DCSINT Handbook No. 1.02

Critical Infrastructure Threats and Terrorism

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

10 August 2006

This 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. This handbook supersedes the 2005 ***Cyber Operations and Cyber Terrorism handbook 1.02***. 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. An area that is most threatened and easily fits into the targeting criteria of the terrorist is our Critical Infrastructures. Critical Infrastructures are those systems or assets, whether physical or virtual, that if incapacitated or destroyed would have a debilitating affect on U.S. security, health, or overall safety. Although the forms and methods under which terrorism takes places are covered in the capstone terrorism handbook, this supplement provides detail and insight into the targets of the terrorist "behind the tip of the spear."

Purpose. This informational document supplements the basic terrorism handbook and supports operational and institutional training, and professional military education for U.S. military forces and Government Civilians within the Global War on Terrorism (GWOT). This document provides an introduction to the Threats to Critical Infrastructures; starting at the macro-level, the handbook addresses the Critical Infrastructure as defined by the Federal Government and those areas the government views as "critical" as well as Critical Infrastructures as defined by DoD. The second half of the handbook uses a "threats" viewpoint by looking at the three subsets within each infrastructure, the physical, human, and cyber assets of each area, and how the terrorist would damage or disrupt critical infrastructures through attacks on these areas of an installation or garrison.

Intended Audience. This document exists primarily for U.S. military forces, however, as larger portions of installations and garrisons are controlled by civilian employees and contractors this handbook is very applicable to groups including interagency; intergovernmental; civilian contractor; and, non-governmental and private volunteer organization. Compiled from open source materials, this supplement promotes a "Threats" perspective on Critical Infrastructure Protection. This supplement is neither a counter-terrorism directive nor an anti-terrorism manual, but it complements and 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) improve 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) will 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 2006 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
Headquarters, Department of the Army G-33, DAMO-ODF, Critical Infrastructure Risk Management

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

Critical Infrastructure Threats and Terrorism

Contents

Introduction

The term Critical Infrastructure came into use during the mid-90's. The United States had the strongest military and the largest economy; these two factors were both reinforcing and dependent on each other. The meteoric increase in cyber communications linked the infrastructures that were vital to the defense and economy of the United States. In 1996, President Clinton formed a commission to study the vulnerabilities of the infrastructures critical to the United States. The commission was formed with representatives from within the government as well as several from outside the government, as many infrastructures are owned and operated by the private sector. The critical infrastructures reviewed included telecommunications, electrical power systems, gas and oil storage and transportation, banking and finance, transportation, water supply, emergency services. The threats were broken into two categories, physical threat (damage to the tangible property) and threat to the electronic/computer-based systems (cyber attack). While the committee researched the vulnerabilities to the United States' infrastructures, the Infrastructure Protection Task Force (IPTF) was formed within the Department of Justice, chaired by the FBI. The initial charter of the IPTF was to:

1. Provide expert guidance to critical infrastructures to detect, prevent, halt or confine an attack and to restore service
2. Issue threat and warning notices
3. Provide training and education on methods of reducing vulnerabilities and responding to attacks
4. Coordinate with law enforcement during/after an attack to facilitate any investigation

The commission found that one of the biggest challenges facing the United States government in the coming decade was the effective protection of the country's critical infrastructures. Computers and the connectivity they brought to our lives, and businesses, while increasing productivity and creativity also increased our vulnerability to attacks by criminals, and terrorists. The commission's work was hailed as a success for starting the process of education and information sharing between the private sector and the government, a linkage critical to any improvement in protection. The commission looked at a wide range of threats; naturally occurring events such as earthquakes, fires and weather related incidents; physical attacks such as the World Trade Center bombing (the VBIED attack in February of 1993) and the bombing of the Oklahoma Federal Building. The commission also addressed the potential use of cyber axis's to attack U.S. national assets. A year later the commission's findings resulted in a White Paper, (The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 63).

The White Paper tasked organizations within the government to establish systems to protect their infrastructures, and train their personnel to protect their systems. The paper addressed the idea that our military strength would deter future enemies, whether nations,

groups or individuals, from launching a direct attack, but most likely would result in a non-traditional attack against our infrastructures.

The White Paper authorized the FBI to expand the current organization of the IPTF to the National Infrastructure Protection Center (NIPC). The Department of Defense (DoD), as a result of the taskings within PDD #63, developed the Department of Defense Critical Infrastructure Protection (CIP) Plan, dated 18 November 1998. This document described the way the DoD would organize to identify and protect DoD owned infrastructure assets, as well as coordinate with other elements of the national program to ensure protection. The document explained how the DoD would coordinate for CIP from national level through installation level. The document set milestones for progress within CIP for the next several years.

In January 2003, the DoD produced a CIP Security Classifications Guide which provided updated definitions concerning DoD CIP topics as well as setting security levels for topics related to CIP.

19 August 2005, The Department of Defense issued a Directive Number 3020.40, the subject being the Defense Critical Infrastructure Program (DCIP). This directive superseded earlier plans and programs written in the late 90's. Directive 3020.40 provided new definitions, policies, and updates on responsibilities concerning the identification, assessment, and security enhancements required for defense of critical infrastructures.

Most recently the Department of Defense issued the Defense Critical Infrastructure Program (DCIP) Interim Implementation Guidance, dated 13 July 2006. this document references DoD Directive 3020.40 and Homeland Security Presidential Directive 7 among others. This document provides additional definitions as well as DCIP Acronyms, Procedures and Assessment Standards.

On 17 April 2002 the Department of Defense announced the establishment of the U.S. Northern Command (USNORTHCOM). All existing homeland defense and civil support missions previously executed by other organizations would be consolidated under USNORTHCOM. USNORTHCOM, located at Peterson Air Force Base, Colorado Springs, Colorado, began the arduous task of planning, organizing and coordinating military support to all of the nation's homeland defense and civil support missions.

The Cyber Threat

To highlight the importance of Cyber technology to the U.S. military, in July 2003, DOD had more than 3 million individual computers on 12,000 local area networks (LANs). [1]

[1] 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

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.[2]

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.[3]

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 requirements.[4] 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)

---

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

[2] "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.

[3] Ibid.

[4] "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.

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.[5]

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

Objectives

The objectives of this handbook are to explain the history and background behind critical infrastructure protection, the areas designated as critical infrastructures, and provide installation and garrison military and civilian staffs a better understanding of identifying that which is critical and assessing the threats to those areas.

[5] 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.

Section I: Defining Critical Infrastructures, their Components, and their Threats

"To your parents and grandparents the question that begins "Where were you when…" would always end with "when Kennedy was shot" or "when the Japanese bombed Pearl Harbor." Today though, the question can only end "when the World Trade Center was hit."

The Economic Impact of September 11th, Internet Article, isu.indstate.edu/guell/ecn100/sept11., accessed 1 April 2006.

There are certain systems in place within the United States today that are taken for granted. Americans expect to pick up the phone and have a dial tone, turn a switch and have power, adjust their thermostat and make their home warmer or cooler, be able to move from one part of the U.S. to another, turn a faucet for drinking water and call 911 and receive aid. These infrastructures which support our everyday life are much more fragile than we think. A simple act of Mother Nature or the deliberate act of a terrorist can disrupt or destroy these systems and delay their return to normalcy.

Some infrastructures at the national level are so vital that their incapacity would have a devastating affect on the defense and economic security of our entire country. We have seen over the past decade how a single attack can adversely impact multiple areas of our lives. The term "Critical Infrastructure" came into vogue in the last decade to describe those systems that keep the nation secure.

Today the term "Critical Infrastructure" is defined as "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on the security, national economic security, national health or safety, or any combination of those matters."[6]

The assets mentioned above are further sub-divided into three categories:

1. Physical – Physical assets may include both tangible property (e.g., facilities', components, real estate, animals, and products) and the intangible (e.g., information). Physical protection becomes an even more difficult task when one considers that 85% of the nation's critical infrastructures are not federally owned. Proper protection of physical assets requires cooperation between all levels of the government and within the private sector.

2. Human – Human assets include both the employees to be protected and the personnel who may present an insider threat (e.g., due to privileged access to control systems,

[6] USA Patriot Act of 2001, incorporated into 2002 Act, from Interim National Infrastructure Protection Plan, Feb 2005

operations, and sensitive area and information). Those individuals who are identified as critical require protection as well as duplication of knowledge and authority.

3. Cyber – Cyber assets include the information hardware, software, data, and the networks that serve the functioning and operation of the asset. Damage to our electronic and computer networks would cause widespread disruption and damage, including casualties. Cyber networks link the United State's energy, financial and physical securities infrastructures.

Terrorists throughout the world are already exploiting information technologies and the Internet to plan attacks, raise funds, spread propaganda, collect information, communicate securely and recruit. As terrorists gain experience and technology, cyber attacks on all infrastructures becomes an increasing threat.

Since the late 1990's commissions and organizations were formed to review the vulnerabilities of U.S. critical infrastructures and determine the best courses of action to protect them. The current definition of Critical Infrastructure Protection (CIP) used by the Department of Defense is, "The actions taken to prevent, remediate, or mitigate the risks resulting from vulnerabilities of critical infrastructure assets. Depending on the risk, these actions could include changes in tactics, techniques, or procedures; adding redundancy; selection of another asset; isolation or hardening; guarding, etc.[7]"

A later section will discuss how to determine which infrastructures are critical to an organization. But once determined critical, how do we protect these infrastructures? After identifying those infrastructures that are critical to our organization, we need to look at them from the threats' point of view. The threat could be a man-made or natural attack or occurrence on any of the three above mentioned areas. The Army has developed methods to view "ourselves" from the threat's perspective.

The Contemporary Operational Environment (COE) is a dynamic and adaptive process for being more aware, better prepared, and ready to counter any adversity that could negatively impact an operation or task. These variables allow U.S. planners to understand impacts and changes within a "state", country or situation. These same variables can be used to view ourselves in a form of "Red Teaming". Red teaming is "a technique that involves viewing a potential target from the perspective of an attacker to identify its hidden vulnerabilities, and to anticipate possible modes of attack.[8]" Red teaming deepens understanding of options available to adaptive adversaries and provides groups an insight into their vulnerabilities. The result of a good red teaming session will provide a basis for plans to mitigate risks to your critical infrastructures.

---

[7] DOD Directive, 19 Aug 2005

[8] "Jane's Consultancy to use its Red Teaming Service to Assess US Terrorism Threat", Jane's Defense Weekly, 26 July 2002; available from http://www.janes.com/press/pc020726_1.shtml; Internet; accessed 1 April 2006.

To understand the complex interactions of the COE, a framework of "systems" assists in assessing and gaining situational awareness. Joint doctrine uses systems of Political, Military, Economic, Social, Infrastructure, and Information (PMESII) to shape and conduct missions. PMESII, with other variables such as physical environment and time, affect circumstances and influence operations throughout the domains of air, land, sea, and space. This broader perspective, combined with mission, enemy and belligerents, friendly forces and partners, cultural sensitivities and resolve, are critical to mission success. Defining physical environmental conditions include terrain or urban settings (super-surface, surface and subsurface features), weather, topography, and hydrology. The variable of time influences action such as planning, multi-echelon decision cycles, tempo of operations, and projected pacing of popular support for operations. Whether a real world threat or an opposing force created to simulate relevant conditions for training readiness, PMESII and other variables such as physical environment and time describe the OE.

PMESII and Other Variables

- Political
- Military
- Economic
- Social
- Information
- Infrastructure
- Physical Environment
- Time

The Threat's Viewpoint

Systems Warfare is a technique or method that identifies critical systems components and attacks them to degrade or destroy the use or importance of the overall system. The enemy targets "single points of failure" to cripple larger systems. Examples of systems that might be targeted by systems warfare are; logistics, command and control, Medical evacuation, commerce, and transportation. A tactical level example is an enemy attacking a fuel convoy so that combat vehicles such as tanks or personnel carriers cannot pursue him. The enemy cannot defeat the tanks or personnel carrier's superior armor or weapons capabilities, but he can target that which supports the tank and personnel carrier. The fuel convoy is the "weak link" in the combat system that the enemy can attack and achieve a greater success. The enemy came to this realization, and identified the weak link through analysis of our systems.

The next section will explore those critical infrastructures of the United States as they are identified by the Federal Government. Observe the federal areas and see how they compare to the infrastructures within your organization, installation, or garrison.

This Page Intentionally Blank

Section II: Critical Infrastructures at the National Level

"To build and implement a robust strategy to protect our critical infrastructures and key assets from further terrorist exploitation, we must understand the motivations of our enemies as well as their preferred tactics and targets."

The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets, February 2003

The Federal Government identified 12 areas as Critical Infrastructures requiring protection from threats. These infrastructures provide the goods and services that contribute to the national defense and strong economy. The reliability, survivability, and resiliency of these systems allow Americans to maintain a sense of confidence in their country and themselves. These infrastructures identify the quality of life within the United States, and set a standard for how other countries view America. When something happens to any of these areas we expect a rapid restoration along with an explanation as to why there was an interruption.

The National Strategy for Homeland Security has identified these twelve areas:

Agriculture & Food

The production and distribution of food within the United States is one of the most efficient systems in the world. The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets defines the Agriculture and Food sector as:

- Supply Chains for feed, animals, and animal products

- Corp production and supply chains of seed, fertilizer, and other necessary related materials
- Post-harvesting components of the food supply chain, from processing, production, and packaging through storage and distribution to retail sales, institutional food services, and restaurant of home consumption[9]

This industry accounts for close to 20% of the U.S. Gross Domestic Product. Areas of concern include: Supply chains for feed, animals and animal products; Crop production and supply chains of seed, fertilizer and other related materials; post-harvesting components of processing, production and packaging, storage, distribution. As for geographic concentration of potential targets; approximately 27% of U.S. hog inventories are located in Iowa, and another 16% are located in the eastern counties of North Carolina.[10]

Water

This sector is divided into two areas: fresh water supply and wastewater collection. The water sector criticality extends to both public health and the economy. The nation has over 170,000 public water systems which include reservoirs, dams, wells, aquifers, treatment facilities, pumping stations, aqueducts and transmission pipelines. Waste collection extends to 19,500 municipal sanitary sewer systems, and 800,000 miles of sewer lines.[11]

---

[9] The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets (February 2003): 36.
[10] U.S. Departure of Agriculture, National Agriculture Statistics Service (NASS), *Quarterly Hogs and Pigs*, Sept 30, 2005: 5.
[11] The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets (February 2003): 39.

Public Health

This area consists of state/local health departments, hospitals, health clinics, mental health facilities, laboratories, mortuaries, and pharmaceutical stockpiles. All of these would be critical after any form of attack or natural event. The personnel and facilities within this sector are trained and ready to react to emergency situations, but not as the target of a terrorist attack. Of geographical concern is the fact that 25% of all pharmaceuticals are manufactured in Puerto Rico, primarily in the San Juan metropolitan area.[12]

Emergency Services

This area includes fire, rescue, emergency medical service (EMS), and law enforcement organizations. These areas provide the U.S. the essential protection and services that we depend on day to day. Unfortunately past and present, foreign and domestic, experiences indicate that emergency services response infrastructure and personnel can be the target

[12] U.S. Census Bureau, *Pharmaceutical Preparation Manufacturing*: 2002, Economic Census, Manufacturing Industry Series. EC02-31I-325412(RV), Dec. 2004. Table 2; *Puerto Rico Manufacturing*. 2002 Economic Census of Island Areas. IA02-00I-PRM (RV). Oct. 2005: Table 1.

of deliberate direct or secondary attacks. The emergency services sector differs from other infrastructures in its focus and criticality is in its personnel and equipment, rather than a facility.

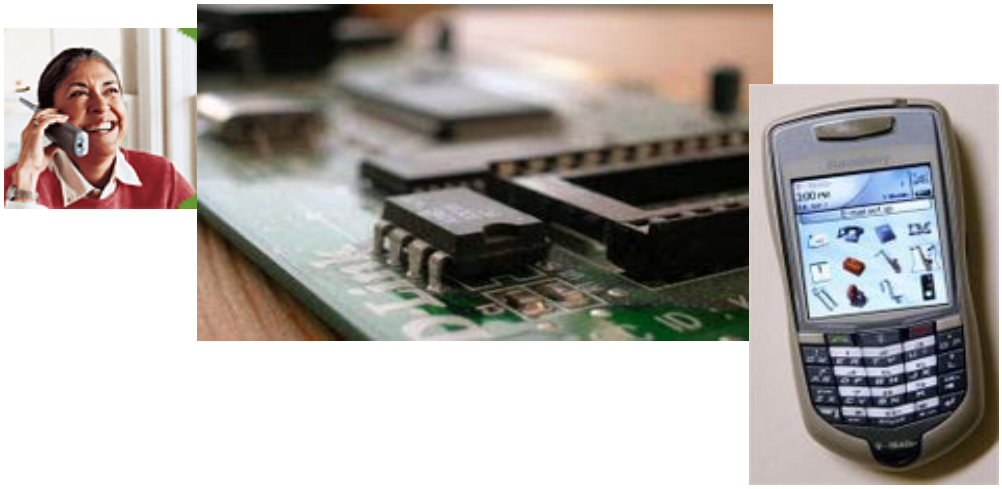
Government

The government itself can be viewed as a critical infrastructure, with its ability to command and control the response to any attack, terrorist or natural to any of our infrastructures. Government facilities are also key assets; they represent our nation's heritage, traditions and values. These facilities draw large amounts of tourism, and any disruption of them would impact public confidence and the economy.

Defense Industrial Base

The private sector is critical to the Department of Defense effectively conducting core defense missions, mobilizing and deploying of our military forces abroad. Private industry within the United States manufactures and provides the majority of the equipment, materials, services, and weaponry used by our armed forces. The Department of Defense has identified its own critical assets and systems over the last decade. The DoD is addressing its dependency on the Defense Industrial Base, and is taking the issues of private industry into its critical infrastructure protection efforts. As an example of the geographical focus of the DIB, over 31% of U.S. naval shipbuilding and repair capacity is in and around Norfolk, VA.[13]

Information ands Telecommunications



The telecommunications sector is vast and dispersed, containing both cyber and physical elements. The telecommunications sector provides voice and data service to the public and private users through use of the Public Switched Telecommunications Network (PSTN), the internet, and private enterprise networks. The telecommunications sector provides robust and reliable communications, meeting the needs of business and government despite its extremely dynamic nature. The communications sector, potentially more than any other infrastructure, reaches into every other critical sector.

[13] Colton Company. "Employment in the Major Shipbuilders." Oct. 26, 2005. {http://www.coltoncompany.com/shipbidg/statistics/jobsbyyard.htm] Capacity estimate based on 2003 shipyard relative employment data.

Energy

Energy is the infrastructure that supplies the driving force in most of American life today. Energy of some kind heats our homes, moves us for one point to another and drives our businesses and industry. The energy sector is critical to the well being of our economy, national defense and quality of life. The sector is divided into to areas, electricity and oil/natural gas. Electricity is required to operate and maintain homes, hospitals, schools, businesses and industrial plants; it is also necessary to refine oil. Disruption of electrical flow or a power grid would impact the economy and defense as well as response and recovery. Natural Gas consists of three major components: exploration and production, transmission, and distribution, with the U.S. producing 20% of the world's natural gas supply.[14] Oil's infrastructure consists of five components: production, crude oil transport, refining, product transport and distribution, and control and other external support systems.[15] The thousands of miles of pipelines offer an endless list of targets for terrorist attacks, and during transport there are opportunities for impacting more than one critical infrastructure. Over 43% of the total U.S. oil refining capacity is clustered along the Texas and Louisiana coasts.[16] This area is subject to natural attacks as well as those of terrorists.

[14] The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets (February 2003): 52.
[15] Ibid.
[16] Energy Information Administration (EIA). *Petroleum Supply Annual 2004, Volume 1*. DOE/EIA-0340(04)/1. June 2005. Table 36.

Transportation

The area includes aviation, rail, pipelines, highways, trucking and busing, and public mass transit. The scope of the transportation sector makes it critical to both our economy and national security. The ability to provide near unlimited mobility to the U.S. population reinforces one of our most cherished individual freedoms. Interdependencies exist between transportation and nearly every other sector of the economy. As redundant as our vast transportation network is there are geographic "choke-points", that require mentioning; nearly 32% of all U.S. waterborne container shipments pass through the ports of Long Beach and Los Angeles in southern California.[17] Dangerous clusters for rail movement exist in central U.S., with over 36% of U.S. freight railcars pass through Illinois, primarily around Chicago, and nearly 25% of freight railcars pass through Missouri, primarily around St. Louis.[18]

[17] Army Corps of Engineers, Waterborne Commerce Statistics Center (WCSC). "U.S. Waterborne Container Traffic by Port/Waterway in 2003." December 1, 2004. See internet: [http://www.iwr.usace.army.mil/ndc/wcsc/by_portname03.htm.].
[18] Association of American Railroads (AAR). "Rail Carloads Carried by State: 2003." Oct. 26, 2005. See [http://www.aar.org/PubCommon/Documents/AboutTheIndustry/RRState_Rankings.pdf].

Banking and Finance

This sector is made up of physical structures and assets as well as personnel and cyber assets. Retail and wholesale banking institutions are located in large office buildings with large groups of people. The financial sectors infrastructure includes computer networks, storage devices and telecommunications networks. This sector is also extremely vulnerable to public perception; an impression of weakness could easily result in a damaging cascading effect. Normal operations are necessary to maintain public confidence. Geographically, the banking sector is focused with nearly 46% of all U.S. securities traded on the floors of the New York and American Stock Exchanges in lower Manhattan[19] and approximately 22% of U.S. security industry employees are located in New York City.[20]

[19] New York Stock Exchange. *Annual Report 2004*; American Stock Exchange. *Annual Report 2004*.
[20] Securities Industry Association (SIA). "Securities Industry Employment." Sept. 2005. 5. See internet [http://www.sia.com/research/pdf/NYMonthly.pdf].

Chemical Industry ands Hazardous Materials

This sector impacts several other sectors; finance, agriculture, water, health care, etc. This sector is currently the U.S.'s top exporter, accounting for more than ten cents of every dollar. The Chemical industry produces fertilizer for agriculture, chlorine for water purification and polymers that create plastics from petroleum, more than $97 billion of the sectors products go to health care alone.[21] The sector is also a lucrative terrorist target due environmental impact from the physical destruction of many of its sites. One geographic cluster is in danger from nature and man; with over 38% of U.S. chlorine production is located in coastal Louisiana.[22]

Postal and Shipping

[21] The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets (February 2003): 65.
[22] U.S. Census Bureau, Alkalies and Chlorine Manufacturing: 2002, Economic Census, Manufacturing Industry Series, EC02-31I-325181 (RV), Dec. 2004, Table 2, Table 6b.

The postal system is interconnected with other infrastructure systems, especially transportation. The postal service controls thousands of points of entry as well as millions of facilities. The United States Postal Service (USPS) and private industry mailing and shipping revenues exceed $200 billion annually. Everyday, more than two-thirds of a billion pieces of mail enter the U.S. postal system and are delivered by over 300,000 carriers to more than 137 million addresses nationwide.[23] In the fall of 2001 anthrax attacks through the postal system caused mail stoppages across the U.S. as well as widespread anxiety resulting in significant economic impact.

Direct and Indirect Effects of Infrastructure Attacks

The direct effects of infrastructure damage would be the disruption or stoppage of the functions of critical infrastructures or key assets through direct attacks on a critical node, system or function
World Trade Center, which contained critical assets, was an example of a direct attack on the Banking and Finance infrastructure.

The indirect effects of an infrastructure attack would be the disruption and problems that result from a reaction to attacks on a critical infrastructure. The drawdown in air travel and other modes of mass transportation as a result of the 9/11 attacks, resulted in financial damage to each of these forms of travel. The loss of revenue in these industries resulted in loss of business and jobs.

The exploitation of an infrastructure as part of an attack would be using the capabilities of one infrastructure to damage or destroy another infrastructure. An example is the use of the aviation portion of the transportation infrastructure to attack the World Trade Center (business and finance infrastructure) and the Pentagon (Government). Osama Bin Laden has repeatedly spoken of using e-mail or the internet (Telecommunications) to launch a cyber attack on the investment sector and the stock market (Banking and Finance).

Department of Homeland Security

The Department of Homeland Security (DHS) was established on 25 November 2002, by the Homeland Security Act of 2002. DHS is designed to work in the civilian arena to protect the United States within, at, and outside its borders. Its goal is to prepare for, prevent, and respond to domestic emergencies, particularly terrorism. DHS defines Critical Infrastructure as "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."

[23] The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets (February 2003): 67.

The Defense Critical Infrastructure Program (DCIP)

The Department of Defense Directive 3020.40, dated 19 August 2005 established the Defense Critical Infrastructure Program (DCIP). The directive requires the Army to establish, resource and execute an organizational critical infrastructure program. The directive set responsibilities for each of the different sectors of the DCIP:

DEFENSE SECTOR	LEAD AGENT
Defense Industrial Base (DIB)	Director, Defense Contract Management Agency
Financial Services	Director, Defense Finance & Accounting Service
Global Information Grid (GIG)	Director, Defense Information Systems Agency
Health Affairs	Assistant Secretary of Defense of Health Affairs
Intelligence, Surveillance, and Reconnaissance (ISR)	Director, Defense Intelligence Agency
Logistics	Director, Defense Logistics Agency
Personnel	Director, DoD Human Resources Activity
Public Works	Chief, U.S. Army Corps of Engineers
Space	Commander, U.S. Strategic Command
Transportation	Commander, U.S. Transportation Command

This Page Intentionally Blank

Section III: Identifying Weaknesses in a Critical Infrastructure

> **"The War against America and its allies will not be confined to Iraq…As for similar operations taking place in America; it's only a matter of time. They are in the planning stages, and you will see them in the heart of your land as soon as the planning is complete"**
>
> Osama Bin Laden, al-Jazeera, 19 January 2006

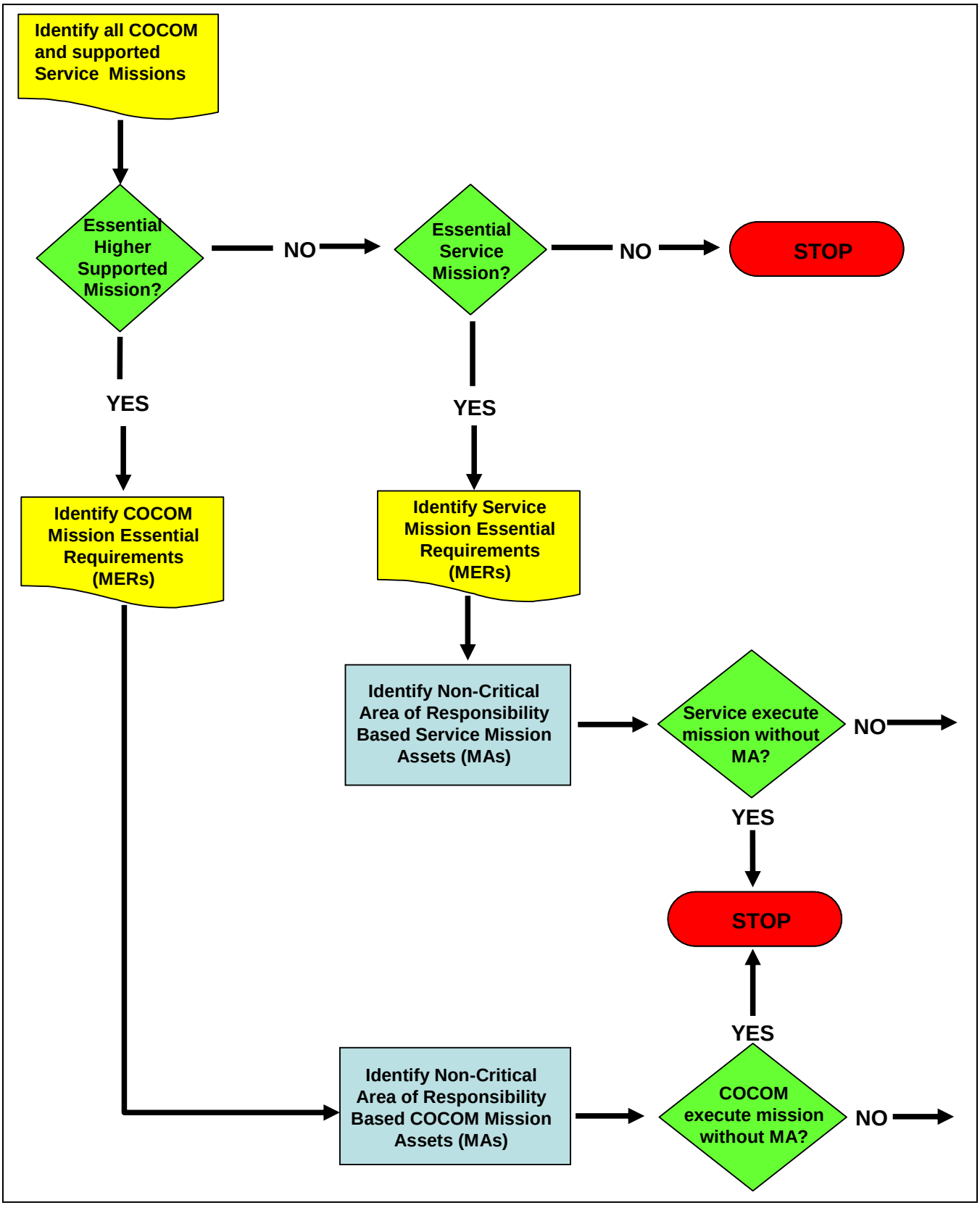
The definition of critical infrastructure has been given and examples of the critical infrastructures of the United States are provided, but what are our critical infrastructures within our own areas of responsibility, influence and interest? Some of these are provided to us by our higher organizations and their commands. Those higher infrastructures and parts of infrastructures located in our areas of responsibility are listed to us and we ensure their protection. These areas can be labeled Mission Essential Vulnerable Areas (MEVAs). Unfortunately a list of critical infrastructures and sites is not always provided; oftentimes staffs have to decide what are their critical infrastructures and the key assets supporting them. The staff or command will need to understand the infrastructures, how they function and which parts they need to protect.

On the following two pages is a flow chart designed to assist in the understanding of what is critical and the weaknesses within those systems. The flow chart was designed by NORTHCOM's J34, Assessments Branch, to assist units and organizations in looking at themselves, their missions and to identify weaknesses and single points of failure within the infrastructures.

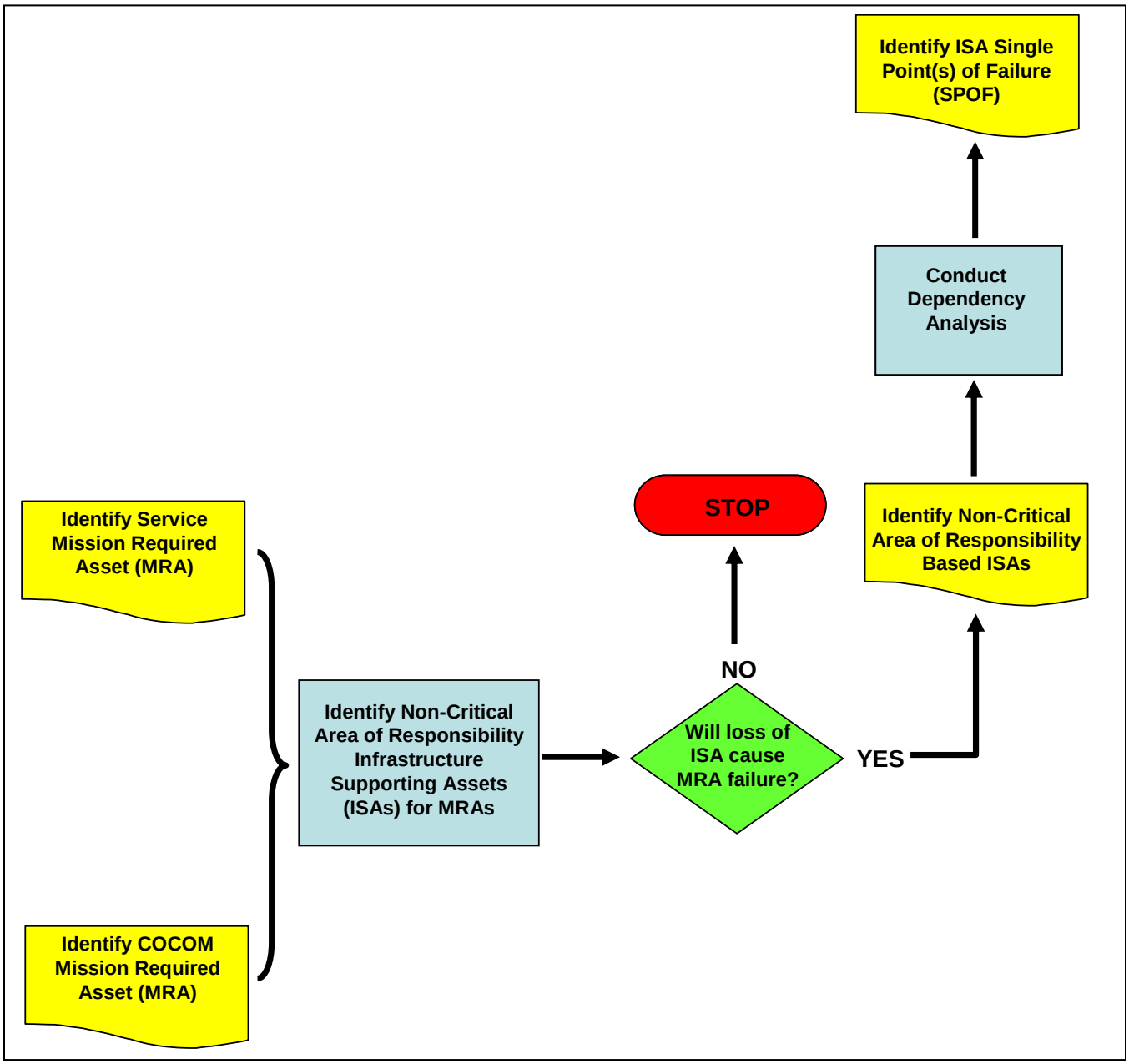
The process starts with identifying all of the missions the higher headquarters has directed the unit to perform as well as those functions the higher headquarters perform that are located within the unit's area of responsibility. The staff works their way through the process identifying missions and requirements at their own level, their higher's level as well as those they support, and decide if each are critical. When the staff reaches the end of the process they must conduct a Dependency Analysis in an effort to identify Single Points of Failure (SPOF). These SPOFs are the likely targets of attack as they will result in most damage for the least expenditure.

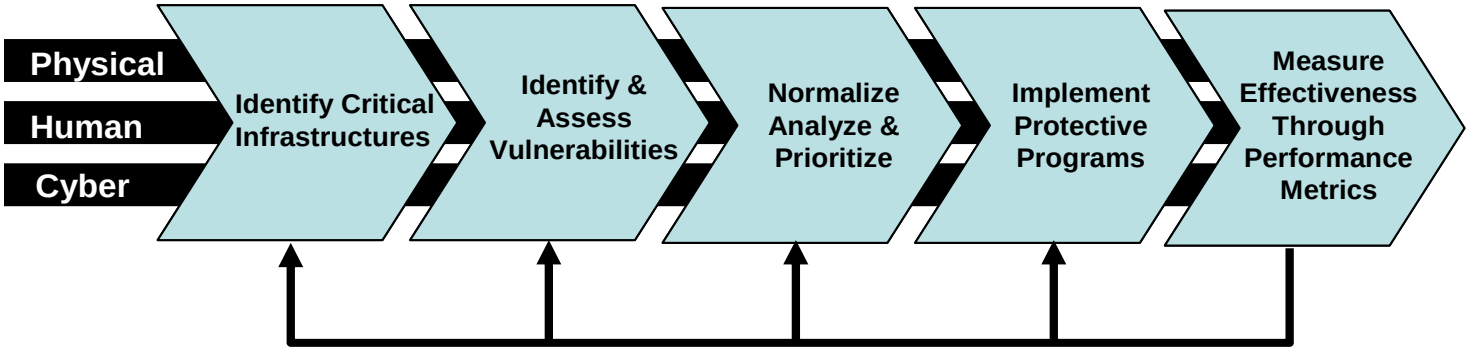
The process on the following pages is designed to help garrisons and staffs to determine what are their critical infrastructures and where are they vulnerable. These vulnerabilities are above and beyond those single points of failure that a higher office or headquarters may already have identified as critical to their operations but the physical asset is located on the lower headquarters facility or post. The list of critical infrastructures and their vulnerabilities, those of each level of command, must be nested together so that the individuals responsible for the security of the installation know the entire lists of assets that must be secured. Simply put, what is critical to one person or level of command

might not be critical to another, but those responsible for the security where the critical asset resides must know it is critical in order to protect and secure it. The nesting of these various layers can only be insured through coordination and synchronization between all levels of command. Once a list of assets and single points of failure exists it must be updated as plans and priorities change.



Critical infrastructures are composed of physical, personal, and cyber components, and as any of those three portions change so does the list of critical assets requiring security. If a plan or mission changes the need to review a CIP list is often obvious, but a change in personnel, a piece of equipment or even software can also require a review. Periodic reviews of all CIP plans is necessary to ensure that missions are updated, information from higher and lower is incorporated and changes within organizations are included.





Five-Step Process

The national CIP program is based on a risk management framework. It is continuously influenced by the ever changing threat environment, both physical and natural. The goal is to reduce the vulnerabilities to our nation's assets from attack and natural disaster. The same methodology used at the national level can be used by garrison, installation, and command staffs as part of the ongoing process of narrowing down the list or set of assets that are critical. The five steps are explained below:

1. Identifying critical assets – The first step will be to identify the critical assets located within your area of responsibility. The process should be an ongoing with constant review of unit missions, higher headquarters missions and requirements, as well as the overall operations within your location. The information collected should be used as the base for further discussion.

2. Identifying and assessing vulnerabilities – Vulnerability assessments should be conducted on those items identified in step 1. Potential areas of weakness need to be identified as well as protective measures that need to be undertaken to mitigate those vulnerabilities. Interdependencies within and between infrastructures need to be identified to minimize cascading effects. The vulnerability assessment needs to take into account effects which might cascade into other organizations.

3. Normalizing, analyzing, and prioritizing study results – The staff or group accumulating the vulnerability assessments needs to normalize the information from each subordinate section or staff, and then prioritize against all of the assets the higher organization is responsible for. This step will identify which areas offer the greatest risk and the best benefit from protective measures.

4. Implementing protective programs – The information gathered during the process will assist in developing and executing programs to protect or minimize damage to infrastructures. The staff or organization can find assistance in developing programs

from their higher headquarters or through various federal agencies such as the Department of Homeland Security (DHS).

5. Measuring performance – Metrics need to be established for each protective measure to ensure they are being performed consistently, are sustainable and are effective. Continuous review of the metrics will result in improvements to the framework and the protection plan

Defense Critical Infrastructure Program Procedures

Enclosure #3 of the DCIP Interim Implementation Guidance dated July 2006 outlines the DoD DCIP risk management procedures for all critical infrastructures. The purpose of the DCIP is to ensure the availability of assets critical to all DoD missions.

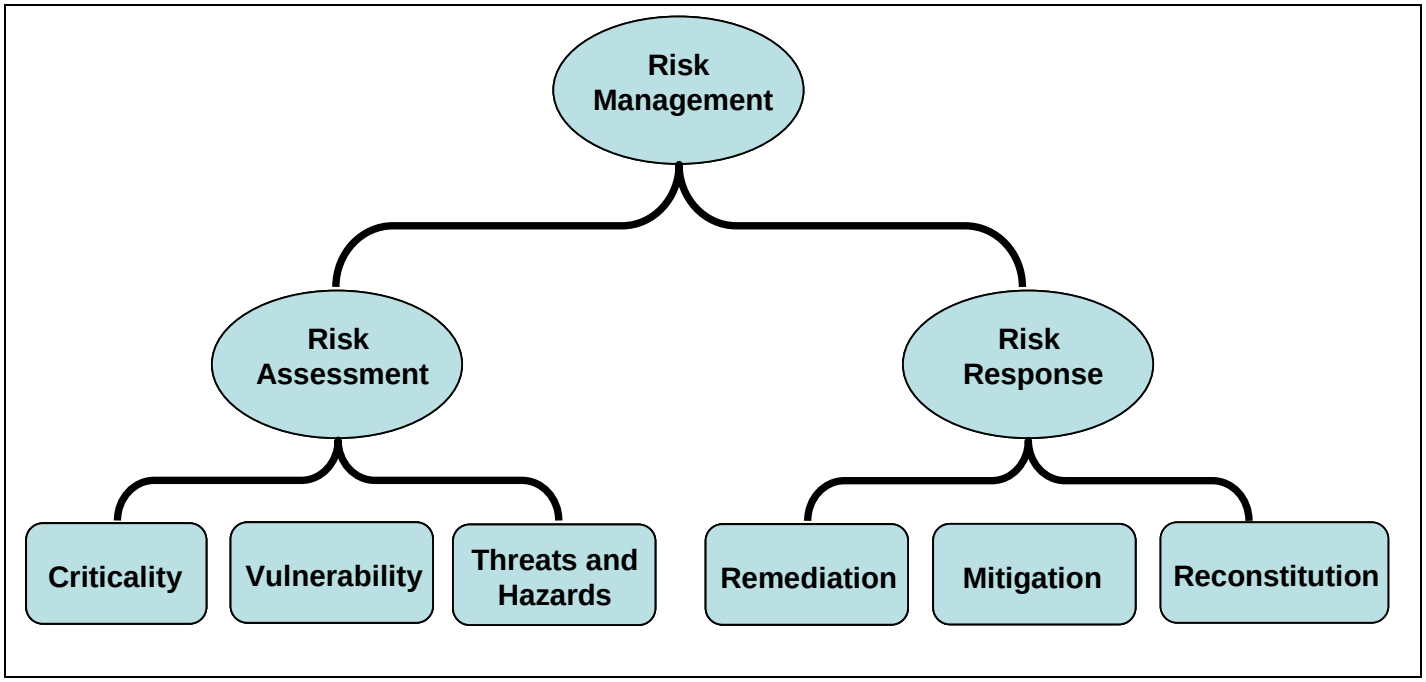


Diagram of the DCIP Risk Management program found in Enclosure 3 of the DoD Interim Implementation Guidance

Once risks are assessed in all tasks and missions then possible responses can be reviewed and emplaced to ensure all missions will be accomplished no matter what actions are taken against an infrastructure. The DCIP Interim Implementation Guidance stresses that Risk management is cyclical, as changes are constantly made to systems and personnel are replaced, risks to infrastructures must be re-assessed.

This Page Intentionally Blank

Section IV: Physical Attacks

"Al-Qaeda's Battle is an Economic Battle, Not a Military One"

Abu Musab al-Najdi's posting on the MinbarSuriya al-Islami Forum

Agriculture

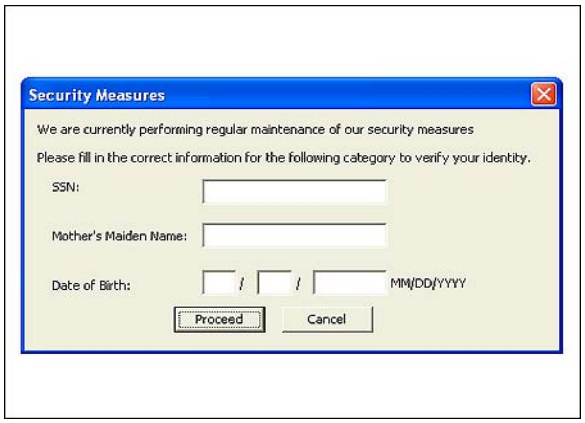
In 1984, a cult group poisoned salad bars at several Oregon restaurants with *Salmonella* bacteria as the first recorded event of bioterrorism in the United States. This resulted in 750 people becoming sick.[24] A review of the agriculture infrastructure results in vulnerable areas such as the high concentration of the livestock industry and the centralized nature of the food processing industry. The farm-to table chain contains various points into which an attack could be launched. The threat of attack would seriously damage consumer confidence and undermine export markets. Understanding the goal of the threat points to the area most likely attacked. If the intent was economic disruption the target would be livestock and crops, but if the intent was mass casualties the point of attack would be contamination of finished food products. Damage to livestock could be very swift, the USDA calculated that foot-and mouth disease could spread to 25 states in 5 days.[25] CDC is presently tracking and developing scenarios for the arrival of Avian Flu.

Banking

Prior to the destruction of the Twin Towers, physical attacks against the banking industry, such as the destruction of facilities, were rare. Unfortunately, evidence indicates that may change, in March 2005 three British al-Qa'ida operatives were indicted by a U.S. federal court on charges of conducting detailed reconnaissance of financial targets in lower Manhattan, Newark, New Jersey, and Washington, D.C. In addition to video taping the Citigroup Center and the New York Stock Exchange in New York City, the Prudential Financial building in Newark, and the headquarters of the International Monetary Fund and the World Bank in Washington D.C., the men amassed more than 500 photographs of the sites.[26] The Banking infrastructures primary weakness is along its cyber axis of attack. Through phishing and banking Trojan targeting specific financial institutions, attackers reduce confidence among consumers. Recently American

[24] Lawrence J. Dyckman, BIOTERRORISM: A Threat to Agriculture and Food Supply, GAO, 19 November 2003: 4.
[25] Ibid
[26] Dan Eggen, "Indictment Cites Plans to Target Financial Hubs: 3 Britons' Extradition to Be Sought," *Washington Post*, 13 April 2006.

Express posted an alert online, including a screenshot of a pop-up that appeared when users log in to its secure site.[27]



The attack not only attempts to obtain personal information that can be used for various operations, but also launches a virus into the user's computer. CitiBank, and Chase Manhattan Bank have both been victim during 2005 and 2006 to phishing schemes misrepresenting their services to their clients.

Energy

Recently the oil industry occupied the headlines, and the criticality of this infrastructure is not lost on terrorists. In mid-December 2004, Arab television aired an alleged audiotape message by Usama bin Laden in which he called upon his followers to wreak havoc on the U.S. and world economy by disrupting oil supplies from the Persian Gulf to the United States.[28] The U.S. uses over 20.7 million barrels a day of crude oil and products and imports 58.4% of that requirement.[29] On 19 January 2006 al-Qaeda leader Osama bin Laden announced in a video release that, "The war against America and its allies will not be confined to Iraq…..", and since June of 2003 there have been 298 recorded attacks against Iraqi oil facilities.[30] Terrorists conduct research as to the easiest point to damage the flow of oil or to the point where the most damage can be done. Scenarios involving the oil fields themselves, a jetliner crashing into the Ras Tanura facility in Saudi Arabia could remove 10 percent of the world's energy imports in one act.[31] Maritime attacks are also option for terrorists; on October 6, 2002 a French tanker carrying 397,000 barrels of crude oil from Iran to Malaysia was rammed by an explosive laden boat off of the port of Ash Shihr, 353 miles east of Aden. The double-hulled tanker

[27] Ryan Naraine, "Computer Virus 'Hijacks' American Express Web Site", Fox News.com, 01May 2006.
[28] Threats to Pipeline/Energy Sector, U.S. Department of Homeland Security: 1.
[29] Bernard E. Munk, "Energy Independence is not Energy Security", Foreign Policy Research Institute (FPRI), 24 March 2006.
[30] Institute for the Analysis of Global Security, http://www.iags.org/iraqpipelinewatch.htm, accessed 23 February 2006.
[31] John C. Daly, "Saudi Oil Facilities: Al-Qaeda's Next Target?", Terrorism Monitor, Volume 4, Issue 4, http://www.jamestown.org/terrorism/news/article.php?articleid=2369910&printthis=1: 23 February 2006.

was breached, and maritime insurers tripled the rates.[32] Energy most travel often long distances from the site where it is obtained to the point where it is converted into energy for use, a catastrophic event at any of the sites or along its route can adversely impact the energy infrastructure and cause ripples in other infrastructures. The security of the pipeline in Alaska increases in importance as efforts are made to make America more independent on energy use.

Economy

The U.S. economy is the end-state target of several terrorist groups as identified in the introduction quote. The means by which terrorists and other threats attempt to impact the economic infrastructure is through it's linkage to the other infrastructures. Attacks are launched at other infrastructures, such as energy or the Defense Industrial Base in an effort to achieve a "cascading" result that impacts the economy. Cyber attacks on Banking and Finance are another effort to indirectly impact the economy. The short term impacts of the 9/11 attacks on Lower Manhattan resulted in the loss of 30% of office space and a number of businesses simply ceased to exist. Close to 200,000 jobs were destroyed or relocated out of New York City. The destruction of physical assets was estimated in the national accounts to amount to $14 billion for private businesses, $1.5 billion for state and local government enterprises and $0.7 billion for federal enterprises. Rescue, cleanup and related costs are estimated to at least $11 billion for a total direct cost of $27.2 billion.[33] The medium and long term effects cannot be accurately estimated but demonstrate the idea of cascading effects. The five main areas affected over a longer period were Insurance, Airlines, Tourism and other Service Industries, Shipping and Security and military spending. At various times terrorist rhetoric has mentioned attacks against Wall Street proper, but the more realistic damage to the economy will come through the indirect approach of cascading effects.

Transportation

The attack on commuter trains in Madrid in March of 2004 and the London bombings in July of 2005, which together killed 243 people, clearly indicated the threat to the transportation infrastructure. Statistics provided by the Brookings Institute in Washington DC show that between 1991 and 2001 42% of worldwide terrorist attacks were directed against mass transit. Transportation is viewed by terrorists as a "soft target" and one that will impact the people of a country. Mass Service Transportation (MST) is the likely target of a terrorist attack.

- MST caters to large volumes of people, crammed into narrow confined spaces
- MST is designed to move large numbers of people quickly and efficiently, which is often counter to protective measures

[32] Ibid
[33] Economic Costs to the United States Stemming From the 9/11 Attacks, Center for Contemporary Conflict http://www.ccc.nps.navy.mil/rsepResources/si/aug02/homeland.asp, accessed 1 April 2006.

- MST assets are enclosed, serving to amplify explosions

- MST attacks can result in "cascading effects" because communications and power conduits are usually collocated in proximity to their routes

The Department of Homeland Security sent a "public sector notice" in May of 2006 based on two incidents of "suspicious videotaping" of European mass-transit systems.[34] The individual had several tapes besides the one in his camera, none of which showed any tourist sites. The tapes focused on the insides of subway cars, the inside and outside of several stations and exit routes from the stations. In June of 2003 the FBI arrested Iyman Faris, a 34 year old naturalized American citizen who had been in contact with Al Qaeda conducting research and reconnaissance in an effort to destroy the Brooklyn Bridge.[35] Mr. Faris had traveled to Afghanistan and Pakistan in 2000, meeting with Osama bin Laden, he returned to the U.S. and began gathering information concerning the Brooklyn Bridge and communicating via coded messages with Al Qaeda leaders. An attack on the bridge would have not only damaged the transportation infrastructure, but also a known American landmark. On 24 May 2006, a Pakistani immigrant was convicted on charges of plotting to blow up one of Manhattan's busiest subway stations in retaliation for the U.S. actions at the Abu Ghraib prison.[36]

Terrorist threats to the transportation infrastructure extend beyond land to the sea. Vice Admiral Jonathan Greenert, commander of the U.S. Seventh Fleet, said "one of my nightmares would be a maritime terrorism attack in the Strait of Malacca".[37] "There is a strain of al-Qaida in Southeast Asia, called Jemaah Islamiya. They are actively pursuing a maritime terrorism capability that includes diving and mining training."[38] As how this might impact on the economy, $220 billion in trade comes through the Seventh Fleet area of responsibility and 98% of the commerce is moved by sea. Just as ports can be viewed a SPOF within the maritime transport system, there are certain waterway chokepoints or heavily trafficked areas that can be viewed as a high payoff target to a terrorist or result in catastrophic damage from a natural disaster.

Local Threat

The above examples demonstrate the physical threats to infrastructures at the national level, but what are the physical threats to the infrastructures within your area of responsibility? There are guards and security checks at the gates of your installation, but what of the rail line that runs through the post? What is the cargo of the trains that pass through daily? These are the questions for staffs and command groups to consider as

[34] Spencer Hsu, "Videotaping Sparks Warning of Possible Terror Surveillance", Washington Post, 4 May 2006, 19.
[35] Eric Lichtblau, "U.S. Cites Al Qaeda in Plan to Destroy Brooklyn Bridge", The New York Times, 20 June 2003, 1.
[36] "Man Guilty In New York Bomb Plot", Washington Post, 25 May 2006, 8.
[37] David M. Brown, "Admiral Warns of Terror Threat, Pittsburgh Tribune-Review, 14 February 2006, 1.
[38] Ibid

they conduct threat assessments and review the dangers to the critical infrastructures of their organization.

This Page Intentionally Blank

Section V: Human Attacks

The safety and security of personnel is discussed in several Force Protection manuals and handbooks. The purpose of this section is not to provide ways to protect personnel, but to explain ways to ensure infrastructures are protected from loss of personnel. The human links of a critical infrastructure are all too often the overlooked potential points of failure.

The loss of an individual within a military unit rarely results in the unit failing to accomplish its mission. The military trains and prepares for losses within its personnel structure so that no matter what the cause, natural or man-made, the system continues to function with little or no interruption. Unfortunately, this often is not the case within many organizations that do not practice and train for the loss of individuals responsible for issuing instructions or experts in procedures or special equipment.

The loss of the Information Management Officer (IMO) during critical computer operations, the absence of a specialized technician if the water treatment plant's or electrical grid's systems fail or a multi-situational event resulting in a shortage of health or emergency personnel. Military units train everyday for the loss of a leader, member of the chain of command or special systems operator, but this contingency planning does not always extend to everyday operations or crisis planning. Even those organizations that plan for replacement of individuals rarely train for their loss which can result in delay or lack of coordination.

As an organization's critical infrastructures are identified the weaknesses and single points of failure are identified. If personnel are identified as one of the weaknesses or single points of failure, due to training, numbers of personnel, or responsibilities, a plan must be developed and trained against to ensure their absence will not result in the breakdown of the infrastructure.

Different methods of protection against damaging critical infrastructures from absence of "key personnel":

- Designate a sequence of personnel to cover the missing key personnel, and conduct training to ensure the echelon of replacements understands the specific function of the key person to the critical infrastructure.

- Reconfigure the infrastructure to negate the single point of failure or reduce the damage to the infrastructure if key personnel are absent.

- Ensure the key personnel have redundant communications available in order to provide guidance or instructions if needed.

- Ensure the key personnel have created readily available files covering situations where their importance to the infrastructure is understood to the point other could fulfill their purpose.

Too often key personnel's input into a critical infrastructure is forgotten until the crisis is at hand. Rehearsals that include the loss of certain individuals can easily identify problems early and result in reduction of risk to the critical infrastructure.

Section VI: 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.[39] Additionally, these encryption programs can scramble telephone conversations when the phones are plugged into a computer.[40]

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.

[39] 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.
[40] 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."[41] 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

[41] 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.[42]

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."[43] 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.

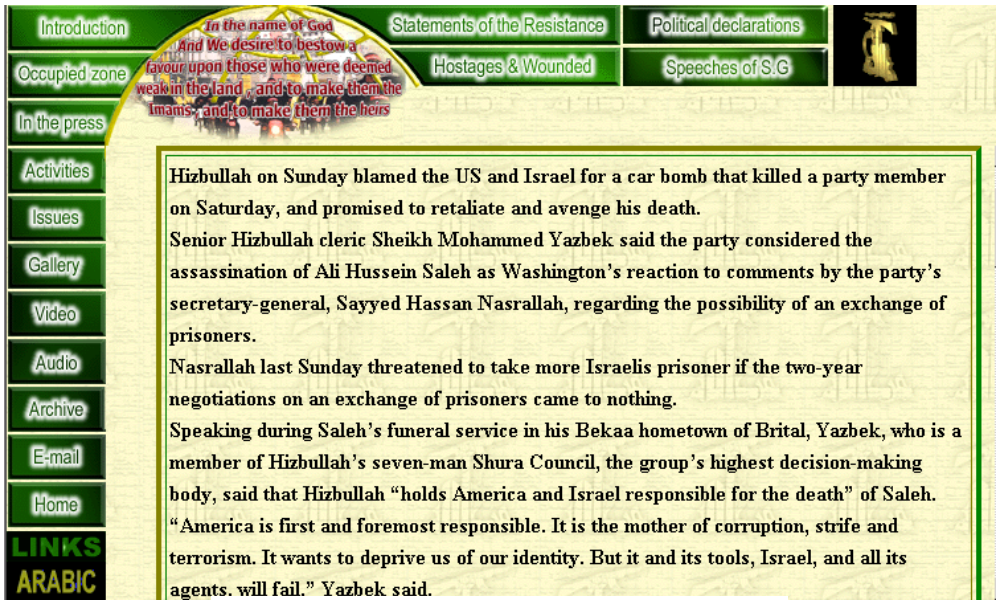


Figure VI-1. Hizballah Website Example

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.

[42] 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.
[43] Christopher C. Harmon, *Terrorism Today* (London: Frank Cass Publishers, 2000; reprint, Portland: Frank Cass Publishers, 2001), 55.

This Page Intentionally Blank

Section VII: Cyber-Terrorism

Time and again the message was: Be prepared for lethal acts of terrorism, always keep in mind that the war has three fronts – on the ground, in cyberspace and in ideology.

Reoccurring theme within the US Special Operations community, 2006 Annual Meeting

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.[44]

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

[44] John Arquilla and David Ronfeldt, ed., *Networks and Netwars* (Santa Monica: RAND, 2001): 5.

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.[45] Terrorists could exploit 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."[46] 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."[47] 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."[48]

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

---

[45] "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.

[46] Joint Publication 1-02, *DOD Dictionary of Military and Associated Terms*, 12 April 2001, as amended through 17 December 2003.

[47] 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.

[48] 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.

respondents detected computer security breaches within the previous twelve months.[49] 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.[50] 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.[51]

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, [52] 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

[49] Ibid., 2-3.
[50] 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.
[51] 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.
[52] 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.

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 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.[53] 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

[53] 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.

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.[54]

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 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.[55]

- "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),

[54] 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.
[55] 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.

United States Army, United States Navy, Department of Energy and National Institutes of Health.[56]

- 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 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.[57] 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.[58]

- 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 excellent workers 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.

---

[56] 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.
[57] 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.
[58] Ibid., 2-3.

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.[59]

- 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."[60]

  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:[61]

  - 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.[62]

[59] Ibid., 3.
[60] 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.
[61] 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.
[62] 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.

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
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 VII-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: [63]

    - 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

[63] "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.

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.[64] 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 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.

[64] 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.

- 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).

This Page Intentionally Blank

Section VIII: 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: [65]

- 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.[66]

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

[65] 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.
[66] 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.[67]

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.[68]

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.

[67] 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.
[68] 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.

Summary

Peace really does not exist in the Information Age.

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

The events of the first decade of this century demonstrate the need to view ourselves and our enemies differently. Threats that in the past were considered an OCONUS problem are now better understood to be also a CONUS issue. Threat elements will plan to avoid friendly forces and will seek to damage those targets which are not well defended and cause the most physical and psychological damage.

The infrastructures that support the lives of Americans and those that support the U.S. military are the threat targets inside as well as outside of the United States. Terrorist attacks aimed at weaknesses within critical infrastructures will allow the terrorists to gain the attention they desire, and avoid the damaging conflict to their own organizations. Understanding our infrastructures, their criticalities and the threats facing them is necessary to continue our way of life as we know it. The handbook offers examples of attacks on infrastructures that support the U.S. and our military, both here in the U.S. and abroad. As new technologies increase the speed of operations, the flow of information, or the timeliness of the common operating picture, opportunities to damage or destroy also increase. We must constantly assess new system as well as assess the capabilities of the threat to ensure every move forward does not expose a weak link to attack.

This 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.

Area of Influence: (DOD, NATO) A geographical area wherein a commander is directly capable of influencing operations by maneuver or fire support systems normally under the commander's command or control.

Area of Interest: (AOI) (DOD) That area of concern to the commander, including the area of influence, areas adjacent thereto, and extending into enemy territory to the objectives of current or planned operations. This area also includes areas occupied by enemy forces who could jeopardize the accomplishment of the mission.

Area Of Responsibility: (AOR) (DOD) The geographical area associated with a combatant command within which a combatant commander has authority to plan and conduct operations.

Asset (Infrastructure): A distinguishable network entity that provides a service or capability. Assets are people, physical entities, or information located either within or outside the United States and owned or operated by domestic, foreign, public or private sector organizations. (DoD Directive 3020.40, 19 August 2005)

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).

Critical: A characteristic denoting extraordinary importance. (DoD CIP Security Classification Guide, Jan 2003)

Critical Asset: A specific entity that is of such extraordinary importance that its incapacitation or destruction would have a very serious, debilitating effect on the ability of the Department to conduct successful military operations. Impairment or loss of such entities requires near-term, if not immediate, remediation. (DoD CIP Security Classification Guide, Jan 2003)

Critical Infrastructure Protection: Actions taken to prevent, remediate, or mitigate the risks resulting from vulnerabilities of critical infrastructure assets. Depending on the risk, these actions could include changes in tactics, techniques, or procedures; adding redundancy; selection of another asset; isolation or hardening; guarding etc.. (DoD Directive 3020.40, 19 August 2005)

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 Critical Asset: An asset of such extraordinary importance to DoD operations in peace, crisis, and war that its incapacitation or destruction would have serious, debilitating effect on the ability of the Department of Defense to fulfill its missions. (DoD Directive 3020.40, 19 August 2005)

Defense Critical Infrastructure: DoD and non-DoD networked assets essential to project, support, and sustain military forces and operations worldwide. (DoD Directive 3020.40, 19 August 2005)

Defense Critical Infrastructure Program (DCIP): A DoD risk management program that seeks to ensure the availability of networked assets critical to DoD missions. Activities include the identification, assessment, and security enhancement of assets essential for executing the National Military Strategy. (DoD Directive 3020.40, 19 August 2005)

Defense Industrial Base (DIB) Defense Sector: The Department of Defense, the U.S. Government, and private sector worldwide industrial complex with capabilities to perform research and development, design, produce, and maintain military weapons systems, subsystems, components, or parts to meet military requirements. (DoD Directive 3020.40, 19 August 2005)

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.

Defense Infrastructure: Those systems and assets owned. Operated, or provided by DoD that support the planning, mobilization, deployment, and sustainment of military operations. (DoD CIP Security Classification Guide, Jan 2003)

Defense Infrastructure Sector: A virtual infrastructure entity that encompasses the end-to-end functionality of that portion of the Defense Infrastructure that performs a similar function in the support of the DoD CIP program. (DoD CIP Security Classification Guide, Jan 2003)

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).

Facility: A building, structure, utility system, pavement, and underlying land. Facilities are assigned to sites and comprised of assets.

Financial Services Defense Sector: The DoD, government, and private-sector worldwide network and its supporting infrastructure that meet the financial services needs of DoD users across the range of military operations.

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.

Global Information Grid (GIG) Defense Sector: The globally interconnected, end-to-end set of information capabilities, associated processes, and personnel for collecting, processing, storing, disseminating, and managing information on demand to warfighters, policy makers, and support personnel including all owned and leased communications and computing systems and services, software (including applications), data, security services, and other associated services necessary to achieve information superiority. It also includes National Security Systems as defined in Section 5142 of the Clinger-Cohen Act of 1996. (DoD Directive 3020.40, 19 August 2005)

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.

Hazard (Infrastructure): Non-hostile incidents such as accidents, natural forces, technological failures, etc., that causes loss or damage to infrastructure assets. (DoD Directive 3020.40, 19 August 2005)

Health Affairs Defense Sector: The DoD, government, and private-sector worldwide health care network and its supporting infrastructure that meet the health care needs of DoD users across the range of military operations.

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.

Infrastructure: 1. The framework of interdependent physical and cyber-based systems comprising identifiable industries, institutions, and distribution capabilities that provide a continual flow of goods and services essential to the defense and economic security of the United States, the smooth functioning of government atr all levels, and society as a whole. (DoD CIP Security Classification Guide, Jan 2003) **2.** The framework of networked assets that comprise identifiable industries, institutions, or distribution capabilities that enable a continued flow of goods and services. (DoD Directive 3020.40, 19 August 2005)

Installation Preparedness: The integration of key activities on DoD installations and facilities that addresses all efforts pertaining to prevention, detection, protection, response, and remediation against all threats and hazards. (DoD Directive 3020.40, 19 August 2005)

Intelligence, Surveillance, and Reconnaissance (ISR) Defense Sector: The DoD, government sand private sector worldwide facilities, networks, and systems that conduct and support the collection, production, and dissemination of intelligence, surveillance and reconnaissance information, in support of activities that meet the needs of DoD users across the range of military operations. (DoD Directive 3020.40, 19 August 2005)

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.

Logistics Defense Sector: The DoD, government, and private-sector worldwide facilities, networks, and systems that support the provision of supplies and services to the U.S. forces.

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)

Mission Assurance: A process to ensure that assigned tasks or duties can be performed in accordance with the intended purpose or plan. It is a summation of the activities and measures taken to ensure that required capabilities and all supporting infrastructures are available to the DoD to carry out the National Military

Strategy. It links numerous risk management program activities and security related functions – Such as force protection; antiterrorism; critical infrastructure protection; information assurance; continuity of operations; chemical, biological, radiological, nuclear, and high-explosive defense; readiness; and installation preparedness – to create the synergistic effect required for DoD to mobilize, deploy, support, and sustain military operations throughout the continuum of operations. (DoD Directive 3020.40, 19 August 2005)

Mission Essential Tasks: (METs) Those tasks, identified by the command, as essential to mission success.

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.

Network: A group or system of interconnected or cooperating entities, normally characterized as being nodes (assets) and the connections that link them.

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)

Phishing: A form of criminal activity using social engineering techniques. An attempt to fraudulently acquire sensitive information, such as passwords, social security numbers and credit card details, by masquerading as a trustworthy person or business in an apparent official electronic communication. Examples are fraudulent emails from know banks, internet sites, etc asking for information. **"Spear" Phishing** is phishing used to target a specific group of people or site in an effort to gain a specific piece of information.

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)

protection: The means of providing physical and cyber security enhancements. Protection techniques include, but are not limited to, hardening, mobility, dispersal, threat effects tolerance, redundancy, signature reduction, access control, and personnel reliability. (DoD CIP Security Classification Guide, Jan 2003)

Public Works Defense Sector: The DoD, government, and private-sector worldwide network, including the real property inventories (environment, land, buildings, and utilities), that manages the support, generation, production, and transportation of commodities (e.g., electric power, oil and natural gas, water and sewer, emergency services, etc.) for and to DoD users.

Risk: Probability and severity of loss linked to threats or hazards. (DoD Directive 3020.40, 19 August 2005)

- **Risk Assessment:** A systematic examination of risk, using disciplined processes, methods, and tools. IT provides an environment for decision making to continuously evaluate and prioritize risks and recommend strategies to remediate or mitigate those risks. . (DoD Directive 3020.40, 19 August 2005)

- **Risk Management:** A process by which decision makers accept, reduce, or offset risk. . (DoD Directive 3020.40, 19 August 2005)

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.

Single Point Of Failure: (SPOF) phrase for any component of a system that upon failure will cause a malfunction in the entire system or network.

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.

Space Defense Sector: The DoD, government, and private-sector worldwide network, including both space and ground-based systems and facilities, that supports launch, operation, maintenance, specialized logistics, control systems, etc., for DoD users.

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.

Standards for Assessment (for the DCIP): A series of statements for the DCIP assessment process for use as a rule foir measuring, judging, or comparing Supporting Foundational Infrastructure Networks (SFINs), Supporting Material and Services (SMS), and DCAs. (DoD Interim Implementation Guidance, 13 July 2006)

- **DCA Assessment Standards:** Standards that pertain to sites owned or operated by DoD. These sites can be Continental United States (CONUS) or Outside Continental United States (OCONUS) installations/sites and commercial sites (e.g., ports, etc.) with the exclusion of Defense Industrial Base (DIB) Sites.

- **Supporting Foundational Infrastructure Network (SFIN) Assessment Standards:** Assessment standards that include a consideration of the potential risks inherent in the infrastructure "grids" upon which the DCA resides and from which the DCA is supported. Key infrastructure grids include power resources (e.g., natural gas, petroleum, and electric); transportation networks (e.g., rail, roads, air, and seaports); communications (e.g., electronic data, video, and voice communications); water (e.g., potable, firefighting, industrial, and

waste); supporting utilities (E.g., heating, ventilation, and air conditioning (HVAC)), and chemicals and chemical products.

- **Supporting Material Services (SMS) Standards:** Assessment standards that consider the potential risks inherent in the commercial support to a DCA, including supplier contractual obligations regarding the production, transportation, and security of material and se4rvices during both peacetime and periods of conflict. Attention is also paid to the ownership and ownership/control, and the vulnerabilities inherent therein.

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.

Tactical Control: (TACON) (DOD) Command authority over assigned or attached forces or commands, or military capability or forces made available for tasking, that is limited to the detailed direction and control of movements or maneuvers within the operational area necessary to accomplish missions or tasks assigned. Tactical control is inherent in operational control. Tactical control may be delegated to, and exercised at any level at or below the level of combatant command. When forces are transferred between combatant commands, the command relationship the gaining commander will exercise (and the losing commander will relinquish) over these forces must be specified by the Secretary of Defense. Tactical control provides sufficient authority for controlling and directing the application of force or tactical use of combat support assets within the assigned mission or task.

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.

Threat: An adversary having the intent, capability, and opportunity to cause loss or damage. . (DoD Directive 3020.40, 19 August 2005)

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

Transportation Defense Sector: The DoD, government, and private-sector worldwide network that provides U.S. military lift support (surface, sea, and air) for military operations.

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.

Vulnerability (Infrastructure): The characteristics of an installation, system, asset, application, or its dependencies that could cause it to suffer a degradation or loss (incapacity to perform its designated function) as a result of having been subjected to a certain level of threat or hazard. . (DoD Directive 3020.40, 19 August 2005)

Vulnerability Assessment (Infrastructure): A systematic examination of the characteristics of an installation, system, asset, application, or its dependencies to identify vulnerabilities. . (DoD Directive 3020.40, 19 August 2005)

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).

This 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), 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.

Staten, Clark, "Reflections on the 1997 President's commission on Critical Infrastructure Protection (PCCIP) Report", Emergency Response and Research Institute, October 1997. Available from http://www.emergency.com/pcciprpt.htm; Internet; Accessed 6 March 2006.

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. Critical Infrastructure Protection (CIP) Plan. 18 November 1998. Available from http://www.fas.org/irp/offdocs/pdd/DOD-CIP_Plan.htm; Internet; Accessed 2 March 2006.

U.S. Department of Defense. Critical Infrastructure Protection (CIP) Security Classification Guide, January 2003.

U.S. Department of Defense. Defense Critical Infrastructure Protection (DCIP) Interim Implementation Guidance, July 2006.

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 Defense. Directive Number 3020.4. Defense Critical Infrastructure Program (DCIP), 19 August 2005.

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.

U.S. President. Decision Directive 63, Critical Infrastructure Protection, 22 May 1998. Available from http://www.fas.org/irp/offdocs/pdd-63.htm; Internet; Accessed 2 March 2006.

U.S. President. Executive Order 13010, Critical Infrastructure Protection, 15 July 1996. Available from http://www.fas.org/irp/offdocs/eo13010.html; Internet; Accessed 6 March 2006.

U.S. President. Executive Order 13231, Critical Infrastructure Protection in the Information Age, 16 October 2001. Available from http://www.whitehouse.gov/news/releases/2001/10/print/20011016-12.html; Internet; Accessed 1 March 2006.

U.S. President. Homeland Security Presidential Directive 7, Critical Infrastructure Identification, Prioritization, and Protection, 17 December 2003. Available from http://www.whitehouse.gov/news/releases/2003/12/print/20031217-5.htm; Internet; Accessed 3 March 2006.

White Paper, The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 63, Critical Infrastructure Assurance Office, 22 May 1998. Available from http://www.fas.org/irp/offdocs/paper598.htm; Internet; Accessed 3 March 2006.

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.

This Page Intentionally Blank

This 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 *Critical Infrastructure Threats and Terrroism*
to DCSINT Handbook No.1 *A Military Guide to Terrorism in the Twenty-First Century,* Version 4.0
U.S. Army Training and Doctrine Command, Deputy Chief of Staff for Intelligence
Assistant Deputy Chief of Staff for Intelligence-Threats, Fort Leavenworth, Kansas