NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

CRITICAL INFRASTRUCTURE PROTECTION: HOW TO ASSESS AND PROVIDE REMEDY TO VULNERABILITIES IN TELECOM HOTELS

by

Michael A. Ordonez

September 2006

Thesis Advisor:	Ted Lewis
Second Reader:	Rudy Darken

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE	*Form Approved OMB No. 0704-0188*

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.

1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** September 2006	**3. REPORT TYPE AND DATES COVERED** Master's Thesis

4. TITLE AND SUBTITLE: Critical Infrastructure Protection: How to Assess and Provide Remedy to Vulnerabilities in Telecom Hotels	**5. FUNDING NUMBERS**
6. AUTHOR Ordonez, Michael A**.**	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000	**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A	**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited	**12b. DISTRIBUTION CODE** A

13. ABSTRACT

America's open society includes a vast array of critical infrastructure and key resources that are vulnerable to terrorist attacks. While it is not possible to protect or eliminate vulnerabilities of all critical infrastructures in the United States, strategic improvements can be made to harden these assets and mitigate any damaging effects if an attack were to occur. Current network assessment methods and protective measures are inadequate. As a consequence, the need for a scientific methodology for implementation of critical infrastructure protection is required. A standardized vulnerability assessment/risk analysis tool needs to be developed and implemented for the Critical Infrastructure Protection Programs to analyze complex networks and examine critical nodes. This will help to prevent, deter, and mitigate the effects against terrorist attack in accordance with HSPD-7. This thesis examines ways that vulnerability analysis is currently conducted and it could be improved to establish an all-encompassing methodology to identify, prioritize, and protect critical infrastructure. By analyzing and research, this thesis recommends that the National Communications System under the DHS establish the required policy initiatives to mandate the National Reliability and Interoperability Council's current and future "best practices," and set a vulnerability assessment/analysis standard based on MBVA and JSIVA methodologies.

14. SUBJECT TERMS Telecommunications, Carrier Hotel, Critical Infrastructure Protection, Telecom Hotel, Joint Staff Integrated Vulnerability Assessment, Model-Based Vulnerability Analysis, Local Exchange Carriers, Inter-Exchange Carriers, Meet-me-rooms, Data center, Central office, Colocation facility, Network Access Point	**15. NUMBER OF PAGES** 109
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UL

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release, distribution is unlimited

CRITICAL INFRASTRUCTURE PROTECTION: HOW TO ASSESS AND PROVIDE REMEDY TO VULNERABILITIES IN TELECOM HOTELS

Michael A. Ordonez
Civilian, TREX Branch Chief, United States Northern Command
B.S., Marquette University, 1989
M.B.A., Texas A&M University, 2002

Submitted in partial fulfillment of the
requirements for the degree of

**MASTER OF ARTS IN SECURITY STUDIES
(HOMELAND SECURITY AND DEFENSE)**

from the

**NAVAL POSTGRADUATE SCHOOL
September 2006**

Author: Michael A. Ordonez

Approved by: Ted Lewis
Thesis Advisor

Rudolph Darken
Second Reader

Douglas Porch, PhD
Chairman, Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

America's open society includes a vast array of critical infrastructure and key resources that are vulnerable to terrorist attacks. While it is not possible to protect or eliminate vulnerabilities of all critical infrastructures in the United States, strategic improvements can be made to harden these assets and mitigate any damaging effects if an attack were to occur. Current network assessment methods and protective measures are inadequate. As a consequence, the need for a scientific methodology for implementation of critical infrastructure protection is required. A standardized vulnerability assessment/risk analysis tool needs to be developed and implemented for the Critical Infrastructure Protection Programs to analyze complex networks and examine critical nodes. This will help to prevent, deter, and mitigate the effects against terrorist attack in accordance with HSPD-7. This thesis examines ways that vulnerability analysis is currently conducted and it could be improved to establish an all-encompassing methodology to identify, prioritize, and protect critical infrastructure. By analyzing and research, this thesis recommends that the National Communications System under the DHS establish the required policy initiatives to mandate the National Reliability and Interoperability Council's current and future "best practices," and set a vulnerability assessment/analysis standard based on MBVA and JSIVA methodologies.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ABBREVIATIONS, ACRONYMS, AND SYMBOLS

CIP	Critical Infrastructure Protection
DHS	Department of Homeland Security
DoD	Department of Defense
DOS	Denial of Service
EMP	Electromagnetic Pulse
FCC	Federal Communications Commission
HLD	Homeland Defense
HLS	Homeland Security
HPM	High Powered Microwave
ISAC	Information Sharing and Analysis Center
IEC	Inter-Exchange Carrier
IT	Information Technology
JSIVA	Joint Staff Integrated Vulnerability Assessment
LEC	Local Exchange Carriers
MMR	Meet Me Room
MBVA	Model-Based Vulnerability Analysis
NAP	Network Access Point
NCC	National Coordinating Center
NCS	National Communications System
NRIC	National Reliability and Interoperability Council
NSTAC	National Security Telecom Advisory Committee
NTIA	National Telecommunications and Information Administration
Telecom	Telecommunications
Telco	Telecommunications Company
VBIED	Vehicle Borne Improvised Explosive Device

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

I thank my advisors, Professor Ted Lewis and Professor Rudy Darken, for their time and their insightful and rapid feedback. Additionally, several individuals from the Telecommunications industry who wish to remain anonymous are also recognized for providing critical information along the way. I also thank my leadership, Col Larry "Bullet" Jones and Mr. Tim Croft. Without their endorsement and strong support, it would not have been possible for me participate in the National Security Affairs, Homeland Security, Master's Degree Program.

A special debt of appreciation is owed my fellow learners in Cohort 0401 and 0402. The friendships gained and stories shared were an invaluable aspect of this program.

I thank my son Andrew for his love and support throughout this learning process and for giving me the time to complete this thesis.

Finally, I wish to express my thanks to my wife Beth who put her life on hold, along with mine, so that I could participate in this project. She has always been a determined and supportive spouse who is a great source of inspiration and comfort.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. PROBLEM STATEMENT

How do officials effectively assess whether terrorists would be successful in attacking telecom hotels, and how do they assess the likely consequences of such attacks?

This is a study of the vulnerabilities of the critical telecommunications industry infrastructure in the United States. The study focuses on "telecom hotels"—large facilities that house several network carriers, telephone and internet service providers, and Web hosting organizations.

This study assesses the vulnerability of the telecom industry and investigates the possibility that terrorists might be successful in an attack against telecom hotels. This information will allow security planners at all levels to devise protective measures based on changes in telecommunications regulations or regulatory structure. This study is designed to help the reader understand the ramifications of an attack on the telecommunications industry and to provide recommendations for policy regarding telecom hotel vulnerabilities.

What methodology for determining vulnerabilities should be used? What measures are needed to reduce vulnerabilities?

Several policy options are explored in this thesis. The first is to determine which, if any, agency or organization is in the best position to set strategic security policy for telecom hotels, or whether the hotels should be self-regulated. Several potential candidates would be capable of setting policy, including the Federal Communications Commission (FCC), National Coordinating Center – Information Sharing and Analysis Center (NCC-ISAC), Department of Homeland Security, the National Telecommunications and Information Administration NTIA, and National Security Telecommunications Advisory Committee (NSTAC). Once the best agency or organization to undertake this mission is identified, the stage must be set for strategic policy making. This is accomplished by establishing potential policies that would help to reduce the vulnerabilities in telecom hotels and the telecommunications industry, protecting critical infrastructure. Finally, a net assessment attempts to ascertain a set of vulnerability assessment methods that are scientific, structural, economical, and can be replicated. Most of the sources were found in reports and journals and take an overall look at all recommendations, pros and cons, from previous arguments. A synopsis based on personal experience and open source intelligence provides insight from an "outside" viewpoint.

Empirical data to accurately assess the benefits of a strategic policy implementation are difficult to find, and this is a common problem for any topic or strategy dealing with homeland security or defense. The terrorist planning cycle may span a period of several years for just one tactical operation. One could argue that there have been no attacks on this industry in the United States to date, and that the current self-regulated or other non-homeland security telecommunication policies are adequate. It is quite possible that many of the strategic changes to homeland security policy have not been evaluated for their effectiveness due to the difficulty in the assessment. The criteria for measuring pros and cons of a policy option will naturally be somewhat subjective, but a method of weighing and prioritizing each must be included in the appraisal. Another method of assessment may be to create a theoretical change of policy, model the changes that occurred in the system, and then note these changes. This method, if possible, would not be easy to accomplish, but it is explored throughout the research of this topic.

B. THESIS ORGANIZATION

Chapter I provides both an introduction to the thesis and basic overviews of critical infrastructure protection and telecommunications networks. Chapter II addresses threats, both physical and cyber, and vulnerabilities of telecom hotels. Chapter III presents current network analysis methods, with focus on a standard to correctly analyze complex networks; network theory makes possible the precise identification of critical components comprising telecom hotels. The Core Vulnerability Assessment Management Program (CVAMP) is a DoD methodology for managing vulnerability assessments as part of an anti-terrorism/force protection (AT/FP) campaign. This chapter concludes with an examination of the Asset Prioritization Model (AMP), as DoD is responsible for the Defense Industrial Base for Critical Infrastructure Protections. Chapter IV begins with an examination of telco operations, based on interviews with experts in the sector. It briefly describes the current regulatory dilemma and also the interdependencies with other critical infrastructure sectors. Included is a case study of the organization of telecommunications within DoD, as well as a look at some telco initiatives. Chapter V provides recommendations for countermeasures against the threats and proposes regulatory changes for all responsible organizations, including federal, state, local, tribal, and private sector.

C. INFRASTRUCTURE PROTECTION OVERVIEW

One of the six critical mission areas defined in the National Strategy for Homeland Security is Critical Infrastructure Protection (CIP). The Information and Telecommunications Sector is one of thirteen interconnected sectors. In reducing vulnerabilities to the terrorist threat, action must be taken to ensure that critical infrastructure and key assets are protected. The USA PATRIOT Act (Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001) defines *critical infrastructure* as those

> 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.[1]

CIP began in 1995 with Presidential Decision Directive 39 (PDD-39), U.S. Policy on Counterterrorism. The latest documentation on CIP is the Interim National Infrastructure Protection Plan (February 2005). As a result of shifts in the sectors, via additional PPDs, there is now a Sector Specific Agency aligned with each sector. The seventeen sectors are Agriculture and Food, Public Health and Healthcare, Water, Energy, Banking and Finance, National Monuments and Icons, Defense Industrial Base, Information Technology, Telecommunications, Chemical, Transportation Systems,

[1] USA Patriot Act is [The] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, U.S. H.R. 3162, S. 1510, Public Law 107–56, SEC. 1016. Critical Infrastructures Protection, (e).

Emergency Services, Postal and Shipping, Dams, Government Facilities, Commercial Facilities, and Nuclear Reactors, and Materials and Waste. The Interim NIPP is the first integrated effort between federal, state, local, tribal, public, and private entities to implement CIP efforts.[2]

Effective communication is essential in any business or marriage, and especially in a military operation potentially directing the use of nuclear weapons. The earliest known example of CIP was most likely the National Communication System (NCS), initially established by President John F. Kennedy in 1963 to form a single unified communications system. Its role was to serve the president, Department of Defense, diplomatic and intelligence activities, and civilian leaders. The NCS charter was to

> link together, improve, and extend, on an evolutionary basis, the communications facilities and components of the various federal agencies … to provide necessary communications for the federal government under all conditions ranging from a normal situation to national emergencies and international crisis, including nuclear attack.[3]

In 1984, with Executive Order 12472, the NCS focus was changed. The order generated the new mission of assisting the president, the National Security Council, the director of the Office of Science and Technology Policy and the director of the Office of Management and Budget in exercising wartime and non-wartime emergency communications responsibilities, while coordinating emergency telecommunications planning for the federal government. Thus, the mission of the NCS developed from a centralized, focused role of implementing a single, federal telecommunications system, to a rather decentralized, unfocused role of advising and coordinating among several entities. With the establishment of the Department of Homeland Security (DHS), and in order to provide better communications support to critical government functions during emergencies, the NCS moved from DoD to DHS.[4] One system within NCS to help in the

[2] Department of Homeland Security, "The Interim National Infrastructure Protection Plan," February 2005 (Washington, D.C.: Office of Homeland Security, 2005), 3.

[3] Mark D. Baines, Lieutenant Colonel, "The National Telecommunications Infrastructure: A 21st Century Organizational Paradox," Strategy Research Project (Carlisle Barracks, PA: U.S. Army War College, April 7, 2003), 11.

[4] SHARES Bulletin 04–14, March 2004, [http://www.ncs.gov/library/SHARES/SHARES%20Bulletin%2014.pdf] Accessed September 17, 2005.

HLS mission is the Government Emergency Telecommunications Service (GETS), which gives priority to the government to gain access to phone networks during an emergency, utilizing an access code.[5] The Priority Access System (PAS) is similar to GETS, but it gives priority to wireless services. For an in-depth overview of the telecommunications history, see the Appendix.

[5] National Communications System. [http://gets.ncs.gov/] Accessed September 17, 2005.

THIS PAGE INTENTIONALLY LEFT BLANK

II. TELECOM HOTELS

A. DEFINITIONS: CIP VS. CYBER-TERRORISM

Two major aspects are considered when accessing telecommunication hotel vulnerabilities. The problems can be classified as Cyber-Terrorism and Critical Infrastructure Protection; so first a clear definition of these problems must be given.

This telecom vulnerability problem must be classified into a task in order to determine the Office of Primary Responsibility (OPR). This is a question of both cyber terrorism and critical infrastructure protection. In trying to define cyber terrorism, the two terms are combined. The definition of cyber is simply computer or computer network. Terrorism is defined by The American Heritage Dictionary as "the unlawful use or threatened use of force or violence by a person or an organized group against people or property with the intention of intimidating or coercing societies or governments, often for ideological or political reasons." When the definitions are combined, the result is "the use or threatened use of force or violence against people or property using computers or computer networks." In addition, the FBI defines cyber-terrorism as "The premeditated, politically motivated attack against information, computer systems, computer programs, and data which results in violence against noncombatant targets by sub-national groups or clandestine agents."[6] Critical Infrastructure Protection (CIP) will be defined using the same methodology. *Critical* is defined as indispensable or essential. *Infrastructure* is an underlying base or foundation, especially for an organization or system. (It is interesting to note that this definition is similar to the English translation of *Al Qaeda:* "the foundation" or "the base". Protection is defined as the act of protecting, or the state of being protected; preservation from loss, injury, or annoyance; defense; shelter, as in, "the weak need protection." Combining the terms, CIP is defined as protecting the essential foundation of the United States. In redefining the problem, this thesis proves that there are two issues at hand in reducing telecommunications vulnerabilities. The first is to prevent cyber terrorist attacks, and the

[6] Mark M. Pollitt, Cyberterrorism – Fact or Fancy? Proceedings of the 20th National Information Systems Security Conference, October 1997, 285–289.

second is to reduce vulnerabilities by protecting the critical infrastructure. This paper mainly addresses the CIP aspect, but references cyber terrorism when required. To be fully in alignment with the strategic objectives in the National Strategy for Homeland Security, a role of minimizing the damage and recovering from possible attacks must also be assumed.

B. WHAT IS A TELECOM HOTEL?

There are many different names that can be used to describe a telecom hotel. Some of the more common names are carrier hotel, interconnection facility, colocation center (COLO), data center, gateway, network exchange center, commercial internet exchange, mondo condo, internet farm, cyber hotel and data bunker. It is a centrally located building that is constructed or rebuilt for datacenters, typically houses network carriers, service providers (such as Telcos or Internet service providers), Web hosting organizations, and large enterprises.[7]

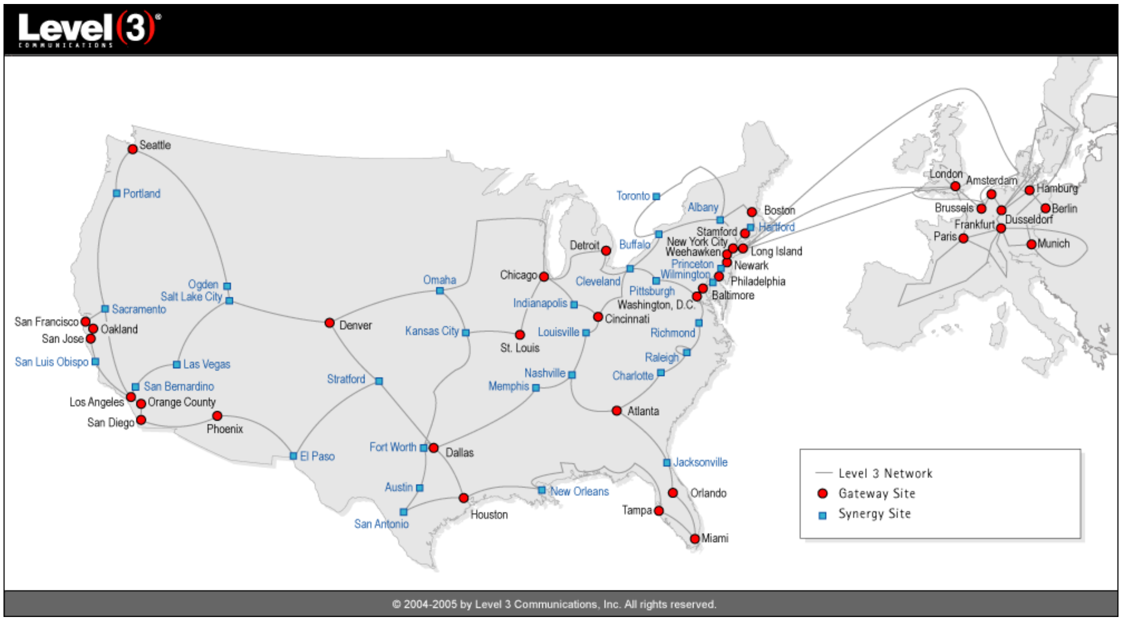
With increasing costs to interconnect large carriers within large regions, these telecommunication facilities have, over time, consolidated resources into the critical nodes known as telecom hotels. Economic reasons (as well as the Telecommunications Act of 1996 that requires linking LECs (Local Exchange Carriers) and IECs (Inter-Exchange Carriers), telecommunications companies, Internet ISPs, and businesses) have caused companies to co-locate their equipment and services into the same building. This saves money, because the infrastructure costs can be shared among a large number of tenants.

There are two main aspects or attributes of telecom hotels. The first is the colocation piece, so that customers can have a place to operate their equipment. The second facet is to facilitate direct cross-connections and to permit access to multiple local and long-haul networks. This interconnection aspect is also referred to as "meet-me-rooms" in which facilities are centrally located within carrier hotels where tenants

[7] Tech Web Encyclopedia. [http://www.techweb.com/encyclopedia/defineterm.jhtml?term=telecomhotel] Accessed September 17, 2005.

interconnect among themselves and others who desire access to their networks.[8] Carrier hotels are typically large buildings in major cities, each with a floor that acts as a central point of interconnection for all of the carriers. It is economically attractive to locate a network where both customers and vendors can interconnect and the carriers can provide better service and lower costs, a business phenomenon known as clustering. There are similarities to IP peering in which IP networks can directly connect to each other. Core Interconnection Facilities can contain not only IP, but also ATM, Frame Relay, Synchronous Optical Network (SONET), Synchronous Digital Hierarchy (SDH), (rates, protocols and technologies for Telephony), Ethernet, and Wavelength-Division Multiplexing (WDM) protocols; therefore, the more networks that are present, the greater the savings for all operators and providers. Another new term to telecom hotels is that of a neutral facility, which is owned or operated by a third party, with no partisanship or influence to utilize certain carriers. The antithesis, a non-neutral facility, is likely to be a large central office that (again, due to the Telecommunications Act of 1996) had to open its doors to CLECs (Competitive Local Exchange Carriers) and provide connection points. In this case, one of the previous Regional Bell Operating Companies (RBOCs), such as SBC, Verizon, or Qwest, would own the facility. In some cases, a carrier may own the building, but have it managed by a third party and lease its own space back in order to maintain the benefits of a neutral facility.

[8] Hunter Newby. “I Now Pronounce You VoIP and Ethernet: Not Just a Marriage of Convenience.” Feb, 2004. Wall Street Technology Association. [http://www.wsta.org/publications/articles/0204_article01.html] Accessed September 17, 2005.



© 2004-2005 by Level 3 Communications, Inc. All rights reserved.

Figure 1. Level (3) Communications Gateway/Network Map.[9]

Carrier Neutral Colocations, sometimes known as Carrier Neutral POPs, encourage LECs, CLECs, and other carriers to bring large-capacity fiber infrastructure into the facility. With infrastructure in place from multiple local and long-haul carriers, building owners can attract ISPs and other service providers who need this service and large capacity connectivity. A Carrier Neutral POP is also appealing to the CLECs and IECs because it can easily interconnect their networks with a simple cross-connect within the facility to any other carrier, instead of with costly circuits or fiber construction between all facilities.

The protocol for a carrier-neutral POP or telecom hotel model is as follows. A non-carrier third party provides the physical space near the carriers' infrastructure. Carriers are responsible for extending their cabling infrastructure into the carrier-neutral POP. The third party, sometimes called the landlord, hotelier, or building management team, provides floor space to each carrier for equipment racks as well as electrical power,

[9] Level (3) Communications, "(3) Center Colocation." [http://www.level3.com/558.html] Accessed September 17, 2005.

HVAC, and security. Carriers are free to negotiate the terms of their inter-connections. The third party is merely a facilitator of these negotiations, by providing the facility.[10]

A neutral CO (Central Office) gives new entrants to the market access to a number of fiber backbone providers, such as Level 3, Williams, MCI, and emerging Ethernet providers such as Yipes Communications. Neutral COs are becoming big business as companies such as Core Location, MetroNexux, Equinix, WarnerColo, MFNs, CRG West, Cervalis, FIBERNET, and Switch & Data are expanding into major telecom hubs. Unlike the initial telecom hotel model where carriers lease physical space from a building owner, neutral COs provide air conditioning, backup DC power, HVAC, dust control, and high-level security in addition to real estate.

C. PUBLIC INFORMATION

One of the problems with neutral COs is that they have active marketing campaigns, and they post much of the information about their buildings on web pages. The web addresses of two of the largest telecom hotels available, one in New York and the other in Los Angeles: http://www.111eighth.com, http://www.onewilshire.com. Information available on their web sites includes the exact location of the building and building specifications to include electricity, emergency power, HVAC, and fiber optic services. The buildings also advertise their security and life safety systems, floor plans, spaces available, other tenants, and details about the building infrastructure and floor loading. The 111 Eighth Avenue building covers an entire New York city block between 15th and 16th Streets, from Eighth to Ninth Avenues. It is an immense building and contains a huge amount of telecommunications gear.

[10] Gratiot County Government, MI, "Appendix VI: Carrier Neutral POP and Circuit Termination Guidelines." [http://www.co.gratiot.mi.us/administration/Link_Mich_Report_2004/AppendixVIPhysicalNetwork.pdf] Accessed September 17, 2005.

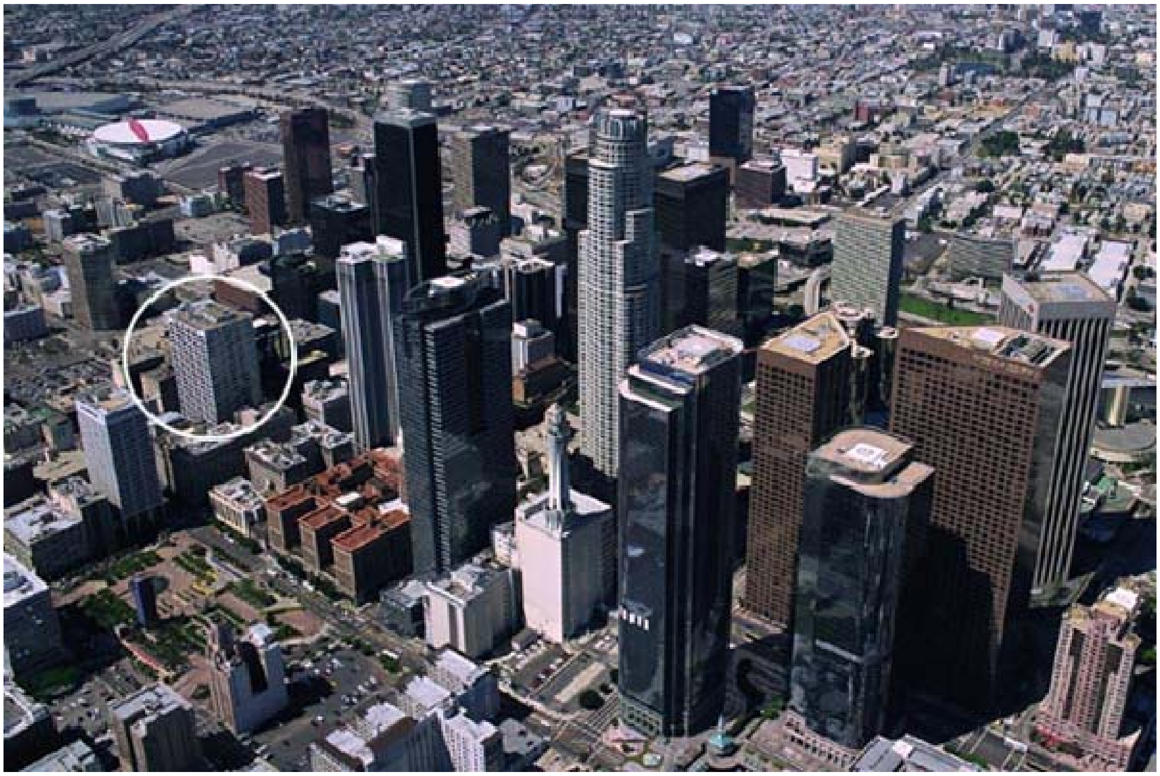


Figure 2. One Wilshire Building.[11]

One major vulnerability to the centers is that much of the information on how to exploit design attributes and security flaws of computer networks is freely available on the Internet. CRG West, the management company for the One Wilshire Building, claims, "One Wilshire — the most connected building in the world!"[12] They also state that almost all of the buildings surrounding One Wilshire are connected via an underground street conduit. The building provides a connection point for international fiber networks converging with the Pacific Bell tandem switch with undersea cable networks and transcontinental transmission resources. Their customers consist of the largest service providers in the world, numbering over 200 voice and data carriers and over 400 network and network service providers. They also mention that the building offers three diverse points of entry for fiber optic cabling, with plans to increase this even more. In interviewing building property managers for many telecom hotels, it was

[11] One Wilshire, CRG West. [http://www.onewilshire.com/about_us/management.htm] Accessed September 17, 2005.

[12] Ibid.

discovered that it is up to the customer to maintain the diversity within their own network, usually based on the importance and type of traffic flowing through their network.

A service provider with a contract for 911 services or emergency priority services would maintain the most diversity and redundancy that was available at the site. The one positive piece of news posted was that CRG West has redundant fiber optic connections between the Market Post Tower Meet-Me-Room in San Jose and the One Wilshire Meet-Me-Room in Los Angeles. Wikipedia defines a "meet me room" (MMR) as "a place within a colocation facility where multiple telecommunication service providers can physically connect to one another. By placing equipment belonging to each service provider within an MMR, carriers and enterprises can exchange data without incurring local loop fees."[13]

A negative aspect of the web site is that they also state that these two buildings are the home of MAE West, which is discussed later in this chapter. Another drawback of Telco web sites is that they allow terrorists to virtually case the location from anywhere in the world by offering virtual tours, pictures of the facilities, and pictures of features such as cellular antennas, satellite dishes, and back-up power, in addition to roadside viewpoints. In many cases with carrier hotels and their attendant web sites, better detail and information can be gained from the web site than from being physically present.[14]

[13] Wikipedia Encyclopedia. [http://en.wikipedia.org/wiki/] Accessed September 17, 2005.

[14] Switch and Data. [http://www.switchanddata.com/subpage.asp?navid=3&id=18] Accessed September 17, 2005.

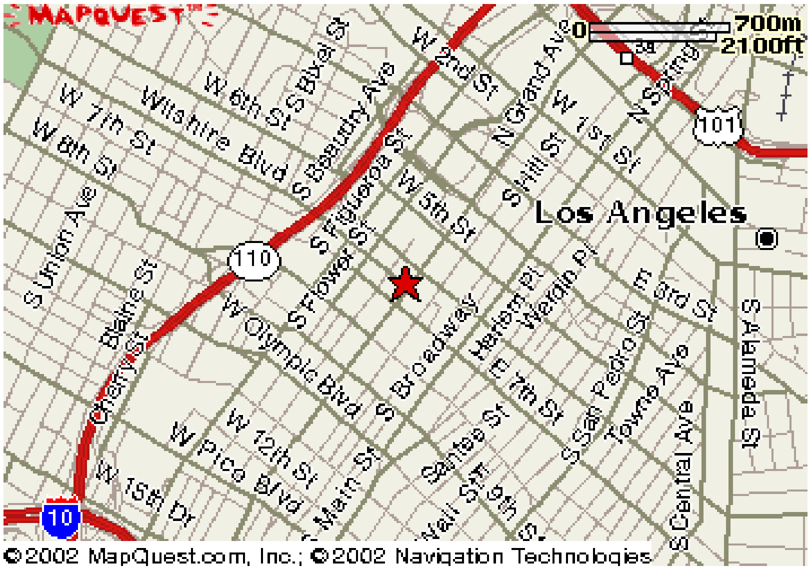


Figure 3. Mapping functions for Telecom Hotels.[15]

Another large facility in New York is a Carrier-Neutral Interconnection Facility at 60 Hudson Street, New York; it is described as "one of the world's busiest carrier hotels" and also as "the most important carrier hotel in the world" due to its location and relevance to international telecommunications. Their information, along with many others, is listed at http://www.carrierhotels.com.[16] Telecom hotels are attractive to carriers because they provide high-speed connections (fiber, satellite, microwave), roof access for antennas, physical security to include key card access, video surveillance, biometric scanners, access control and building escort, power and backup generators, VESDA air sampling (imminent fire detection), fire protection, redundant HVAC, and seismic strength. Because these functions are expensive and bothersome for businesses to supply on their own, many telecom hotels also contain key assets outsourced by their clients. Computers, databases, and other business operating assets are often co-located in a telecom hotel.

[15] One Wilshire, CRG West. [http://www.onewilshire.com/contact_us/map.htm] Accessed September 17, 2005.

[16] Carrier Hotels. [http://www.carrierhotels.com] Accessed September 17, 2005.

A typical colocation center consists of the following service that are normally offered to make the telecom hotels self-sufficient, redundant, and protected:[17]

Building:

- Usually built near a glass fiber ring.
- Fiber has multiple access points into building to provide diversity.
- "Clean" rooms to ensure optimal running conditions for computer and network hardware.
- Empty pipe fire suppression.
- Relay racks, cabinets, or cages for mounting equipment.

Power:

- Connected to two or more different power stations/grids.
- Inline power backup using a system of UPS batteries.
- Possibility to connect two different grids of power distribution to one server.
- Most also have backup diesel generator standby to support power delivery.

Connections:

- Because of the high concentration of servers inside a colocation center, most carriers will be interested in bringing direct connections, to include diverse routing. Service providers can make connections with 20–30 various providers.

Security:

- 24/7 monitoring with onsite guards
- Closed-circuit cameras.
- Biometric readers
- Secure Card access entry
- Worker background checks

In most cases, larger Internet exchanges will be hosted inside a colocation center on which customers can connect for peering.

Telecom hotels may also be attractive to terrorists, and are among the most vulnerable nodes in the telecommunications infrastructure. They are prime targets for

[17] Ted Lewis, "Critical Infrastructure Protection."

asymmetric attacks based on the modus operandi of some large terrorist organizations due to the linkage to the U.S. economic sector. The telecom sector is most vulnerable at these telecom hotel facilities.

D. ASSOCIATED CRITICAL NODES: MAE AND NAP

There are two types of critical nodes that should be associated due to the similarities with telecom hotels. The first is MAE, which initially was referred to as MAE East or MAE West. Computer Knowledge defines MAE as a Metropolitan Area Exchange, previously known as Metropolitan Area Ethernet. It is described as a major Internet Network Access Point (NAP) where different providers and networks hand off traffic to each other. This definition sounds remarkably similar to telecom hotels. A company formerly known as MFS (Metropolitan Fiber Service) constructed the first MAE outside of Washington, D.C. (known as MAE-East) and then a second in Silicon Valley (known as MAE-West). Through a series of mergers and acquisitions, MFS was purchased by WorldCom, which in turn became MCI WorldCom. The company re-emerged from bankruptcy in 2004 under the MCI name. According to the MCI web site, MAE® is a registered MCI trademark for Internet exchange services and MAE is not an acronym. MCI MAE facilities are considered carrier-neutral POPs (Point of Presence) where customers can interconnect to exchange Internet traffic. So MAE is specific to MCI facilities, but MAE and NAP are becoming synonymous.[18]

NAP (Network Access Point) is the second type of associated critical node and a major Internet interconnection point that allows Internet access providers and carriers to exchange traffic and services with each other. It seems that the only differences between MAE and NAP are when they were initially constructed and who actually built them. Another way to look at a NAP is as a hub network for commercial airline carriers. Passengers fly on the "Backbone" between hubs and then are exchanged to express, connection, or regional carriers so they can get to their ultimate destination. These airport hubs, such as O'Hare in Chicago, DFW in Dallas/Ft. Worth, or Reagan

[18] "MAE-Metropolitan Area Exchange (Ethernet)," *Computer Knowledge*. [http://www.cknow.com/ckinfo/questions/414/__print] Accessed September 17, 2005.

International in Washington, exchange passengers rather than packets. (It is interesting to note that these major airport hubs are located in the same cities as many of the NAPs and MAEs.[19])

As previously noted, MFS established MAE East in 1992, modeled after FIXs (Federal Internet Exchange) East and West. Prior to the commercialization of the Internet, three original Internet exchanges were built. This was to facilitate interconnection of the first networks like ARPANET and CSNET to form the Internet. Two were FIXs, located in College Park, Maryland, and in Mountain View, California, and serving as the connection points for government internets and the Internet.[20] The third was a CIX (Commercial Internet Exchange) now in Palo Alto, which connected the first private internets.[21]

The National Science Foundation was charged with setting up four NAPs in order to facilitate growth of the commercial Internet. There were four original NAPs, regionalized to facilitate national connections. One was operated by PacBell in San Francisco,[22] the second by Ameritech in Chicago,[23] the third by Sprint in New York (actually in Pennsauken, New Jersey)[24] and the fourth by MFS in Washington DC (also under the name of MAE-East).[25] MAE-East was originally a fiber-optic data ring around Washington D.C. established to connect companies inexpensively. MAE-West was later constructed, and both operate, in effect, as NAPs. Most records account for 11 different NAPs. These include the historic NAPs (CIX, FIX-East, FIX-West), the four original NAPs listed above and four new MAE locations: MAE West in San Jose, MAE Los Angeles, MAE Dallas and MAE Chicago. There are additional NAPs being constructed constantly. Some additional NAPs coming soon are MAE Houston and “Big East” by

[19] NAP of the Americas. [http://www.napoftheamericas.net/faq.cfm] Accessed September 17, 2005.

[20] National Aeronautics and Space Administration. [http://www.arc.nasa.gov/] Accessed September 17, 2005.

[21] United States Internet Service Provider Association. [http://www.cix.org] Accessed September 17, 2005.

[22] SBC Communications Inc. [http://www.aads.net/pdf.html] Accessed September 17, 2005.

[23] Ibid.

[24] Sprint Corporation. [www.sprintlink.net] Accessed September 17, 2005.

[25] MCI Inc. [http://www.mae.net/fac/mae-east.htm] Accessed September 17, 2005.

ICS Network Systems, headquartered in Bohemia, New York. All information about the "Big East" location has been removed from the corporate web site.[26]

Another NAP is described as a tenant of a telecom hotel. This telecom hotel is named and marketed as TECOTA (Technology Center of the Americas). One of the tenants is NAP of the Americas, which links the fiber networks of Latin America with North America. TECOTA is located at 50 NE 9th Street, Miami, FL, 33132. In addition to this NAP, the company has a new one, NAP of the Americas/West in Santa Clara, California.[27] There are also many unconfirmed or self-proclaimed NAPs like ATLNAP in Atlanta, Georgia, MAE-Houston, the Baltimore NAP, and the Tucson NAP.[28]

In addition to those listed above, MCI has increased its number of MAEs, and they are classified as MAE East, MAE West, MAE Central and MAE Miami. MAE West consists of two locations in San Jose and one in Los Angeles. One location in San Jose is located at 55 S Market St., which is housed at the Market Post Tower telecom hotel. Information about this location states that the building offers three diverse points of entry for the fiber conduits. This is the same number of fiber entry points described for the One Wilshire location in downtown Los Angeles, which is connected to the MAE-LA location. MAE East is comprised of four locations: one in New York and three in Washington D.C. (Vienna, Reston and Ashburn, VA), one of which is located at 1919 Gallows Rd Vienna, VA 22182-3964. MAE Miami has only one location and MAE Central has two locations, one in Dallas and one in Chicago.[29] Tallying the four original NAPs, the three historic NAPs and the additional nine MAEs, there are at least 16 NAPs, not including some of the smaller, lesser known NAPs listed above. It can be deduced that MAEs and NAPs are synonomous and that they are the Internet traffic portion of telecom hotels. Add this to the telephony traffic in a facility to equal a telecom hotel.

[26] SearchWebServices. [http://searchwebservices.techtarget.com/sDefinition/0,,sid26_gci214106,00.html] Accessed September 17, 2005.

[27] NAP of the Americas. [http://www.napoftheamericas.net/faq.cfm#1L] Accessed September 17, 2005.

[28] Indonesian Internet Society. [http://www.isoc-id.org/iidp/table_5_selected_us_networks_exchange_points.php] Accessed September 17, 2005.

[29] MCI Inc. [http://www.mae.net/peer/] Accessed September 17, 2005.

For practical purposes and close associations, the physical locations of MAEs, NAPS and international cable landings will be included in this study as telecom hotels.

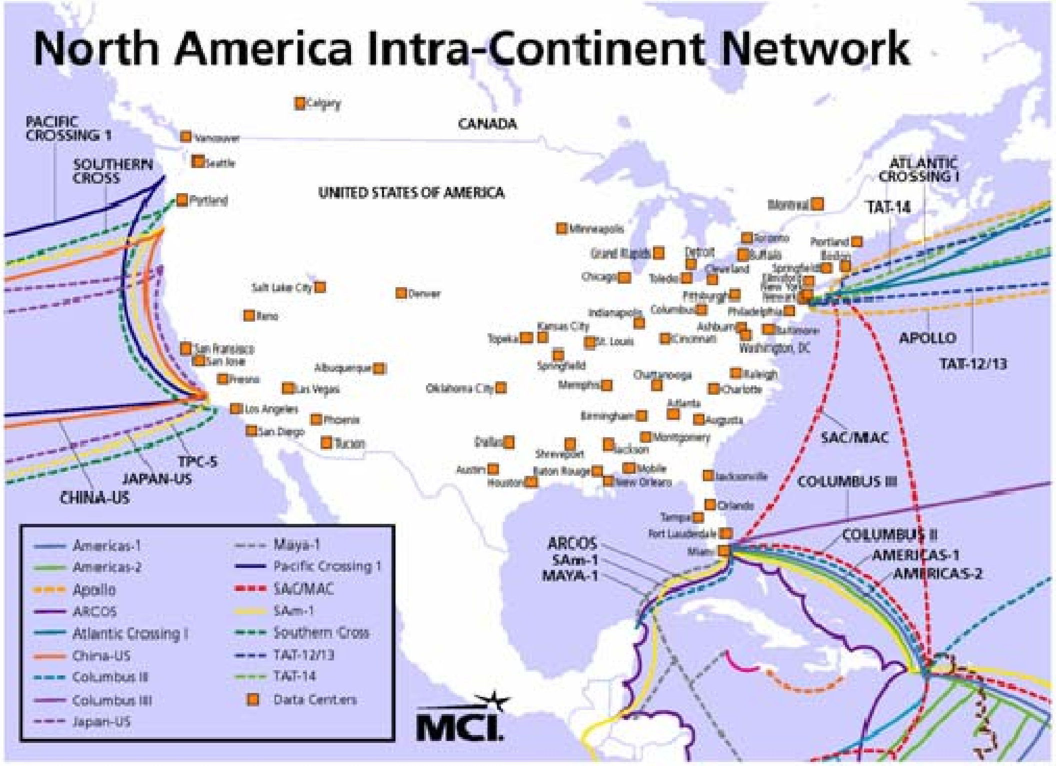


Figure 4. MCI Network illustrating International Cable Landings and Data Centers.[30]

E. THREATS

1. Overview

The telecommunications sector must cope with natural and human threats every day. These threats include natural weather events like tornados, hurricanes, and flooding, and unintentional events like fiber cuts and maintenance or power outages. Other human threats would consist of physical and cyber sabotage from insiders. A fiscal threat also exists due to the economic downturn in the industry in the past few years. This has

[30] MCI Inc. MCI Network illustrating International Cable Landings and Data Centers [http://global.mci.com/about/network/global_presence/northamerica/mci_global_presence_NORTHAMERICA.pdf] Accessed September 17, 2005.

caused companies to spend capital on operations instead of research and development, recapitalizing, securing, and enhancing the infrastructure.

Is there a valid terrorist threat? Specific threats to the telecom industry or toward the telecom infrastructure sector from actionable intelligence are beyond the scope of this unclassified paper. There have been general threats and information released about the financial district in New York and New Jersey, and specific buildings that have been monitored and targeted for attacks. Al-Qaeda has not engaged in cyber attacks in the past; however, Usama Bin Laden has suggested that Al-Qaeda has the expertise to use the computer as a weapon.[31] (The 9/11 attacks documented the secondary effects on the telecom infrastructure that existed either on the twin towers or in their basements.) In limiting the discussion to Al Qaeda, it has been reported that some members have been trained in cyber terrorism and have researched U.S. CIP web sites. Is there a desire or intent to attack telecom hotels? The desire for causing mass casualties would not be gained by attacking telecom hotels, but one goal of Al Qaeda has been to economically destroy the U.S.

A terrorist attack can cause mass disruption of the many interconnected layers of systems. U.S. Northern Command utilizes SOSAs (System Of Systems Analysts) to explore what effect the damage to one system or sector would have on another. These concentrations of the sector's key assets are becoming attractive targets even if they have not been directly targeted by terrorists in the past.

There are many forms in which threats can arrive, some of which may not be known or even imagined. Physical attacks, electromagnetic attacks, cyber attacks, or a combination of all of these methods can occur on a network if the terrorist or group is well trained.[32]

[31] Joyce E. Elliott, Colonel, "Cyber Terrorism: A Threat to National Security," Strategy Research Project, U.S. Army War College, April 9, 2002.

[32] Investigative Research for Infrastructure Assurance (IRIA) Group – Institute for Security Technology Studies, "Information and Telecommunications Sector Vulnerabilities and Threats," (Hanover, DE: Dartmouth College, 2002), 2.

2. Physical

Physical attacks like 9/11, using sophisticated hi-jacking schemes, take an enormous amount of money and training, but simple Vehicle Borne Improvised Explosive Devices (VBIEDs)—like the ones used daily in Iraq—are probably the most likely and, potentially, the most deadly. Physical threats are probably the greatest threat to critical communication nodes like telecom hotels and NAPs. Aside from the potential loss of life, there is also a major financial loss in the equipment in a telecom hotel, and additionally a great psychological aspect when people cannot communicate or get information after an attack. The easiest and most likely physical attack would come from a bomb or IED (Improvised Explosive Device). These take minimal skill to put together, are easy to acquire, and simple to deploy. The effects of a simultaneous attack on half a dozen critical nodes could cause a major regional outage for at least short amounts of time. One problem with Telcos is that the perception of the likelihood of a major attack is comparatively low when analyzing it with the routine damage and disruptions like the accidental damage to telecommunications lines from a backhoe.

Electromagnetic (EM) attacks, Electromagnetic Pulse (EMP) or High Powered Microwave (HPM) could be the most economically devastating weapons. EMP, RF (Radio Frequency), or HPM, while possible, have been considered unlikely in both the September 2002 study, "Information and Telecommunications Sector Vulnerabilities and Threats," by the Investigative Research for Infrastructure Assurance (IRIA) Group's Institute for Security Technology Studies[33] and by all service providers surveyed. Most buildings are not fully hardened, but are RF shielded/protected and not vulnerable to less sophisticated weapons of this nature. It is easy to recognize the old Bell Central offices, as they are typically square brick buildings with no windows, part of the shielding design. Smaller powered attacks would result in a computer re-boot or a dropped call without any major damage. Also, even a major RF type attack would result in equipment failure or damage, but no personnel casualties.

Lastly, a chemical, biological, or radiological attack is possible against a telecom hotel. Most of the buildings do not have adequate ventilation or filtration systems and

[33] IRIA Group, *Institute for Security*, 2002, 2.

would be susceptible to such an attack. The result would be limited, as the buildings typically house enormous amounts of equipment and not many telecom personnel. Most equipment would continue to run after such an attack, so an open-air gathering place, such as a sporting event or mall, would be a more likely place of attack.

3. Cyber

Cyber attacks, Denial of Service (DoS), worms, virus attacks, and hacking may be the most difficult to deter. Cyber attacks (termed Network Centric Warfare, or NCW, by the military) on our military, economic, or telecommunications infrastructure can now be launched from all reaches of the globe, and can be used to transport the problems of a distant conflict directly to the homeland.[34] There is a growing connectivity between secure and insecure networks, creating new opportunities for unlawful intrusions into sensitive or proprietary computer systems within critical U.S. infrastructures, such as the nation's telephone system. Companies make it easier to control their networks from remote locations to save on the costs of physically traveling to fix or upgrade software or services. This operations advantage is also a security disadvantage. Allowing company access to remote terminals or servers can also allow unauthorized access to the same facilities. Another issue with protecting the telephony critical infrastructure is that the complexity of computer networks is growing faster than the ability to understand and protect them. Proprietary information makes it difficult to identify critical nodes, verify security, and monitor activity of these networks.

More resources are being dedicated for Critical Infrastructure Protection, but there is an insufficient amount being spent on stopping a well-planned cyber attack. A successful cyber attack on routers or DNS servers would require a high level of technical ability, but would be devastating to the IT community. There are many cyber controls (firewalls, system configurations, intricate password systems, awareness training, and new standards for IP security) available to prevent cyber terrorism. One problem is that these controls are underutilized and sometimes bypassed by security personnel for ease of running the network. One of the most damaging cyber scenarios includes an insider who

[34] Jacques S. Gansler and Hans Binnenkijk, "Information Assurance: Trends in Vulnerabilities, Threats, and Technologies," Working Paper, National Defense University, 2003, 21.

has specialized knowledge and is working for a foreign nation or terrorist group. While the damage of this scenario is catastrophic, the likelihood is deemed as low.

Now that the threats are known, who are the actors that will attack these networks? Al-Qaeda has previously been mentioned as one of the groups of terrorists willing to attack. Another group are the hackers who threaten networks for thrill or notoriety, but aren't a major threat to critical defense infrastructure. The next group is labeled "Hacktivists" and is a slightly bigger threat, because such people possess a motive to carry out an attack.[35] This group uses hacking to further its activist goals. Another medium-level threat is from industrial spies and organized crime groups. Their motivation is monetary and must be considered a potential threat. Terrorists are at the top of the list for many, due to the malice they have for those who are against their cause. Many people discount the terrorists' abilities to conduct a cyber attack because of their apparent preference for deadly explosions versus attacks that may create an economic downturn or limited network chaos. One of the largest threats for the U.S. Military is from state actors and national governments.[36] These cyber warfare programs are more sophisticated and receive the required funding. Even if their only purpose is to gather information, rather than shut down military systems, a disclosure of classified information to these entities could be devastating to national security. One of the fears from any of these groups is that technology will feed into new methods or complexity of cyber attacks. Some even fear software "agents" that have some form of intelligence to gather or conduct information operations.

4. DoD Example

U.S. government and defense networks are becoming increasingly reliant on the private industry. Commercial software is also replacing relatively secure proprietary network systems by U.S. telecommunications providers and other operators of critical infrastructure. As more and more U.S. software companies go offshore for their

[35] Lawrence K. Gershwin, "Cyber Threat Trends and U.S. Network Security," Statement for the Record to the Joint Economic Committee, National Intelligence Council, June 21, 2001. [http://www.cia.gov/nic/NIC_speeches.html] Accessed September 17, 2005.

[36] Lieutenant General Kenneth Minihan, USAF, "Vulnerabilities of the National Information Infrastructure," Testimony to the Senate Governmental Affairs Committee Hearing, June 24, 1998. [http://hsgac.senate.gov/62498minihan.htm] Accessed September 17, 2005.

programming expertise, many of these products will provide opportunities for foreign exploitation or insertion of attack tools, threatening national security. Convergence of voice, data, and video onto one network is leaving the military susceptible to a physical attack on critical infrastructure, just as convergence to a few software systems makes the nation more vulnerable to a cyber attack. A final note on commercial software reliance is that as the technology revolution continues, civilian technology will increasingly drive military technology, and enemies will be able to concentrate their attack on the less secure civilian sector, thus causing a cascading effect to the defense sector.

Is a successful attack, either cyber or physical, possible? Using the DoD networks, which are some of the most protected networks available as an example, the answer is an astounding *yes*. ER 97, or Eligible Receiver 1997, was a JCS (Joint Chiefs of Staff) exercise to check the vulnerabilities in the military's critical infrastructure and computer networks. Four days of hacking, using COTS (Commercial Off The Shelf) products, crippled the DoD computer systems.[37] The exercise utilized hackers from NSA to attack DoD networks using commercially available tools. The results showed DoD not only that vulnerabilities existed in the national information infrastructure, but that deficiencies also existed in the ability to counter or respond to those attacks. There is a close connection between telecommunications networks and the internet, in that all internet traffic rides on telecom infrastructure due to convergence. Not only are phone calls to mom affected in a failure, but also all internet traffic. This includes B2B (Business to Business) traffic, banking/financial market transactions, and all government coordination activity and email. Again, this was evidenced by both the first World Trade Center attack and the events of 9/11.[38] The devastating effects of taking out a small portion of the telecom infrastructure were evident, as virtually all communications in lower Manhattan were inoperable on September 11, 2001. Among the hardest hit were services provided by the telecom giant Verizon.[39]

[37] Minihan, *Vulnerabilities*.

[38] U.S. GAO, "Potential Terrorist Attacks," Report to House of Representatives, Committee on Financial Services, GAO-03-414, February 2003.

[39] Robert F. Dacey, Director, Information Security Issues before the House of Representatives, Subcommittees on Cybersecurity, Science, and Research & Development and Infrastructure and Border Security, Select Committee on Homeland Security, U.S. GAO, GAO-04-699T, April 21, 2004.

Is it really feasible that terrorists would get into the most vital systems, or is this just in theory? A presentation from the SANS Institute listed the .mil or .gov domains that had been hacked within a 100-day window. Thirty-seven sites were listed, including web sites maintained by the Army, Navy, and NASA.[40] The presentation goes on to discuss how companies like Microsoft issued security bulletins to warn their users of vulnerabilities in the programs. This concept also lets potential hackers know of the same vulnerabilities. At that point, the race is on for hackers to develop malicious code to attack a system and for company programmers to develop a software patch to eliminate the vulnerability. More proof comes from testimony from the director of Central Intelligence to Congress that "computer-based information operations could provide the enemy with an asymmetric response, thus degrading the U.S. military superiority, and that attacks on the military or telecommunications infrastructure can be launched from anywhere in the world."[41]

The "Honeynet Project" was a study in which computers were placed on the Internet to see how quickly hackers would find and attack them. The average timeframe was eight hours, but, if on a university system, the average time was reduced to only 45 minutes.[42] Further proof that vulnerabilities exist is found in the testimony of Lieutenant General Minihan, who was the director of the National Security Agency (NSA) at the time of this Senate Committee Hearing. One example mentioned in his statement was that the nation, and specifically DoD, faces significant threats due to its dependence on cyberspace and worldwide connectivity.[43] He also emphasized the vulnerabilities through the previously noted Joint Chiefs of Staff (JCS) exercise, Eligible Receiver 97.

F. VULNERABILITIES

The majority of the telecom infrastructure protection problem lies in its vulnerabilities. It is difficult to determine the amount of vulnerability within the sector, as

[40] Alan Paller, "Fighting Back Against Cybercrime: What Works?" The SANS Institute, 2004. [www.sans.org] Accessed September 17, 2005.

[41] Gershwin, *Cyber Threat Trends*.

[42] Ibid.

[43] Minihan, *Vulnerabiliti*es.

much of it is privately owned. In addition, if there are vulnerabilities, no company or government office or agency would want to reveal such weaknesses. Some of these vulnerabilities are based in the economics of scale and the technology improvements within the telecom and IT (Information Technology) fields. The evolution of switching technology is one development that has resulted in a concentration of assets, or clustering.. There is a concentration of control in switches, due to fewer switches being deployed, and therefore a greater susceptibility to damage from a terrorist attack. The continued concentration of an assortment of transmissions into single large buildings, due to convergence, has already been mentioned. This has changed the infrastructure into a series of key critical nodes or key assets. A catastrophic failure to such a building would cause a disruption of almost all communications, to include internet services (email, LAN, WAN, dial-up services), wireless internet, local and long distance phone service, cellular phone service, satellite communications, and paging services from an abundance of telecom or internet service providers.[44]

General weaknesses reported in open source publications have listed several areas of vulnerability in telecommunications infrastructure, to include telecom hotels, Internet peering points, trusted access to telecommunications facilities, equipment chain of control issues, cable landings, and International Gateways (locations where internet and voice traffic arrives from submarine cable or satellite downlinks). There are only a few connections points for traffic with Europe and Asia. These physical facilities include thousands of switches and components that make up the telecom infrastructure.

Another concern in the overall telecom infrastructure is the vulnerability of two billion miles of underground fiber in many remote areas, primarily along easements and rights of way. There are larger amounts of traffic being transmitted along these optical fibers, which allow fewer transmission routes and increased concentrations of traffic along less diverse routes.

[44] Pete Moulton, “Can Your Network Hold Up to Terrorism?” (Prentice Hall PTR, January 25, 2002). [http://www.phptr.com/articles/article.asp?p=25087] Accessed September 17, 2005.

Lastly, the Public Switched Telephone Networks (PSTN) are very reliant on software in a time when computer viruses and worms are becoming more and more prevalent.

Possibly the best list of telecom vulnerabilities, compiled by the Network Reliability and Interoperability Council (NRIC) VI,[45] listed eight separate influences in the telecommunications industry that could conceivably be vulnerabilities:

- Environment: Buildings, conduits, right of way
- Power: Interdependency with Power sector, HVAC, batteries, generators
- Hardware: Hardware frames, electronics, copper and fiber optic cables
- Software: Software releases, beta or test loads, version management and control
- Networks: Configuration of NEs (Network Elements), types of networks, Protocols, diversity
- Payload: Data packets, overhead, statistics, corruption
- Policy: Industry standards, governmental mandates, legal issues
- Human: Deliberate and accidental behavior, education

[45] Network Reliability and Interoperability Council VI, Homeland Security Physical Security Focus Group 1A, Prevention Report Issue 1, December 2002.

THIS PAGE INTENTIONALLY LEFT BLANK

III. VULNERABILITY ANALYSIS

Because there is no standardized methodical approach for analyzing complex networks, managers of these networks are restricted in their capability to identify and reduce vulnerabilities. Current network assessment methods and protective measures are not deliberate actions, and the need for a scientific methodology for implementation of critical infrastructure protection is required. Also, it is economically impossible to eliminate all vulnerabilities, so prioritization of funds must occur. A recent proposal, called Model-Based Vulnerability Analysis (MBVA), merges analysis with risk assessment and risk reduction.[46] Another method is the Department of Defense's Core Vulnerability Assessment Management Program (CVAMP).

A. MBVA

While telecom hotels have existed in one form or another for years and have been determined to be a vulnerable aspect of the telecommunications sector, there have been no studies to assess the specific vulnerabilities, or methods to remedy or reduce those vulnerabilities. This research is intended to serve as a basis for evaluating telecom hotel vulnerabilities and establish a standard for all private industry infrastructure owners. An initial assessment of telecom hotels will be made using the Model-Based Vulnerability Analysis (MBVA) method. There are five steps in that provide a comprehensive method of analysis: [47]

a. Asset Inventory
b. Network Analysis
c. Fault Tree Analysis
d. Event Tree Analysis
e. Budget Allocation

[46] Ted G. Lewis, *Critical Infrastructure Protection in Homeland Security: Defending a Networked Nation*, (Hoboken, NJ: John Wiley & Sons Inc., 2004).

[47] Ibid.

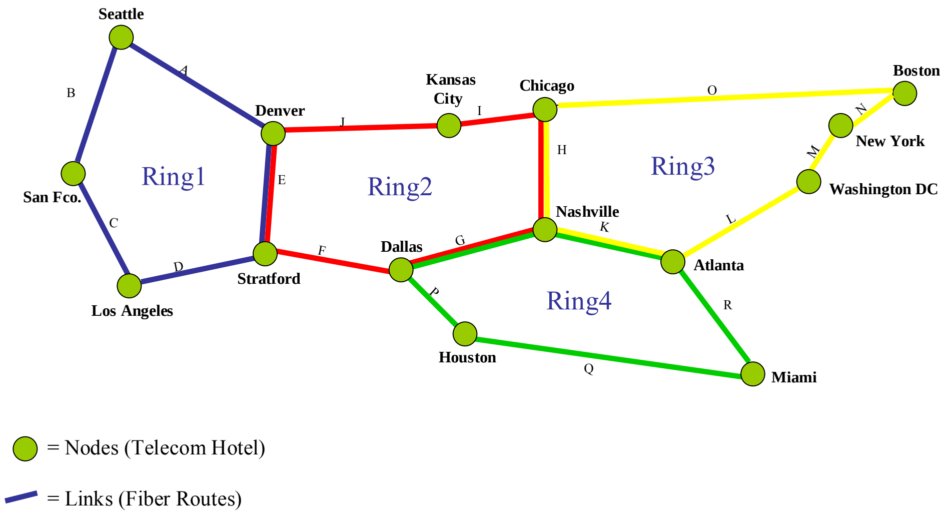
1. Telecom Hotel Example MBVA

The first step in the MBVA process is building an inventory of all assets that comprise the infrastructure. This starts with the vulnerabilities listed above and include environment, power, hardware, software and human. The list is limited to those vulnerabilities associated with telecom hotels.

- Environment: buildings, conduits, and risers where fiber enters and exits the building, air conditioned spaces with fire protection
- Power: HVAC, backup power, batteries, generators
- Hardware: due to convergence, almost all types of telecom and IT equipment would be present in a telecom hotel, including switches, routers, hubs, transmission equipment, multiplexors, computers, fiber, copper, cat 5 cabling, equipment racks, etc.
- Software: software releases, beta or test loads, network operations management software
- Payload: the type of data and services provided by operators
- Human: personnel operating out of the telecom hotel

Other items that are not located with the telecom hotels, but need to be included due to association, are the network operations centers, data backup, and storage centers, and diverse routing of all networks that are present within the telecom hotel. One point of distinction is that the list above would be accurate for an ILEC who is responsible for both the building and his own network. One of the problems with CIP, in reference to a telecom hotel, is that there are several different responsibilities in which everyone must play his part. In a neutral telecom hotel, the building owner and management are only looking at the aspects of the building. Service providers and operators are only looking at the equipment and assets within their designated colocation spaces. This makes it difficult to determine the effects of the loss of a telecom hotel as there are many tenants with very different types of networks and services.

The next step in the MBVA process is to construct a network model to show relationships and linkages.



Note: Colors used to denote ring topology used to build in redundancy

Figure 5. Generic Nationwide Fiber Network.

This modeling will assist in determining if the network is scale free, small world, or random. The first two are defined in Network Theory as complex networks and the latter is a simple network. Scale free networks have a few highly connected "hubs" and the rest of the nodes have a low degree of connections. Small world networks are nodes that can reach all other nodes with a small number of hops and similarly illustrates the hypothesis of six degrees of separation between all persons on earth. Random networks are as defined, random and unstructured.[48] At this point, network hubs or critical nodes and links are identified. The example uses an entire fiber optic network as seen by an IEC. In actuality, there would be hundreds of metro fiber rings located throughout a major city that would connect through a telecom hotel and identify it as the critical node. For simplicity, and lack of access to this detailed proprietary information, a basic national view was used. Perhaps a different picture is required to demonstrate the single point of failure in getting to the IEC backbone. Also, note the bigger "pipes" associated with the COs and telecom hotel on the right side of the diagram.

[48] Ted G. Lewis, *Critical Infrastructure Protection*).

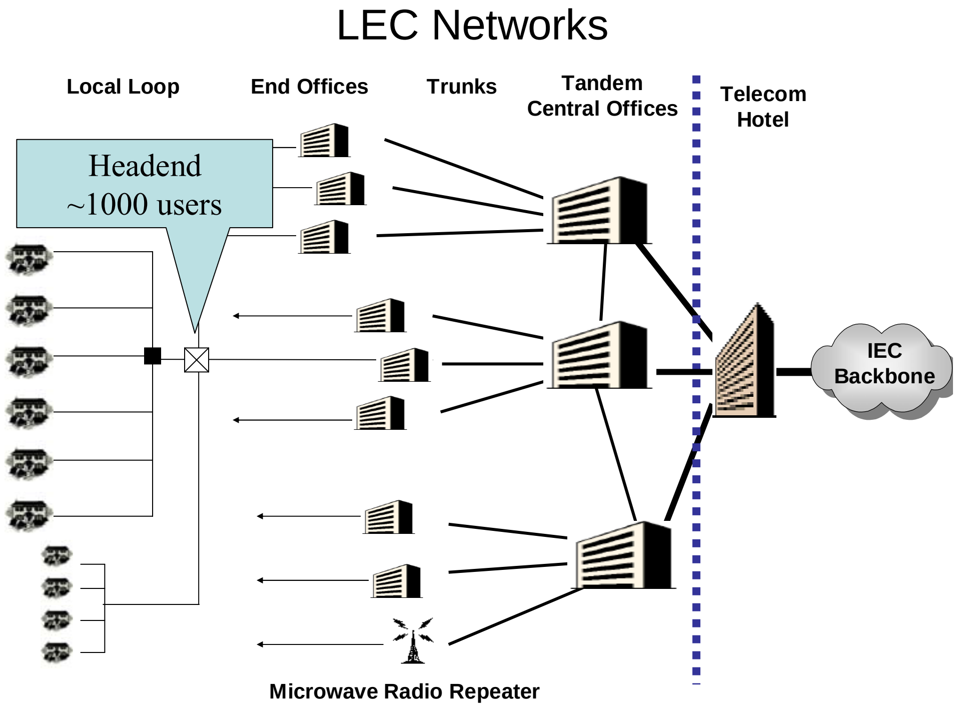


Figure 6. LEC connection to IEC network via Telecom Hotels.[49]

Using the scale free test histogram, it can be seen that the network is, in fact, scale free. One other observation from the topology diagram, above, is that there are no critical links in the fiber routes. This is due to the diversity and redundancy of a ring topology.

[49] Ted Lewis, "Critical Infrastructure Protection."

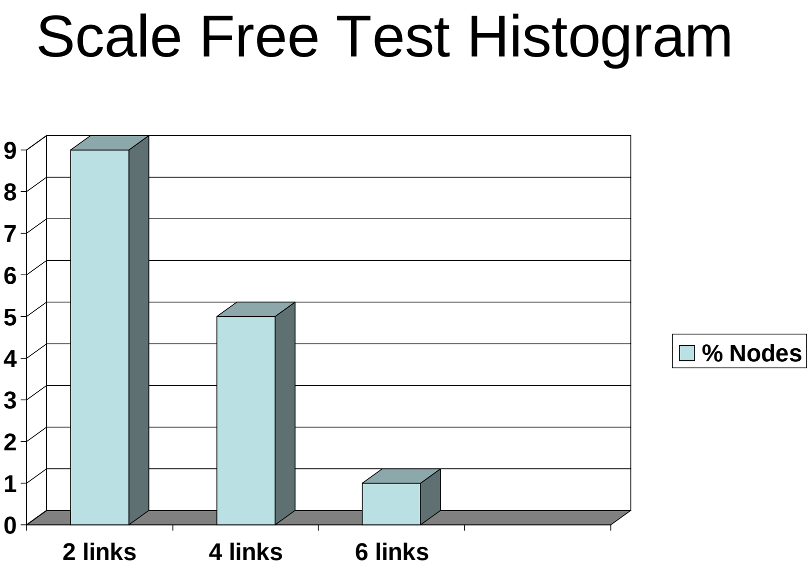


Figure 7. Scale Free Test Histogram

The third step is building a fault tree and recognizing specific vulnerabilities that are associated with the critical node that was identified in the previous step. Fault tree models depict potential vulnerabilities associated with the hubs from the initial network modeling. This illustration depicts a failure to a telecom hotel and the vulnerabilities that are associated. Analyzing the fault tree model using an event tree is the fourth step in the MBVA process. Fault tree analysis depicts all possible faults and estimates their probability of successful attack resulting in a failure.

It is important to state that the probability assumptions noted in the subsequent illustrations are only assumptions. The examples precisely demonstrate the need to employ an appropriate methodology like the in-depth analysis of JSIVA, to establish the likelihood of component failure. The results of JSIVA, or other vulnerability assessment tools, would be complementary to the MBVA process, especially when allocating limited funding. For the illustration, percentages were scaled for the probability of the threat succeeding if an attack occurred. Five percent was considered a low threat, 15% would be a medium threat, and 25–30% was considered to have a high probability of success.

The probabilities in the example are estimates from the subject matter experts who were interviewed during the research process. Their experience and knowledge are from engineering and physical security backgrounds in the telecommunications sector. Sources of estimates for probabilities could also come from historical data, exercises, or simulations if this expertise is not available.

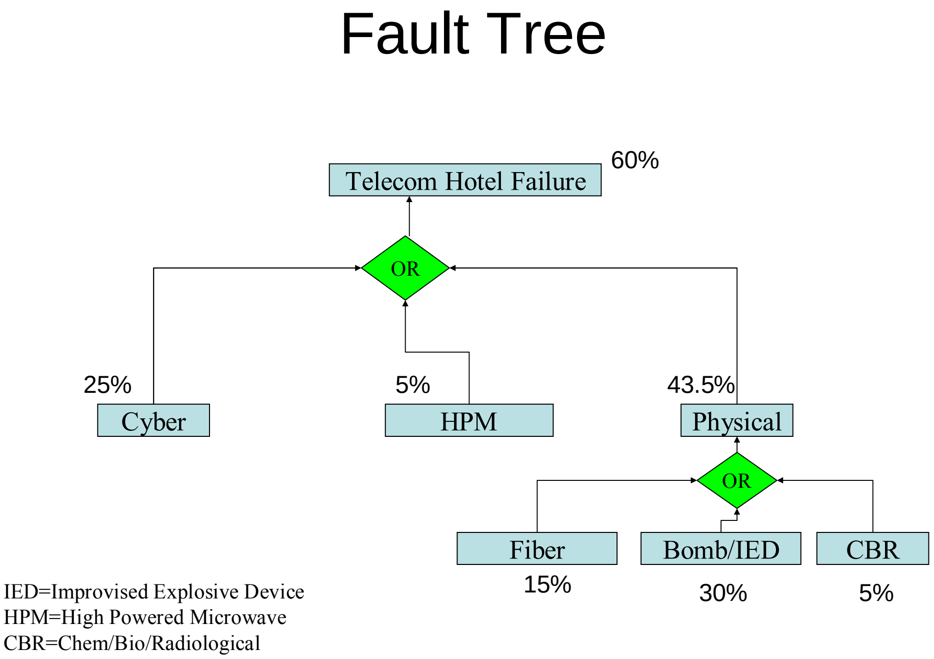


Figure 8. Fault Tree Analysis for Telecom Hotels.

The event tree illustrates the enumeration of all possible outcomes of the fault tree and shows the consequences of a failure or adverse event. Starting with an initiating event, the consequences are followed through a series of possible paths, and each path has an assigned probability of occurrence. For N vulnerabilities in the fault tree, there are 2^N possible outcomes in the event tree. In the example, five vulnerabilities give 32 possible outcomes. The total probability of successful attack resulting in failure in this example is 60%, which is the same result determined by both the fault tree and event tree analyses.

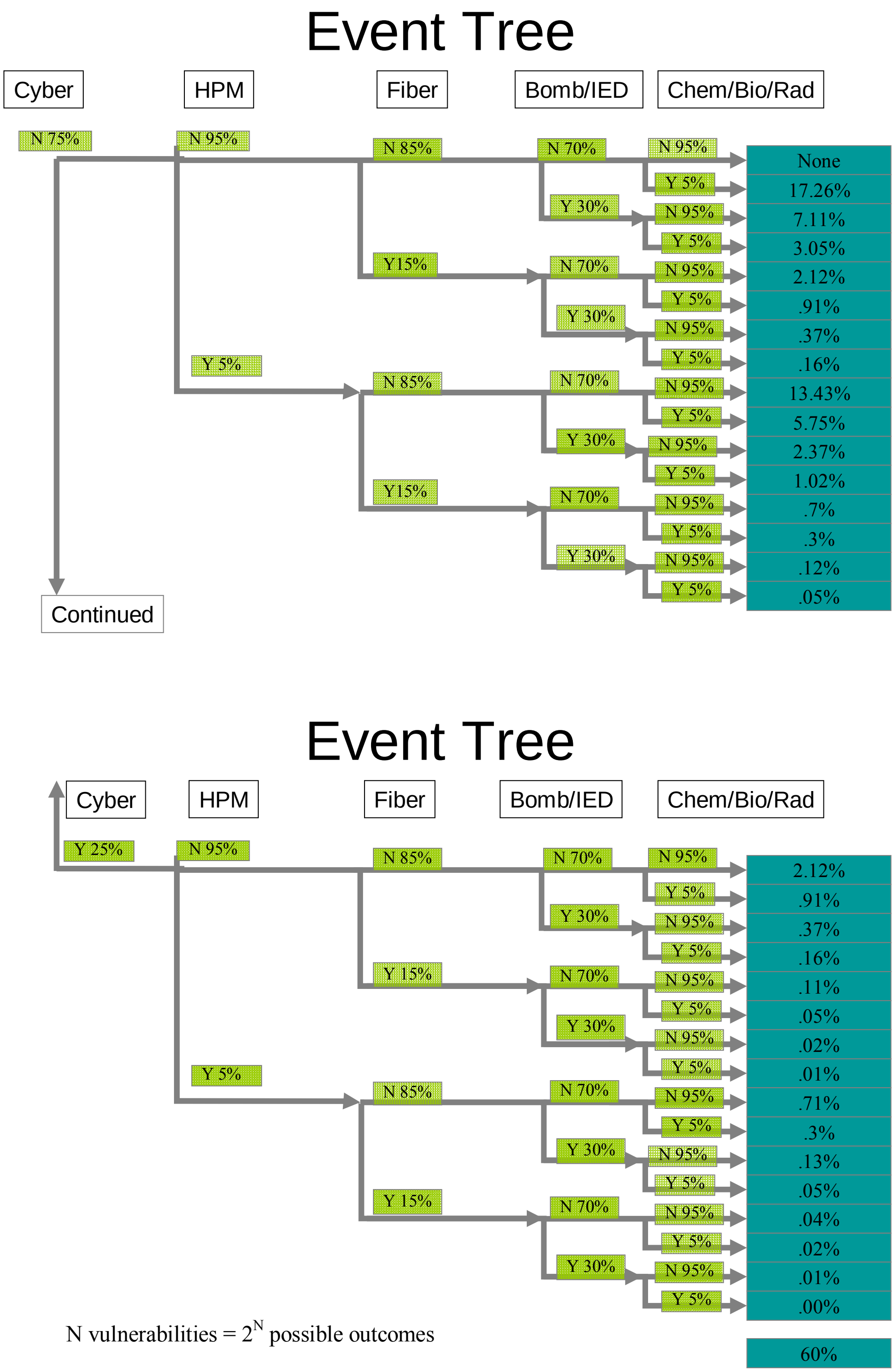
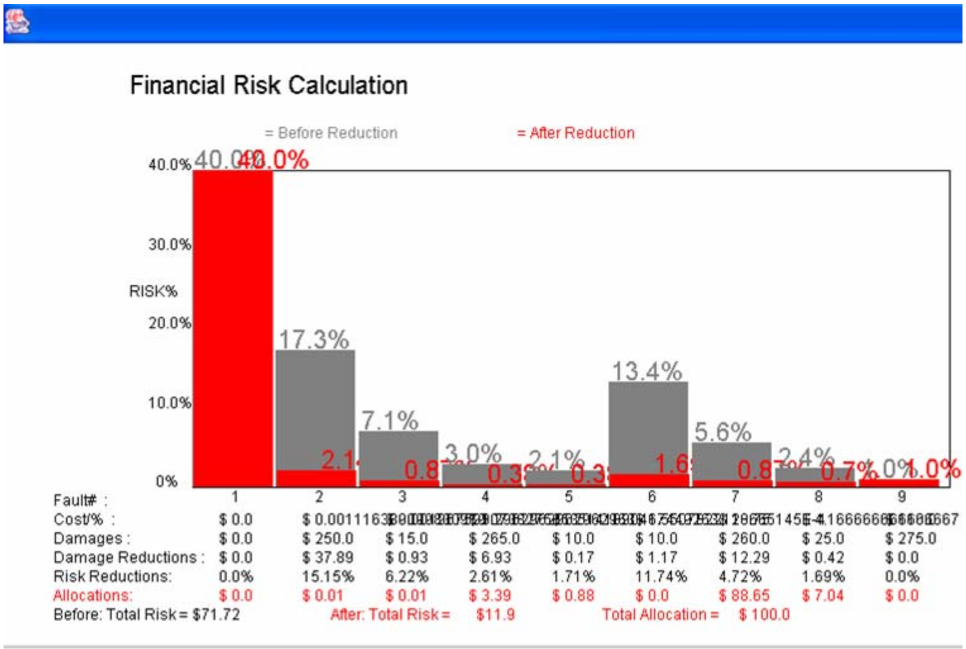


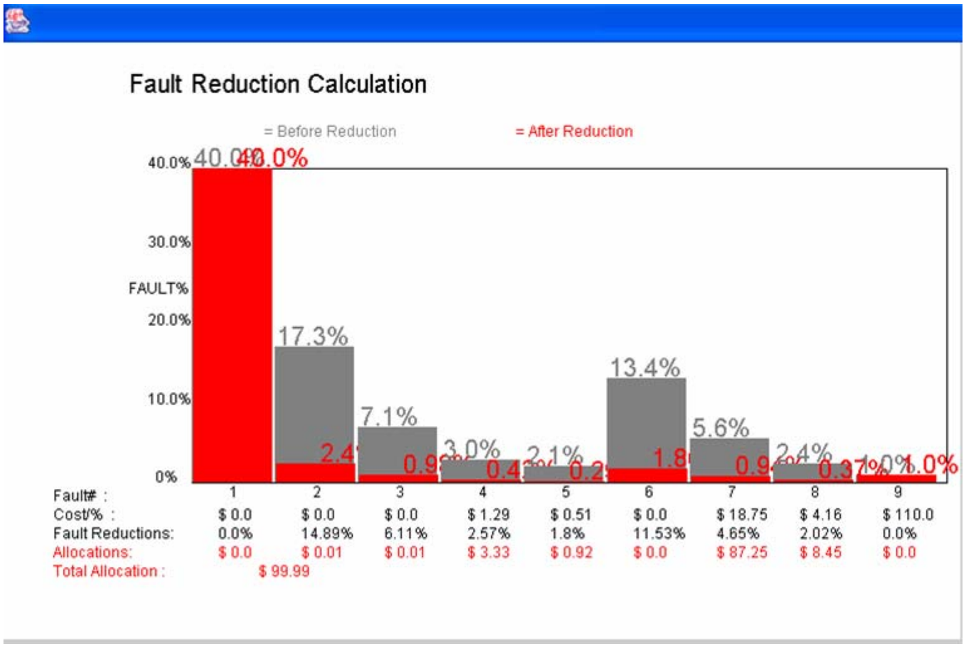
Figure 9. Event Tree Analysis for Telecom Hotels.



Financial Risk Calculation

Fault# :	1	2	3	4	5	6	7	8	9
Cost/% :	$ 0.0	$ 0.0011163[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
Damages :	$ 0.0	$ 250.0	$ 15.0	$ 265.0	$ 10.0	$ 10.0	$ 260.0	$ 25.0	$ 275.0
Damage Reductions :	$ 0.0	$ 37.89	$ 0.93	$ 6.93	$ 0.17	$ 1.17	$ 12.29	$ 0.42	$ 0.0
Risk Reductions:	0.0%	15.15%	6.22%	2.61%	1.71%	11.74%	4.72%	1.69%	0.0%
Allocations:	$ 0.0	$ 0.01	$ 0.01	$ 3.39	$ 0.88	$ 0.0	$ 88.65	$ 7.04	$ 0.0

Before: Total Risk = $71.72 After: Total Risk = $11.9 Total Allocation = $ 100.0



Fault Reduction Calculation

Fault# :	1	2	3	4	5	6	7	8	9
Cost/% :	$ 0.0	$ 0.0	$ 0.0	$ 1.29	$ 0.51	$ 0.0	$ 18.75	$ 4.16	$ 110.0
Fault Reductions:	0.0%	14.89%	6.11%	2.57%	1.8%	11.53%	4.65%	2.02%	0.0%
Allocations:	$ 0.0	$ 0.01	$ 0.01	$ 3.33	$ 0.92	$ 0.0	$ 87.25	$ 8.45	$ 0.0

Total Allocation : $ 99.99

Figure 10. Financial Risk and Fault Risk Calculations.[50]

[50] Center for Homeland Defense and Security, Allocate Simulation, August 2005. [https://www.chds.us/course/studies.cfm?course_id=77&cci=animation_test] Accessed September 17, 2005.

The final step in the MBVA process is analyzing the budget to optimally allocate resources. This involves developing an investment plan that minimizes the chances of faults occurring, as identified by the fault distribution.

In this case, both the fault reduction program and the financial risk program calculated very similar results. This is due in part to many of the failures having similar estimated damage costs and recovery costs. The main emphasis is to allocate 89% of resources toward reducing cyber and bomb attacks. Another 7% will be allocated toward both cyber and fiber protection, and 3% should go toward reducing fiber and bomb vulnerabilities. Allocating resources in this way, the associated risk will be reduced from 72% down to 12%.

There are advantages and disadvantages to every vulnerability assessment methodology; MBVA is no exception. Model-based vulnerability analysis provides analysts with a comprehensive tool for accomplishing critical infrastructure protection under budgetary constraints.[51] MBVA is a thorough method of examination that brings together network, fault, event, and risk analysis, as an integrated process in an effort to mathematically optimize, quantitatively evaluate, and justify funding for critical nodes such as telecom hotels.[52]

A limitation of model-based vulnerability analysis is that fault and event trees are static in nature and do not provide sequencing of events. Numerous fault trees would be required to analyze an entire sector, and once that was done, the resulting event trees would grow at an alarming rate. For N vulnerabilities in a fault tree, one must list 2N possible outcomes in the event tree. Also, because it is often difficult to obtain valid systems reliability data from vendors, the probabilities derived from a quantitative FTA are approximate in nature. It is also necessary to be able to estimate the probability of a successful attack and the costs associated, and these will be approximate at best. Lastly, “least squares” is used in the optimization during the allocation phase, which can be sensitive to estimates.

[51] Ted Lewis, *Critical Infrastructure Protection*.

[52] Ibid.

Despite the limitations, MBVA provides an essential methodology needed to prevent, protect, and mitigate damage to critical telecom hotels, while effectively examining associated risks. MBVA also assists with the management of limited resources by concentrating on the identification of critical nodes and the prioritization of "hardening" the most important systems.

B. CVAMP

Core Vulnerability Assessment Management Program is a DoD web-based application that captures results of vulnerability assessments, prioritizes areas of responsibility vulnerabilities, identifies deficiencies, and lists corrective actions needed or completed.[53] Vulnerability Assessments are typically conducted using the DoD standard, JSIVA, or Joint Staff Integrated Vulnerability Assessment.

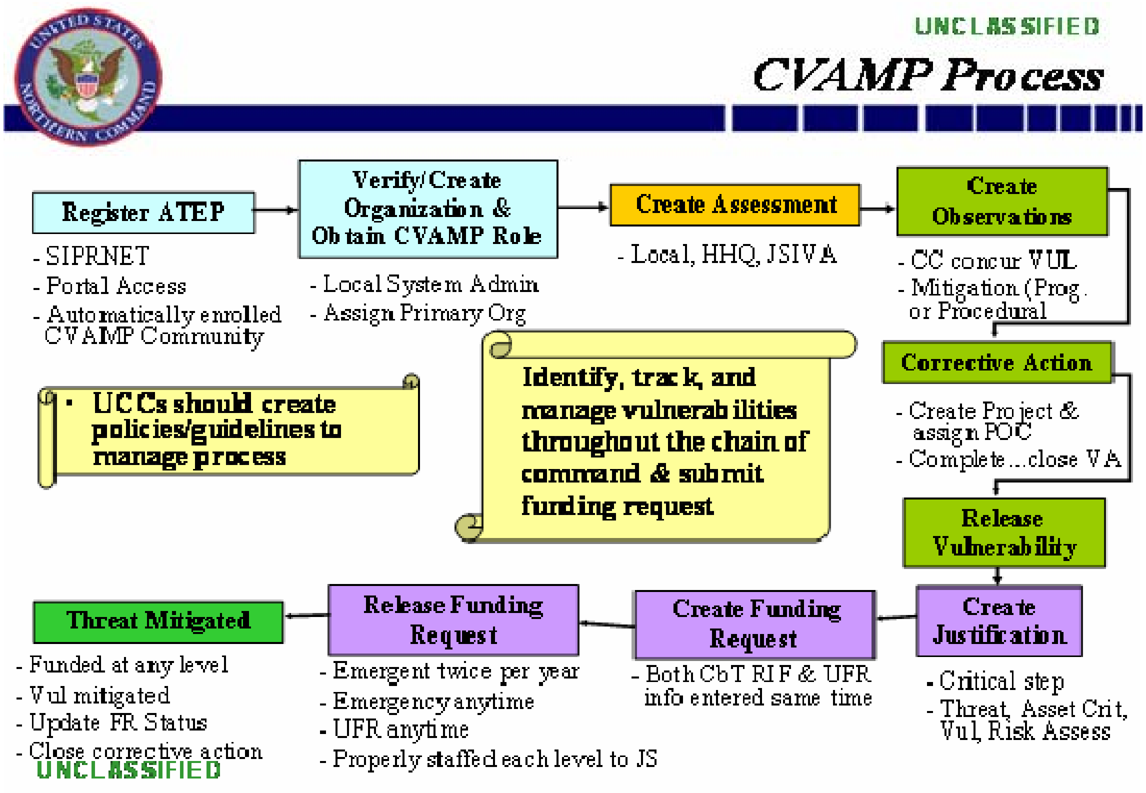
Figure 11. 365 Main Building, San Francisco.[54]

[53] Defense Threat Reduction Agency Link, Combat Support. [http://www.dtra.mil/toolbox/directorates/cs/programs/assessments/joint_staff.cfm] Accessed September 17, 2005.

[54] 365 Main Inc. [http://www.365main.net/company.html] Accessed September 17, 2005.

CVAMP was initially developed by U.S. European Command and has been in use since 1998. It has since been adopted by all services and combatant commands. Initially, many commands had inadequate Anti-Terrorism/Force Protection (AT/FP) vulnerability management programs. DoD Directive 2000.12 (Aug 2003) addressed this shortfall and directed the Joint Staff to maintain a centralized vulnerability database.[55]

This program is only accessible on the Secret Internet Protocol Router Network (SIPRNET) to authorized users via the Antiterrorism Enterprise Portal (ATEP). The CVAMP Process has several steps that include tracking and managing AT vulnerabilities, generating justification for requirements to resolve vulnerabilities, standardizing and automating the AT resource request process, and highlighting AT readiness shortfalls due to unmitigated vulnerabilities.



UNCLASSIFIED

CVAMP Process

Register ATEP
- SIPRNET
- Portal Access
- Automatically enrolled CVAMP Community

Verify/Create Organization & Obtain CVAMP Role
- Local System Admin
- Assign Primary Org

Create Assessment
- Local, HHQ, JSIVA

Create Observations
- CC concur VUL
- Mitigation (Prog. or Procedural

Corrective Action
- Create Project & assign POC
- Complete…close VA

Release Vulnerability

Create Justification
- Critical step
- Threat, Asset Crit, Vul, Risk Assess

Create Funding Request
- Both CbT RIF & UFR info entered same time

Release Funding Request
- Emergent twice per year
- Emergency anytime
- UFR anytime
- Properly staffed each level to JS

Threat Mitigated
- Funded at any level
- Vul mitigated
- Update FR Status
- Close corrective action

- **UCCs should create policies/guidelines to manage process**

Identify, track, and manage vulnerabilities throughout the chain of command & submit funding request

UNCLASSIFIED

Figure 12. CVAMP Process.[56]

[55] Major Robert Gray, USAF, J34 Assessments Branch. [https://www.noradnorthcom.mil/j3/j34] Accessed September 17, 2005.

[56] Ibid.

Once a person gains access to ATEP, he or she can follow the process, which eventually results in the threats being mitigated. The main steps are: to create the organization, to create a vulnerability assessment using JSIVA, to create observations and respective corrective actions, to release the vulnerability and create a justification, to create and release prioritized funding requests, and to mitigate the threat once funding is received.

This methodology follows a different funding procedure. Rather than assign funds that will go into CIP, the CVAMP process discovers vulnerabilities that must be mitigated and then acquires the funding to mitigate the threat. Using this procedure, funds are not spent only in areas of homeland security that have no requirement. This also ensures that funds are put into the programs where justified and not "skimmed off" to pet projects or non-critical mission areas. There are two funding mechanisms in this process. The first is a special fund for combating terrorism and is called the Combating Terrorism Readiness Initiatives Fund (CbTRIF). The second mechanism is an Unfunded Requirement (UFR) as part of the DoD Planning, Programming, Budgeting and Execution (PPBE) System.

1. JSIVA

Possibly the biggest part of the CVAMP program is the Joint Staff Integrated Vulnerability Assessments (JSIVA) process. This was initially a Defense Threat Reduction Agency (DTRA) derived model that was conducted annually at DoD installations worldwide. The teams determine vulnerabilities and provide options to assist installation commanders in mitigating or overcoming them. The JSIVA team concept was in place well before 9/11, and in fact, was formed following the 1996 terrorist attack on Khobar Towers, Saudi Arabia. A taskforce studied the security, force protection funding, resources and coordination of intelligence and antiterrorism countermeasures, not only at Khobar Towers, but across the board.[57] The report revealed that DoD did not have published standards for force protection at fixed facilities. A new instruction, DoD STANDARD 26: Higher Headquarters (HHQs) Vulnerability Assessments (VAs) (DoDI 2000.16, DoD AT Stds), requires each installation to have

[57] Defense Threat Reduction Agency Link. [http://www.dtra.mil/] Accessed September 17, 2005.

higher headquarters anti-terrorism and force protection assessments at least every three years. DTRA continues to help installations meet this requirement, along with service and combatant command AT/FP personnel through JSIVAs.

The JSIVA process takes an all hazards look at any military installation or facility. There are teams that conduct either a five-day JSIVA or a three-day Higher Headquarters Vulnerability Assessment (HHQVA) as mentioned above. This program is in the process of expanding into the Defense Industrial Base (DIB). The JSIVA teams consist of Subject Matter Experts (SMEs) in the following areas: Security Operations (Blue Team), Terrorist Operations (Red Team), Emergency Management (CBRNE, Medical, Fire vulnerabilities), structural engineering, and infrastructure (cyber, tenant commands, other areas). Once the vulnerability assessment is accomplished, the results are briefed to the base commander. A final report is completed approximately 60 days later; the results go into the CVAMP database and are also sent to the appropriate service chain of command and the secretary of defense.

As part of the JSIVA, the Carver Matrix is used to provide both an offensive and a defensive methodology. A qualitative and quantitative vulnerability assessment is used to evaluate a facility.[58] The following are the key factors of the Carver Matrix: criticality, accessibility, recoverability, vulnerability, effect, and recognizability. The Carver Methodology is also used in Target Analysis/Vulnerability Assessment (TAVA), which is used by the civilian sector. Another civilian tool used is a combination of Petri network theory and risk analysis. The following are the six steps involved in risk analysis that follow similar lines as both MBVA and JSIVA: 1) Identify system characteristics, 2) identify threats to network assets, 3) identify vulnerabilities to the specified threats, 4) identify methodologies and procedures to counter threats and reduce vulnerabilities, 5) identify residual risks, and 6) prioritize recommendations for reducing residual risks. A benefit of this process is that it looks at behavioral modeling of highly complex and highly distributed systems.

[58] "Target Analysis and Vulnerability Assessment," *Homeland Defense Journal Online.* [http://www.homelanddefensejournal.com/conf_TAVA.htm] Accessed September 17, 2005.

An even more in-depth assessment conducted by DTRA is called the Balanced Survivability Assessment (BSA). BSAs identify and assess vulnerabilities in the nation's critical infrastructure systems. It takes approximately three months for teams of 12–14 specialists to conduct these detailed, multidiscipline assessments of critical infrastructure key nodes. They recommend a series of changes to reduce vulnerabilities and continue to support long-term strategic risk management investment.

Figure 13. Telecom Hotel Interior View.[59]

2. JAT Guide

Another tool used by the military is the Joint Antiterrorism Program Managers Guide (JAT Guide). This is an electronic program management and decision aid tool to assist installation commanders in developing an antiterrorism program. The JAT Guide is a three-CD set that includes the requirements, planning processes, templates and tools to produce and manage a total antiterrorism program. The guide provides consistent and effective antiterrorism program management across the Department of Defense, and allows commanders to prioritize risk and compete for funding on an equal basis.[60] The JAT guide is modeled on and uses the military decision making process. The five-step process is: mission receipt, mission analysis, course of action (COA) development, COA approval, and orders production. This process is based on the commander's intent and

[59] Carrier Hotels. [http://www.carrierhotels.com/properties/ragingwire/index.shtml] Accessed September 17, 2005.

[60] U.S. Army Engineer Research and Development Center. [http://www.erdc.usace.army.mil/pls/erdcpub/www_org_info.show_page?f_id=143318&f_parent=55173] Accessed September 17, 2005.

can be analyzed using the following questions: what is the threat, what is critical, what are the risks, what are options to mitigate, and what is the plan? Military antiterrorism personnel can follow the same planning processes for antiterrorism program management.

C. ASSET PRIORITIZATION MODEL (APM)

CVAMP is a system that allows installation commanders to prioritize risk and compete for funding. The next program falls under the DoD responsibility for the Defense Industrial Base and is described as an asset prioritization model. It was developed by the Defense Contract Management Agency (DCMA) and provides a process for sector specific classification and subsequent prioritization of identified assets. Metrics are assigned to provide a “less subjective” means to categorize assets. The DIB is unlike other CIP sectors as there are fewer tendencies to be networked together. There are still many essential elements of the DIB that require a methodology to prioritize disparate critical infrastructure. The Defense Department identifies and prioritizes DIB critical infrastructure by analyzing them and their impact on military mission achievement, where mission analysis is the key.[61]

This Asset Prioritization Model (APM) is used for prioritization of DIB assets for both analysis and reduction of risk. The APM is an index model where the higher the score, the higher the risk, with scores ranging from 12 to 151. There are 13 distinct factors used to calculate the APM score that are classified into:

- Mission Impact
    - Dependency/Independency Metric
    - Impact on Current Warfighting Metric (not in dictionary)
    - Impact on Projected Warfighting Capabilities Metric
    - Recovery Plan Metric
- Political
    - Impact on Multiple Programs Metric,
    - Political and Secondary Effects Metric
- Threat
    - Chemical/Biological/Radiological/Nuclear/Explosive (CBRNE) Collateral Damage Metric

[61] Anti-terrorism/Force Protection Division, Defense Industrial Base. [https://www.noradnorthcom.mil/j3/j34] Accessed September 17, 2005.

    - Population Metric
    - Threat Metric
- Economic
    - The Financial Risk Metric
    - The Reconstitution Metric
    - Employment Impact Metric
- Other
    - Vulnerability Assessment

Impact on Current Warfighting Metric	
Number	**Factors**
1	A facility that produces no critical products for current missions.
2	A facility that produces one or more critical products, all with a short lead-time (under 60 days), but inventories are above requirements.
3	A facility that produces one or more critical products, with at least one long lead-time (above 60 days), and all inventories are at requirements.
4	A facility that produces one or more critical products, with multiple long lead time items, single source for one or more products, and shortfalls in inventory.
5	A facility that produces one or more critical products, with multiple long lead times, shortfalls inventory, sole source for one or more of those products, and a long surge requirement (30 days or more).
Notes:	Lack of data defaults to 2. Critical products determined by DPO-MA and other sources. Any item on a COCOM or DLA Warstopper list produced by a facility will likely place that facility at 2 or 3 automatically.
Data Source:	DLA, Services, Combatant Commands, DPO-MA, DCMA IAC Surveys and Analysis

Table 1. AMP Current Warfighting Metric.[62]

The purpose of the APM is to provide analysts with a quick means to prioritize DIB Critical Assets. The results of rigorous assessments, such as the other VAs above, are used in producing each metric and sub-metric through further analyses. The APM, along with JSIVA, could be used in other critical infrastructure sectors or sub-sectors like telecom hotels.

[62] Anti-terrorism/Force Protection Division, Asset Prioritization Model.

IV. FINDINGS

A. WHAT TELECOM COMPANIES ARE DOING

Through the course of this paper, several interviews were conducted, both in person and via telephone conversations. The interviews were conducted with all major entities of telecom hotels and include representatives from Interexchange Carriers (IECs, Long-distance Carriers), Incumbent Local Exchange Carriers (ILECs, former RBOCs), and Telecom Hotel Building Management Companies. Most did not want to be identified by name nor disclose the actual companies they worked for, which could have compromised any vulnerabilities that they were aware of. The position of the interviewees varied, but many were associated with the physical security of their organization. The following is the result of those interviews.

The first set of observations came from the IEC. The personnel did not want to comment on who owned their building. In many cases, the parent company initially owned the building, it was subsequently sold, and the buyers could not be named. These spaces are now leased back from the new owners or a third party management company. This would make sense in a business perspective to keep the benefits of a neutral carrier hotel. It is also possible that the ownership of the building was placed under a separate subsidiary or holding company for tax and liability reasons. The company had assigned personnel to a federal group, which worked on the federal customers and coordinated with the Department of Homeland Security. This company had colocation space in several of the large telecom hotels including the 111 Eighth and 60 Hudson locations in downtown New York City. The biggest threats that the personnel saw came from cyber and IEDs.

This company had not conducted vulnerability assessments on its locations, and background checks on personnel entering telecom hotels were up to the companies that they were working for. This company did conduct background checks on its workers. Most of the telecom hotels did not have standoff distance, as many are located directly next to the roads surrounding them. They did not have protection from chemical or biological attacks. Several security improvements had been made since 9/11 due to mandates, but the mandating authority could not be referenced. The company's main headquarters had stanchions put in to protect it from VBIEDs and to provide a standoff distance. Bulletproof glass was also installed in the headquarters, and security personnel were added. Other improvements included a second Network Operations Center (NOC) installed in a geographically separated location, and a secondary data backup added for system and network configurations. Most of the telecom hotels that they occupy had utilized biometrics in the form of palm readers and all had card access readers and security personnel on-site. They mentioned that they had 50–60 gateway locations that would qualify as telecom hotels. There were no additional funding sources or grants for any of the security improvements that had been made. The interviewees would not disclose the number of fiber routes entering and exiting buildings, nor would they answer questions regarding what the effects would be if one of the telecom hotels were disclosed. They did talk about diverse power grids with both battery and generator back-up. They also mentioned that there was equipment readily available in the event of a tragedy and vendors would place a priority in getting new equipment, as was done after 9/11. Most security information they mentioned was proprietary, but they revealed that they had northern and southern, physically diverse, fiber routes.

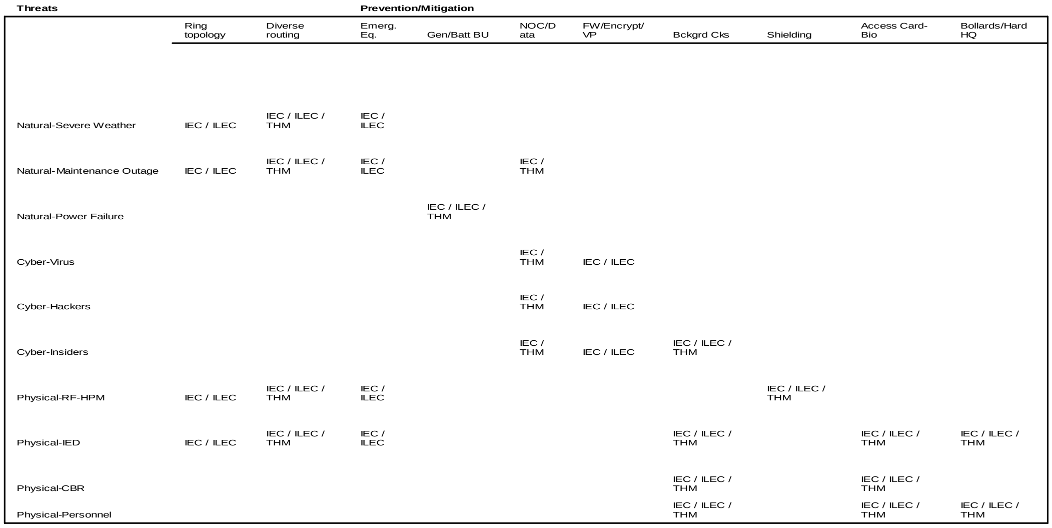
The next set of data came from ILEC interviews. Again, much of the information was proprietary and could not be disclosed for publication. The personnel were not able to comment on whether they owned the buildings or if the space was leased. They also did not have any chem/bio protection, but did not think it was a threat. HPM was not described as a threat due to the shielding as part of the infrastructure of the buildings. Even physical threats were not considered as a high priority because most terrorist attacks in the past have been to cause someone harm. The centers house mainly equipment and there was a minimal threat to personnel. Emergency equipment would be brought in and most services would be back up in three to four days. Cyber protection was the number one priority due to the many locations under their purview. This company had 11 data centers, 1,300 COs and over 30,000 other locations. It was estimated to cost over one billion U.S. dollars to secure all of the facilities. It could not be disclosed whether they had a backup NOC or the locations of either the primary or secondary NOCs. They mentioned that they conduct vulnerability assessments all of the time, but more based on physical security than homeland security. The assessments are based on the following methodology: what is the threat, what is the risk, what is critical, and what is lost? This is similar to what was discussed in Chapter III. It was discovered that they are using NRIC best practices as their minimum standards on the telecom side. They had to create their own IT side requirements. For physical security measures, they had card access alarms, security access, disaster recovery and business continuity programs in addition to some data center unique requirements. They did have a force protection type plan for their personnel, but it was more in reference to evacuation plans, fires, and natural disaster type events than one with a terrorism nexus. The items described as security improvements were in disaster recovery, increased security personnel, headquarters fortification, a separate management network and secure sites.

The last data set comes from management companies. Most of the buildings were owned by capital companies and the personnel that were interviewed worked for operations management or property management companies. They are in the business of colocation services and referred to it as "telecom real estate." They also conducted vulnerability assessments for the properties that they managed. In addition, they manage the diversification of the routes, either for fiber or other traffic, the redundancy of their operations centers, and the redundancy of data warehouses. They had multiple entry/exits for optical fiber routes. One question that was not answered was whether they saw the detailed descriptions of the buildings and locations as a vulnerability. One interesting note from one of these groups was that they had recently been visited by the Department of Homeland Security and that they had been identified as an interest. DHS conducted their research, but no results were relayed. One company had a consulting firm—Daniel, Mann, Johnson, & Mendenhall (DMJM)—conduct an assessment of the facility.[63] DMJM provides comprehensive planning, design services and consulting services as well as program management for architects, engineers, interior designers and planners. Based primarily on the results of this assessment, bollards were installed around the exterior of the facility, and card readers for interior security. Most of the

[63] Candela Spillis, , DMJM, Inc. [http://www.scpmiami.com/Firmprofile.htm] Accessed September 17, 2005.

modifications were implemented, but some were not. Most of the interviewees described their facilities as well-protected and all had some form of vulnerability assessments conducted. As you can see, the neutral telecom hotel property managers were the most proactive and forward about security measures. Part of their marketing plan is to provide safe, secure space and facilities to their customers, and it was in their best interest to make these security improvements.

The threat/mitigation matrix that follows summarizes what is being done by the IEC/ILEC and Telecom Hotel Management, respectively. The threats in Table 2 are based on telecom hotels in particular and match the threats section in Chapter II. The mitigation portion of this matrix is derived from the interviews with telecom company personnel.



Threats			Prevention/Mitigation							
	Ring topology	Diverse routing	Emerg. Eq.	Gen/Batt BU	NOC/Data	FW/Encrypt/VP	Bckgrd Cks	Shielding	Access Card-Bio	Bollards/Hard HQ
Natural-Severe Weather	IEC / ILEC	IEC / ILEC / THM	IEC / ILEC							
Natural-Maintenance Outage	IEC / ILEC	IEC / ILEC / THM	IEC / ILEC		IEC / THM					
Natural-Power Failure				IEC / ILEC / THM						
Cyber-Virus					IEC / THM	IEC / ILEC				
Cyber-Hackers					IEC / THM	IEC / ILEC				
Cyber-Insiders					IEC / THM	IEC / ILEC	IEC / ILEC / THM			
Physical-RF-HPM	IEC / ILEC	IEC / ILEC / THM	IEC / ILEC					IEC / ILEC / THM		
Physical-IED	IEC / ILEC	IEC / ILEC / THM	IEC / ILEC				IEC / ILEC / THM		IEC / ILEC / THM	IEC / ILEC / THM
Physical-CBR							IEC / ILEC / THM		IEC / ILEC / THM	
Physical-Personnel							IEC / ILEC / THM		IEC / ILEC / THM	IEC / ILEC / THM

Table 2. Threat Prevention/Mitigation Matrix.

IEC-Inter Exchange Carrier
ILEC-Incumbent Local Exchange Carrier
THM-Telecom Hotel Management
IED-Improvised Explosive Device
CBR-Chemical, Biological, Radiological Attack
Emerg. Eq.-Emergency Equipment
Gen/Bat BU-Generator/Battery Backup
NOC/Data-Network Operations Center-Data warehouse Backup
FW/Encrypt/VP-Firewall/Encryption/Virus protection
Bckgrd Cks-Background Checks
Access Card/Bio-Access Card Readers/Biometrics
Bollards/Hard HQ-Bollards/Hardening Headquarters

B. WHO IS IN CHARGE?

The last issue in defining the problem is determining who is in charge. There are 52 different organizations involved in CIP integration of commercial industry. Some of the organizations are: the IAIP, the National Infrastructure Advisory Committee (NAIC), the President's National Security Telecommunications Advisory Committee (NSTAC)[64]—30 industry CEOs dealing with CIP, information sharing, priority access, cyber security and crime, and network security (1982)—the President's Information Technology Advisory Committee, the President's CIP Board or Cyber Board, and the FCC. It is simple to see that there are too many organizations involved to effectively implement a protection program.

The National/Federal Agencies' structure and response was immediate and bold after September 11, 2001. The Administration created an Office of Cyberspace Security. The FBI created the National Infrastructure Protection Center (NIPC). The Office of Homeland Security and the Homeland Security Council was established by Executive Order 13228, National Strategy for Homeland Security. This document, published in July of 2002, completely restructured many of the agencies formerly involved in aspects of protecting the nation before it was defined as Homeland Security. The plan also serves as the authority to move the NCS: "The Department of Homeland Security will work to develop comprehensive emergency communications systems. The National Communications System (NCS) would be incorporated into the Department of Homeland Security to facilitate the effort." A report out of the U.S. Army War College states that 13 major departments and agencies are directly involved in the national telecommunications infrastructure.[65] These include major departments such as the Departments of Defense, Homeland Security, Commerce and Justice. There are also several councils, committees and boards that are advisory in nature. The same report also stated that there was strong evidence of duplication and overlapping responsibilities that were associated with the telecommunications sector.

[64] NSTAC (National Security Telecommunications Advisory Committee), "Network Security/Vulnerability Assessments Task Force Report," (Washington, D.C.*:* NSTAC, 2002), 26.

[65] Baines, *National Telecommunications*, 25.

C. CIP INTER-DEPENDENCIES

The initial guiding policy for CIP started well before the events of September 11, 2001. President William Clinton signed Presidential Decision Directive 63 "Critical Infrastructure Protection" in 1998. PDD 63 states that the "United States will take all necessary measures to swiftly eliminate any significant vulnerability to both physical and cyber attacks on our critical infrastructures, including especially our cyber systems."[66] It also categorizes critical infrastructure into 12 different sectors and sets up a public-private partnership to involve and coordinate with the private sector. This task is a difficult one, as it is financially infeasible to build redundant systems to eliminate even a minimal amount of vulnerability in the telecom sector alone.

Virtually every other infrastructure sector is dependent upon a secure and robust telecommunications infrastructure, either through telephones or the internet. One example of how the different sectors are linked is the telecommunications and the Railroads (RR) piece of the transportation sector. Railroad companies are IT businesses and they know where every one of their trains and boxcars are located, what they are loaded with and where they are going. If the IT systems went down due to communications failures, the trains would stop. It is interesting to note that the telecom sector is related to the RR network in other ways as well. The right of way of many RR lines contains the majority of the nation's fiber optic network. Oil lines also co-exist with fiber optic routes, so here is the first interdependency with the energy sector, which represent two birds with one stone if you are a terrorist. Both GAO and the 9/11 commission reported critical infrastructure interdependencies that were not discovered until after the tragic events of that day. Due to these interdependencies among all critical infrastructures, an attack on one could result in cascading effects across many others. For this reason, not only critical assets must be identified, but also what other sectors are connected and what the effects of a failure would be. The president's commission on CIP described the following as being interdependent on telecommunications infrastructure: banking and financial systems, power, energy, transportation, water, medical and healthcare, emergency services and government operations. Another study named the

[66] William Jefferson Clinton, Presidential Decision Directive 63, White Paper, President's Message, 2002. .

following as highly dependent on telecommunications: finance, defense, emergency services and transportation. Another category for interdependency in the report was the vulnerable sectors that heavily rely on telecom: water, sewage, power, transportation, finance, defense, and emergency services.[67]

D. DOD TELECOMMUNICATIONS CASE STUDY

The structure of the DoD is very complex but well ordered; it serves as a good model. General Ralph Eberhardt, at the time commander of USSPACECOM, testified before the U.S. Senate Armed Service Committee Strategic Subcommittee on Computer Network Defense (CND) and Computer Network Attack (CNA). "There is a real and growing threat to Department of Defense unclassified computer systems and networks. It is no secret that the U.S. military's operational capability depends on information superiority—our ability to make smarter, faster decisions. This is both a tremendous advantage and a potential vulnerability."[68]

How does the DoD manage responsibility? The Joint Chiefs of Staff (JCS) provide oversight into the communications programs.[69] Defense Information Systems Agency (DISA) was responsible for management and implementation of the National Communications System (NCS). The National Security Agency (NSA) is responsible for protecting national security telecommunications and information systems. The Defense Advance Research Projects Agency (DARPA) is responsible for the R&D of protecting critical infrastructure.[70] The policy behind this structure is due to the FY 1997 Defense Authorization Act, in which the president assigned USCINCSPACE the responsibility to lead the Computer Network Defense (CND) mission for the Department of Defense.

[67] Lindsey Lack, and Jair Ferrari, MAJ Brazilian AF, "Critical Infrastructure Protection – Telecommunications and Space Interdependencies," Report, CS4920, September 24, 2002 (Monterey, CA: Naval Postgraduate School, 2002), 7.

[68] General Ralph E. Eberhart, Commander in Chief, North American Aerospace Defense Command and U.S. Space Command, Testimony, U.S. Senate Armed Services Committee Strategic Subcommittee. March 8, 2000.

[69] DoD Directive, 4640.7, "DoD Telecommunications System (DTS) in the National Capital Region (NCR)," October 7, 1993.

[70] Jack L. Brock, Jr., Director, Government Information and Financial Management Issues, Testimony before the House of Representatives, Subcommittee on Telecommunications and Finance Committee on Energy and Commerce, US GAO/T-IMTEC-89-10, July 20, 1989.

This now belongs to USSTRATCOM—U.S. Strategic Command in Omaha, NE. A subordinate command of USSTRATCOM that is tactically responsible for this mission is Joint Task Force-Global Network Operations (JTF-GNO). JTF-GNO is responsible for coordinating and directing activities related to computer attack.

The Department of Defense portrays an image of protection, security, and confidence when imagining its bases and infrastructure, patrolled by armed guards and with concertina wire fencing around its perimeter. There is no doubt that the U.S. military is a most formidable opponent and will use all the strength it has to protect its personnel, but what about its telecommunications networks? Does this same logic hold true for Department of Defense computer systems networks and telecommunications networks? The military tends to devote an enormous amount of resources to protecting these networks, but can terrorists pierce this armored coating through the civilian sector? How vulnerable is the military to cyber or physical attacks that could conceivably cripple its command and control structure?

The Department of Defense (DoD) currently operates two to three million computers, 100,000 local area networks, and 100 long distance networks to include the systems required for the Command and Control (C2) of forces. These systems support distributed collaborative planning for crises and contingencies and manage logistics and supplies, as well as distributing sensitive intelligence in real time.[71] The main entity that runs the department's networks is the Defense Information Systems Agency (DISA). The mission statement from their web page says:

> 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.

DISA provides services through systems that are interoperable, security assured, survivable, available and of superior quality. The specific services provided are globally classified and unclassified voice, data, video, and transport services through a

[71] Defense Information Systems Agency (DISA), "Information Assurance," [http://www.disa.mil/main/about/infoops.html] Accessed September 17, 2005.

combination of terrestrial and satellite assets.[72] The majority of the assets are commercially acquired and complemented with military value-added features. Also included are military satellites and a small portion of military terrestrial infrastructure, Outside the Continental United States (OUTCONUS). The value-added by the military is the aspect that separates the DoD system from a commercial system by adding features like robust encryption, personal and physical security, diversity of route and media, and controllable assets. This is critical to insuring that U.S. forces maintain superiority in information warfare.

DISA began in Washington, D.C., as the Defense Communications Agency (DCA) in May of 1960, with 450 employees. Its mission then was to manage the Defense Communications System (DCS), which was a consolidation of the independent long-haul communications networks of the Army, Navy and Air Force.[73] Later, in the 1960s, DCA moved to Arlington, Virginia, and picked up several other major organizations to include what is now known as the White House Communications Agency. Through the 1970s and 1980s the agency continued to grow until June 1991, when DCA was renamed DISA to reflect the larger role of providing a total information systems management package to DoD. To indicate the size and emphasis DoD places on its information systems networks, this agency alone employs approximately 8,000 personnel. This does not include the IT and telecommunications professionals in each of the military services that add to the communications mission.

DISA runs the Defense Information System Network (DISN), which provides both data services and voice communications. There are many sub-elements to the DISN network. Data services such as secure Internet Protocol (IP) and Asynchronous Transfer Mode (ATM) data communications services are provided via the NIPRNet and SIPRNet.[74] The NIPRNet or Non-secure Internet Protocol Router Network provides seamless interoperability for unclassified combat support applications and controlled

[72] Defense Information Systems Agency (DISA), [http://www.disa.mil/main/about/communications.html] Accessed September 17, 2005.

[73] Ibid.

[74] Defense Information Systems Agency (DISA), “DISN Data Services,” [http://disa.dtic.mil/main/prodsol/data.html] Accessed September 17, 2005.

access to the internet. The data rates range from 56 Kbps (Kilobits per second or thousands of bits per second) to 155 Mbps (Megabits per second or millions of bits per second). The SIPRNet, on the other hand, is the Secret IP Router Network and is the DoD's largest interoperable command and control data network.[75] The SIPRNet also supports the Global Command and Control System (GCCS, pronounced "geeks"), the Defense Message System (DMS), and many other classified warfighter applications. The SIPRNet runs at a data rate of up to 45 Mbps.

Besides the primary tasks, DISA runs other essential services. Enhanced Mobile Satellite Services (EMSS) is a Personal Communications System (PCS) providing secure and non-secure voice and data services utilizing commercial satellites. DISN Video Services provide for Video Teleconferencing (VTC) and Secure Video Teleconferencing (SVTC—pronounced "civits") up to a top-secret classification. DISA also provides computer processing, utilizing over 1,400 applications with more than 55 mainframe computers and 1,350 servers.[76] DISA also plays the major role of protecting, monitoring, analyzing, detecting, and responding to unauthorized activity of the networks through Computer Network Defense (CND). DoD is currently implementing the Public Key Infrastructure (PKI) for cryptographic security services for the networks. Lastly, there is another method by which DISA is keeping networks secure: There was an announcement last year that DISA was signing up to a three-year agreement with Symantec to provide early signs of attacks on its networks.[77] Is this a good thing, or just another way of the military outsourcing the critical functions of securing its networks?

While DISA is responsible for the Engineering, Furnishing and Installation (EF&I) of the DISN, another agency is responsible for the 24/7 operations of the Defense Information Systems Network. This agency, which is heavily involved in monitoring the DoD Global Information Grid (GIG), formerly known as the Defense Information Infrastructure, is Joint Task Force-Global Network Operations (JTF-GNO). The mission of JTF-GNO is:

[75] Defense Information Systems Agency (DISA), "DISN Data Services."

[76] Ibid.

[77] Security, "The Secure Platform," [http://www.securify.com/vision/] Accessed September 17, 2005.

> Subject to the authority and direction of the Commander, U.S. Strategic Command (CDR USSTRATCOM), the Joint Task Force - Global Network Operations (JTF-GNO), in conjunction with Department of Defense (DoD) Combatant Commands, Services and Agencies (CC/S/A), operates and defends the Global Information Grid (GIG), ensuring that our nation's warfighting forces get the right information at the right place at the right time with appropriate protection of that information.[78]

In December 1998, Joint Task Force-Computer Network Defense was created and, in 1999, was assigned to the United States Space Command (USSPACECOM). It was later renamed Joint Task Force-Computer Network Operations (JTF-CNO) and, in 2002, was placed under United States Strategic Command (USSTRATCOM). Since June 2004, the Director of DISA is the Commander, JTF-GNO and also Deputy Commander for Global Network Operations and Defense, USSTRATCOM Joint Forces Headquarters—Information Operations (JFHQ-IO).[79] The director of DISA, Lieutenant General Harry D. Raduege, Jr., USAF, is in charge of basically all "information" in the DoD arena. The Global NetOps Center (GNC) of JTF-GNO is the product of a merger of the Operations Directorate, DISA's Global Network Operations and Security Center (GNOSC), the DoD Computer Emergency Response Team (DoD-CERT), and the Global SATCOM Support Center.[80] The GNC is responsible for the daily activities associated with policy, defense of the GIG, information assurance, information management, and satisfying strategic information priorities. JTF-GNO is a much smaller organization, consisting of only 255 personnel.

An ever-increasing concern is the challenge of civilian dependency. An inherent problem with the DoD's Defense Information Systems Network is that once the traffic (multimedia-data, voice, video) leaves the base or federal installation, it rides on commercially leased telephone lines called the Public Switched Telecommunications Network (PSTN). The majority of the two billion miles of optical fiber runs along the rights-of-way of railroad companies or along utility or oil/gas rights-of-way. DoD is increasingly reliant on the civilian infrastructure, which in turn increases its vulnerability.

[78] Joint Task Force-Global Network Operations (JTF-GNO), "JTF-GNO Mission," [http://www.cert.mil/misc/mission.htm] Accessed September 17, 2005.

[79] Ibid.

[80] Ibid.

A terrorist or an adversary could identify and attack critical nodes, and that could severely degrade the network, exposing a potential vulnerability based on this dependence. Another issue in many of the CIP fields, but especially in the telecom sector, is that the infrastructure is privately owned. Private sector infrastructure, in many cases, directly supports military operations (with communications, logistics, etc.) These private sector systems come with many benefits as well as problems, and are increasingly being incorporated into military systems. To amplify the dependence of the military on civilian infrastructure, during Operation Desert Storm over 90% of inter-theater communications utilized commercial satellites.[81]

Another source of weakness is DoD's increasing emphasis on Commercial, Off-The-Shelf (COTS) systems and software. For purposes of standardization and economics, it is better to use available COTS systems. The problem is that as vulnerabilities are identified in a COTS system, they can be exploited to attack all the users of that same system. Software companies warn users of vulnerabilities in their programs to avoid lawsuits and bad press. This also serves as notification for hackers to exploit this vulnerability, and many accomplish this before company programmers are able to implement a "bug" fix.

A new way that terrorists may attempt to attack a network is through employment in the civilian sector; with increasing reliance on outsourcing, this method may be possible. While companies have security background checks for employees, they may not be sufficient to catch a well-trained terrorist. A web page ad for General Dynamics Network Systems lists the IT solutions it provides for voice, video and data for the Navy-Marine Corps team. It goes on to say

> We are the leader in modernizing the Navy-Marine Corps' voice switches and telecommunications systems. We are the largest DoD distributor of Nortel Networks Telephone Switching Systems.[82] General Dynamics and its subcontractors are modernizing the Department of Defense Command, Control, Communications-Computer, and Intelligence (C4I) infrastructure, by obtaining state-of-the-art distribution systems. Our technical support

[81] Gansler and Binnenkijk, *Information Assurance*, 17.

[82] General Dynamics, "Network Systems," [http://www.gd-ns.com/about_us/index.html] Accessed September 17, 2005.

> service capabilities include advanced engineering, management and support services to the Officer of Naval Intelligence, Commander Naval Security Group and other Department of Defense customers.

This is very alarming, because it is not only General Dynamic's employees, but also its subcontractors that have access to the military and its equipment. Even more alarming is that this company is furnishing and installing DoD's critical components of its C4I to customers like the Office of Naval Intelligence. Another report said that an official from the U.S. Navy's telecommunications systems IT operations thinks his branch needs to do a better job of ensuring that outsourced contractor software is secure.[83] Again, another vulnerability is discovered as DoD continues to outsource network solutions; and terrorist insiders in a company could gain access to critical networks or render them useless through software bugs and viruses.

One more example of outsourcing critical functions is from a Marconi press release announcing 10 Gbps encryption for surveillance data to be used on military intelligence assets such as the Global Hawk and Predator Unmanned Aerial Vehicles (UAVs).[84] Again, does this add value to the security efforts within DoD, or does it allow more vulnerabilities by utilizing another company that is not U.S.-owned? The list goes on, from a Canadian Company called Wescam that provides intelligence, surveillance and reconnaissance, and communications to DoD and all of the U.S. military services, to a company called Techsoft that provides out-sourced E-commerce solutions to DoD agencies.[85]

The Navy is taking positive steps to reduce vulnerabilities that were initially discovered during the Y2K (Year 2000) crisis. Every mission function in the Navy is tied to Information Technology (IT). Another discovery is that the Navy relies on the private sector, state, and local governments for telecommunications, in addition to public utilities

[83] Paul McDougall, "Navy Seeks Secure Software," *Information Week*, May 31, 2004. [http://www.informationweek.com/] Accessed September 17, 2005.

[84] "Marconi Demos 10-Gig Encryption," *Light Reading,* July 1, 2003. [www.lightreading.com/document.asp?doc_id=36331] Accessed September 17, 2005.

[85] Techsoft, Technical Software Services, Inc., "Experience." 2004. [http://www.techsoft.com/] Accessed September 17, 2005.

and road systems.[86] One of the steps in reducing the Navy's vulnerabilities is the creation of a process called the Naval Integrated Vulnerability Assessment Process. This process takes a look at the physical security of U.S. infrastructures, Anti-Terrorism/Force Protection (AT/FP) issues, Computer Network Defense (CND), and commercial dependencies on telecommunications and public utilities.[87] One other area that has heavy civilian influence is the new Navy-Marine Corps Intranet (NMCI). EDS has now taken responsibility for the majority of the new enterprise network for all members of the Naval Service. This contract leads to a new vulnerability, which is the economic trouble within the telecom sector. Many telecom companies started having economic difficulty prior to the events of 9/11. On the edge of financial health was Worldcom, as the company had been in Chapter 11 bankruptcy filing for several years.[88] At the time, Worldcom filed the largest corporate bankruptcy filing in history, and they are also the major telecom provider for NMCI. The Navy is focusing even more on being connected through the internet for services like tele-maintenance, tele-medicine, and distance-learning with the new Navy Knowledge On-line (NKO). As Americans make themselves more connected through the internet, they also become more vulnerable if an attack on these systems is successful.

A different measure of security comes from an organization called Joint Program Office for Special Technology Countermeasures (JPO-STC), which has been identifying DoD's mission-essential infrastructure since 1990. The Department of Defense relies heavily on commercial and defense infrastructure to support its missions and operations. An Infrastructure Assurance Program (IAP) has been established to provide DoD decision-makers, Geographical Combatant Commanders (GCCs), and operational commanders with the analysis and assessment capability to identify susceptibilities in critical infrastructure and operational dependencies that, if not assured, could adversely

[86] Dave Wennergren, Chief Information Officers Council, "Ask The CIO," November 3, 2003. [http://www.cio.gov/documents/wtop_ask_cio_wennergren_nov_03_2003.html] Accessed September 17, 2005.

[87] Ibid.

[88] Judi Hasson, "Telecom Troubles," *Federal Computer Week*, August 19, 2002. [http://www.fcw.com/article77436-08-19-02-Print] Accessed September 17, 2005.

impact mission accomplishment and military operations vital to national security.[89] One of the vulnerabilities that JPO-STC has discovered is the Programmable Logic Controllers (PLCs) that reside in Supervisory Control and Data Acquisition (SCADA) systems. These PLCs control utilities that the military requires to accomplish its mission and they are also used in controlling U.S. Navy Warships. This is a vulnerability that falls under the cyber realm and one where zero tolerance to any form of attack must be maintained.

Another method by which DoD maintains a secure network is through its use of DoD directives and instructions. The Secretary of Defense can issue a directive for all members of the DoD. The Chairman of the Joint Chiefs of Staff (CJCS) also has the authority to issue DoD-wide guidance through CJCS Instructions. One such directive is DoD Directive 4640.7, which is titled "DoD Telecommunications System (DTS) in the National Capital Region (NCR)."[90] It states that anyone acquiring, managing, or operating telecommunications in the NCR is required to follow certain processes and procedures in compliance with this and other associated directives. Another DoD Directive, 5100.41, titled "Executive Agent Responsibilities for the National Communications System (NCS)," listed the duties of members of the DoD for which they were responsible with respect to the NCS.[91] This overall responsibility was moved to the Department of Homeland Security (DHS) in March 2003.[92] A third directive is DoD Directive 4640.13, Management of Base and Long-Haul Telecommunications Equipment and Services. This directive establishes policy and assigns responsibility for the use of base and long-haul telecom equipment and services.[93] The last and possibly most important of the sampling of directives and instructions is Joint Publication 6.0. This

[89] Mike Burks, "Control Systems Vulnerabilities," Presentation for Tri-Service Power Expo, July 15–17, 2003. (Dahlgren, VA: Joint Program Office for Special Technology Countermeasures, 2003).

[90] DoD Directive 4640.7, "DoD Telecommunications System (DTS) in the National Capital Region (NCR)," October 7, 1993.

[91] DoD Directive 5100.41, "Executive Agent Responsibilities for the National Communications System (NCS)," May 1, 1991.

[92] National Security and Emergency Preparedness Telecom News, Published by the Office of the Manager, National Communications System, Mr. Brenton Greene, Issue 1, 2003 (Washington, D.C.: Office of the Manager, NCS, 2003).

[93] DoD Directive 4640.13, "Management of Base and Long-Haul Telecommunications Equipment and Services," December 5, 1991.

publication establishes Doctrine for Command, Control, Communications, and Computer (C4) Systems Support to Joint Operations. In 88 short pages, this document covers the following aspects of C4 systems: the role, objectives, components, principles, responsibilities, and standardization.[94]

The Army has also implemented measures to protect its networks. A vulnerability that the Army Signal Command discovered was an attack on the Domain Name Servers (DNS) within the Army. DNS serves to translate numbers like 140.183.234.10 into a World Wide Web (WWW) address like www.army.mil. This command ran a mission to counter an attack on military networks called "Solar Sunrise."[95] The Army continued working on this vulnerability issue along with many other IT issues to minimize any effects of an attack on its systems.

To see how the U.S. Air Force (USAF) is implementing information security, you can observe how they are structured. The 68th Information Operations Squadron is located at Brooks City-Base, Texas. This organization provides personnel to identify deficiencies in USAF telecommunications and computer security programs.[96] Their mission is to conduct Command, Control, Communications and Computer (C4) security assessments. They observe, analyze and make recommendations to reduce telecom vulnerabilities.

In summary, the information revolution has changed all aspects of Americans' lives, and this is especially true in the DoD. The advantage that the U.S. military gains from information technology has a negative effect that makes it dependent on computers and networks. A second dependency, on the civilian/private industry telecom infrastructure, adds greatly to this vulnerability. Fortunately, the Department of Defense has one master organization, the Defense Information Systems Agency, which provides strategic direction for the overarching network, the Defense Information System

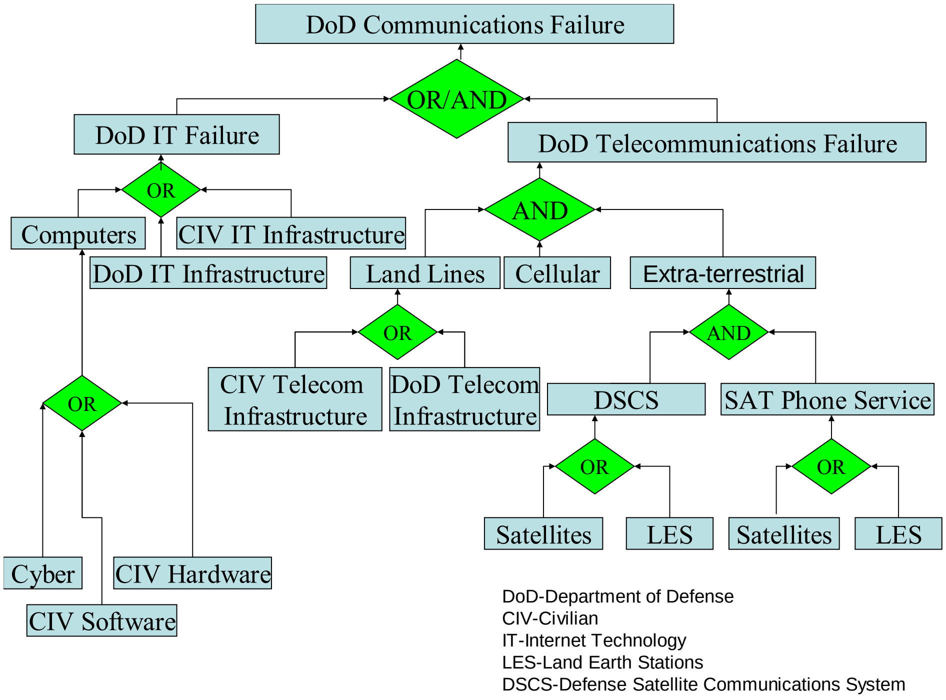
[94] Joint Publications 6-0, "Doctrine for Command, Control, Communications, and Computer (C4) Systems Support," May 30, 1995 (Washington, D.C.: Joint Chiefs of Staff, 1995).

[95] Larry Barker, "Information Assurance: Protecting the Army's domain-name system," *Army Communicator On-line*, February 5, 2003. [http://www.gordon.army.mil/ocos/rdiv/] Accessed September 17, 2005.

[96] United States Air Force Fact Sheet, "68th Information Operations Squadron," October 2002. [http://www.brooks.af.mil/HSW/PA/68IOS%20fact.htm] Accessed September 17, 2005.

Network, which encompasses the majority of DoD voice and data traffic. This agency has thousands of personnel to monitor and provide support to JTF-GNO, which is the task force responsible for network operations.

The secretary of defense, along with the chairman of the Joint Chiefs of Staff, issues directives and guidance to delegate responsibility and ensure that standards are met. In addition, each of the military services has its own personnel to ensure information assurance and network security. Military networks are vulnerable to a variety of attacks from a number of actors due to the interaction with private industry, but this vulnerability has been minimized through the efforts of DISA and the military value-added telecom technologies. DoD networks are among the most secure, due to encryption and secure, diverse routed networks, but the weakest link in the chain is the majority of privately owned networks that make up the civilian telecom infrastructure. Military command and control communications have many redundant and back-up systems built in, to ensure that orders from the chain-of-command get to the soldiers in the field. DISA is up to the task of keeping a technological information advantage over the nation’s adversaries, and U.S. National Security depends upon it.



DoD-Department of Defense
CIV-Civilian
IT-Internet Technology
LES-Land Earth Stations
DSCS-Defense Satellite Communications System

Figure 14. Vulnerabilities of DoD Communications Sector Fault Tree

Figure 14 is a portrayal of the entire communications sector for DoD, including both telecom and IT. It was designed based on the case study to emphasize the interdependencies with the civilian sector as described above. What cannot be depicted is the dependency of cellular and extra-terrestrial systems on terrestrial land lines. The IT infrastructure is very dependent on the DoD owned assets that are run by civilian vendors (e.g., Navy-Marine Corps, the Telecommunications Infrastructure). There are too many variables and unknowns to show these dependencies in the illustration. This really shows that while the majority of DoD owned systems are physically secure, have diversity of routes, and have robust cyber protection, there is a major dependency on civilian owned infrastructure. Even some internet (NMCI) is run by EDS. An additional vulnerability comes from large scale EMP, which would make all non-hardened circuits inoperable. All of the vulnerabilities of fiber, IED and Cyber are contained within the various infrastructures. There is redundancy built in to the commercial satellite phone services, as many companies own their own satellites, such as Iridium, INMARSAT, Globalstar, and Thuraya. Many of these signals, however, feed into the same land earth stations. DoD is very dependent on all of these civilian systems, as demonstrated by Hurricane Katrina. Only satellite based communications were initially operable.

E. TELCO INITIATIVES

Telecommunications companies are delivering several initiatives. . The first is from Verizon and deals directly with homeland security issues such as disaster recovery, contingency planning, and network security.[97] To the skeptic, these are probably the same services that they offered years ago for high QoS-level customers for natural disasters, but now are under a new name. Services offered include: security testing and assessments, security policy planning, firewall design, technology planning for security, intrusion detection services, and virus detection. The Verizon division that markets this

[97] Verizon Communications Inc. [http://www22.verizon.com/enterprisesolutions/Includes/SiteUtilities/JCMSSkeleton.jsp?filePath=/Anonymous/Default/ProductDetail/BusContinuity/Business_Recovery_m.html] Accessed September 17, 2005.

is Business Recovery and Continuity Services (BRCS), which is an outsourced organization to help run the network. They will help protect, restore, and recover the client's network.

AT&T also offers Homeland Security related services. AT&T Government Solutions covers Government Continuity of Operations (COOP).[98] They offer diversely routed networks, backup wireless solutions, alternate call routing, mirrored data backup, and network monitoring. These services have always existed, but normally have an exorbitant cost associated with them. Small ISPs would not consider these types of services, but 911 and emergency services or high levels of federal government entities have had them for years.

The last initiative is from 365 Main, a telecom hotel, which passed the Statement of Auditing Standards No. 70 representing service organizations that have been through an in-depth audit of their control activities, including controls over information technology and related processes.[99] This was in addition to the already completed ISO 9000:2000. These are difficult standards to attain and show a dedication, as service providers, to maintain the highest levels of auditing control over their internal processes. To show the reliance expected in the telecom industry, or so the company's press release claimed, 365 Main is the only data center to continuously exceed the industry standard of 99.999% uptime since its inception.

[98] American Telephone and Telegraph Company (AT&T), "AT&T Government Solutions," [http://www.att.com/gov/] Accessed September 17, 2005.

[99] Sarah Miller, "Main Passes SAS70 Type 2 Audit," Axis Marketing & PR, LLC [http://www.365main.net/pr_02_7_05_sas_70.html] Accessed September 17, 2005.

THIS PAGE INTENTIONALLY LEFT BLANK

V. CONCLUSION

A. CONCLUSION

In summary, action must be taken in order to ensure both prevention of cyber - terrorism and protection of CIP. This research discovered that terrorists have the capability and desire to commit attacks against the telecom industry. The structure and strategy required to reduce vulnerabilities and to deny and defeat the enemy need a considerable amount of work. Prevention and protection are needed through many agencies, departments, localities, and especially industry/private sector, but there has not been one coordinated effort. The U.S. is still vulnerable to attack. Many new programs have been started as a result of 9/11, but a guiding light is needed. This thesis offers a few alternatives for what needs to be done. There are a lot of gray areas that need to be defined in order to protect the nation from, and prevent, a telecommunications 9/11.

It is ironic, but 911 emergency systems are on the same circuits and lines and just as vulnerable as other components listed above. A carefully planned and successful telecom terrorist attack would severely degrade the nation's ability to recover. If terrorist organizations can teach their members to fly aircraft, it would be expected that they could also teach their members to work on telecom equipment and gain access to these already vulnerable locations. For this reason, a "watch list" type of screening needs to be implemented for employees that access critical telecom areas. On initial review, this may seem far-fetched or extreme, but the precedent has already been made with the TSA's Transportation Worker Identification Credential (TWIC) program. This program conducts background checks on transportation workers at the port and issues ID cards for those workers. Another program, US-VISIT, requires visitors to the U.S. applying for a visa to go through a program that checks biographical information and biometric data of the visitor against watch lists.

The initiatives mentioned, along with initiatives already implemented, will be effective in reducing vulnerabilities in the telecommunications infrastructure, but they will take time. Patience will be key in the Global War on Terrorism and the Department of Homeland Security must be given time to effect a change.

B. RECOMMENDATION

1. Strategic Budgeting

A comprehensive strategic planning and budgeting process needs to be considered by all owners of critical telecommunications facilities. Most "for-profit" companies have previously accomplished some form of strategic planning and budgeting for their organizations. Budgeting functions take place annually, but the strategic planning process is usually less frequent, and strategic plans need to be re-evaluated in this new HLS environment. For telecommunications companies, there are certain minimum HLS measures that need to be taken into account:

- Physical security improvements to account for IEDs (Improvised Explosive Devices)
- CBRNE (Chemical, Biological, Radiological, Nuclear and High Yield Explosive) detection
- Cyber security controls
- Redundant NOCs (Network Operations Centers)/data warehouses
- Biometric security measures for internal workers, and access control systems

Because there are no currently mandated requirements for companies to improve their HLS measures, there needs to be a tie-in to HLS measures like the NIPP (National Infrastructure Protection Program). As previous strategic planning was based on core competencies related to ROI and profit; they didn't include costs associated with HLS security measures. Even though HLS security measures are not a core competency, they are an essential cost center, like HR or recruiting. It is a necessity for private companies to improve the measures as suggested above to maintain a standard in the protection of workers, U.S. citizens, and the economy. An additional possibility is to again use the DoD model for identifying vulnerabilities and providing for a method of sourcing shortfalls or unfunded requirements. A separate line in the federal budget would provide for emergent vulnerabilities that are short-term or based on new threat information or new terrorist modus operandi. Long-term budgeting should be handled through the organizations' strategic budgeting processes.

2. Mandates

The most effective policies and strategies start from the top and work down. For this reason, Congress needs to construct and pass into law a bill that will give the Department of Homeland Security authority to set standards for CIP, above and beyond what is directed in HSPD-7. The Homeland Security Council Deputies Committee (HSC-DC) should provide the oversight required for this program. It has already been established that the agency under DHS that is responsible for providing specific coordination and policy direction on a daily basis is Information Analysis and Infrastructure Protection (IAIP). IAIP needs to receive the executive power to enforce standards for building codes and protection systems. DHS has also been tasked to maintain the National Communication System. In addition, DHS is the sector-specific agency for the telecommunications sector. It also has control of the ISAC through NCC. NCS, under the Department of Homeland Security, needs to take the lead role in establishing policy for the telecommunications infrastructure sector. This will include setting the baseline standard for conduct of vulnerability assessments based on combined methodologies like MBVA and JSIVA. NTIA should be in an advisory role only for the executive branch, and overlapping HLS roles should be removed from its charter. NRIC has been extremely successful with its best practices; it should be DHS's responsibility to examine these and determine which ones should become mandates. DHS would be responsible for inspecting companies to ensure that they are in compliance with those standards, the way the Transportation Security Agency (TSA) takes responsibility for ensuring safe air travel through inspection of passengers and luggage.

3. Overall

What must be done? The answer is simple: security and protection measures must be increased and implemented at all areas of vulnerability previously listed. The execution is difficult, as the cost to secure the hardware and fiber would easily run into the billions. There are redundant systems that have been put into place for natural types of disasters, but nothing that will remain in place after a holocaust type of catastrophic event. Another problem of vulnerability is that telecommunications systems have been designed to be run out of an NOC, or Network Operations Center. This allows maintenance and upgrades to be performed from one central site, rather than having to physically deploy maintenance personnel to perform these functions, which is a very costly endeavor. This also means that it is feasible for people to hack into that same network.

The structure and strategy to defend these networks must be determined. The structure and strategy to protect from terrorism is not clear, but it is necessary to understand what has been done so far to protect the nation's telecommunications CIP and essential communications networks. There must be continued emphasis on redundancy and diversity within the telecommunications infrastructure. The U.S. must continue to move away from single points of failure, as is being done with the additional MAEs and NAPs being added to the networks. All levels of government have a role to play, including an increased level of coordination and increased responsiveness by private industry as the primary owners of the infrastructure.

> Individual commitment to a group effort—that is what makes a team work, a company work, a society work, a civilization work.
>
> —Vince Lombardi

C. CHALLENGES AHEAD

Integration of commercial industry (private sector) with federal agencies is clearly one of the most significant challenges facing the task of protecting critical infrastructure and, specifically, the national telecommunications networks. As stated previously, roughly 95% of the national telecommunications infrastructure traverses through commercial networks. Another challenge is the lack of a federal mandate for the private sector to reduce vulnerabilities. Many times, the telecom companies own the optical fiber or the communications hardware, but they do not own the right-of-way or the buildings that house the equipment. This leaves less incentive for any parties to spend large amounts of money on someone else's interests. A final challenge is the problem of certification and standardization, as there are too many standards boards involved: ATIS (Alliance for telecom industry standards), ITU (International Telecom Union), and ANSI (American National Standards Institute). There are different perspectives between stakeholders on what constitutes a secure and reliable network. Standards must be developed based on roles within the telecommunications sector. The NRIC best practices list is a good example of how to implement this strategy.

It is the opinion of this author that the telecommunications infrastructure sector, including telecom hotels, is safe and secure at this time and free from the existence of any significant new threats. This is not due to homeland security initiatives or recommendations, but rather from competition in the market place, redundancy, and diverse routing due to expected high levels of service. The PSTN was built to withstand many natural disasters, including floods, hurricanes, tornados, and earthquakes. Building owners and managers rely on survivable facilities, and they guarantee these services as part of their contracts. Equipment manufacturers are under the same guidelines, as the equipment is built to be survivable and under strict specifications. Service providers also want to provide a high quality of service to their customers, and when all is factored in, this is what makes a robust and redundant telecommunications and IT network. The cyber threat is probably the most damaging and feasible threat to the sector. A cyber threat can attack all buildings and networks and systems almost instantaneously, where even a simultaneous attack on several telecom hotels would only result in local or, at best, regional outage, and only for a limited amount of time.

Based on information provided by the interviewees, and aligned with other resource material, there would seem to be no single point of failure. Some small local failures may occur, but only on the edge of the telecommunications infrastructure. As you get closer to the core, or the backbone of either the PSTN or the internet, the redundancy increases. Ring architecture, geographically diverse routing and other technological advances have accounted for the robust nature of the system due to the diversity of providers. Service redundancy and Quality of Service (QoS) have also helped to make reliable networks. Two sectors combined, telecom and IT, have also helped with making a reliable network. Even though convergence and the marketplace have brought these two sides together, they continue to have different redundancy methods built in, to further protect the survivability of the networks. The conclusion of a study on information and telecommunications stated that the sector was resilient, robust and redundant and would recover quickly in the likelihood of a small attack.[100] A well timed attack on specific assets could cause both economic and psychological destruction. The effects of such an attack could be excessive as other sectors would also be affected. It would take extensive preparation, ability and resources to pull off such an attack. A final thought: despite the reassurances of the telecommunications companies and operators, there must continue to be an in-depth look for vulnerabilities that may not be noticed on the surface.

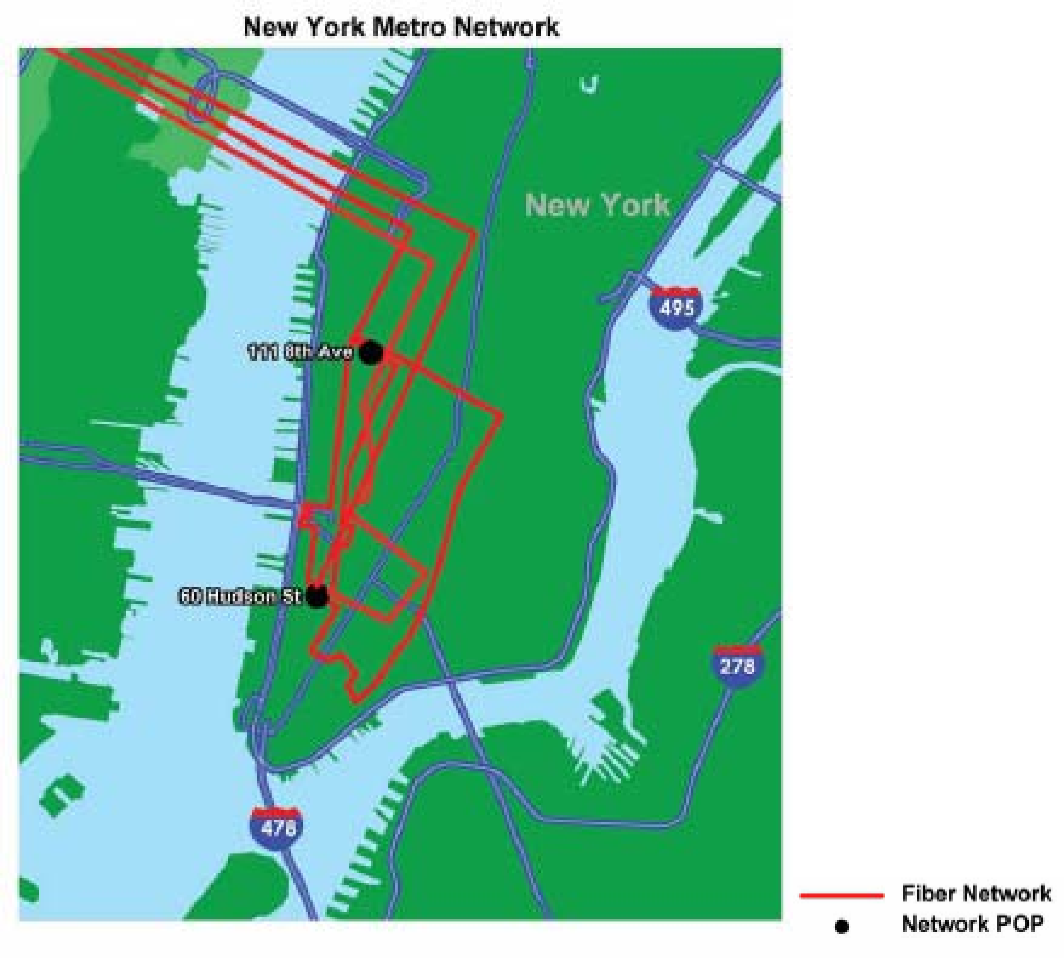


Figure 15. NYC Metro Fiber Network.[101]

[100] IRIA Group, *Institute for Security*, 2002, 3.

[101] Progress Telecom LLC. [http://www.epik.net/pdf/Tier%201%20(300dpi)V13.pdf] Accessed September 17, 2005.

Richard Clarke, Special Advisor to the President for Cyberspace Security, in remarks made before the business session of the President's National Security Telecommunications Advisory Committee (NSTAC) on March 13, 2002, shows the significance of telecom hotel vulnerabilities:

> I'm told, for example, that although TransAtlantic Fiber lands at about 10 different places in Massachusetts, Rhode Island, Long Island and New Jersey that, after having landed, it all goes to one of two facilities -- 60 Hudson Street or 111 Eighth Avenue in Lower Manhattan. If that's true, that would seem to be a problem.
>
> And what is the role of Government in the burden sharing, the cost sharing of increasing the diversification of routing? But I suspect this statement, which I am told is true, is true, that if you blew up 60 Hudson Street and 111 Eighth Avenue, we could not communicate via fiber optic with Europe. [102]

[102] Lack and Ferrari, "Critical Infrastructure Protection," 4.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX

A. TELECOMMUNICATIONS NETWORK OVERVIEW

Telecom 101: Telecom is short for telecommunications. Wikipedia defines telecommunication as "the extension of communication over a distance. In practice it also recognizes that something may be lost in the process; hence the term *telecommunication* covers all forms of distance and/or conversion of the original communications, including radio, telegraphy, television, telephony, data communication and computer networking." [103] Webster's defines it as communication at a distance (as by telephone). This process starts with a telephone in the home. A call is dialed and the signal is directed, through switching equipment, to the person who was called. The signal initially rides on a Plain Old Telephone Service (POTS) line, where it enters the local loop. From this "headend" the signal passes to a Local Exchange Carrier (LEC) end office and then to a central office. If this is a long distance call, the call is routed to a Point of Presence (POP) at a Inter-Exchange Carrier (IEC), which is a long-distance company such as AT&T or MCI. The call rides along that carrier's network until it arrives at the city of the recipient of the call. Along the way, the signal is placed onto bigger "pipes" through a process called *multi-plexing*. There is an economy of scale in allowing this call to travel with other calls, or even internet data. The signal normally starts as an analog call, is transferred to digital, and then to optical as it rides on optical fiber; the process is reversed at the other end. Once it transforms to a digital signal, it looks similar to data on a computer, which is a series of *1* and *O* characters.

Many pieces of hardware originate at the home office or RBOC (Regional Bell Operating Center); some of these are the PC, Ethernet, Hub, router, switch, ADM (add/drop multiplexer), and fiber optic DWDM (Dense Wave-Division Multiplexer). A DWDM takes different frequency wavelengths and amplifies several optical signals on one fiber optic line. Terabits of information can be passed through these networks. To connect to the Internet, one may use dial-up, cable modem, or ISDN (Integrated Services

[103] Wikipedia Encyclopedia. [http://en.wikipedia.org/wiki/Telecommunication] Accessed September 17, 2005.

Digital Network). Dial-up is at a rate of 28.8 to 36.6 Kbps, or 28,800 to 36,600 bits per second. The Photonic optical network can work at speeds currently up to 1.76 terabits of information per second. A terabit is one *trillion* bits of data. This is also equivalent to 320 OC-192's (Optical Carrier signal) or 10 Gigabits.[104] Ten Gbps is the equivalent of 129,000 voice conversations. So, there are 41,280,000 voice conversations on one fiber optic line, and this is all done with DWDM. Everyone is familiar with WMD (Weapons of Mass Destruction), but WDM or DWDM (Wave Division or Dense Wave-Division Multiplexing) is splitting the frequencies or colors of light and then combining them onto one single fiber. This illustrates the immense volume of bandwidth that is as risk, through millions of phone calls or data transfers or transactions.

The Telecommunications Act of 1996 created open competition and caused the PSTN and Internet to become more and more connected, software driven, and remotely managed. Previous sections of this thesis demonstrated how this has increased vulnerabilities in the sector. The telecom and Information Technology (IT) assets are becoming increasingly concentrated into these large shared facilities. This issue is compounded in today's global world of IT, and a rash of industry mergers, due to *Convergence*. If you were to diagram telecommunications and computer networks across the U.S., they would look like one is overlaid onto the other. This network may also overlay and is interdependent on oil lines and railroads, because much of the fiber in the ground runs along the right-of-way of these two industries. As the technology in the IT and telecom fields increases, so do the vulnerabilities, as the two industries cross-pollinate.[105] All traditional telephony and internet traffic passes through the same physical places. This also includes wireless traffic from a Wi-Fi hotspot using the 802.11 standard cellular phone traffic that passes from the cell towers into the PSTN (Public Switched Telephone Network). Even satellite communications and data pass from the satellite down to a LES (Land Earth Station) and then get routed over the PSTN. This convergence is the cause of the first major significant vulnerability in the systems.

[104] Gerald R. Hust, Major, "Taking Down Telecommunications," Thesis, Maxwell AFB, AL, School of Advanced Airpower Studies, May 28, 1993.

[105] Warren G. Reed, Director, Information Management and Technology Division, Testimony before the House of Representatives, Subcommittee on Transportation, Aviation, and Materials Committee on Science & Technology, October 17, 1983 (Washington, D.C.: U.S. GAO, 1983).

Convergence is the combining of data, voice, video, internet traffic, wireless, and landline (wireline).[106] Your banking information, credit card/ATM (automated teller machine) transactions, email, video for cable television, voice communications, conference calls, VTCs (Video Teleconferences), and IPTV (Internet Protocol TeleVision) all ride on fiber optic cables throughout the United States and across the globe.

Several types of critical nodes contain this convergence of media: international gateways like New York and San Francisco, telco hotels in the major cities, NAP (Network Access Points), where all internet traffic merges—formerly in New York, Washington D.C., Chicago, and San Francisco. The merger of computers and the Internet with telecommunications has created a huge area for possible exploitation of networked information systems.

B. AGENCIES INVOLVED

Several agencies or organizations are involved in telecommunications. The following is a listing and brief synopsis of each organization's role.

NCS (National Communications System), created after the Cuban Missile crisis in 1963. NCS is responsible for making sure the communications systems work. NCS became part of DHS (Department of Homeland Security) in 2003; it had previously been in DoD. Government emergency priority services like GETS, TSP and WPS are regulated and authorized by NCS. Subordinate to NCS is the NCC (National Coordinating Center), and within NCC lies NCC-ISAC (the Information Sharing and Analysis Center) for the Telecommunications and Information sector. PDD-63 established the NCC-ISAC to handle CIP issues. The wealth of members includes: A&T, Cisco Systems, CSC, EDS, ITT, Nortel Networks, SAIC, Sprint, Verizon Communications, and WorldCom. The membership changes over time, but it consists of major telecom providers and vendors.[107]

[106] NSTAC (National Security Telecommunications Advisory Committee), "Network Security/Vulnerability Assessments Task Force Report," Report (Washington, D.C.: NSTAC, 2002), 28.

[107] National Coordinating Center for Telecommunications. [http://www.ncs.gov/ncc/main.html] Accessed September 17, 2005.

NTIA (National Telecommunications & Information Administration) was created in 1978 under EO 12046. NTIA operates under the Department of Commerce and combines the White House Office of Telecommunications Policy (OTP) with Commerce's Office of Telecommunications. Their main role has been to sell spectrum to telephone, radio, and television companies and to regulate the airwaves. They have also played a major role in the commercialization of the Internet in the late 1990s. PDD-63 (1998) designated the U.S. Department of Commerce as the lead agency and the National Telecommunications and Information Administration (NTIA) as the Sector Liaison Official for the Information and Telecommunications Sector. NTIA claims to be President George W. Bush's principal adviser on telecommunications and information policy issues.[108]

NSTAC (National Security Telecom Advisory Committee) was created in 1982 under EO 12382. This is an organization of telephone company CEOs who serve as an advisory board to the president on Telecom security matters. NSTAC has been given a governmental oversight role with direct access to President Bush. Its members are currently from BellSouth, Lucent, Unisys, Boeing Company, Microsoft, SBC, Northrop Grumman Corp., Qwest, AT&T, SAIC, Bank of America Inc., and others. The alliance is limited to no more than 30 members.[109]

PCIPB (President's Critical Infrastructure Protection Board) was created under EO 13231, Critical Infrastructure Protection in the Information Age on October 16, 2001. The order created a federal "critical infrastructure protection" board and charged it with recommending policies and coordinating programs for protecting information systems for critical infrastructure. The Board's wide domain includes outreach to the private sector and state and local governments, information sharing, incident coordination, and crisis response. Its members are made up of senior officials or their designees from all the cabinets of federal government, and all members are employees of the government.[110]

[108] National Telecommunications and Information Administration. [http://www.ntia.doc.gov/] Accessed September 17, 2005.

[109] National Communications System. [http://www.ncs.gov/nstac/nstac.html] Accessed September 17, 2005.

[110] President George W. Bush, White House Executive Order, Information Warfare Site, October 2001. [http://www.iwar.org.uk/cip/resources/bush/executive-order.htm] Accessed September 17, 2005.

NIAC (National Infrastructure Advisory Committee) was also established by EO 13231, and makes recommendations regarding the security of the cyber and information systems of the United States' national security and economic critical infrastructures. The members represent the major sectors of the economy, including banking and finance, transportation, energy, and manufacturing, as well as emergency government services from the private sector, academia, and state and local government. Twenty-four individuals sit on this advisory board.[111]

NSIE (National Security Information Exchange) was established by a recommendation in 1991 from NSTAC and NCS. The recommendation was to create a Government-Industry partnership to reduce vulnerabilities of the nation's telecommunications systems from electronic intrusion. NSIE serves as a forum in which government and industry can share information in a trusted and confidential environment. PDD-63 called for the establishment of similar information exchange forums to reduce vulnerabilities in all critical infrastructures in 1998.[112]

NRIC (the Network Reliability and Interoperability Council), under the FCC, was established by Congress in 1993. The FCC was concerned with the Y2K problem in computers and communications equipment. NRIC was dismantled after the Y2K threat diminished, but then was re-chartered in 2002, after the events of 9/11. Its charter was recently reestablished in its seventh iteration, with a new focus on homeland security, reliability, and vulnerability analysis. NRIC seems to be the authoritative source of recommendations on security of telecommunications infrastructure, through its list of 801 best practices. These are further categorized into the following industry roles: Service Provider, Network Operator, Equipment Supplier, Property Manager, and Government. NRIC also has an extensive membership list: Nextel Communications Inc., Alcatel, ALLTEL, AT&T, BellSouth Communications, Boeing Company, Cisco Systems, Comcast Cable Communications Inc., Ericsson Inc., Level 3 Communications Inc., MCI, Lucent Technologies, Microsoft Corporation, Motorola, T-Mobile, Qwest, Verizon

[111] President George W. Bush, The White House. Office of the Press Secretary, September 18, 2002. [http://www.whitehouse.gov/news/releases/2002/09/20020918–12.html] Accessed September 17, 2005.

[112] National Communications System. [http://www.ncs.gov/nstac/nstac.html] Accessed September 17, 2005.

Communications, and the National Communications System (NCS). A total of 54 major telecommunications companies and organizations make up this seventh edition.[113]

CWIN (Critical infrastructure Warning Information Network); NCS developed CWIN to facilitate the immediate sharing of critical infrastructure and cyber information with government and its industry partners. It provides a continuous, 24/7 alert and notification capability. Several news releases state that CWIN has no logical dependency on the Internet or the public switched network and remains viable under emergency conditions, establishing connectivity to the 50 states and District of Columbia. CWIN establishes a strong base for ensuring connectivity between DHS and the states during emergencies. This is a classified system and not much is available through OSINT (Open Source Intelligence). There are many similarities to various secure DoD communications systems.[114]

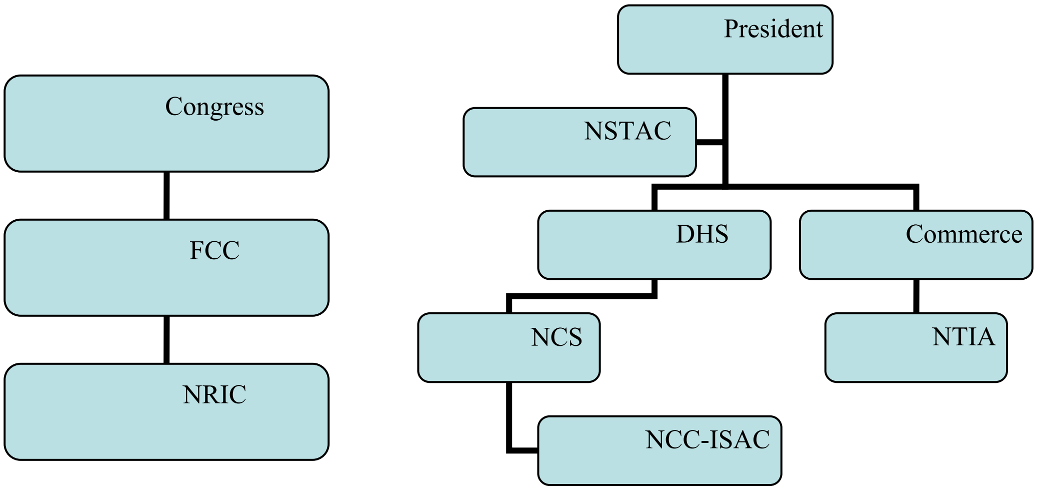


Figure 16. Telecom C2/Regulatory Structure.[115]

[113] National Reliability and Interoperability Council. [http://www.nric.org/charter_vii/nric_vii_org.html] Accessed September 17, 2005.

[114] Arrowhead Global Solutions Inc., "Critical infrastructure Warning Information Network (CWIN) Connects to All 50 States," April 14, 2005. [http://www.arrowhead.com/news/detail.php?news_ID=8] Accessed September 17, 2005.

[115] Ted Lewis, "Critical Infrastructure Protection."

As diagramed in Figure 1, several agencies oversee telecommunications: the FCC with NRIC, Commerce with NTIA, DHS with NCS and, farther down, the NCC-ISAC and NSTAC working for the president. Each organization plays a regulatory role, summed up by the following: FCC – spectrum, NTIA – business, executive branch – advisory, NCS – operations, and NRIC – security. Although the template of duties seems simplistic, there is much crossover and blurring of the lines in each of these roles and responsibilities. The most influential of these to date in implementation of security measures for Telcos are NCS mandates and NRIC's best practices.

C. TELECOMMUNICATION HISTORY/REGULATIONS

"Mr. Watson — come here — I want to see you."[116]

—Alexander Graham Bell, March 10, 1876

It all started with Alexander Graham Bell and two financiers. After his invention of the telephone in 1876, Bell and the others formed the Bell Telephone Company. AT&T became incorporated in 1885, known as the American Telephone and Telegraph Corporation, a subsidiary of the American Bell Telephone Company. This Company formed a natural monopoly on what is now known as the telecommunications sector. Ma Bell and the Justice Department reached a settlement in 1913, in which AT&T agreed to federal regulation as a regulated monopoly.[117]

The next attempt to regulate this new medium was in the 1930s under President Franklin D. Roosevelt when the Federal Communications Commission was established and produced the Communications Act of 1934. This act was to ensure that the emerging radio market would serve the public interest and to prevent domination of the new medium by large national monopolies. Fifty years later, a U.S. district court took a dramatic step toward breaking up Ma Bell with the 1984 AT&T divestiture. This caused

[116] Alexander Graham Bell, [http://www.loc.gov/exhibits/treasures/trr002.html/] Accessed September 17, 2005.

[117] American Telephone and Telegraph Company (AT&T). [http://www.att.com/history/] Accessed September 17, 2005.

AT&T to break its local service into seven RBOCs (Regional Bell Operating Companies) known as the “Baby Bells”. AT&T remained in business, providing competitive long-distance service.

The Telecommunications Act of 1996 sought to bring about competition across various telecommunications markets by deregulating the telecommunications marketplace. Since passage of the 1996 act, economic and market conditions and technical innovations have helped to bring competition to nationwide markets more so than regulatory efforts.[118] The act mandated that incumbent carriers open their networks to competitors. Carriers began to concentrate their equipment in colocation facilities and buildings, now known as telecom hotels. Carriers did not have to install their own cables, making it less expensive. These were also peering points for ISPs, which allowed for reduced costs when exchanging traffic with other ISPs.

[118] Federal Communications Commission, “Telecommunications Act of 1996,” [http://www.fcc.gov/telecom.html] Accessed September 17, 2005.

LIST OF REFERENCES

365 Main Inc. [http://www.365main.net/company.html] Accessed September 17, 2005.

American Telephone and Telegraph Company (AT&T). "AT&T Government Solutions." [http://www.att.com/gov/] Accessed September 17, 2005.

———. [http://www.att.com/history/] Accessed September 17, 2005.

Anti-terrorism/Force Protection Division. Asset Prioritization Model. [https://www.noradnorthcom.mil/j3/j34] Accessed September 17, 2005.

Arrowhead Global Solutions Inc. "Critical infrastructure Warning Information Network (CWIN) Connects to All 50 States." April 14, 2005. [http://www.arrowhead.com/news/detail.php?news_ID=8] Accessed September 17, 2005.

ATIS (Alliance for Telecommunications Industry Solutions). "Security of Service Provider Infrastructure in an Era of Convergence." ATIS Security Summit Report, February 4-5, 2003. Washington, D.C., *Alliance for Telecommunications Industry Solutions*, 2003.

Baines, Mark D., Lieutenant Colonel. "The National Telecommunications Infrastructure: A 21st Century Organizational Paradox." Strategy Research Project. Carlisle Barracks, PA: US Army War College, April 7, 2003.

Barker, Larry. "Information Assurance: Protecting the Army's domain-name system." Army Communicator On-line, February 5, 2003. [http://www.gordon.army.mil/ocos/rdiv/] Accessed September 17, 2005.

Barrett, Randy. "Telecom networks no easy target." *Government Security News*. [http://www.gsnmagazine.com/nov_04/telecom_networks.html] Accessed November 20, 2004.

Brock, Jack L., Jr., Director. Government Information and Financial Management Issues, Testimony before the House of Representatives, Subcommittee on Telecommunications and Finance Committee on Energy and Commerce. US GAO/T-IMTEC-89-10, July 20, 1989. Washington, D.C.: US GAO, 1989.

Burks, Mike. "Control Systems Vulnerabilities." Presentation for Tri-Service Power Expo 2003, Joint Program Office for Special Technology Countermeasures. July 15-17, 2003. Dahlgren, VA: Joint Program Office for Special Technology Countermeasures, 2003.

Bush, George W., President. White House Executive Order. Information Warfare Site, October 2001. [http://www.iwar.org.uk/cip/resources/bush/executive-order.htm] Accessed November 20, 2004.

———. The White House.gov. Office of the Press Secretary, September 18, 2002. [http://www.whitehouse.gov/news/releases/2002/09/20020918-12.html] Accessed November 20, 2004.

Carrier Hotels. [http://www.carrierhotels.com] Accessed September 17, 2005.

Center for Homeland Defense and Security. Allocate Simulation, August 2005. [https://www.chds.us/course/studies.cfm?course_id=77&cci=animation_test] Accessed August 17, 2005.

Clinton, William Jefferson. Presidential Decision Directive 63. White Paper, President's Message, January 7, 2000. Washington, D.C.: The White House, 2000.

Computer Knowledge. "MAE-Metropolitan Area Exchange (Ethernet)." [http://www.cknow.com/ckinfo/questions/414/__print] Accessed September 17, 2005.

Coopers & Lybrand L.L.P.. "Liability and Insurance, Infrastructure Assurance." Report to the President's Commission on Critical Infrastructure Protection, 1-21, 1997. Washington, D.C.: The Commission, 1997. [http://permanent.access.gpo.gov/lps19694/www.ciao.gov/resource/pccip/LiabilityInsurance.pdf] Accessed September 17, 2005.

Dacey, Robert. Director, Information Security Issues before the House of Representatives, Subcommittees on Cybersecurity, Science, and Research & Development and Infrastructure and Border Security, Select Committee on Homeland Security. U.S. GAO, GAO-04-699T, April 21, 2004. Washington, D.C.: U.S. GAO, 2004.

Defense Information Systems Agency (DISA). "Information Assurance" "Communications" "History of DISA." [http://www.disa.mil/] Accessed September 17, 2005.

———. [http://disa.dtic.mil/] Accessed November 20, 2004.

Defense Threat Reduction Agency Link. Combat Support. [http://www.dtra.mil/toolbox/directorates/cs/programs/assessments/joint_staff.cfm] Accessed September 17, 2005.

Department of Homeland Security (DHS). “The Interim National Infrastructure Protection Plan.” February 2005. Washington, D.C., Office of Homeland Security, 2005.

DoD Directive 4640.13. “Management of Base and Long-Haul Telecommunications Equipment and Services.” December 5, 1991. Washington D.C.: Department of Defense, 1991.

———.Directive 4640.7. “DoD Telecommunications System (DTS) in the National Capital Region (NCR).” October 7, 1993. Washington D.C.: Department of Defense, 1993.

———. Directive 5100.41. “Executive Agent Responsibilities for the National Communications System (NCS).” May 1, 1991. Washington D.C.: Department of Defense, 1991.

Eberhart, Ralph E., General. Commander in Chief, North American Aerospace Defense Command and U.S. Space Command. Testimony, U.S. Senate Armed Services Committee Strategic Subcommittee. Washington D.C., March 8, 2000.

Elliot, Joyce E., Colonel. “Cyber Terrorism: A Threat to National Security.” Strategy Research Project. Carlisle Barracks, PA: U.S. Army War College, April 9, 2002.

Executive Order 12472. “Assignment of National Security and Emergency Preparedness Telecommunications Functions.” April 3, 1984.

Federal Communications Commission. “Telecommunications Act of 1996.” [http://www.fcc.gov/telecom.html] Accessed September 17, 2005.

Gansler, Jacques S. and Binnenkijk, Hans. “Information Assurance: Trends in Vulnerabilities, Threats, and Technologies.” Working Paper. Hanover, NH: National Defense University, 2003.

General Dynamics. “Network Systems.” [http://www.gd-ns.com/about_us/index.html] Accessed November 20, 2004.

Gershwin, Lawrence K.. “Cyber Threat Trends and U.S. Network Security.” Statement for the Record, Joint Economic Committee, National Intelligence Council, June 21, 2001. [http://www.cia.gov/nic/testimony_cyberthreat.html] Accessed September 17, 2005.

Gratiot County Government, MI. “Appendix VI: Carrier Neutral POP and Circuit Termination Guidelines.” [http://www.co.gratiot.mi.us/administration/Link_Mich_Report_2004/AppendixVIPhysicalNetwork.pdf] Accessed September 17, 2005.

Gray, Robert, Major, USAF. J34 Assessments Branch. [https://www.noradnorthcom.mil/j3/j34] Accessed September 17, 2005.

Hasson, Judi. "Telecom Troubles." *Federal Computer Week* (August 19, 2002). [http://www.fcw.com/article77436-08-19-02-Print] Accessed September 17, 2005.

Homeland Defense Journal. "Target Analysis and Vulnerability Assessment." [http://www.homelanddefensejournal.com/conf_TAVA.htm] Accessed September 17, 2005.

Hust, Gerald R., Major. "Taking Down Telecommunications." Thesis, Maxwell AFB, School of Advanced Airpower Studies, May 28, 1993.

Indonesian Internet Society. [http://www.isoc-id.org/iidp/table_5_selected_us_networks_exchange_points.php] Accessed September 17, 2005.

Investigative Research for Infrastructure Assurance (IRIA) Group – Institute for Security Technology Studies. "Information and Telecommunications Sector Vulnerabilities and Threats." Institute for Security Technology Studies. Hanover, NH: Dartmouth College, September 2002.

Joint Publications 6-0. "Doctrine for Command, Control, Communications, and Computer (C4) Systems Support." Washington D.C.: Joint Chiefs of Staff, May 30, 1995.

Joint Task Force-Global Network Operations (JTF-GNO). "JTF-GNO Mission." [http://www.cert.mil/misc/mission.htm] Accessed September 17, 2005.

Lack, Lindsey, and Ferrari, Jair, MAJ. Brazilian AF. "Critical Infrastructure Protection – Telecommunications and Space Interdependencies." Report, CS4920. Monterey CA: Naval Postgraduate School, September 24, 2002: 1-11.

Level (3) Communications. "(3)Center Colocation." [http://www.level3.com/558.html] Accessed September 17, 2005.

Lewis, Ted. *Critical Infrastructure Protection in Homeland Security: Defending a Networked Nation*. Hoboken, NJ: John Wiley & Sons Inc., September 2004.

———. CS 3660 Telecom Sector Presentation. Monterey, CA: Naval Postgraduate School, 2004.

Light Reading. “L-3 Acquires Wescam.” September 18, 2002. [www.lightreading.com/document.asp?doc_id=21368] Accessed September 17, 2005.

———. “Marconi Demos 10-Gig Encryption.” July 01, 2003. [www.lightreading.com/document.asp?doc_id=36331] Accessed September 17, 2005.

McDougall, Paul. “Navy Seeks Secure Software.” *Information Week*, May 31, 2004. [http://www.informationweek.com/] Accessed September 17, 2005.

MCI Inc. [http://global.mci.com/about/network/global_presence/northamerica/mci_global_presence_NORTHAMERICA.pdf] Accessed September 17, 2005.

———. [http://www.mae.net/peer/] Accessed September 17, 2005.

MerriamWebster Online Dictionary. [http://www.m-w.com/cgi-bin/dictionary?book=Dictionary&va=telecommunication] Accessed September 17, 2005.

Messmer, Ellen. “DISA fortifying military’s IT defenses.” *Network World Fusion* (June 2, 2003). [http://www.networkworld.com/news/2003/0602disa.html] Accessed September 17, 2005.

Miller, Sarah. “Main Passes SAS70 Type 2 Audit.” Axis Marketing & PR, LLC. [http://www.365main.net/pr_02_7_05_sas_70.html] Accessed September 17, 2005.

Minihan, Kenneth, Lieutenant General, USAF. “Vulnerabilities of the National Information Infrastructure.” Testimony to the Senate Governmental Affairs Committee Hearing, June 24, 1998. [http://hsgac.senate.gov/62498minihan.htm] Accessed September 17, 2005.

Moulton, Pete. “Can Your Network Hold Up to Terrorism?” Prentice Hall PTR, Jan 25, 2002. [http://www.phptr.com/articles/article.asp?p=25087] Accessed September 17, 2005.

Nagle, Timothy J. “The President’s National Security Telecommunications Advisory Committee (NSTAC).” (Presentation. ABA Information Security Committee, November 7, 2001). [http://www.abanet.org/scitech/ec/isc/PDF/TimothyNagle.pdf] Accessed September 17, 2005.

NAP of the Americas. [http://www.napoftheamericas.net/faq.cfm] Accessed September 17, 2005.

National Aeronautics and Space Administration. [http://www.arc.nasa.gov/] Accessed September 17, 2005.

National Communications System. [http://gets.ncs.gov/] Accessed September 17, 2005.

National Coordinating Center for Telecommunications. [http://www.ncs.gov/ncc/main.html] Accessed September 17, 2005.

National Reliability and Interoperability Council. [http://www.nric.org/charter_vii/nric_vii_org.html] Accessed September 17, 2005.

National Security and Emergency Preparedness Telecom News. Published by the Office of the Manager, National Communications System, Mr. Brenton Greene. Issue 1, 2003. Washington, D.C.: NCS, 2003.

———. Ms. Diann McCoy. Issue 2, 2000. Washington, D.C.: NCS, 2000.

National Telecommunications and Information Administration. [http://www.ntia.doc.gov/] Accessed September 17, 2005.

Network Reliability and Interoperability Council VI. Homeland Security Physical Security (Focus Group 1A). Prevention Report Issue 1, December 2002. Washington, D.C.: NRIC Council VI, 2002.

Newby, Hunter. “I Now Pronounce You VoIP and Ethernet: Not Just a Marriage of Convenience.” Wall Street Technology Association. [http://www.wsta.org/publications/articles/0204_article01.html] Accessed September 17, 2005.

NSTAC (National Security Telecommunications Advisory Committee). “Convergence Task Force Report” June 2001. Report. Washington, D.C.: NSTAC, 2001: 1-32.

———. “Network Security/Vulnerability Assessments Task Force Report.” March 2002. Report. Washington, D.C.: NSTAC, 2002: 1-75.

———. “Vulnerabilities Task Force Report Concentration of Assets: Telecom Hotels” February 12, 2003. Report. Washington, D.C.: NSTAC, 2003: 1-12.

Ogren, Joel G., and Langevin, James R.. “Responding to the Threat of Cyberterrorism through Information Assurance.” Thesis. Monterey, CA: Naval Postgraduate School, 19990817-106, June 1999.

Olsen, Karen, and Tebbutt, John. NIST (National Institute for Standards and Technology). "The Impact of the FCC's Open Network Architecture on NS/NP Telecommunications Security." Special Publication 800-11, August 21, 1995. Gaithersburg, MD: NIST, U.S. Department of Commerce, 1995.

One Wilshire, CRG West. [http://www.onewilshire.com/about_us/management.htm] Accessed September 17, 2005.

Paller, Alan. "Fighting Back Against Cybercrime: What Works?" The SANS Institute. [www.sans.org] Accessed November 20, 2004.

Progress Telecom LLC. [http://www.epik.net/pdf/Tier%201%20(300dpi)V13.pdf] Accessed September 17, 2005.

Reed, Warren G., Director. Information Management and Technology Division, Testimony, House of Representatives, Subcommittee on Transportation, Aviation, and Materials Committee on Science & Technology. Washington D.C.: U.S. GAO, October 17, 1983.

SAIC (Science Applications International Corporation). "Securing the Homeland." Brochure. McLean, VA: SAIC, 2003.

SBC Communications Inc. [http://www.pacbell.com/Products/NAP/] Accessed September 17, 2005.

SearchWebServices. [http://searchwebservices.techtarget.com/sDefinition/0,,sid26_gci214106,00.html] Accessed September 17, 2005.

Securify. "The Secure Platform." [http://www.securify.com/vision/] Accessed November 20, 2004.

SHARES Bulletin 04-14. March 2004. [http://www.ncs.gov/library/SHARES/SHARES%20Bulletin%2014.pdf] Accessed November 20, 2004.

Spillis, Candela. DMJM, Inc. [http://www.scpmiami.com/Firmprofile.htm] Accessed September 17, 2005.

Sprint Corporation. [www.sprintlink.net] Accessed September 17, 2005.

Switch and Data. [http://www.switchanddata.com/subpage.asp?navid=3&id=18] Accessed September 17, 2005.

Tech Web Encyclopedia. [http://www.techweb.com/encyclopedia/defineterm.jhtml?term=telecomhotel] Accessed September 17, 2005.

Techsoft, Technical Software Services, Inc. “Experience.” 2004. [http://www.techsoft.com/] Accessed September 17, 2005.

The National Strategy for Homeland Security. Washington D.C.: Office of Homeland Security, July 2002.

The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets. Washington D.C.: The White House, February 2003.

The President’s National Security Telecommunications Advisory Committee. “Vulnerabilities Task Force Report—Concentration of Assets: Telecom Hotels.” 1–7, February 12, 2003. Washington, D.C.: NSTAC, 2003.

U.S. Army Engineer Research and Development Center. [http://www.erdc.usace.army.mil/pls/erdcpub/www_org_info.show_page?f_id=143318&f_parent=55173] Accessed September 17, 2005.

U.S. GAO. “ADP, IRM & Telecommunications” (ADP-Automatic Data Processing, IRM-Information Resources Management). GAO-IMTEC-85-9, April 1985. Washington, D.C.: *U.S. General Accounting Office*, 1985.

———. “Potential Terrorist Attacks—Additional Actions Needed to Better Prepare Critical Financial Market Participants.” Report to Congressional Requesters, GAO-03-251, February 2003. Washington, D.C.: U.S. General Accounting Office, 2003.

———. “Potential Terrorist Attacks.” Report to House of Representatives, Committee on Financial Services, GAO-03-414, February 2003. Washington, D.C.: U.S. General Accounting Office, 2003.

United States Air Force Fact Sheet. “68th Information Operations Squadron.” October 2002. [http://www.brooks.af.mil/HSW/PA/68IOS%20fact.htm] Accessed September 17, 2005.

United States Internet Service Provider Association. [http://www.cix.org] Accessed September 17, 2005.

Verizon Communications Inc. [http://www22.verizon.com/enterprisesolutions/Includes/SiteUtilities/JCMSSkeleton.jsp?filePath=/Anonymous/Default/ProductDetail/BusContinuity/Business_Recovery_m.html] Accessed September 17, 2005.

Wennergren, Dave. Chief Information Officers Council. “Ask The CIO.” November 3, 2003. [http://www.cio.gov/documents/wtop_ask_cio_wennergren_nov_03_2003.html] Accessed September 17, 2005.

Wikipedia Encyclopedia. [http://en.wikipedia.org/wiki/Telecommunication] Accessed September 17, 2005.

Young, Stephen. “Telecom Hotels.” Interview. *E AI Journal*. November/December 2000. [http://www.bijonline.com/PDF/Telecom%20Hotels.pdf] Accessed September 17, 2005.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

3. Ted Lewis
   Naval Postgraduate School
   Monterey, California

4. Rudy Darken
   Naval Postgraduate School
   Monterey, California