 2004.

"Defense Information System Network." Defense Information Systems Agency, Network Services [Website on line, n.d.]. Available from http://www.disa.mil/ns/gig.html; Internet; Accessed 7 Apr 04.

Dobson, Christopher, and Ronald Payne. *The Terrorist: Their Weapons, Leaders, and Tactics.* New York: Facts on File, Inc, Revised Edition, 1982.

"Eligible Receiver." *Global Security.org*, 9 June 2002. Available from http://www.globalsecurity.org/military/ops/eligible-receiver.htm; Internet; Accessed 24 June 2004.

Falkenrath, Richard A. "Problems of Preparedness: US Readiness for a Domestic Terror Attack." *International Security* 25, no. 4 (Spring 2001): 147-186.

"False Calls on Casualties Upset Camp Pendleton Spouses." *Mustang Daily Online News*, 11 April 2003. Available from http://www.mustangdaily.calpoly.edu/archive/20030411/print.php?story=inat; Internet; Accessed 13 August 2004.

Fischer, Lynn F. *The Threat Of Domestic Terrorism.* The Terrorism Research Center, 2002. Available from http://www.terrorism.com/terrorism/DomesticThreat.shtml; Internet; Accessed 10 Sept 2002.

Fuller, Fred L. "New Order Threat Analysis: A Literature Survey." *Marine Corps Gazette*, 81 (April 1997): 46-48.

Gellman, Bartom. "Cyber-Attacks by Al Qaeda Feared," *Washingtonpost.com*, 27 June 2002. Available from http://www.wahsingtonpost.com/ac2/wp-dyn/A50765-2002Jun26; Internet; Accessed 12 Apr 04.

"Global Information Grid." Defense Information Systems Agency, Network Services Website on line, n.d. Available from http://www.disa.mil/ns/gig.html; Internet; Accessed 7 April 2004.

Gray, Colin S. "Thinking Asymmetrically in Times of Terror." *Parameters* (Spring, 2002): 5-14.

Harmon, Christopher C. *Terrorism Today*. London: Frank Cass Publishers, 2000;Reprint, Portland: Frank Cass Publishers, 2001.

Hendershot, Harold M. "CyberCrime 2003 – Terrorists' Activity in Cyberspace." [Briefing slides from the Cyber Division] Federal Bureau of Investigation, Washington, D.C. Available from http://www.4law.co.il/L373.pdf; Internet; Accessed 6 April 2004.

International Encyclopedia of Terrorism, 1997 ed., s.v. "The Media and International Terrorism."

"Joint Task Force-Computer Network Operations." Offutt Air Force Base: U.S. Strategic Command Fact Sheet, 2003. Available from http://www.stratcomaf.mil/factsheetshtml/jtf-cno.htm; Internet; Accessed 25 June 2004.

Kaihla, Paul. "Forging Terror." *Business 2.0* December 2002: 1-3. Available from http://www.business2.com/articles/mag/0,1640,45486%7C5,00.html; Internet; Accessed 22 Nov 2002.

Kaplan, Robert. *The Coming Anarchy: Shattering the Dreams of the Post Cold War*. New York: Random House, 2000.

Kelley, Jack. "Terror Groups Hide Behind Web Encryption." *USA Today*, 5 February 2001. Available from http://www.usatoday.com/tech/news/2001-02-05-binladen.htm; Internet; Accessed 6 April 2004.

Kushner, Harvey W. *Terrorism in America: A Structured Approach to Understanding the Terrorist Threat*. Springfield, IL. : Charles C. Thomas, Publisher, Ltd., 1998.

Lemos, Robert. "What are the Real Risks of Cyberterrorism?" *ZDNet*, 26 August 2002. Available from http://zdnet.com.com/2102-1105_2-955293.html; Internet; Accessed 6 April 2004.

Liang, Qiao and Wang Xiangsui. *Unrestricted Warfare.* Translated by Department of State, American Embassy Beijing Staff Translators. Washington, D.C., 1999.

McGuire, Frank G., ed. *Security Intelligence Sourcebook, Including Who's Who in Terrorism*. Silver Spring, MD. : Interests, Ltd., 1990.

"NE-NE Remote Login Initial Solution Evaluation Criteria." *SONET Interoperability Forum* Document Number SIF-RL-9605-043-R4, (12 June 1996): 4. Available from http://www.atis.org/pub/sif/approved/sif96008.pdf; Internet; Accessed 9 April 2004.

Newman, David, ed. *Boundaries, Territory and Postmodernity.* Portland: Frank Cass Books, 1999.

Oman, Paul, and Edmund Schweitzer, and Jeff Roberts, "Protecting the Grid from Cyber Attack Part I: Recognizing Our Vulnerabilities." *Utility Automation and Engineering T&D*, November 2001. Available from http://uaelp.pennnet.com; Internet; Accessed 24 June 2004.

Paz, Reuven. *Hamas Publishes Annual Report on Terrorist Activity for 1998.* Herzliya, Israel: International Policy Institute for Counterterrorism, May 3, 1999. Available from http://www.ict.org.il/spotlight/det.cfm?id=259; Internet; Accessed 6 December 2002.

Poulsen, Kevin. "Rumsfeld Orders .mil Web Lockdown." *The Register*, 17 January 2003. Available from http://www.theregister.co.uk/2003/01/17/rumsfeld_orders_mil_web_lockdown; Internet; Accessed 8 Apr 04.

Powell, William. *The Anarchist Cookbook.* Secaucus, NJ: Lyle Stuart, Inc., 1971.

Quinn, Andrew. "Teen Hackers Plead Guilty to Stunning Pentagon Attacks." *Reuters*, 31 July 1998, 1. Available from http://www.geocities.com/Area51/Shadowlands/6583/project395.html; Internet; Accessed 14 April 2004.

Raufer, Xavier. "New World Disorder, New Terrorisms: New Threats for the Western World." In *The Future of Terrorism*, edited by Max. Taylor and John Horgan. Portland: Frank Cass Publishers, 2000.

Robinson, Colin. *Military and Cyber-Defense: Reactions to the Threa.t* Washington: Center for Defense Information Terrorism Project, 2002. Available from http://www.cdi.org/terrorism/cyberdefense-pr.cfm; Internet; Accessed 24 June 2004.

"Software - Programming Jobs are Heading Overseas by the Thousands. Is there a Way for the U.S. to Stay on Top?" *BusinessWeek online*, 1 March 2004. Available from http://businessweek.com/magazine/content/04_09/b3872001_mz001.htm; Internet; Accessed 9 Apr 04.

"Sprint Inks Outsouring Pacts with EDS, IBM." *Dallas Business Journal*, (16 September 2003). Available from http://www.bizjournals.com/dallas/stories/2003/09/15/daily21.html; Internet; Accessed 9 Apr 04.

Taylor, Max, and John Horgan, ed. *The Future of Terrorism*. Portland: Frank Cass Publishers, 2000.

The White House, *The National Strategy for the Physical Protection of Critical Infrastructure and Key Assets.* Washington, D.C., February 2003. Preface by The President of the United States of America. Available from http://www.whitehouse.gov/pcipb/physical_strategy.pdf; Internet; Accessed 8 December 2003.

The White House. *The National Security Strategy of the United Sates of America*, 1, 17 September 2002. Available at http://www.whitehouse.gov/nsc/nss.html; Internet; Accessed 30 April 2004.

The White House. *The National Strategy to Secure Cyberspace.* Washington, D.C., February 2003. Preface by The President of the United States of America. Available from http://www.whitehouse.gov/pcipb/cyberspace_strategy.pdf; Internet; Accessed 8 December 2003.

U.S. Congress. House. Armed Services Special Oversight Panel on Terrorism, *Cyberterrorism*, Testimony by Dorothy E. Denning, Georgetown University. Washington, D.C., 23 May 2000. Available from http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html; Internet; Accessed 9 April 2004.

U.S. Congress. House. Armed Services Subcommittee on Terrorism, Unconventional Threats and Capabilities. *Cyber-Terrorism.* Statement by Major General James D. Bryan, U.S. Army Commander, Joint task Force-Computer Network Operations, U.S. Strategic Command and Vice Director, Defense Information Systems Agency. Washington, D.C., 24 July 2003. Available from

http://www.defenselink.mil/search97/s97is.vts? Action=FilterSearch&Filter=dl.hts&query=cyber-terrorism; Internet; Accessed 6 April 2004.

U.S. Congress. Senate. Judiciary Subcommittee on Terrorism, Technology, and Homeland Security, Cyber *Terrorism.* Testimony of Keith Lourdeau, Deputy Assistant Director, Cyber Division, FBI, Washington, D.C., 24 February 2004, 3. Available from http://www.fbi.gov/congress/congress04/lourdeau022404.htm; Internet; Accessed 15 April 2004.

U.S. Department of Defense. "A Global Terror Group Primer," by Jim Garamone. *Defense Link* (14 February 2002): 1-7. Available from http://www.defenselink.mil/news/Feb2002/n02142002_200202141.html; Internet; Accessed 29 August 2002.

U.S. Department of Defense. Defense Security Service, Technology Collection Trends in the U.S. Defense Industry 2002. Alexandria, VA, n.d. Available from http://www.wright.edu/rsp/Security/TechTrends.pdf; Internet; Accessed 19 April 2004.

U.S. Department of Justice. Federal Bureau of Investigation. Counterterrorism Threat Assessment and Warning Unit. Counterterrorism Division. *Terrorism in the United States 1999.* Report 0308. Washington, D.C., n.d.

U.S. Department of Justice. U.S. Attorney, Northern District of California. Press Release, *Louisiana Man Arrested for Releasing 911 Worm to WebTV Users*, (San Francisco, CA, 19 February 2004), 1. Available from http://www.usdoj.gov/criminal/cybercrime/jeansonneArrest.htm; Internet; Accessed 12 April 2004.

U.S. Department of Justice. U.S. Attorney, Southern District of California. Press Release, *President of San Diego Computer Security Company Indicted in Conspiracy to Gain Unauthorized Access into Government Computer*. San Diego, CA, 29 September 2003. Available from http://www.usdoj.gov/criminal/cybercrime/okeefeArrest.htm; Internet; Accessed 12 April 2004.

U.S. Department of State. Office of the Coordinator for Counterterrroism. *Patterns of Global Terrorism 2001*. Washington, D.C., May 2002.

U.S. Department of State. Office of the Coordinator for Counterterrorism. *Patterns of Global Terrorism 2002.* Washington, D.C., 2003.

U.S. Department of State. Office of the Coordinator for Counterterrorism. *Patterns of Global Terrorism 2004.* Washington, D.C., 2004, revised 22 June 2004.

U.S. Department of the Treasury. Office of the Comptroller of the Currency. *Infrastructure Threats from Cyber-Terrorists*, OCC Bulletin 99-9. Washington, D.C., 5 March 1999, 2. Available from http://www.occ.treas.gov/ftp/bulletin/99-9.txt; Internet; Accessed 6 April 2004.

U.S. General Accounting Office. *Information Security: Computer Attacks at Department of Defense Pose Increasing Risks*, Report AIMD-96-84. Washington, D.C., 22 May 1996. Available from http://www.fas.org/irp/gao/aim96084.htm; Internet; Accessed 12 April 2004.

"U.S. Officials Charge Briton for Hacking Pentagon." *Asian School of Cyber Laws*, November 2002. Available from http://www.asianlaws.org/cyberlaw/archives/11_02_penta.htm; Internet; Accessed 16 April 2004.

Zakis, Jeremy. *Annual Report of International Terrorist Activity, 2001*. Chicago: The Emergency Response and Research Institute, 2002. Available from http://www.emergency.com/2002/erri_ter2001.pdf; Internet; Accessed 7 November 2002.

Page Intentionally Blank

"The battle is now joined on many fronts.
We will not waiver, we will not tire,
we will not falter, and we will not fail.
Peace and freedom will prevail…
To all the men and women in our military,
every sailor, every soldier, every airman,
every coast guardsman, every marine,
I say this: Your mission is defined.
The objectives are clear. Your goal is just.
You have my full confidence, and you will have
every tool you need to carry out your duty."

George W. Bush
The President of the
United States of America

Supplemental Handbook No. 1.02 *Cyber Operations and Cyber Terrorism*
to DCSINT Handbook No.1 *A Military Guide to Terrorism in the Twenty-First Century,* Version 3.0
U.S. Army Training and Doctrine Command, Deputy Chief of Staff for Intelligence
Assistant Deputy Chief of Staff for Intelligence-Threats, Fort Leavenworth, Kansas

DISTRIBUTION RESTRICTION: Approved for public release;