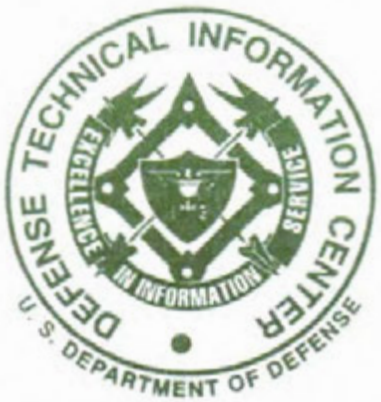
(3)

UNCLASSIFIED/LIMITED

DEFENSE TECHNICAL INFORMATION CENTER



UNCLASSIFIED/LIMITED

DEFENSE INFORMATION SYSTEMS AGENCY
DEFENSE TECHNICAL INFORMATION CENTER
8725 JOHN J. KINGMAN ROAD, SUITE 0944
FORT BELVOIR, VIRGINIA 22060-6218

Information Warfare - Defense

- Assessing CONUS Vulnerabilities and Adversary Offensive Capabilities

Seminar Materials Book

8-10 April 1997

Sponsored by:
Office of the Secretary of Defense, Net Assessment (OSD/NA)
Pentagon, Room 3A930
Washingon, DC 20301

Booz·Allen & Hamilton Inc.
4301 North Fairfax Drive
Arlington, VA 22203
(703) 902-4844

Proprietary

Administrivia

- Classification of Seminar
  - Seminar discussions at the TS SI/TK level
  - NO classified discussions in the hallways
- Mail-Stop
  - Fill out notebooks with name and mail-stop
- Messages
  - Received at 703-902-4844 or 703-908-4300

IW-Defense Seminar
Agenda

Tuesday, 8 April 1997

0730 - 0800 .....**Breakfast** and Registration

0800 - 0805 .....**Welcome/Opening** Remarks

0805 - 0830 .....**IW** Net Assessment
COL Scott Rowell, USA, OSD/NA

0830 - 0900 .....**Seminar** Overview
Melissa Hathaway, Booz·Allen & Hamilton

0900 - 0930 .....**Overview** of the PCCIP
Brent Greene, DUSD/Policy

- Break -

0945 - 1000 .....**Overview** of the NII/DII
Mark Jacobsohn, Booz·Allen & Hamilton

1000 - 1030 .....**Transportation** Infrastructure
Rich Phares, Booz·Allen & Hamilton

1030 - 1130 .....**Power** Infrastructure
Brad Bigelow, NCS-N53

--- Working Lunch ---

1215 - 1315 .....**Telecommunications** Infrastructure
Mel Sobotka, Booz·Allen & Hamilton

1315 - 1415 .....**System** Security and Information Warfare: Networks At Risk
Ted Phillips, Booz·Allen & Hamilton

-- Break --

1430 - 1500 .....**IW-D** Indications & Warning
LT Sean Heritage, USN, JCS-J2-J

Tuesday, 8 April 1997 Continued

-- Break --

1515 - 1615 .....Reading

1615 - 1700 .....Discussion

Wednesday, 9 April 1997

0730 - 0800 ..... Breakfast and Registration

0800 - 0830 ..... Deliverable Overview
Melissa Hathaway, Booz·Allen & Hamilton

-- Break --

0845 - 1700 ..... Break into two teams

(Working Lunch served at 1200)

Team Responsibilities

- Select CONUS targets (targets critical to military operations)
- Identify targeting criteria (why chosen, how to attack, when to attack)
- Attack objectives (disrupt, delay, deny, destroy) (what nodes?)
- Identify implications of attacks (impact on ultimate objective of attacks)
- Assess operational implications on U.S. force projection and operations

Thursday, 10 April 1997

0730 - 0800 .....Breakfast and Registration

0800 - 0900 .....Team 1 Briefing

0900 - 1000 .....Team 2 Briefing

- Break -

1030 - 1200 .....Structured Discussion of Team Results

- Working Lunch -

1230 - 1430 .....Structured Discussion of Current and Potential Nations/Actors

1430 - 1500 .....Seminar Wrap-Up

Information Warfare-Defense Seminar

8-10 April 1997

Sponsored by:
Office of the Secretary of Defense, Director of Net Assessment
COL Scott Rowell
Pentagon Room 3A930
Washington, DC

Conducted at:
Booz-Allen & Hamilton Inc.
4301 North Fairfax Drive
Arlington, Virginia
(703) 902-4844

Purpose of Seminar

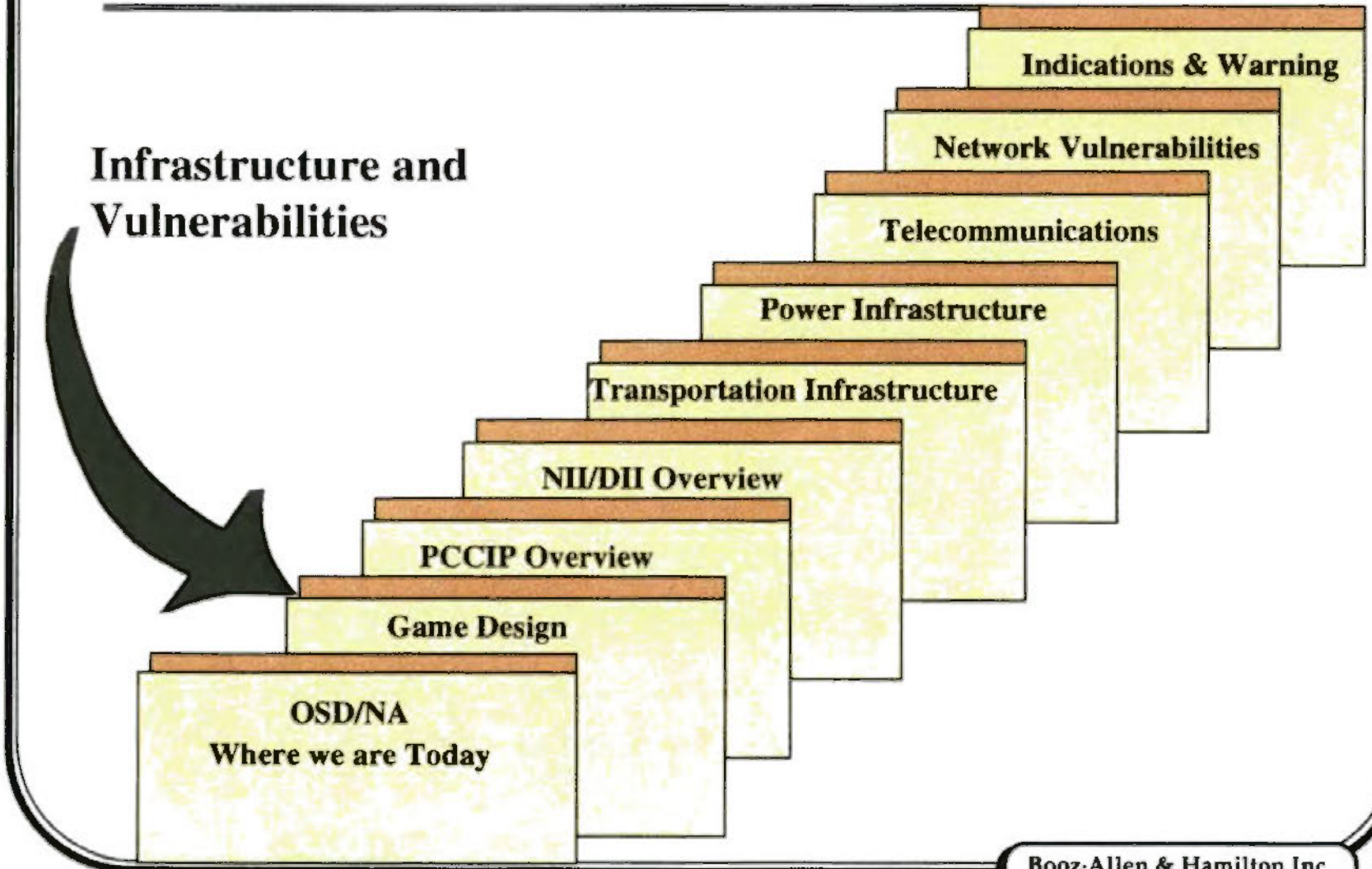
- Review critical CONUS infrastructures and identify/assess their vulnerabilities and impact (if targeted) on military force projection and theater operations.

- Provide a framework to focus the Net Assessment.

Seminar Objectives

- Review and understand infrastructures and identify and explore their vulnerabilities.
- Identify and evaluate interdependencies between civil and military infrastructures.
- Identify technologies and capabilities necessary to exploit infrastructure vulnerabilities and the implications of exploitation (risks).
- Identify nations/actors that maintain or could obtain those offensive capabilities.
  - Identify potential sources of critical technologies and capabilities.

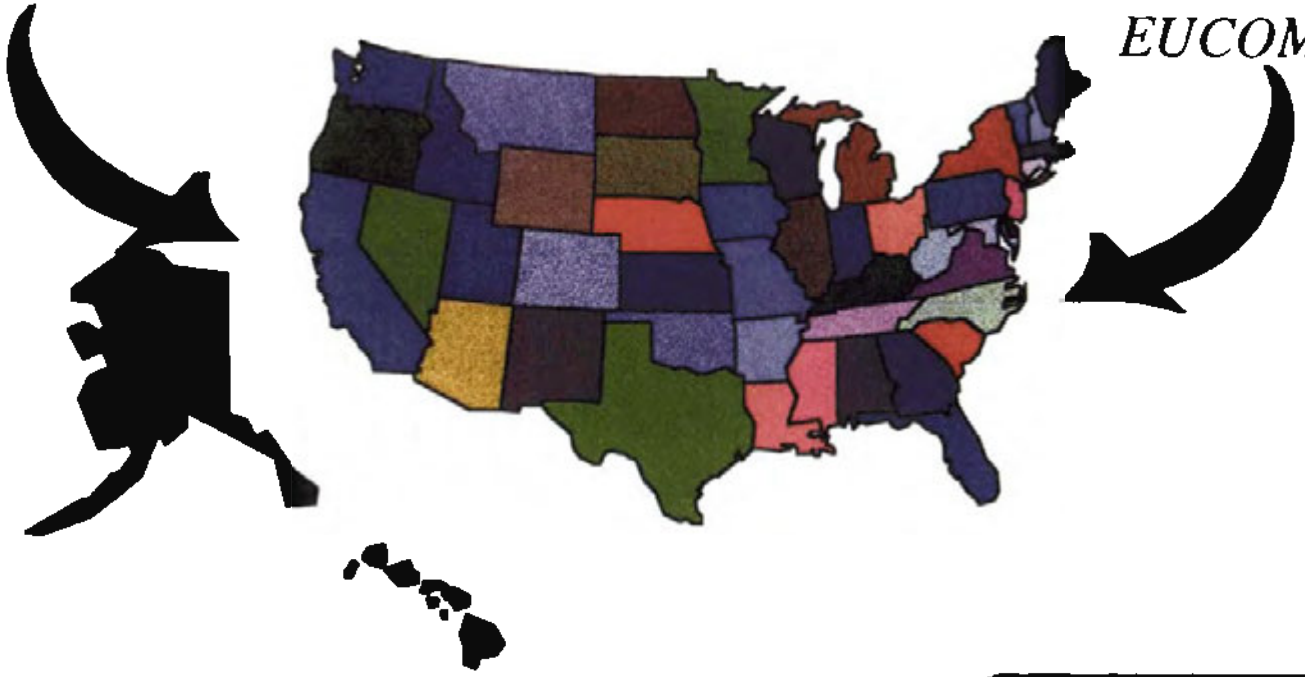
Overview Day One



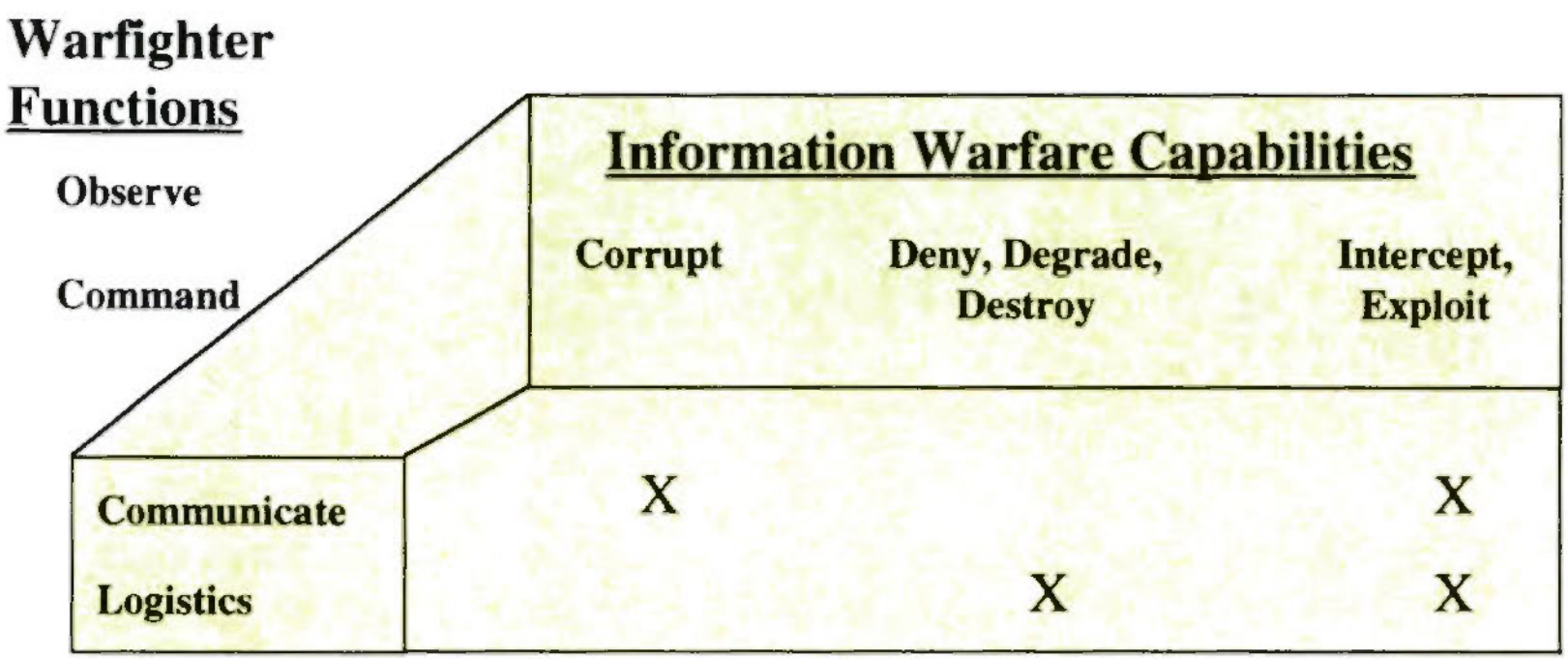
Day Two: Players Divide into 2 Teams

Team One:
PACOM
SOUTHCOM

Team Two:
ACOM
CENTCOM
EUCOM



Net Assessment Focus for Seminar



Focus on the Operational Level of War
What does it mean to a CINC if one of these functions is vulnerable?
What does it mean to a Theater level operation?

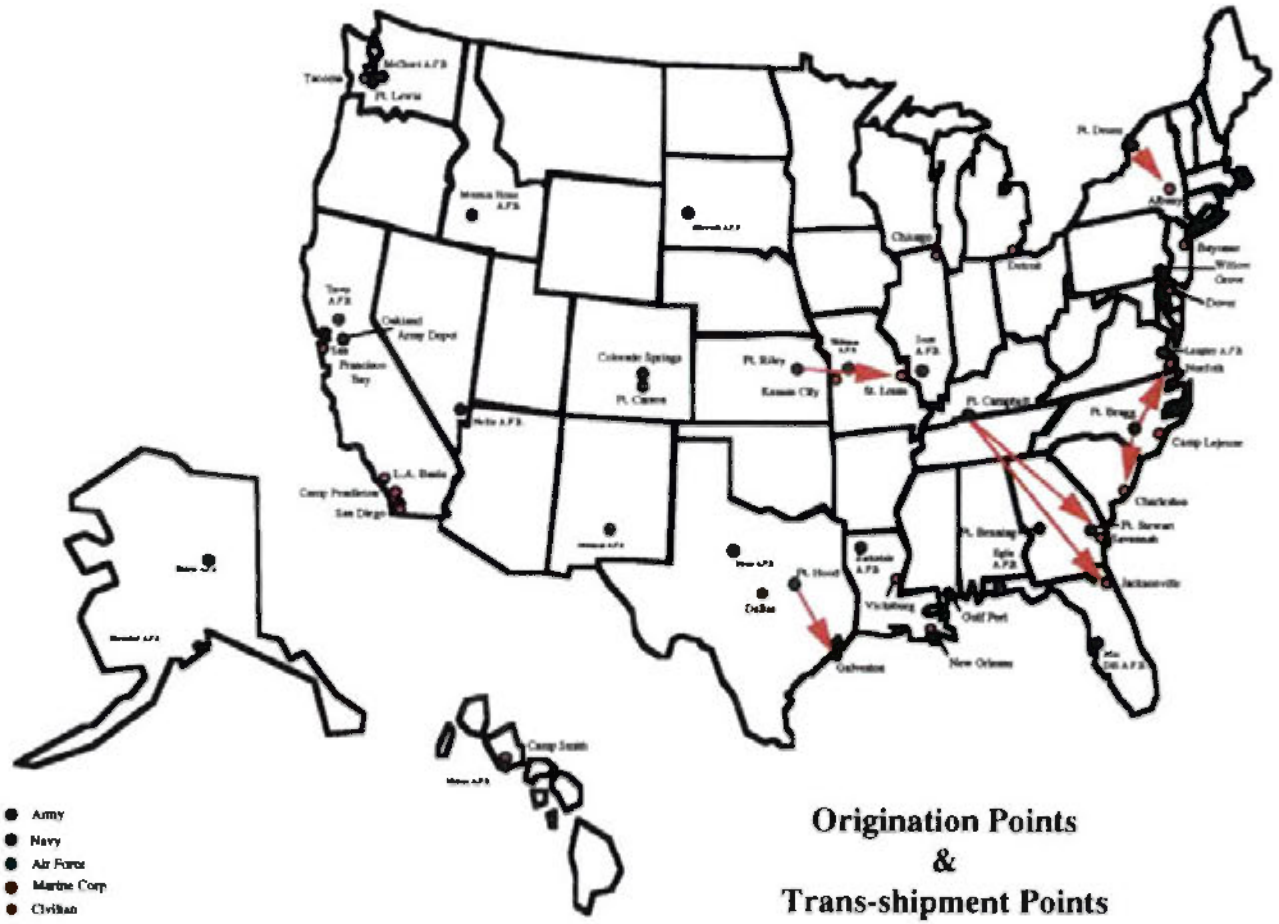
Team Mission Objective

- Delay, deny, exploit a notional deployment of a Corps and its supporting assets (air, sea, communications, etc.) to any AOR.

Overview of Day Two

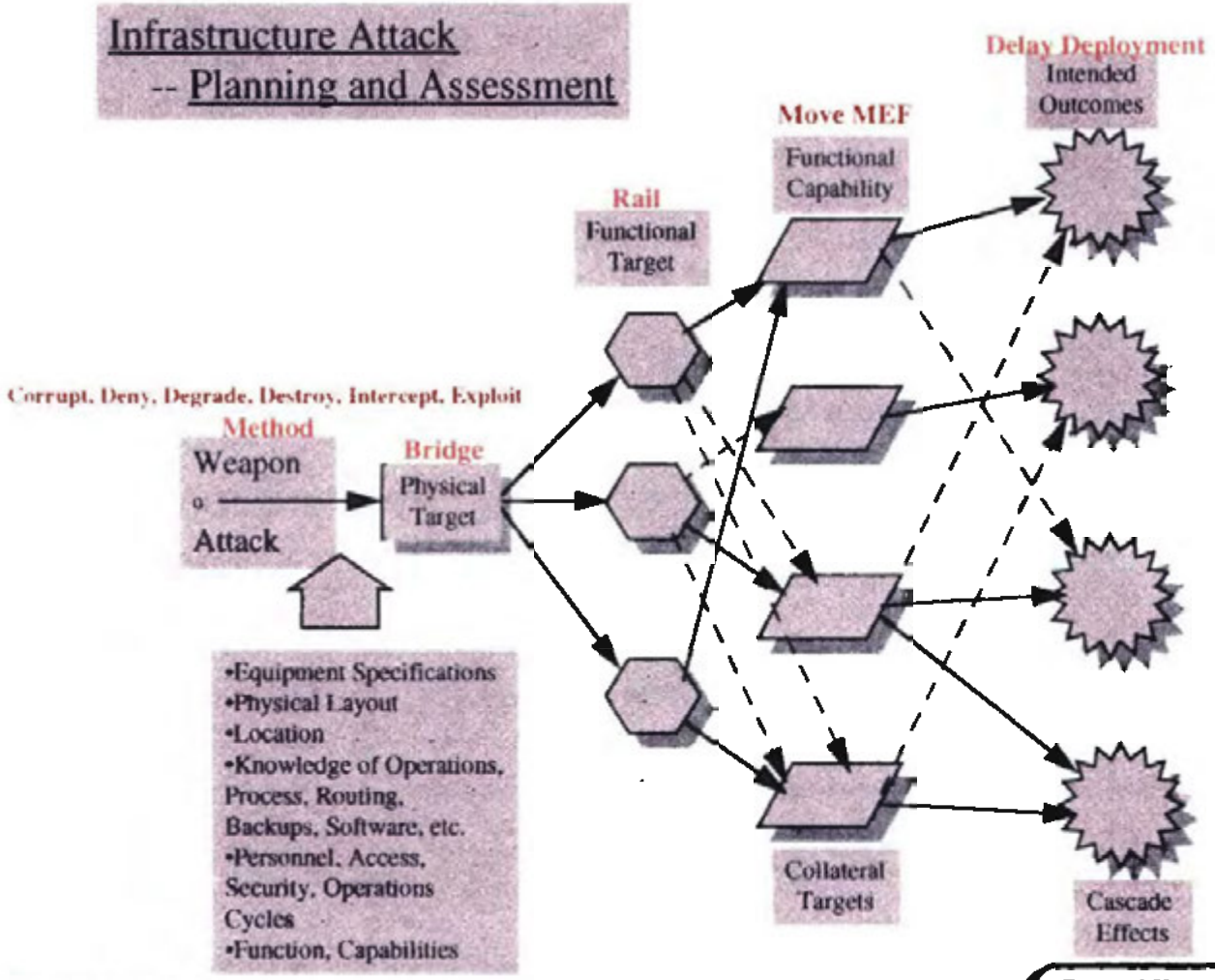
- Teams identify target sets (critical nodes, etc.) in the sectors of power, telecommunications, and transportation.
  - Identify why targets chosen.
  - Identify what offensive capabilities used.
  - Identify and discuss implication of targeting choices.

Analysis of CINC Dependencies



Origination Points
&
Trans-shipment Points

Nominated Methodology



Deliverables

- Teams prepare briefings for plenary session highlighting the most significant vulnerabilities by sector that will impact:
  - Notional military deployment - to overseas AOR.
  - Logistics associated with the deployment.
  - Communications that support military operations.

Overview of Day Three

- Teams brief results of Day Two sessions.
- Participants discuss results of Day Two sessions.
  - Target set choices.
  - Offensive capabilities used.
  - Nations/actors that possess or could obtain/ develop those capabilities (at what cost).

Seminar Discussion Questions

- What are the 2 or 3 most critical (vulnerable) nodes in each of the three infrastructures (telecommunications, power, transportation)?
- What measures must be taken to fortify these nodes?
- What is the major offensive capability or action that could be used to destroy, delay, disrupt, deny, or degrade CINC deployments/operations in each AOR (e.g., physical destruction, electronic, human)?

Seminar Discussion Questions

- What specific countries currently possess (or could purchase) the capabilities necessary to carry out the postulated attacks cited in the previous questions?
- What additional countries could carry out these attacks in 10 years?
  - Sources of technology and capabilities
  - Importance of management and planning
- Which CINC AOR is the most vulnerable (easiest to impact), if the CONUS infrastructures are attacked?
  - What is this based upon, fewer critical nodes, less redundancy?
  - Easier access to critical networks or nodes supporting that CINC?

Seminar Discussion Questions

- Which infrastructure's outages impact the deployment/ operations the most?

- Are there operational work-arounds to avoid serious delays or disruptions in deployment/operations for that CINC AOR?

CLASSIFICATION: _____

ATTACK PLANNING FORM

Team: _____

Mission Objective: _____

_____

❑ Corrupt ❑ Deny ❑ Delay ❑ Degrade ❑ Destroy ❑ Intercept ❑ Exploit

Method of Attack:

❑ Physical Destruction ❑ Computer/Electronic ❑ Human

Military Installation Affected: _____

Target(s)/Sector(s): Transportation Electric Power Telecommunications
(Circle one)

Physical Target(s): _____

_____

_____

Functional Target(s): _____

_____

_____

Functional Target(s) Characteristics:

	Know	Need to Know
Physical:	_____	_____
	_____	_____
	_____	_____
	_____	_____
	_____	_____
Electronic:	_____	_____
	_____	_____
	_____	_____
	_____	_____
	_____	_____
Operational:	_____	_____
	_____	_____
	_____	_____
	_____	_____

CLASSIFICATION: _____

CLASSIFICATION: _____

Countermeasures Now in Place:
(Protection and Security, Redundancies)

Likely Future Countermeasures:
(Protection and Security)

Operational Alternatives:
(Contingency Plans)

Measures of Effectiveness[1]:
(Primary and Cascading)

Operational Implications for US Force Deployment, Projection and Operations:

[1] Include Primary, Secondary or Collateral and Cascading or Synergistic effects

CLASSIFICATION: _____

CLASSIFICATION: _____

ATTACK PLANNING FORM

Example

Team: **ACOM, CENTCOM, EUCOM**

Mission Objective: **Delay deployment of 2nd MEF out of Camp Lejeune**

❑ Corrupt ❑ Deny ☒ **Delay** ❑ Degrade ❑ Destroy ❑ Intercept ❑ Exploit

Method of Attack:

❑ Physical Destruction ☒ **Computer/Electronic** ❑ Human

Military Installation Affected: **Camp Lejeune, NC**

Target(s)/Sector(s): **Transportation** Electric Power Telecommunications
(Circle one)

Physical Target(s): **Switch Control Center**

Functional Target(s): **Rail Network**

Functional Target(s) Characteristics:

	Know	Need to Know
Physical:	approx. location	exact building/room
Electronic:	computer operated	operating system firewalls? network protocol
Operational:	Systems Administrator Monitors	Administrator on line 24 hours?

CLASSIFICATION: _____

Countermeasures Now in Place: Monitor unusual switching activities
(Protection and Security, Redundancies)

Likely Future Countermeasures: Hardening of rail switch, firewalls
(Protection and Security)

Operational Alternatives: 2nd MEF moves by other means (e.g., road);
(Contingency Plans) 2nd MEF deploys out of another base
Another MEF is deployed

Measures of Effectiveness[1]: Delaying the 2nd MEF, delays all forces from deployment because the 2nd MEF is the "spear-head" force and must establish position before any of the other forces can leave CONUS.
(Primary and Cascading)

Operational Implications for US Force Deployment, Projection and Operations:

Delaying the 2nd MEF, delays all forces from deployment because the 2nd MEF is the "spear-head" force and must establish position before any of the other forces can leave CONUS.

[1] Include Primary, Secondary or Collateral and Cascading or Synergistic effects

Table of Military Bases

BASE	CINC RESPONSIBILITY	ASSETS/FORCES	MILITARY C2 NODES	LONG-HAUL POWER	TRANSPORTATION
Barksdale AFB, LA					
	SOUTHCOM	8th Air Force		2 nodes	3 interstates
		2nd Bomb Wing (B-52s)		2 lines	3 major highways
		917th Wing (A-10s, B-52s)			10 rail lines
					1 airport
Camp Lejeune, NC					
	ACOM	II MEF		4 nodes	4 major highways
	CENTCOM	2nd Marine Division		8 lines	1 rail line
	EUCOM				
	SOUTHCOM				
Camp Pendleton, CA					
	PACOM	I MEF		3 nodes	4 major highways
		1st Marine Division		2 lines	1 rail line
Camp Smith, HI					
	PACOM	PACOM HQ (Camp Smith)	PACOM HQ	3 nodes	3 ports
		JICPAC (Pearl Harbor)			
		PACAF (Hickam AFB)			
		PACFLT HQ (Pearl Harbor)			
Charleston, SC					
	ACOM	Naval Facilities	Submarine	6 nodes	1 interstate
		POE for forces from	Transportation Node	12 lines	3 major highways
		Ft. Bragg			4 rail lines
					1 port
					1 airport

BASE	CINC RESPONSIBILITY	ASSETS/FORCES	MILITARY C2 NODES	LONG-HAUL POWER	TRANSPORTATION
Colorado Springs, CO					
	SPACECOM	NORAD	NORAD	4 nodes	2 interstates
	ACOM	Falcon AFB (50th Space	Falcon AFB (satellites)	7 lines	3 rail lines
	CENTCOM	Wing, Space Warfare Center)	SPACECOM		1 airport
	EUCOM	Peterson AFB (Air Force			
	SOUTHCOM	Space Command, 21st Space			
	PACOM	Wing)			
Dyess AFB, TX					
	ACOM	7th Wing (B-1B, C-130H)		4 nodes	2 interstates
	CENTCOM			6 lines	2 major highways
	EUCOM				3 rail lines
	SOUTHCOM				
	PACOM				
Dover AFB, DE					
	ACOM	436th Airlift Wing (C-5s)	Transportation Node	3 nodes	3 major highways
	EUCOM	512th Airlift Wing		6 lines	
	CENTCOM				
Eglin AFB, FL					
	ACOM	53rd Fighter Wing	AFSOC	2 nodes	4 major highways
	CENTCOM	(F-15C/D/Es, F-16s)		4 lines	
	EUCOM	33rd Fighter Wing (F-15C/D)			
	SOUTHCOM	919th Special Operation Wing			
	PACOM				

BASE	CINC RESPONSIBILITY	ASSETS/FORCES	MILITARY C2 NODES	LONG-HAUL POWER	TRANSPORTATION
Ellsworth AFB, SD					
	ACOM	28th Bomb Wing (B-1s)		4 nodes	2 interstates
	CENTCOM			7 lines	2 major highways
	EUCOM				3 rail lines
	SOUTHCOM				
	PACOM				
Ft. Benning, GA					
	PACOM	3rd Bde, 3rd ID		7 nodes	3 major highways
	ACOM	75th Ranger Regiment		8 line	4 rail lines
	SOUTHCOM				
	CENTCOM				
Ft. Bragg, NC					
	ACOM	XVIII Airborne Corps	Special Operations	9 nodes	2 interstates
		82nd Airborne	Command	10 lines	4 major roads
		4th POG			2 rail lines
		Army Special Forces			
		Command			
		7th Special Forces Group			
		3rd Special Forces Group			
Ft. Campbell, KY					
	SOUTHCOM	101st Air Assault Division		5 nodes	2 interstates
	CENTCOM	160th SOAR		3 lines	3 major roads
		5th Special Forces Group			1 rail line

BASE	CINC RESPONSIBILITY	ASSETS/FORCES	MILITARY C2 NODES	LONG-HAUL POWER	TRANSPORTATION
Ft. Carson, CO					
	SOUTHCOM	3rd Armored Cavalry Rgt.		4 nodes	2 interstates
		3rd Bde, 4th ID		7 lines	2 major highways
		10th Special Forces Group			4 rail lines
					1 airport
Ft. Drum, NY					
	ACOM	10th Mountain Division		5 nodes	2 interstates
				7 lines	2 major highways
					1 rail line
Ft. Hood, TX					
	SOUTHCOM	III Corps	Corps HQ	5 nodes	2 interstates
		1st and 2nd Bde,		8 lines	1 highway
		4th Infantry Division			4 rail lines
Ft. Lewis, WA					
	PACOM	1st Special Forces Group		5 nodes	1 interstate
		(Airborne)		10 lines	2 major highways
		2nd Bn (Rangers), I Corps			1 port
		3rd Bde, 2nd ID			1 airport
		3rd Bde, 25th ID			

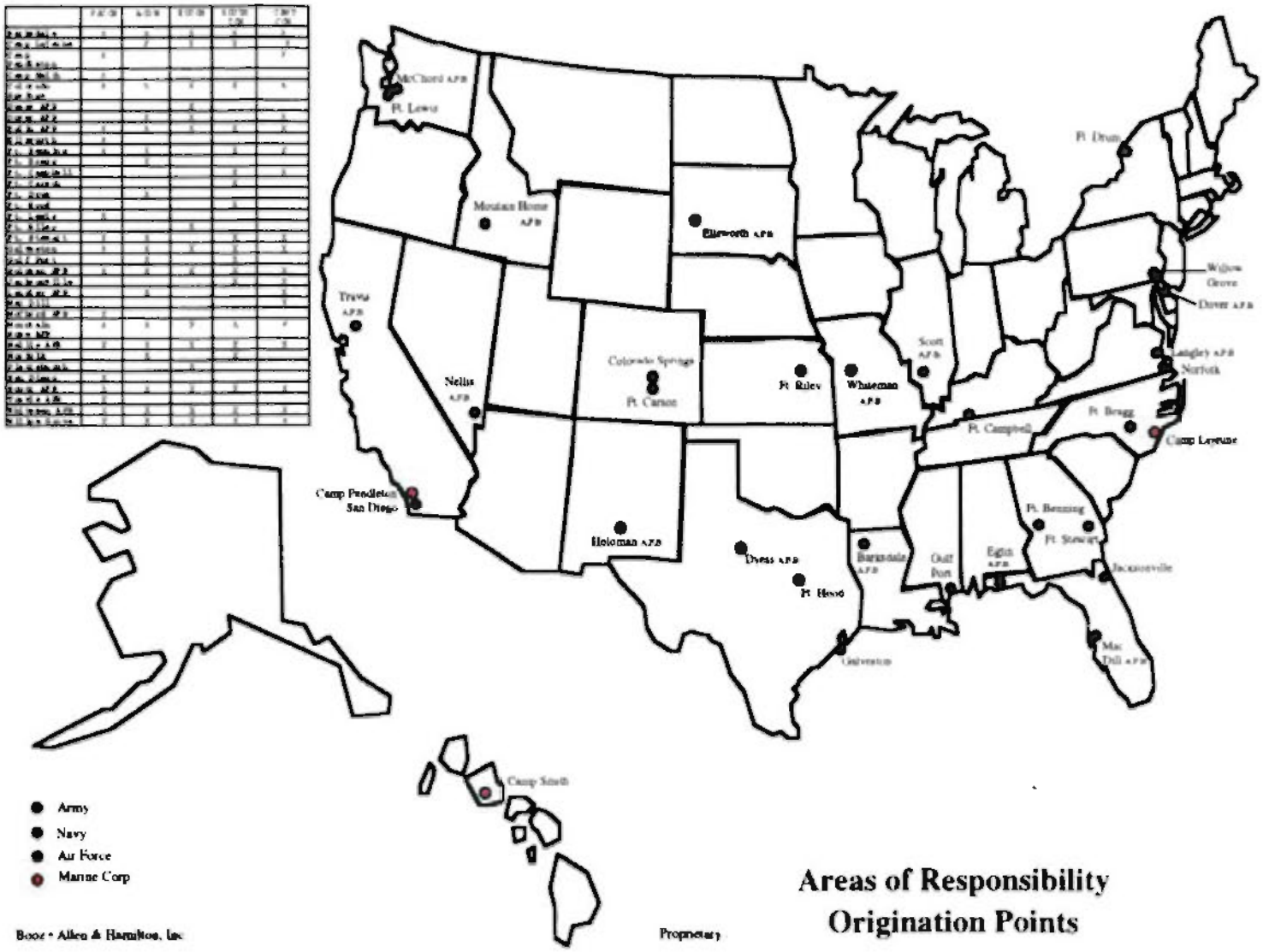
BASE	CINC RESPONSIBILITY	ASSETS/FORCES	MILITARY C2 NODES	LONG-HAUL POWER	TRANSPORTATION
Ft. Riley, KS					
	EUCOM	1st Bde, 1st ID		8 nodes	2 interstates
		3rd Bde, 1st Armored Division		6 lines	1 major highway
Ft. Stewart, GA					
	PACOM	1st Bde, 3rd ID		5 nodes	3 major highways
	ACOM	2nd Bde, 3rd ID		5 lines	2 rail lines
	SOUTHCOM				
	CENTCOM				
Galveston, TX					
	ACOM	Navy MCM HQ	HQ	4 nodes	2 major highways
	CENTCOM			3 lines	1 port
	EUCOM				2 airports
	SOUTHCOM				
	PACOM				
Gulf Port, MS					
	ACOM	2 Frigates		7 nodes	2 interstates
	SOUTHCOM	1 cruiser		6 lines	1 major highway
					3 rail lines
					1 port

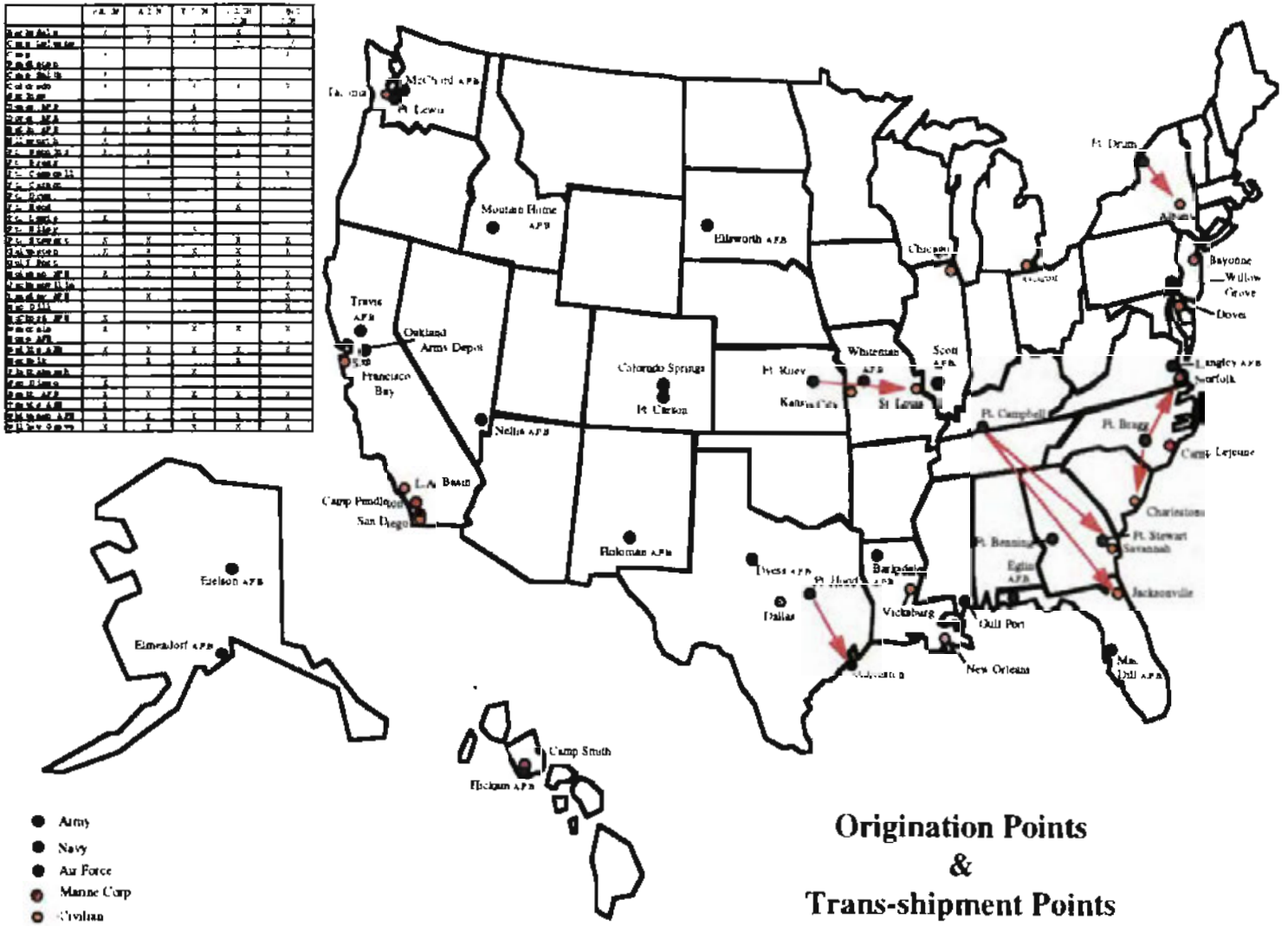
BASE	CINC RESPONSIBILITY	ASSETS/FORCES	MILITARY C2 NODES	LONG-HAUL POWER	TRANSPORTATION
Holoman AFB, NM					
	ACOM	49th Fighter Wing (F-117)		4 nodes	2 major highways
	CENTCOM			5 lines	2 rail lines
	EUCOM				
	SOUTHCOM				
	PACOM				
Jacksonville, FL					
	SOUTHCOM	POE for forces from		7 nodes	3 interstates
	CENTCOM	Ft. Campbell		4 lines	1 major highway
		1 CVBG			5 rail lines
					1 airport
					1 port
Langley AFB, VA					
	ACOM	HQ ACC	HQ	6 nodes	3 interstates
	CENTCOM	1st Fighter Wing (F-15s)		6 lines	2 highways
					2 rail lines
					1 port
					1 airport
Mac Dill AFB, FL					
	CENTCOM	HQ US SOCOM	CINC HQ	9 nodes	4 Interstates
		HQ US CENTCOM		10 lines	2 highways
					5 rail lines
					1 port
					1 airport

BASE	CINC RESPONSIBILITY	ASSETS/FORCES	MILITARY C2 NODES	LONG-HAUL POWER	TRANSPORTATION
McChord AFB, WA					
	PACOM	62nd Airlift Wing	Transportation Node	5 nodes	1 interstate
		(C-141s)		10 lines	2 major highways
					1 port
					1 airport
Mountain Home					
	ACOM	366th Wing (Composite Wing:		4 nodes	1 major highway
	CENTCOM	F-16Cs, F-15Es, F-15Cs,		6 lines	
	EUCOM	KC-135s)			
	SOUTHCOM				
	PACOM				
Nellis AFB, NV					
	ACOM	Air Warfare Center		7 nodes	2 interstates
	CENTCOM	57th Wing (A-10s, F-15s,		11 lines	1 major highway
	EUCOM	F-16s, HH-60s, Predator			2 rail lines
	SOUTHCOM	UAVs)			
	PACOM				
Norfolk, VA					
	ACOM	2 CVBGs	Multiple Naval C2 nodes	5 nodes	1 interstate
	SOUTHCOM	Norfolk Naval Station		10 lines	5 major highways
		Little Creek Amphibious Base			5 rail lines
		NAS Norfolk (carrier escort)			1 port
		NAS Oceana (carrier aircraft)			1 airport

BASE	CINC RESPONSIBILITY	ASSETS/FORCES	MILITARY C2 NODES	LONG-HAUL POWER	TRANSPORTATION
San Diego, CA					
	PACOM	3rd Fleet	Fleet HQ	3 nodes	5 major highways
		2 CVBGs	Submarine	3 lines	2 rail lines
		MCAS Miramar			1 port
					1 airport
Scott AFB, IL					
	ACOM	HQ AMC	Transportation Node	6 nodes	3 interstates
	CENTCOM	HQ US TRANSCOM		6 lines	2 highways
	EUCOM	Tanker Airlift Control Center			3 rail lines
	SOUTHCOM				1 port
	PACOM				1 airport
Travis AFB, CA					
	PACOM	15th Air Force (C-5s,	Transportation Node	6 nodes	2 interstates
		C-141s, KC-10s)		6 lines	3 major highways
					1 port
					1 airport
					3 rail lines
Whiteman AFB, MO					
	ACOM	509th Bomb Wing (B-2s)		3 nodes	2 major highways
	CENTCOM			2 lines	1 rail line
	EUCOM				
	SOUTHCOM				
	PACOM				

BASE	CINC RESPONSIBILITY	ASSETS/FORCES	MILITARY C2 NODES	LONG-HAUL POWER	TRANSPORTATION
Willow Grove, PA					
	ACOM	913th Airlift Wing		7 node	2 interstates
	CENTCOM	193rd SOG		7 lines	3 major highways
	EUCOM	4th POG			1 airport
	SOUTHCOM				1 port
	PACOM				6 rail lines


Army
Navy
Air Force
Marine Corp
Areas of Responsibility
Origination Points
Booz • Allen & Hamilton, Inc.
Proprietary



Origination Points & Trans-shipment Points

Booz • Allen & Hamilton, Inc. - Proprietary

Trans - shipment


McChord AFB
Travis AFB
Sunnyvale
Monterey
San Diego
Offutt AFB
Colorado Springs
Kirtland AFB
Ft. Bliss
Ft. Hood
Scott AFB
LFMF Strategic Communications Site
Walter Reed
New London
Dover
Ft. Meade
Andrews
Langley
Ft. Bragg
Charleston
Hunter Army Airfield
Eglin AFB
Gulf Port
Galveston
Mac Dill AFB
Key West
Pearl Harbor
Hickam AFB
Army
Navy
Air Force
Marine Corp
Other Agency
Booz • Allen & Hamilton, Inc.
- Proprietary
C2 Nodes

National Information Infrastructure (NII) & Defense Information Infrastructure (DII)

Presented by

Mark Jacobsohn
Booz·Allen & Hamilton Inc.
8 April 1997

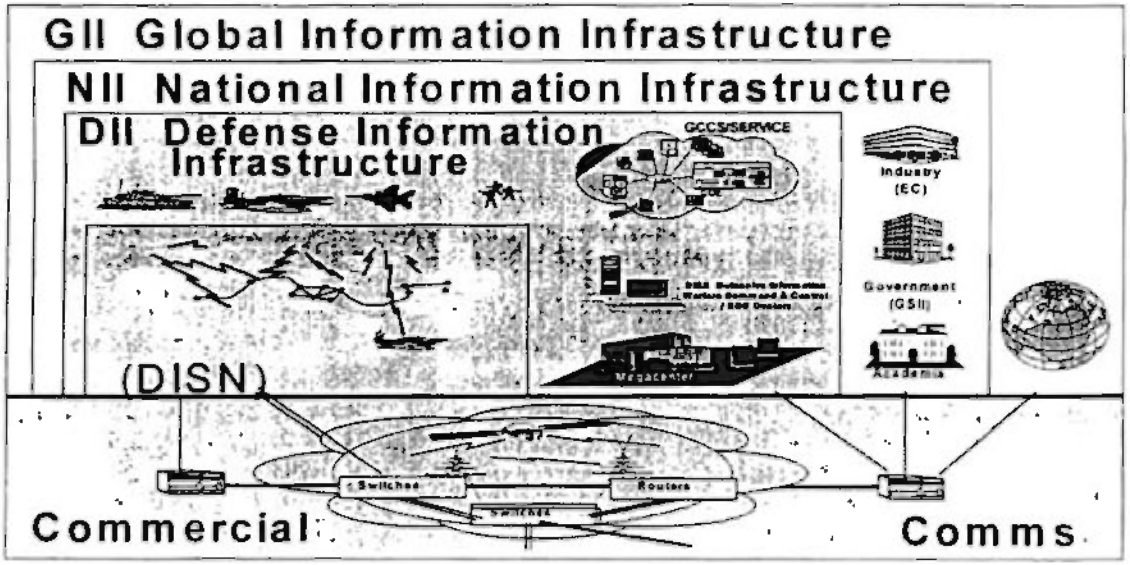
Why the NII and DII are Important

- "For economic reasons, increasing deregulation and competition create an increased reliance on information systems to operate, maintain, and monitor critical infrastructures. This in turn creates a tunnel of vulnerability previously unrealized in the history of conflict."
  - DSB Task Force on Information Warfare (Defense)

- Most DoD communications travel over publicly switched networks.

The Relationship Between the Global, National, and Defense Information Infrastructures

- The Global Information Infrastructure (GII) encompasses both the NII and DII.
- The GII, NII, and DII are inextricably intertwined with near-constant interfacing among the three.



The Information Warfare Battleground

National and Defense Information Infrastructures (NII/DII)

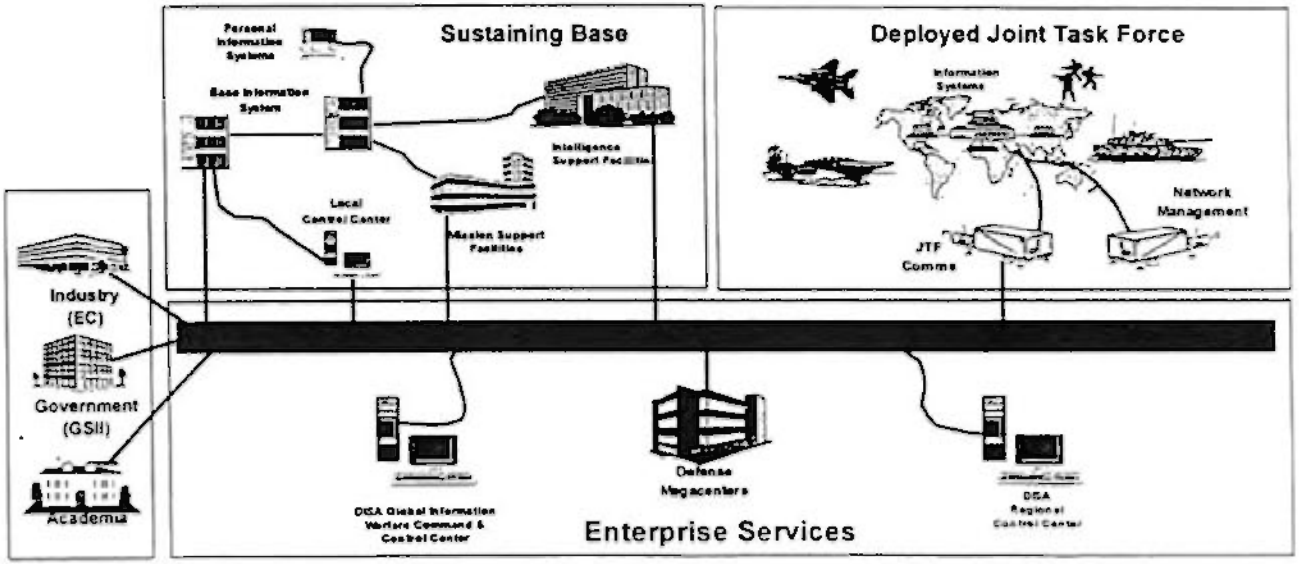
- **National Information Infrastructure (NII)**
  - National interconnection of communications networks, computers, databases, and consumer electronics that allows users to gain access to vast amounts of information.
- **Defense Information Infrastructure (DII)**
  - The DII, a component of the NII, is the shared system of computers, communications systems, data applications, personnel, and other structures supporting Department of Defense (DoD) local, national, and worldwide information needs.
  - DII provides mission support, command and control, and intelligence information through telecommunications, voice, imagery, video and multimedia services. It includes all C2, tactical, intelligence, and commercial communications systems used to transmit DoD data.

National Information Infrastructure

- **Designed, built, owned, operated and used primarily by the private sector**
  - **Lacks central control or oversight**
- **Key characteristics include:**
  - **Rapidly moving technology**
  - **Highly elaborate and interconnected**
  - **Multiple (innumerable?) potential points of entry**
  - **Anonymity/ambiguity**
- **Composed of the following Telecommunication elements:**
  - **Internet**
  - **Public Switched Networks (PSN)**
  - **Cable**
  - **Wireless**
  - **Satellite communications**
  - **Public and private networks**

Defense Information Infrastructure (1)

- **Mission - A new integrated computing and communications environment to provide information services, on-demand, to the DoD user community.**



DII

Defense Information Infrastructure (2)

- DII Components
  - Enterprise Baseline - the global communications infrastructure, processing centers, management control centers and services that support the other baselines and includes:
    - » Defense Information System Network (DISN) - the global long-haul communications infrastructure.
    - » Defense MegaCenters (DMCs) - information processing and business reengineering testing and evaluation.
    - » DII Control Centers - provide management service for the DII.
    - » Value-Added Services (VASs) - additional enhanced capabilities or utilities provided by information systems and/or capabilities that use the DISN.
  - Sustaining Baseline - provides information processing and communications infrastructure to national mission support, intelligence and C2 communities.
  - Deployed Baseline - provides information processing and communications infrastructure to in-garrison and deployed JTF operations.

Defense Information Infrastructure (3)

- Goals are to provide:
  - Information services end-to-end, across the global C4I warfighter space.
  - A seamless interface across infrastructures that incorporates rapidly changing technology in the areas of computing, communications, and information services.
  - Standards-based design and implementation methods.
- Objectives
  - Maximize use of COTS products.
  - Take advantage of dual-use research and development.
  - Ensure mechanisms for emerging technology insertion.

US Transportation System Vulnerabilities

Presented by

Rich Phares
Booz•Allen & Hamilton, Inc.
8 April 1997

Agenda

- Methodology
- Categories Examined
- Analysis by Category
- Ten Most Critical Commercial Nodes
- Vulnerability Examples
- Three Military Deployment Examples
- Army Divisions vs Embarkation Points
- Commercial vs Military

Methodology

- Statistical data was obtained from the U.S. Department of Transportation, Bureau of Transportation Statistics.
- Divided country into region; each region comprised of several nodes:
  - East Coast, Gulf Coast, East Inland, Great Lakes, West Inland and West Coast.
- Selected major urban areas in each region.

Methodology (cont.)

- Analyzed nodes based on several categories of commercial transportation as well as proximity to military facilities.
- Categories were examined for heaviest traffic, most tonnage processed, etc.
- Nodes were ranked in each category, and top ten were chosen.

Categories Examined

- Volume of Rail Freight
- Largest Airline Hubs
- Rail and Bus System Passenger-Miles
- Ports Tonnage
- Interstate Highways
  - Number of highways that feed into a node.
- Highway Delay Hours
  - Amount of hours travel time increased due to traffic congestion.
- Proximity of Military Bases

Analysis by Category

- Heaviest rail activity (>30,000,000 Ton-miles/year)
  - Kansas City
  - St. Louis
  - Chicago
  - Detroit
  - Cleveland

Analysis by Category (cont.)

- Heaviest Air Traffic (>15,000,000 people/year)
  - San Francisco Bay
  - Los Angeles Basin
  - Dallas
  - Chicago
  - New York/Northern New Jersey

Analysis by Category (cont.)

- Heaviest Rail/Bus (> 3,000,000 passenger-miles/year)
  - San Francisco Bay
  - Los Angeles Basin
  - Chicago
  - New York/Northern New Jersey

Analysis by Category (cont.)

- Heaviest Ports (>100,000,000 tons/year)
  - Anchorage
  - Los Angeles/Long Beach
  - Houston
  - New Orleans/Vicksburg
  - Dover/Philadelphia
  - New York/Northern New Jersey

Analysis by Category (cont.)

- Most Interstate connections (3 or more)
  - Los Angeles Basin
  - Dallas
  - Kansas City
  - St. Louis
  - Chicago
  - Atlanta
  - Baltimore/Washington

Analysis by Category (cont.)

- Heaviest Highway delays (>1,000,000 hours/year)
  - San Franciso Bay
  - Los Angeles Basin
  - Chicago
  - Baltimore/Washington
  - New York/Northern New Jersey

Analysis by Category (cont.)

- Proximity to <u>military installations</u> (2 or more major formations - Division, Wing, CVBG, Major Command, or Agency)
  - Baltimore/Washington
  - Norfolk
  - San Diego County
  - Puget Sound
  - Honolulu

Ten Most Critical Commercial Nodes

- Chicago
- Los Angeles Basin
- New York/Northern New Jersey
- Baltimore/Washington
- San Francisco Bay
- St. Louis
- Kansas City
- Dallas

Vulnerabilities

- For any node:
  - Loss of electrical power would:
    - Affect loading and unloading of cargo.
    - Disrupt communications and computer systems at all types of transport facilities.
- Port nodes are:
  - Dependent on electrical power for:
    - Port loading/unloading machinery.
    - Port systems.
  - Dependent on computer systems for:
    - Tracking cargo.
    - Tracking vessels, rail cars, trucks.

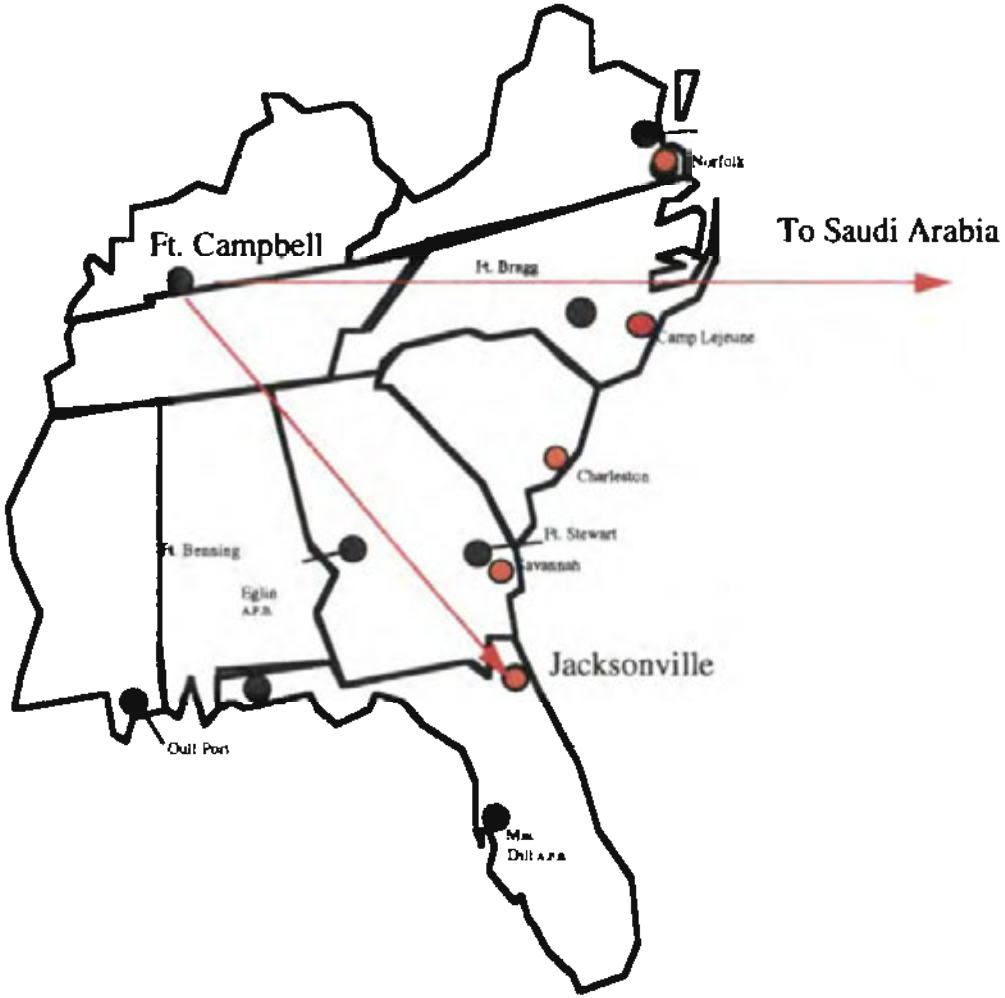
Vulnerabilities (cont.)

- Baltimore/Washington
  - A central control switching facility for east coast rail traffic identified by DSB Task Force as "a potential single point of failure for exploitation".
  - The facility is in Florida, yet impacted on events in the Baltimore/Washington area.

Deploy the 101st Air Assault Division

- 1st Brigade
  - Personnel moved by air (from Campbell Army Airfield).
  - Equipment moved by rail to Jacksonville, Fl, then by ship to Saudi Arabia.
- 2nd Brigade and Aviation Task Force
  - Personnel and equipment flew (60 C-141s and 50 C-5s) directly to Saudi Arabia.
- 3rd Brigade
  - Personnel drove 438 vehicles 787 miles to Jacksonville via interstate highways.
  - Personnel then returned to Campbell AAF to fly on to Saudi Arabia.

Deploy the 101st (cont.)



How to stop the 101st

- Aircraft flew from Campbell Army Air Field.
  - Disruptions against the national and military traffic control systems could be attempted.
  - Personnel processing stations were a possible target.
- Equipment went by rail or interstate.
  - Trains are easier to disrupt than trucks.

Deploy the 366th Wing

- Composite Wing located at Mountain Home AFB, Idaho.
  - Composed of five squadrons: one each of F-15C, F-15E, F-16C, B-1B, and KC-135R.
- Supplemented with E-3C, EF-111A, EC-130H aircraft from other Wings.
- Deploys in three waves 24 to 36 hours apart.
- Flies in groups of 41, 21, and 13 aircraft.
- Requires 80 C-141 lifts for personnel and ground equipment.

Deploy the 366th (cont.)

How to stop the 366th

- Requires coordination between Wing, AMC and ACC.
  - Databases, e-mail and other computer systems used for planning and coordination are possible targets.
- Sabotage of the tankers could have the greatest immediate effect on the deployment.
- The five basic squadrons are co-located together - the supplemental units fly from their own bases.
  - Disruptions could be against the national and military traffic control systems.

Deploy a CVBG

- Carrier Group or Cruiser-Destroyer Group Staff is designated to deploy.
- Carrier Airwing and Destroyer Squadron staffs are assigned to the Group Staff.
- Carrier, escorts, supply vessels and submarines are assigned to the Group Staff.
  - Staffs embark on their assigned platforms.

Deploy a CVBG (cont.)

- Ships sortie from their respective home ports and join the carrier at a specific location.
- The various squadrons assigned to the Carrier Airwing fly into a central location from their respective home bases.
- Once the carrier is underway, the airwing flies onto the carrier.
- The Battlegroup proceeds towards its destination.

Deploy a CVBG (cont.)

How to stop a CVBG

- Requires coordination among several staffs, ships, wing and squadrons at different locations.
  - Databases, e-mail and other computer systems used for planning and coordination are possible targets.
- Any physical attacks against shipboard electronics or the propulsion systems could affect the deployment schedule.

Divisions vs Embarkation Points

- 4th Infantry (rail), 1st Cavalry (rail) - Ft. Hood, TX.
  - Houston/Galveston, TX.
- 1st Brigade, 1st Infantry (rail); 3rd Brigade, 1st Armored (rail) - Ft. Riley, KS.
  - St. Louis, MO (barge to New Orleans, LA/ Vicksburg, MS).
- 10th Mountain (drive) - Ft. Drum, NY.
  - Albany, NY (barge to New York/New Jersey).

Divisions vs Embarkation Points (cont.)

- 3rd Infantry (rail) - Ft. Stewart and Ft. Benning, GA.
  - Savannah, GA.
- 82nd Airborne (rail) - Ft. Bragg, NC.
  - Charleston, SC or Norfolk, VA.
- 101st Air Assault (rail) - Ft. Campbell, KY.
  - Jacksonville, FL or Savannah, GA.
- 3rd Brigade, 2nd Infantry (rail) - Ft. Lewis, WA.
  - Tacoma, WA.

Divisions vs Embarkation Points (cont.)

Commercial vs Military

- Comparison of military embarkation points and critical commercial nodes:

Embarkation	Commercial
Houston	Chicago
Tacoma	Los Angeles Basin
St. Louis	New York
Charleston	Northern New Jersey
Albany	Baltimore
Savannah	Washington
Norfolk	San Francisco Bay
Jacksonville	***St. Louis***
	Kansas City
	Dallas

Commercial vs Military (cont.)

- Nodes most vital to military operations may not match those most vital to national economic operations.
- Overlaps between commercial and military uses must be identified.

Electric Power Networks and Security

Major Brad Bigelow, USAF
Office of the Manager, National Communications System
Government Coordinator

Office of the Manager
National Communications System

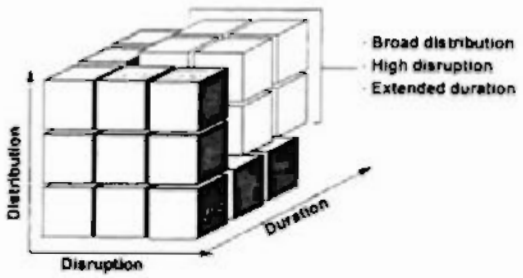
Infrastructure Risk Assessments

- NSTAC is investigating the risks facing the critical elements of the national information infrastructure:
  - Telecommunications
  - Electric power
  - Financial services
  - Transportation
- Focus is on risks derived from reliance on networks and information systems:
  - Internal control networks and applications
  - Interfaces to external networks
  - Dependencies on public networks

March 20 1997

Office of the Manager
National Communications System

Risk Assessment Scope



- Focus is on vulnerabilities that could lead to outages with significant regional or national impacts

March 20 1997

Office of the Manager
National Communications System

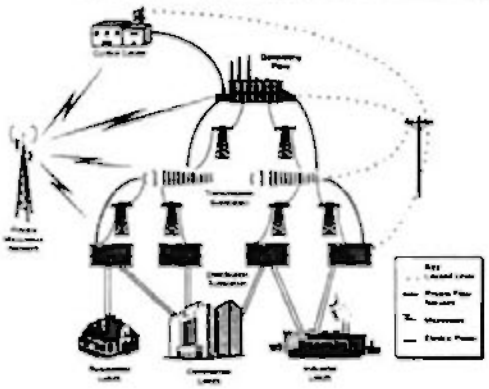
Electric Power Data Collection

- **Meetings with industry associations and government agencies:**
  - Utilities Telecommunications Council
  - Dept of Energy — *Energy incident database*
  - Federal Energy Regulatory Commission — *Open access to transmission system information (OASIS)*
  - North American Electric Reliability Council — *Telecommunications Subcommittee*
  - Electric Power Research Institute — *Information security survey, OASIS, EMS/SCADA security*
  - Joint Program Office for Special Technology Countermeasures — *EMS/SCADA vendor survey*

March 20, 1997

Office of the Manager
National Communications System

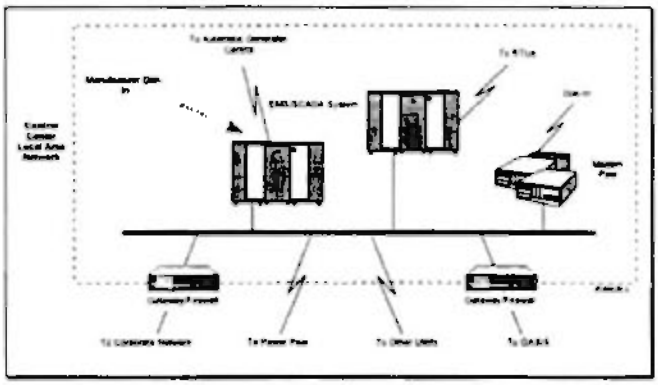
Typical Utility Architecture



March 20, 1997

Office of the Manager
National Communications System

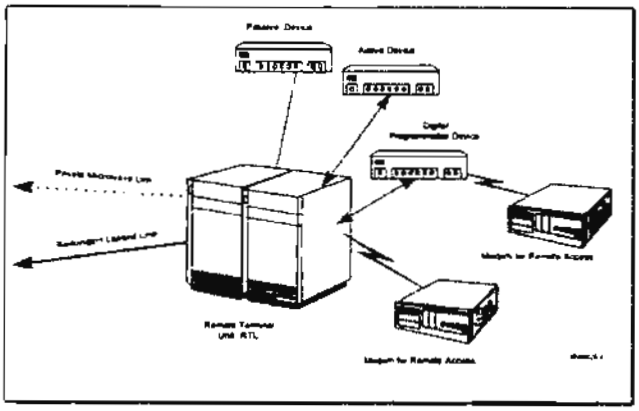
Control center architecture



March 20, 1997

Office of the Manager
National Communications System

Substation automation



March 20, 1997

Office of the Manager
National Communications System

OASIS: Open Access Same-Time Information System

- Requires transmission owners/controllers to post information about availability, services, and pricing
- Information accessible by all users on a comparable basis
- Must support basic merchant transactions:
  - Posting transmission information
  - Service requests/acknowledge receipt
  - Posting of request status: received, pending, accepted, withdrawn, rejected, confirmed for scheduling
  - Confirmation of sale/acknowledge confirmation

March 20, 1997

Office of the Manager
National Communications System

Threats

- Physical destruction still the greatest threat facing the electric power infrastructure
  - Details on physical infrastructure and system capacity more easily accessible than ever
- Electronic intrusion represents an emerging but still relatively minor threat
- Insiders the primary threat to information systems
- Downsizing, increased competition, and the shift to standard protocols will add to the potential sources of attacks

March 20, 1997

Office of the Manager
National Communications System

Deterrents

- Recent legislation increases the jurisdiction over attacks on electric power control systems (as proprietary information)
- Impediments to effective deterrence:
  - Lack of effective reporting mechanisms
  - Inconsistent use of logins, passwords, and warning banners
  - Low probability of being detected, caught, and prosecuted

March 20, 1997

Office of the Manager
National Communications System

Vulnerabilities

- Substations represent the most significant information security vulnerability
  - Poorly protected dial-in access to automated devices
  - Combined with critical node analysis could result in major regional outages similar Western states outages of Jul-Aug 1996
- Other sources
  - Interconnections between control centers and corporate data networks
  - Widespread use of dial-up modems
  - Use of public networks

March 20, 1997

Office of the Manager
National Communications System

Protection measures

- Widespread use of:
  - Contingency analysis
  - Back-up/redundant control centers and communications
  - Dial-back protection
  - Firewalls on OASIS sites and Internet connections
  - Security through obscurity
- Inconsistent organizational approaches to information security
  - Often excludes authority over operational systems
- Lack of convincing threat a major barrier to senior management support for security investments

March 20, 1997

Office of the Manager
National Communications System

Operational discipline

- Real-time contingency analysis standard industry practice
  - Live status (telemetry) fed simultaneously into:
    - Operational energy management system
    - Contingency analysis simulator
  - Flags "next worst" event based current system activity
    - Key to anticipating and preventing ripple effects
- Rigorous discipline of tracking outages
  - Within control center
  - System management and engineering analysis
  - Mandatory reporting to NERC and FERC

March 20 1997

Office of the Manager
National Communications System

Conclusions

- No evidence of a disruption of electric power caused by an electronic intrusion.
- Three trends will increase the exposure of electric power control networks to attacks:
  - The shift from proprietary mainframe control systems to open systems and standard protocols
  - Increasing use of automation, outside contractors, and external connections to reduce staff and operating costs
  - The requirement to provide open access to transmission system information dictated under FERC orders 888 and 889

March 20 1997

Office of the Manager
National Communications System

Recommendations

- Recommendations to
  - President
  - Electric power industry
  - NSTAC
- Structured according to model on increasing information assurance maturity:
  - Awareness
  - Information exchange
  - Mechanisms for prevention, detection, response, and restoration
- ➡ Building consensus on threat is priority
  - Risk management is driven by what's known

March 20 1997

THE PRESIDENT'S NATIONAL SECURITY TELECOMMUNICATIONS ADVISORY COMMITTEE

Information Assurance Task Force

Electric Power Information Assurance Risk Assessment

FINAL

NOT FOR EXTERNAL DISTRIBUTION

December 1996

TABLE OF CONTENTS

TABLE OF CONTENTS (CONTINUED)

National Security Telecommunications Advisory Committee
Information Assurance Task Force
Electric Power Risk Assessment

Executive Summary

The security of electric power control networks represents a significant emerging risk to the electric power grid. This risk assessment is the result of a 6-month effort by the Information Assurance Task Force (IATF) of the National Security Telecommunications Advisory Committee (NSTAC), that included interviews and discussions with representatives throughout the electric power industry.

The electric power grid is a highly interconnected and dynamic system of over 3,000 public and private utilities and rural cooperatives. These utilities have incorporated a wide variety of information and telecommunications systems to automate the control of electric power generation, transmission, and distribution.

The electric power industry is undergoing significant change, fueled by marketplace forces and Federal legislative and regulatory activities. New players are entering the power generation and delivery market, and existing utilities are being required to offer open access to their transmission systems. The functions of power generation, transmission, and marketing—which traditionally have been tightly integrated—are now being separated within utilities and, in some cases, even spun off into new companies. Competition, aging proprietary systems, and reductions in staff and operating margins are leading utilities to rapidly expand their use of information systems and to interconnect previously isolated networks.

Physical destruction is still the greatest threat facing the electric power infrastructure. Compared to this, electronic intrusion represents an emerging, but still relatively minor, threat. Insiders are considered to be the primary threat to information systems. Downsizing, increased competition, and the shift to standard protocols will add to the potential sources of attacks, whether from inside, or outside, a utility.

Recent legislation increases the jurisdiction of Federal, state, and local law enforcement authorities over attacks on electric power control systems. However, the lack of effective reporting mechanisms, inconsistent use of logins, passwords, and warning banners, and a low probability of being detected, caught, and prosecuted hinder effective deterrence of potential attackers.

Substations represent the most significant information security vulnerability in the power grid. Many of the automated devices used to monitor and control equipment within transmission and distribution substations are poorly protected against intrusion. Interconnections between control centers and corporate data networks, widespread use of dial-up modems, and use of public networks (PN) are other sources of vulnerabilities.

Utilities use a variety of mechanisms to protect the electric power grid from disruption, including contingency analysis, redundant control centers, dial-back modems, and firewalls. However, few utilities have an information security function for their operational systems, and the lack of convincing evidence of a threat has led senior managers to minimize information security investments.

The recent U.S. western power outages left 2 million people without power for up to 6 hours on July 2, 1996, and 5.6 million people without power for up to 16 hours on August 10, 1996. A critical node analysis, combined with knowledge of weak protections on substation automation elements, could allow an electronic intruder to achieve similar effects. A major coordinated attack could disrupt activities at a national level.

The study found no evidence of a disruption of electric power caused by an electronic intrusion Three trends, however, will increase the exposure of electric power control networks to attacks:

- The shift from proprietary mainframe control systems to open systems and standard protocols
- Increasing use of automation, outside contractors, and external connections to reduce staff and operating costs
- The requirement to provide open access to transmission system information dictated under FERC orders 888 and 889.

The probability of a nationwide disruption of electric power through electronic intrusion short of a major coordinated attack is extremely low, but the potential for short-term disruptions at the regional level is increasing.

The report closes with a number of recommendations for the President, the electric power industry, and the NSTAC. Of these, the most important recommendation is that the President should consider assigning to the appropriate Department or Agency the mission to develop and conduct an ongoing program within the electric power industry to identify the threat and increase the awareness of vulnerabilities and available or emerging solutions.

1.0 INTRODUCTION

In January 1995, the Director of the National Security Agency briefed the National Security Telecommunications Advisory Committee (NSTAC) on threats to U.S. information systems and the need to improve the security of critical national infrastructures. The NSTAC principals discussed those issues and subsequently sent a letter to the President in March of that year stating that "[the] integrity of the Nation's information systems, both government and public, are increasingly at risk from intrusion and attack . . . [and that] other national infrastructures . . . [such as] finance, air traffic control, power, etc., also depend on reliable and secure information systems, and could be at risk."[1] President Clinton replied to the NSTAC letter in July 1995, stating that he would "welcome NSTAC's continuing effort to work with the Administration to counter threats to our Nation's information and telecommunications systems."[2] The President further asked "the NSTAC's principals—with input from the full range of NII users—to provide me with your assessment of national security emergency preparedness requirements for our rapidly evolving information infrastructure."[3]

In May 1995, the NSTAC formed the Information Assurance Task Force (IATF) to work closely with the U.S. Government to identify critical national infrastructures and their importance to the national interest. Following several meetings with elements of the national security community, civil departments and agencies, and the private sector, the task force determined that electric power, financial services, and transportation were some of the most critical of the infrastructures. The task force determined that it would study these infrastructures to assess the extent to which their dependence on information and information systems puts them at increased risk to denial-of-service attacks.

This document is a report of the findings of the IATF's Electric Power Risk Assessment Subgroup's assessment of the risk that electronic intrusions pose to electric power distribution systems, specifically examining the vulnerability of the systems that manage and control generation, transmission, and distribution. This study represents a 6-month effort that included interviews with representatives from the operations, security, and information systems elements of eight utilities, one power pool association, the Utility Telecommunications Council (UTC), the North American Electric Reliability Council (NERC), the Electric Power Research Institute (EPRI), the Federal Energy Regulatory Committee (FERC), and a number of industry consultants. The utilities interviewed ranged in size and location and included both publicly held companies and government-owned and -operated power administrations.

---

[1] Letter from Mr. William Esrey, Sprint Corporation and Chair of the President's NSTAC, to the President of the United States dated March 20, 1995.

[2] Letter from the President of the United States to the NSTAC dated July 7, 1995.

[3] Ibid.

During the course of the study, interview teams worked under the assumption that the risk to the electric power infrastructure was a function of four factors: threat, deterrence, vulnerabilities, and protection measures. In this model, a threat is any circumstance or event with the potential to cause harm to a system in the form of unauthorized destruction, disclosure, modification of data, or denial of service. A deterrent is an attempt to prevent or discourage an action before it is taken, thus mitigating a threat. Vulnerabilities are points of weakness within a given system and are mitigated by protection measures.

Interviews with the utilities and power pool were conducted in a nondisclosure/nonattribution environment, and utility staff were all forthcoming and helpful throughout the process. In addition, EPRI provided invaluable support to this study, undertaking its own survey of industry managers to assess their views on information security concerns. The UTC also assisted by arranging a meeting at its 1996 annual conference in Kansas City, Missouri, and identifying contacts in a number of utilities.

2.0 OVERVIEW OF POWER GENERATION AND DISTRIBUTION

This chapter provides an overview of the electric power transmission and distribution industry. This overview describes the structure of the electric utility industry, identifies the roles of key industry players, and explains the basic structure of an electric power transmission and distribution system with an emphasis on the mission, functions, and system components of a typical electric utility control center. Finally, it highlights major legislative and industry trends causing change within the electric power industry and reviews previous studies of the security of electric power networks and information systems.

2.1 BACKGROUND

Since Thomas Edison opened the New York City Pearl Street Station in 1882, the U.S. and Canadian electric power grid has grown into a highly interconnected, international asset composed of 3,000 independent utilities. The goal of the modern-day power systems is to generate and deliver electric energy to customers as reliably, economically, and safely as possible while maintaining the important operating parameters (voltage, frequency, and phase angles) within permissible limits. To achieve this goal, electric utilities use centralized automation technology incorporating high-speed digital computers, supervisory and control systems, and a variety of communication systems.

2.2 OVERVIEW OF THE ELECTRIC POWER INDUSTRY

There are about 3,000 independent electric utilities in the United States. Each is interconnected with coordinated controls, operations, telecommunications networks, and sophisticated control centers. These utilities include investor-owned public utilities, government-owned systems, cooperatives, and manufacturing industries that also produce power. Nearly 80 percent of the Nation's power generation comes from the approximately 270 investor-owned public utilities. The Federal Government generates another 10 percent of the Nation's power, primarily through large facilities such as the Tennessee Valley Authority. However, the Federal Government owns few distribution facilities. The remaining power supply is generated by the cooperatives and manufacturing industries. There are approximately 1,000 cooperatives, which generally have limited power-generation capacity and focus primarily on transmission and distribution systems. In addition, some manufacturing industries generate power for their own use but sell surplus power to utilities, accounting for a small portion of the industry total.

The 3,000 companies that compose the North American power grid are divided into four regions: Eastern, Western, Texas, and Quebec. Figure 1 depicts these regional divisions. The Eastern, Western and Quebec regional power grids are linked through an alternating

Figure 1: Interconnections of Utility Systems

current/direct current (AC/DC) interconnection—the Texas regional power grid is not linked to the other regional power grids. The four regions are further broken down into 15 "power pools" that share generation capacity with one another and are generally located within the same geographic region.

Several Federal organizations are involved in various aspects of the electric power industry. The Department of Energy's (DOE's) mission is to formulate a comprehensive energy policy encompassing all national energy resources, including electricity. The Federal Energy Regulatory Commission (FERC) is an independent agency overseeing the natural gas industry, the electric utilities, non-Federal hydroelectric projects, and oil pipeline transport. FERC was created in October 1977 through the Department of Energy Organization Act and replaced the Federal Power Commission. FERC's principal mission is to regulate the wholesale sales of electricity in interstate commerce. Other Federal agencies that oversee the electric power transmission and distribution industry include the Nuclear Regulatory Commission (NRC), the Rural Electrification Agency (REA), the Environmental Protection Agency (EPA), and the Securities and Exchange Commission (SEC).

State public utility commissions (PUCs) play the most significant role regulating the electric power industry. PUCs control the rate structure for all municipal utilities, investor-owned utilities, and rural electric cooperatives that own, maintain, or operate an electric generation, transmission, or distribution system within a state. By controlling what constitutes an allowable charge, classifying accounts, and structuring rates, the PUCs

can exert significant influence over utilities. The PUCs also regulate reliability for both operational and emergency purposes, oversee territorial agreements, and resolve territorial disputes between utilities.

The North American Electric Reliability Council (NERC) is the organization most involved in "keeping the lights on" in North America. NERC does this by reviewing the past for lessons learned; monitoring the present for compliance with policies, criteria, standards, principles and guides; and assessing the future reliability of the bulk electric systems. NERC is a nonprofit corporation composed of nine regional councils focusing on interregional and national electric reliability issues. The members of the regional councils are electric utilities, independent power producers, and electricity marketers. The electric utility members are drawn from all ownership segments of the industry—investor-owned, Federal, State, municipal, rural, and provincial. These members account for most of the electricity supplied in the United States, Canada, and Mexico. NERC was formed in 1968 in response to a cascading blackout that left almost 30 million people in the northeastern United States and southeastern Canada without electricity. Although it is a voluntary industry consortium, the NERC Engineering and Operating Committees set standards for the planning, engineering, and operating aspects of electric system reliability.

While NERC handles operational issues, the Electric Power Research Institute (EPRI) is another significant industry player, with a research and development (R&D) focus. EPRI's mission is to discover, develop, and deliver high-value technological advances through networking and partnership with the electric industry. Founded in 1972, EPRI has more than 700 member utilities, representing approximately 70 percent of the electricity generated in the United States.

The UTC is another technology-focused industry association. UTC represents the telecommunications interests of the Nation's electric, gas, and water utilities before Congress, the Federal Communications Commission (FCC), and other Federal and State agencies. UTC promotes cooperation among its member companies in all matters concerning telecommunications, including the development and improvement of telecommunications media.

Other significant electrical power industry bodies include the following:

- The National Rural Electric Cooperative Association (NRECA)
- The American Public Power Association (APPA)
- The Edison Electric Institute (EEI).

NRECA is a national service organization representing private, consumer-owned cooperative electric utilities. NRECA provides legislative representation on issues affecting the electric service industry and its environment. The APPA represents 2,000 municipal and other state or locally owned public electric utilities. The APPA primary

objective is to expand the publicly held utility base. The APPA lobbies to improve public utility access to other power networks. The association also markets public utilities as the non-profit, low-cost, and innovative alternative to their private competitors. The EEI is an association of shareholder-owned electric companies. The association provides a forum for these companies to exchange information and acts as a representative on issues of public interest. In addition, the association develops informational resources and tools.

2.3 OVERVIEW OF ELECTRIC POWER SYSTEMS

The basic structure of an electric power transmission and distribution system consists of a generating system, a transmission system, a subtransmission system, a distribution system, and a control center. This configuration is illustrated in Figure 2. Power plant generation systems may include steam turbines, diesel engines, or hydraulic turbines connected to alternators that generate AC electricity. Generators produce three-phase current at voltages ranging from 2,000 to 24,000 volts. This electricity must be transformed to higher voltages for efficient long-distance transmission. Modern transmission systems operate at voltages from 69,000 to 765,000 volts. It is the interconnection of the transmission systems that forms the "power grid," which permits the interchange of electricity between utilities. Transmission lines terminate at substations in which the

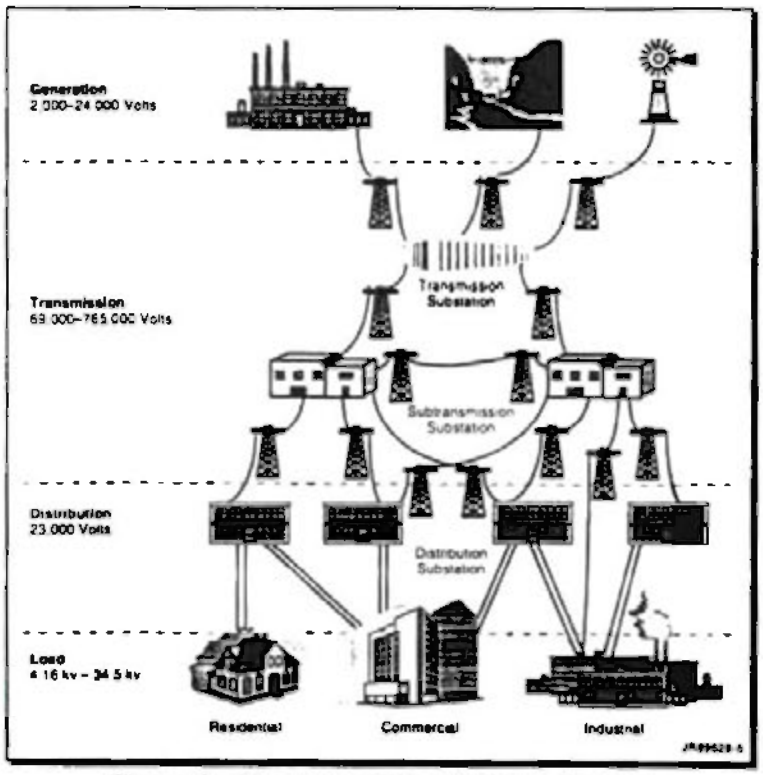


Figure 2. Overview of Electric Power Systems

voltage is reduced to the primary distribution voltage of 34.5 kv to 115 kv. This voltage is then supplied directly to large industrial users or further transformed down to 4.16 kv to 34.5 kv for local distribution.

2.3.1 The Control Center

The control center monitors a utility's generating plants, transmission and subtransmission systems, distribution systems, and customer loads. The primary functions of an electric utility control center is to provide centralized monitoring of power system operations, retain historical data, and allow for the manual and automatic control of field equipment. The control center system presents the electric system data to operations personnel via a modern, graphical user interface. Based on the data gathered, the operators may initiate control signals to various control points in the power system. The control center system may also automatically initiate controls to the field equipment, such as control of generating unit output. Figure 3 provides a schematic of a typical modern, distributed control center configuration.

Generally, the communications between the control center system and the field equipment takes place over utility-owned communications networks. Today, the majority of these networks are based on analog and digital microwave technology, although fiber optics is becoming increasingly more popular among the electric utilities. Other communications media include dedicated leased lines, power line carrier, satellite, spread-spectrum radio, and two-way radio.

Control center systems acquire the electric system data through communications with hardwired or programmable equipment in the field. This field equipment, called remote terminal units (RTUs), acts as a clearinghouse for incoming data by continuously collecting the electric system data directly from the field equipment involved in the generation, transmission, and distribution of electric power. The RTUs in turn support the transmission of this information to the control center system when requested.

Newer, more intelligent data collection equipment is now being deployed in substations by electric utilities as new substations are being built and as the old substations are being refurbished. These computerized field devices that are directly involved with the generation, transmission, and distribution systems are called intelligent electronic devices (IEDs). These devices represent the growing trend in the industry of pushing the intelligence and decision making capabilities farther and farther out into the field, closer to the data collection point. The IEDs are typically networked together at the substation, and communicate with a PC-based unit that replaces the remote terminal unit for the transmission of field data to the control center system.

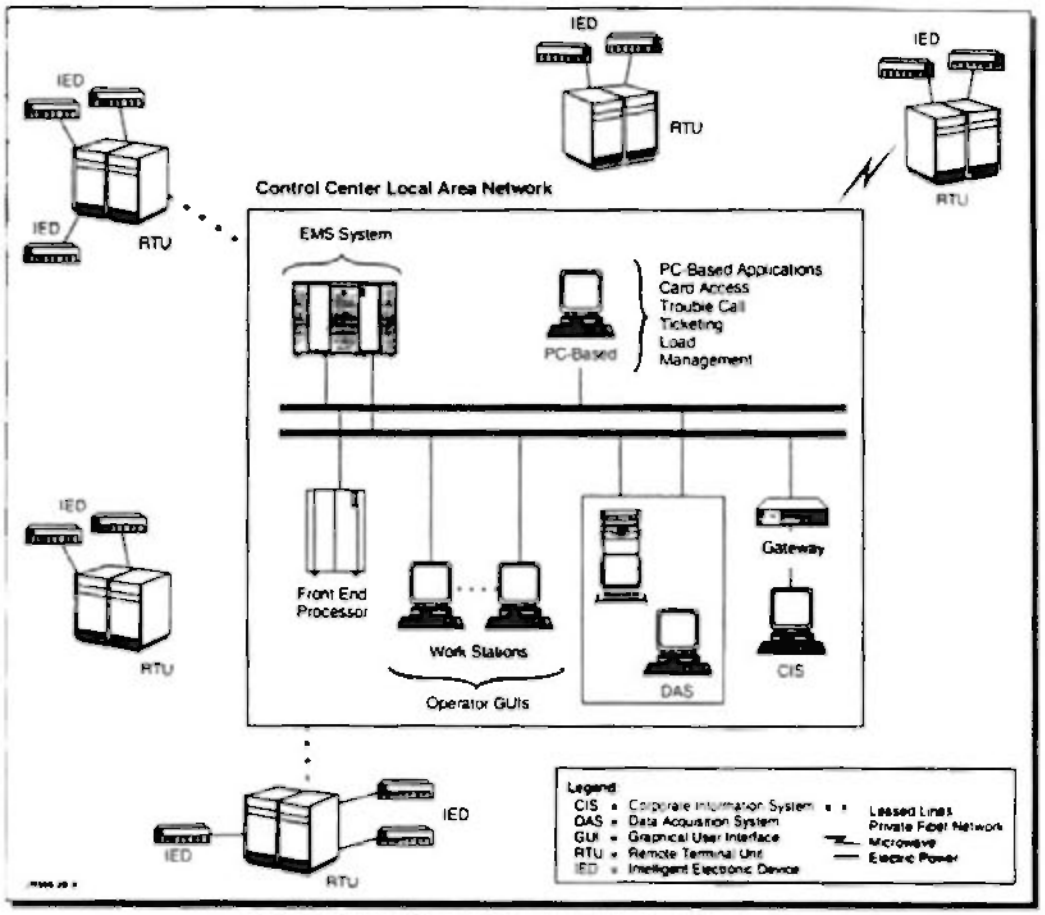


Figure 3: Typical Control Center Configuration

2.3.2 Energy Management System

A control center energy management system (EMS) typically houses the utility's systems' databases, the operational applications and displays, and the power system report-generation function. The need to disseminate valuable electric system data within a utility has resulted in many utilities connecting their EMS systems to their corporate local area network (LAN) or wide area network (WAN) to facilitate data sharing with other departments. Significant historical information systems have been developed to support this requirement. A control center energy management system (EMS) generally consists of four major elements:

- The supervisory control and data acquisition (SCADA) system
- The automatic generation control (AGC) system
- The energy management applications and database
- The user interface (UI) system.

These elements are depicted in Figure 4.

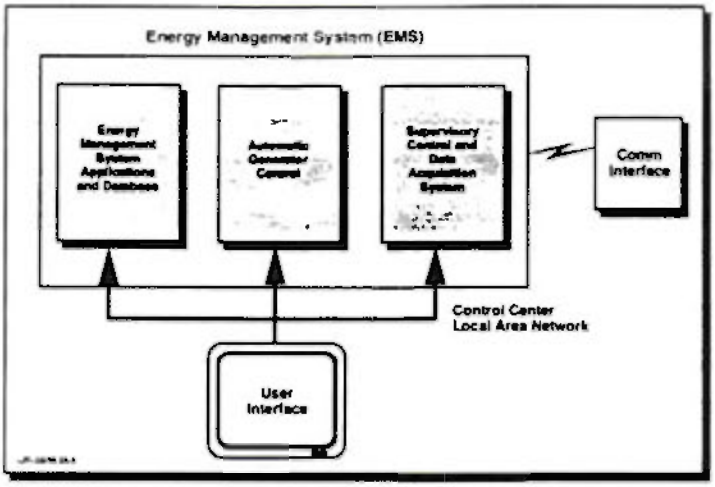


Figure 4: Energy Management System

The SCADA system manages the RTU communications, collects the electric system data from the field through a series of front-end processors, initiates alarms to the operations personnel, and issues control commands to the field as directed by the applications in the control center system. The SCADA system typically consists of a host or master computer, one or more field data-gathering and control units (RTUs), and a collection of standard and/or custom software used to monitor and control remote field data elements. SCADA systems may have 30,000 to 50,000 data collection points and may transmit analog information (e.g., generator megawatts) as well as digital or status information (e.g., breaker open/close state). SCADA systems can also send a control signal (e.g., start a pump) as well as receive a status input as feedback to the control operation (e.g., the pump is started). Current computing power allows SCADA systems to perform complex sequencing operations and provides for frequent collection (e.g., every 2 seconds) of power system data.

The AGC system controls the utility's generating units to ensure that the optimal system load is being met, with the most economical generation available. The AGC system submits supplementary control signals to the generating units to adjust their output based on the load forecast, unit availability, unit response rate, and scheduled interchange with other utilities.

The energy management applications and database are the programs and associated data sets that utility operations personnel use to manage state estimation, power flow, contingency analysis, optimal power flow, load forecasting, and generation unit allocation.

The UI system provides operational personnel with an interactive interface to monitor electric system performance, manage system alarm conditions, and study potential system conditions to ensure that network security criteria are met.

2.4 INDUSTRY LEGISLATIVE ENVIRONMENT

The electric power industry is in the midst of a revolution driven largely by a mix of marketplace forces, and Federal legislative and regulatory activity. An understanding of the legislative actions driving these changes in the U.S. electric power industry is vital to comprehending where these dynamic changes will lead.

The Federal Power Act of the 1950s laid a foundation for a self-sufficient vertically integrated electric utility structure. The late 1960s and 1970s experienced the beginning periods of rapid inflation, higher nominal interest rates, and higher electricity rates. This resulted in the government-sponsored construction of expensive generation facilities. Later, the oil cartel collapse resulted in a glut of low-priced oil, inflation, and surging interest rates. All of these elements substantially increased the costs of these high capacity generating plants resulting in rapidly rising electrical rates.

Congress recognized that the utility-owned generating facilities were increasing rates and harming economic growth and responded by enacting legislation and encouraging electric utilities to develop alternative generation sources. A new class of generating firms, such as independent power producers (IPPs), single-asset generation companies, and utility-organized affiliated power producers (APPs) sprang into existence.

Through these developments, the seeds for a free-market economy were being sown. While consumer-based rates helped to develop competitive bulk power markets, two issues remained: customer access to the transmission services and barriers hindering open access to third parties. The Energy Policy Act of 1992 (EPAC) opened up power generation to competition, while leaving power transmission and distribution a regulated, natural monopoly. In March 1995, FERC clarified the EPAC language by stating that all utilities under the commission's jurisdiction would be required to file nondiscriminatory open-access transmission tariffs available to all wholesale buyers and sellers of electric energy. Concurrently, FERC ruled that transmission owners and their affiliates did not have an unfair competitive advantage over the wholesale buyers and sellers in using transmission to sell power. This rule requires that public utilities obtain information about their transmission system for their own wholesale power transactions, via an open-access same-time information system (OASIS) available on the Internet.

In July 1996, in an effort to complete the deregulation of the power industry, Congress enacted the Electric Consumers' Power to Choose Act of 1996. The bill establishes federal mandates for all electric utilities, including electric cooperatives and municipal utilities, to provide retail choice to all classes of customers by December 15, 2000. After

retail choice in a state has been established, state commissions would be prohibited from regulating the rates for retail electricity services. Reasonable and nondiscriminatory access to local distribution facilities would be provided on an unbundled basis to any supplier seeking to provide retail electricity service. These mandated government actions will soon provide the consumers, generation and distribution firms, and power marketers open access to an unregulated electric power industry.

2.5 INDUSTRY TRENDS

The structure of the electric power industry is changing. The traditional attributes of the power industry, such as monopoly status, government ownership, and government regulations are yielding to free-market forces. The future of the U.S. power industry will be driven by competition, privatization, and deregulation. Global competition, increasing customer demands, capital liquidity, the relatively low price of natural gas, and environmental concerns are all driving forces that, when coupled with deregulation of the industry, will create great change.[4]

A number of key trends are affecting the use of networks and information systems in the power industry. These include the rise of IPPs, significant downsizing and restructuring, the advent of consumer choice, rate restructuring, and structural reorganization of access to transmission lines.

Transmission capacity is controlled by the investor-owned utilities. Under FERC order 888, transmission system operators must provide fair and equal access to their lines. A number of utilities view the creation of independent system operators (ISOs) as the answer to FERC order 888. ISOs would coordinate and schedule transmission service independently of electric companies to ensure fairness and promote reliable operations. ISOs would take over management of regional electric transmission grids owned by various electric companies, though the companies would continue to own their own parts of the regional grid.

Information technology will be the integrating force for many of the initiatives that utilities have undertaken to prepare for deregulation. To prepare for this new focus, industry organizations are successfully instituting standards and inter-utility protocols for the development of utility systems. The Utility Communications Architecture (UCA) and Database Access Integration Service (DAIS) have emerged as *de facto* industry communications and database protocols for data exchange. UCA and DIAS allow the development of more sophisticated and interoperable systems; however, the technical information about these open protocols will be available to a much larger population—and thereby a much larger number of potential attackers.

---

[4]Silverman, Lester, "Electric Power—The Next Generation," *McKinsey Quarterly* (January 1, 1994)

The Telecommunications Act of 1996 also affects the power utilities by allowing public utilities to enter the telecommunications services market. The act allows public utilities to enter the market so long as they do not subsidize their telecommunications activities with moneys from the power side of the business. Some utilities are already exploring using their private, fiber optic networks to offer services ranging from cable TV to telephone service to leased lines.

The deregulation of the electric power industry will force the utilities to move farther and faster than ever before. The next 4 years hold considerable promise for the industry but also portend significant challenges and changes. To succeed, utilities must offer value-added services; optimize the efficiency of their power systems; and develop strong customer ties, an aggressive economic development plan, and a winning corporate culture.

2.6 PREVIOUS STUDIES

This assessment builds on several previous studies of the security of information systems and networks in the electric power industry. These previous studies include the Defense Advanced Research Projects Agency's (DARPA's) 1995 Defensive Information Warfare study, EPRI's analysis of the security of the UCA and DAIS, the National Information Infrastructure (NII) risk assessment prepared by the Reliability and Vulnerability Working Group (RVWG) of the IITF, and a study of electric power's dependence on (PN) by the Air Force's Air Command and Staff College (ACSC). In addition, investigations by the Joint Program Office on Special Technologies Countermeasures (JPO-STC) and the Office of the Secretary of Defense (OSD/Policy) into overall infrastructure vulnerabilities have addressed the security of electric power networks. Although none of these studies were comprehensive, they have all reached similar conclusions.

First and foremost, these independent studies appear to agree that the transition from proprietary systems to standardized systems based on well-known, unsecure protocols and architectures will greatly reduce the security of utility control systems. These studies also noted potentially worrisome trends, such as the reduced skill levels of operations and maintenance personnel, near universal minimal front-end security, and increased interconnectivity through the use of dial-in modem ports and the Internet. One report bluntly stated that "data security is negligible to non-existent." These studies also noted the inherent risk to the utilities resulting from single point-of-failure systems. None of the studies predicted any significant improvements in the near future because tighter operational budgets and efforts to trim costs have made it difficult to justify security expenditures.

3.0 THREAT

This section addresses threats to the electric power grid. A threat is any circumstance or event with the potential to cause harm to a system in the form of destruction, disclosure, modification of data, or denial of service. Generally speaking, threats can be placed into two broad categories— physical and electronic.

3.1 PHYSICAL THREAT

Despite the growing concern about cyberspace attacks, the physical destruction of utility infrastructure elements is still the predominant threat to electric utilities. Physical threats to the infrastructure elements of an electric power utility fall under the general categories of accidental and deliberate events. Natural emergencies are the most significant accidental physical event to affect a utility and are the single greatest cause of outages in the electric power system. However, the impact of natural hazards on the power grid is the most manageable because utilities have years of experience with this threat and have designed facilities and infrastructure elements to minimize the impact of such events. Additionally, service providers design systems and operational procedures to allow them to respond to outages and restore service quickly. Most utilities have extensive experience with storms and other natural disasters and exercise their response systems periodically.

After natural hazards, deliberate physical attacks on utility infrastructure elements cause the most damage to the electric power grid. Transformers, microwave communications towers, and transmission substations can often be found in isolated, unpopulated areas. These pieces of equipment have proven to be popular targets for vandals, criminals, ecological terrorists, and amateur sharpshooters. Every utility visited during the course of this risk assessment recounted anecdotes about teenagers breaking into substations, ecological terrorists blowing up or damaging towers supporting transmission lines, or bored hunters taking potshots at insulators, transformers, and lines. However, transmission and distribution infrastructure elements are not the only target for physical attack—as recently as February 1996, pipebombs were used to attack a SCADA system at a hydroelectric plant in Oregon.[5]

3.2 ELECTRONIC THREAT

The electric power industry does not acknowledge a single incident of a power outage caused by an electronic intrusion. However, a majority of utility members agree that an electronic attack capable of causing regional or widespread disruption lasting in excess of

[5]Bureau of Alcohol, Tobacco and Firearms, *Explosive Incident Listing*,(21 March 1996.)

24 hours is technically feasible.[6] The source for such an attack could come from within the utility or from an external source.

3.2.1 Insider Threat

Insiders can be employees, contractors, or anyone else with legitimate access to system components and/or premises. Generally, insiders are granted varying degrees of access to the software and databases and may use legitimately or surreptitiously acquired computer access privileges to compromise them. The primary motives that drive an insider to exploit a system are usually financial gain or revenge.

Electric utility personnel believe that alienated employees pose the most significant insider security threat to information systems.[7] Considering that between 1986 and 1992 the number of employees working for electric utilities has dropped from 529,664 in 1986 to 506,068 in 1992,[8] there are significant numbers of potentially bitter former utility employees with system knowledge who could attack the power grid. As evidence of this, a letter appeared in the hacker magazine *Phrack* in which the author claimed to be an employee of an electric utility in Texas. In the letter the author claimed to know quite a bit about the systems and hinted that his knowledge would be helpful if someone wanted to attack a utility's systems.[9]

3.2.2 Outsider Threat

An outsider is anyone not legitimately associated with the system in question. Outsiders could be rival companies, criminal elements, or foreign national intelligence agencies. Examples include technical hackers motivated by the challenge; terrorist groups motivated to inflict damage to systems for a variety of political, ideological, or personal reasons; or rival companies seeking competitive information.

Until the passage of the Energy Policy Act, the Electric Consumers' Power to Choose Act, and the FERC rulings, most utilities operated as natural, regulated monopolies. This has changed significantly, and utilities are now competing for customers, power, and transmission capacity. In this newly competitive environment, rivals in the electric power market will have significantly more motivation to collect information, through whatever means possible. As one respondent to the EPRI Electronic Information Security Survey

---

[6] EPRI, *Electronic Information Security Survey* (Summer 1996).

[7] Ibid.

[8] Moulton, Curtis, "More Customers, Fewer Workers," *Electric Perspectives* (September 1, 1995), pg. 68

[9] Letters to the Editor, *Phrack* (April 15, 1995).

said, "As the utility industry has been heavily regulated, many are naive to (the) potential risk of info security violations."

While there have been instances of hackers breaking into electric utilities' business and support systems, the utilities have not encountered the full-scale attacks that the telecommunications services providers have experienced. In the EPRI Electronic Information Security Survey, 35 percent of those polled were not aware of any breaches of information and control systems at any electric utility, and 60 percent were aware of only minor security breaches. This is not to say the hacker community has not tried to enter the utilities' systems—members of a radical environmental group were arrested for trying to hack into a data network.[10] However, with industry deregulation, the stakes are getting higher, perhaps high enough to attract more attention. Stanley Klein, an industry consultant, estimates that the profit at an energy derivative delivery point could be as high as $10 million a day[11]—certainly enough to attract the attention of market manipulators and the intruder community.

Furthermore, if an outside organization had goals beyond financial gain, a structured electronic attack targeting the utility's operations systems could be a way to cause widespread disruption to a given geographic region. Organizations have used structured physical attacks on utility infrastructure elements around the world to achieve a variety of goals—a Department of Energy database records 10,200 incidents over the past 16 years. An organization with sufficient resources, such as a foreign intelligence service or well-supported terrorist group, could conduct a structured attack on the electric power grid electronically—without having to set foot in the target nation and with a large degree of anonymity.

It is important to note that information systems do not just represent a way to directly attack the electric power grid. During the course of this study, many of the electric utility officials interviewed expressed a concern about the amount of information about their infrastructure elements that is readily available to the public. Utility officials felt that the information on the various FERC forms, which are currently available in the public reading room at FERC in Washington DC, and are posted on FERC electronic bulletin boards, would be of value in planning an attack on the power grid. Additionally, the information that FERC is requiring utilities to post on their OASIS node will further simplify the process of target analysis. One utility official was asked to supply a Federal agency with a list of their top ten most vulnerable locations as part of an infrastructure study—the utility refused to supply the agency with the requested information.

---

[10] *Foreign Broadcast Information Service-Western Europe Edition*, #058, (28 March 1989).

[11] Klein, Stanley, *Information Security Implications of FERC Orders 888 and 889 and Related Industry Restructuring*, Stanley Klein Associates, August 1996.

3.3 THREAT CONCLUSIONS

The electric power industry clearly recognizes and has considerable experience in dealing with the risks to the energy infrastructure from physical threats. However, the implications of electronic intrusions are understood less well. Given the limited experience with electronic attacks, government efforts to identify and scope these threats must be coordinated with an industry effort to identify and report intrusion incidents. A clear threat identification, combined with an infrastructure vulnerability assessment and guidelines for protection measures, is critical to stimulating effective response by individual utilities.

4.0 DETERRENTS

A deterrent is an attempt to prevent or discourage an action before it is initiated—generally through fear or doubt. The ability of law enforcement to investigate, prosecute, and convict is the principle deterrent to computer crime. Recent and pending legislation increases the jurisdiction of Federal, state, and local law enforcement authorities over attacks on electric power control systems. However, the lack of effective reporting mechanisms, inconsistent use of logins, passwords, and warning banners, and a low probability of being detected, caught, and prosecuted hinder effective deterrence of potential attackers

The proposed National Information Infrastructure Protection Act (H.R. 4095) would greatly expand the jurisdiction of Federal law enforcement authorities over attacks against the computer systems of critical infrastructures such as electric power. In particular, the act would

- Broaden the jurisdiction of Section 1030 of Title 18 of the U.S. Code from "Federal interest" computers to that of "protected" computers, which would include any use in interstate or foreign commerce or communication

- Expands the definition of "damage" to include any impairment to the integrity or availability of a system that threatens public health and safety or causes any loss over $5,000 in value.

In addition, the recent passage of the Economic Espionage Act of 1996 increases the penalties related to improper disclosure of proprietary information, providing an improved deterrent against electronic intrusions aimed at gaining competitive advantage.

A number of factors tend to greatly reduce the effectiveness of these deterrents. Most network and systems administrators lack efficient tools to detect intrusions reliably. Only 25% of the respondents to EPRI's information security survey reported use of any intrusion detection methods. Even when intrusions are detected, the majority of the organizations effected do not report these events. In a recent survey conducted jointly by the Computer Security Institute, the FBI, and the International Computer Crime Squad, less than 17 percent of the 428 respondents said that they would notify law enforcement if they thought they had been attacked. Most of the respondents, 70 percent, said they feared negative publicity. Furthermore, more than 70 percent of the respondents do not have warning banners stating that computing activities may be monitored, hampering

investigations because law enforcement officials would likely not be able to tap computers or prove trespassing.[12] Use of shared logins and relatively weak passwords further complicates this situation for the electric power industry.

[12] "Computer Study Finds Concern, But Insufficient Action," *Telecom & Network Security Review* (May 1996)

5.0 VULNERABILITIES

An organization's systems are most vulnerable at the point where the connectivity is the greatest and the access control is the weakest. Figure 5 depicts the electric power generation, transmission, and distribution infrastructure with the supporting communications and control systems. If someone opted to attack the electric power grid electronically, rather than physically, he or she would have several options to consider—the **control center**, the **substation,** and the **communications infrastructure**. The following sections address the nature of each vulnerability, any trends affecting the vulnerability, and likely avenues of attack.

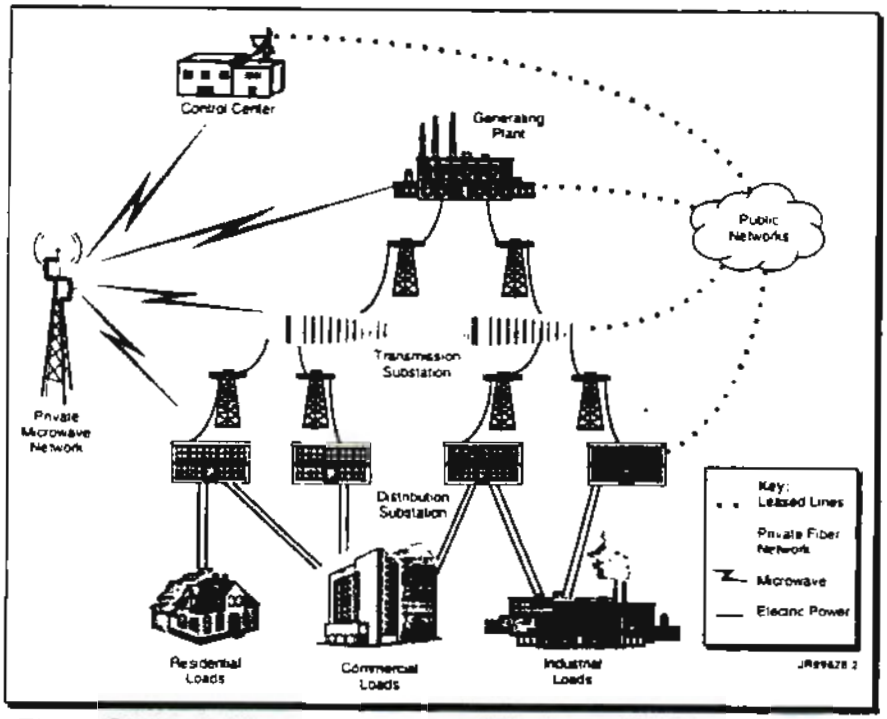


Figure 5: Electric Power Infrastructure With Supporting Communications and Control Systems

5.1 CONTROL CENTER VULNERABILITIES

There is no "standard" control center system configuration—they range from isolated, mainframe-based systems developed in-house more than 20 years ago to off-the-shelf, commercially developed, networked, Unix client/server systems. The industry trend is for utilities to procure "standard" vendor system products, based on the distributed client/server technology, to reduce schedule risk and minimize project costs. They continue to use their private communications networks to support remote data acquisition,

although the use of the public networks is increasing to interconnect corporate facilities, neighbor utilities, and the Internet.

As seen in Figure 6, an electronic intruder may access the control center through several interfaces:

- Links to the corporate information system
- Links to other utilities or power pools
- Links to supporting vendors
- Remote maintenance and administration ports.

The following paragraphs review the details of industry practices for each interface.

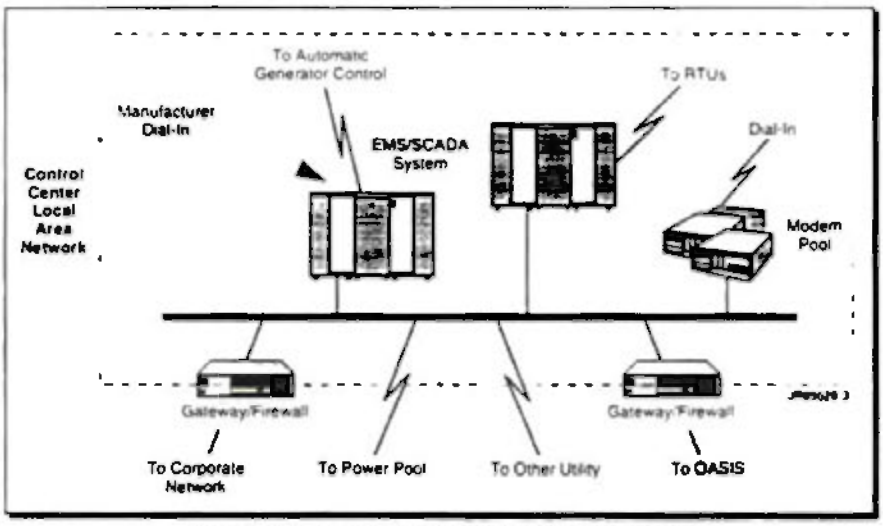


Figure 6: Typical Control Center Interfaces

5.1.1 Corporate MIS

Although not all utilities have an interface between the control center and the corporate information system, the distinct trend within the industry is to link the systems to access control center data necessary for business purposes. One utility interviewed considered the business value of access to the data within the control center worth the risk of open connections between the control center and the corporate network. More common solutions used firewalls or masked subnet routing schemes to create a secure link between the corporate information system and the EMS.

Current trends towards interconnectivity further increase the chances of an attack through the corporate network by providing more access routes into the corporate network.

Internet connectivity, modem pools, and individual modems all can serve as points of access for an electronic intruder into the corporate system and subsequently into the EMS. Despite the protective measures taken to isolate the control center network from the corporate information system, the control systems are still vulnerable to an attack through the corporate system. Utility operations personnel interviewed believed that firewalls and dial-back modems were sufficient to protect their systems from intruders, and they were surprised to learn about the experiences of the telecommunications industry with hackers defeating these measures.

5.1.2 Other Utilities and Power Pools

Many utilities have links between their control room and the control centers of adjacent utilities and the regional power pool. Most of these links are one-way connections carrying system data that operators use to balance the load on the power grid, schedule transmission, compute economic dispatch, and perform security analysis. Application-level controls and proprietary protocols make these links difficult targets for an electronic attack.

Several trends within the industry will increase the risk posed by these links. As the industry migrates to standard protocols, the pool of people with the knowledge to attack the system will grow significantly. The flurry of mergers resulting from deregulation of the industry further creates a need for merger partners to communicate electronically, increasing exposure.[13] The creation of ISOs will significantly increase the amount of traffic exchanged between the utilities and their ISO. In all likelihood, this traffic will require two-way data flows. Furthermore, the information flowing between the organizations (e.g., line capacity and scheduling information) will have significant economic value and will enable a potential attacker to identify critical nodes in the transmission and distribution system. Disabling these links would not, however, cause any direct disruption of the power system.

5.1.3 Supporting Vendors

As they move to client-server architectures, utilities are using more commercially developed software and are outsourcing the customization and maintenance of EMS and supporting applications. To support the installation, debugging, and ongoing maintenance of these new systems, utilities are providing remote access to manufacturers and integrators. Remote access is generally accomplished through a dial-in port on the system, although some utilities have dedicated links in place. These remote access links represent a potential point of access for an intruder. A representative of a major EMS manufacturer confirmed that all of his company's products with a dial-in port will allow the manufacturer's engineering staff to connect to the system to perform software updates and

[13] EPRI. *Electronic Information Security Survey* (Summer 1996).

other maintenance functions. These products frequently share a simple password that has not been changed in years.

One electric utility reported that an intruder accessed a chemistry-monitoring system in its nuclear division through a dedicated link between the system and its manufacturer. Once in the chemistry system, the intruder moved into the utility's nuclear engineering support network, accessed database entries, and altered audit logs to elude detection. Another utility increased access control on a dedicated line to a system integrator after it detected intrusion attempts.

5.1.4 Remote Maintenance and Administration

Many utilities are allowing operations and information systems personnel to access systems remotely for after-hours support. Generally, this is accomplished by configuring dial-up modems on the EMS network. Operations and support personnel can dial into the EMS network through these modem pools and log in to the EMS system. Once in, they can assist in troubleshooting, perform system administration functions, and, in some cases, operate EMS applications.

These dial-in links represent a point of access for electronic intruders. Although some utilities have taken measures to limit the operations that can be performed remotely or have further strengthened access control with token-based authentication systems, other utilities have only minimal protective measures in place.

5.1.5 Impacts

Regardless of the access point, once in the control system network, the intruder may crash the EMS system—a knowledgeable intruder can employ other, more subtle, options. For example, a sophisticated attacker could corrupt the databases, causing significant economic damage to the utility by disrupting billing operations. A knowledgeable intruder could issue false commands to the system—opening and closing relays, shutting down lines, and potentially affecting generation. An extremely knowledgeable attacker could manipulate the flow of data to the control center, causing the control center operators to respond to spurious indications. Fortunately, the technical skills and specific knowledge of an individual utility's applications and procedures limit this kind of attack to a very small number of potential attackers. Furthermore, most utilities can revert to manual coordination if all control center functions are lost—however, this is a costly measure for the utility.

5.2 SUBSTATION VULNERABILITIES

A substation serves as a clearinghouse for power as it is stepped down from the high voltages used to transmit the power across the service area and then directed to

distribution systems for delivery to residential and commercial customers. In an effort to provide higher service levels to customers and reduce staffing requirements, the electric power industry is automating substation operations with remote terminal units and a variety of intelligent electronic devices. An automated substation is depicted in Figure 7. Digital programmable breakers, switches, and relays are being produced by several manufacturers, and utilities are now using them in place of fixed, or manually set, devices Both the RTUs and the new automated devices are susceptible to electronic attack.

5.2.1 Digital Programmable Devices

By dialing into a port on a digital breaker, a utility engineer can reset the device or select any of six levels of protection. An electronic intruder who could identify the telephone

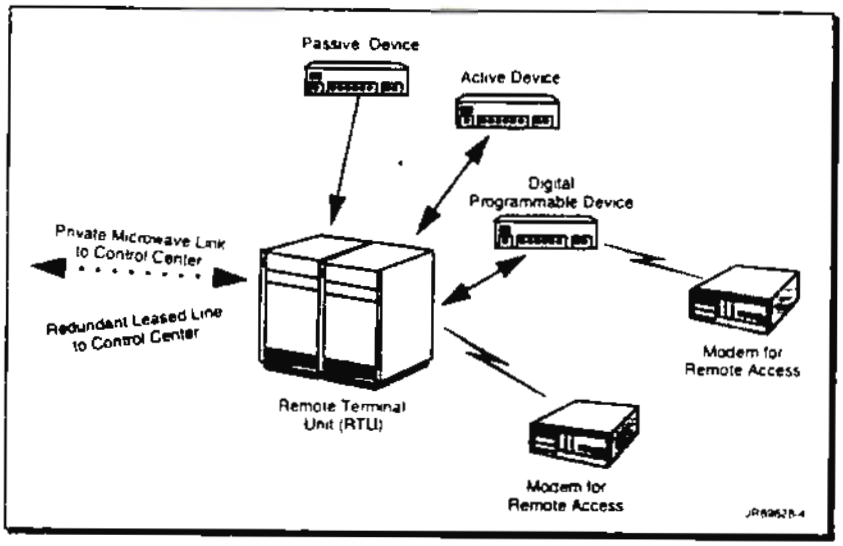


Figure 7: Typical Substation Interfaces

line serving such a device could dial into an unprotected port and reset the breaker to a higher level of tolerance than the device being protected by the breaker can withstand. By doing this, it would be possible to physically destroy a given piece of equipment within a substation. The intruder could also set the device to be more sensitive than conditions for normal operations and cause the system to shut down for self-protection. Several of the utilities visited did not have any type of security or access control on these dial-in devices. In either case, utilities reported that such an intrusion, capable of a major impact, would result in no more than a minor alarm.

5.2.2 Remote Terminal Units

Besides collecting data for the control center, an RTU operates as a clearinghouse for control signals to transmission and distribution equipment. A number of utilities reported having maintenance ports on substation RTUs that can be remotely accessed through a dial-up modem—some without even dial-back protection. An intruder could dial into this port and issue commands to the substation equipment or report spurious data back to the control center. Due to the highly networked nature of the power grid, knocking out an RTU can have a significant impact on any systems or customers "downstream" from the substation housing the RTU.

5.3 COMMUNICATIONS VULNERABILITIES

Utilities rely on a mix of private microwave radio, private fiber, and the public networks for communications among control system elements. Any one of these mediums could be exploited in an electronic attack. In most cases, an attack on the communications infrastructure alone would constitute a nuisance attack. In such an event, most utilities would equip personnel with cellular phones and mobile radios and dispatch them to key sites to report operating data back to the control center.

However, an attack on the communications infrastructure in conjunction with an attack on the electric power control system was characterized by one utility official as a "nightmare scenario." Restoring power would be extremely difficult and dangerous if all means of coordination between the control center and generation and transmission elements were lost.

5.3.1 Private Infrastructure Vulnerabilities

Microwave systems operating in the 2 and 6 gigahertz range and aerial or buried fiber optics make up the majority of utility private communications networks. Utilities view their private communications network as a key asset—several utilities stated that they would rather lose access to the public networks than to their private systems. In several cases, utilities sell excess capacity on these networks to commercial carriers, or plan to use these infrastructures to enter the telecommunications market.

A utility's private communications infrastructure is nearly as vulnerable to intrusion and physical attack as the public network. Utilities reported instances of theft of voice services, as well as the loss of voice and data service resulting from physical damage. One utility lost access to most of its private fiber network when a truck knocked down a pole at a critical juncture in the system. Microwave communications can be intercepted or jammed quite easily. There are multiple sites on the Internet with direction for assembling an inexpensive microwave jamming unit. One utility interviewed was experiencing severe disruption of its microwave communications system which it finally traced to frequency

spillover from a cellular service provider. Despite all of this, utilities seem to believe that because their private systems are isolated from the public networks, they are safe and secure.

5.3.2 Public Infrastructure Vulnerabilities

Roughly a third of the electric utility control communications traffic is carried on the PN. Most utilities use the PN to augment their private networks in the form of redundant communications lines to key substations, in geographically remote regions, or in "last mile" situations. Utilities appear to be aware of the threats to the PN and take risk mitigation measures on critical control links, such as requiring diverse routing in leased line contracts or providing for redundant transmission media. Several utilities reported that PN outages had isolated parts of their control networks and led them to increase private networking to key facilities.

It is worth mentioning that the single greatest source of interdependence between the electric power infrastructure and the PN is in their use of common rights-of-way. In many cases, public carriers lease spare conveyances or share transmission paths with utilities. In such a situation, a physical attack is more likely to disrupt multiple infrastructures than an electronic attack would.

6.0 PROTECTION MEASURES

Electric utilities use a variety of mechanisms to protect the electric power grid from disruption. The most significant measure is a double contingency analysis system, which uses a real-time simulator to look for the two worst things that could happen to the grid at any instant and offers operators corrective actions to consider and initiate. These "security" systems are powerful; however, the system does not look at elements beyond the power grid and is only as accurate as the data that it receives from the field. If the flow of this information from the field is cut off, the value of this system is reduced drastically.

Beyond actively monitoring the status of the power grid, most utilities have taken measures to guard their control centers and EMS systems from both physical attack and system failure. Practically all utilities have established back-up control centers—some collocated, others in separate facilities—that include uninterruptible power supplies and backup generators. Other utilities have installed completely redundant telecommunications facilities with their own telecommunications control center. In most cases, wherever the EMS interfaces with the outside world, utilities have installed dial-back modems and firewalls. Furthermore, most EMS systems support individual logins and passwords, and have extensive alarms and event logs.

Organizationally, all utilities have a robust physical security department, and most utilities have some information systems security function to handle the information security requirements for corporate systems. The corporate information system security office in conjunction with the internal auditing departments will generally conduct, or contract for, security evaluations and audits of corporate systems. But these audits rarely extend into the operational elements of the utility, and few utilities have an equivalent information security function for their operational control systems.

In an effort to improve security, utilities reported that they are considering a variety of improvements:

- Conducting intensive security evaluations and audits
- Ensuring dial access control (i.e., modem security)
- Using existing security features
- Eliminating security holes
- Evaluating and deploying new security technologies

- Improving coordination between operations staff and corporate information security staff
- Improving skills of the security staff
- Establishing security awareness programs.

However, utility personnel consistently stated that such investments were difficult to sell to senior managers, who were often unaware of, or skeptical of, the risks to their information systems. Many expressed concern that reduced operating margins would further threaten their ability to implement effective security. Forty percent of the respondents to the EPRI Summer 1996 Electronic Information Security Survey believed that internal priorities in a competitive environment were the most significant obstacle to maintaining a high level of information security.

7.0 POTENTIAL IMPACTS

The electric power grid is a complex, highly networked entity, whose elements are highly interdependent. A by-product of the highly networked power grid is the potential for a cascading power failure. When transmission capacity is unexpectedly lost, generation must immediately be taken off-line; otherwise, the generator's output will reroute and overload remaining transmission lines. This creates "voltage oscillations" that will ripple through the power grid. Unless corrective action is taken, these oscillations can pull down significant portions of the electric power grid.

The largest instance of such a widespread event was the famous New York City blackout of November 9, 1965, which knocked out power for up to 13 hours and affected 30 million people in eight States and Canada. More recently, on July 2, 1996, a cascading power failure in the Western Interconnect region affected 2 million customers in 14 States, Canada, and Mexico. Most customers had power restored within 30 minutes, but some did not regain service for over 6 hours. This situation was repeated on August 10, 1996, when all major transmission lines between Oregon and California were dropped. This outage affected 5.6 million users for up to 16 hours in 10 western States (see Figure 8).

Even regional outages can have wide-ranging effects. On May 14, 1996, an improper setting on a high-voltage circuit breaker at a single substation resulted in an 8-hour blackout affecting 290,000 customers through southern Delaware and across the eastern shores of Maryland and Virginia. Michael Conte, an economist at Towson State

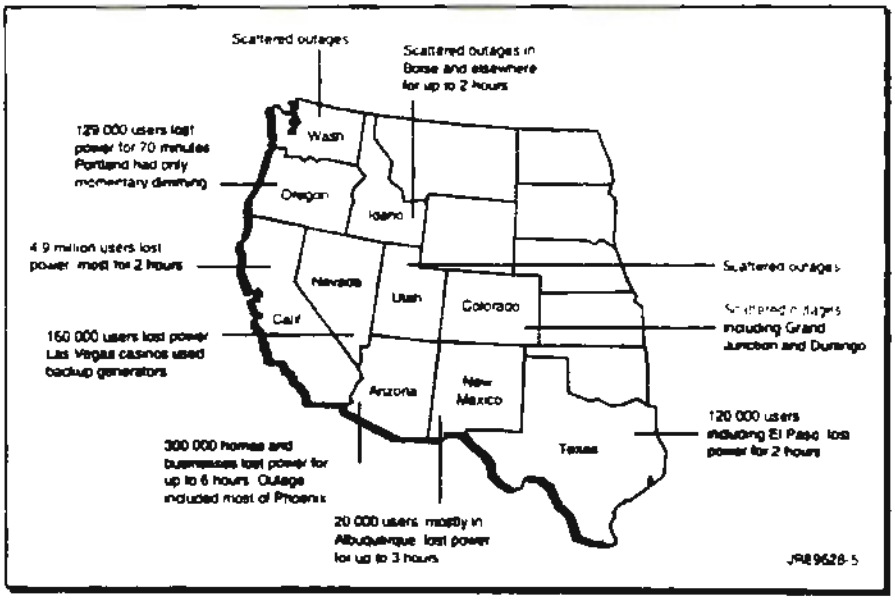


Figure 8: Effects of August 1996 Western Outage

University, estimated the loss for regional businesses to be as high as $30.8 million.[14]

These outages illustrate the tremendous effects a disruption of the electric power system can have on a given region. Significant portions of the U.S. economy and infrastructure are dependent on electric power, including, and certainly not limited to, transportation, financial services, health care, and telecommunications services. While many facilities have back-up generators, these systems are not foolproof and in many cases are not exercised on a regular basis. During these aforementioned outages, traffic lights stopped working, flight operations were suspended, schools were closed, and nuclear reactors were shutdown. In addition, a sewage treatment plant released six million gallons of sewage into the Pacific when electrically powered pumps stopped working.

Critical node analysis combined with an attack on poorly protected elements of substation automation systems can achieve effects equivalent to these recent outages. More than 50 percent of the electric utility personnel who responded to the EPRI survey believed that an intruder in the information and control systems at an electric utility could cause "serious impact on, or beyond, the region for more than 24 hours." Open sources, including FERC filings, electric industry publications, regional maps, and the Internet would provide enough information to identify the most heavily loaded transmission lines and most critical substations in the power grid. Relatively simple hacking techniques could then be used to locate dial-in ports to these points and modify settings to trigger an outage. Only a detailed review of logs or the elimination of all other factors would lead to the detection of such an attack.

[14]Humphrey, Theresa, "Power Outage Darkens Delmarva Peninsula," *The News-Times* (May 15, 1996)

8.0 CONCLUSIONS

The Electric Power Risk Assessment subgroup found no evidence of power outages attributed to deliberate electronic intrusion into utility control systems. The greatest risk facing the electric power infrastructure of the United States remains physical damage and destruction. Compared to the threat posed by natural disasters and physical attacks on electric power infrastructure elements, electronic intrusion represents an emerging, but still relatively minor, threat. However, changes within the electric power industry and in technology are increasing the risk posed by electronic intrusion.

As detailed in the preceding sections, the security of electric power control networks and information systems varies widely from utility to utility. In general, though, three trends will increase the exposure of electric power control networks to attacks and raise the probability of disruptions due to electronic intrusions.

- First, the shift from mainframe-based control applications relying on proprietary communications protocols to client-server applications using the Utility Control Architecture or other publicly documented protocols built on the transmission control protocol/Internet protocol (TCP/IP) expands the population of attackers with sufficient technical knowledge to attack these systems. This migration to client-server applications also introduces a potential for extended disruptions as the complexity of interactions continues to outpace the skills and tools of systems administrators.

- Second, the pressures to downsize, streamline, automate, and cut costs resulting from increased competition in the wholesale—and eventually, retail—power market will drive utilities to rely even more on remote automation, administration, and maintenance; on outside contractors for applications development and support; and on internetworking of control systems with corporate networks. Without a clear business case to support investments in information security, the relatively immature level of information assurance within the industry is likely to continue.

- Third, the requirement to provide open access to transmission system information dictated under FERC orders 888 and 889 introduces two new sources of exposure to attack—the interface to the OASIS host and new links required for the separate power marketing effort.

Having to post transmission system information on a World Wide Web server connected to the Internet requires utilities to establish some kind of interface between their EMS and the Internet. Although in all known cases this will be an indirect connection tightly controlled with firewalls, screened subnets, or proxy servers, the individual utility's

interface to its OASIS host creates a new and significant point of exposure. Apart from insider attacks, the Internet is the greatest potential source of information system attacks Utilities are, in many cases, relatively new to Unix and TCP/IP security, and the short timeline given for activating an OASIS site increases the opportunity for vulnerabilities to be introduced in the rush to meet FERC's deadline.

These rulemakings are forcing utilities to separate power marketing from transmission system management. These functions were formerly tightly integrated and operated on the unquestioned principle that system reliability always took precedence over economic profit. The procedures for resolving system problems between utilities were relatively informal, which was understandable given the consistency of operating philosophies and exposure to risk of the players involved.

At the information systems level, the separation of these functions is forcing utilities to disconnect networks and applications, often in the midst of already ongoing redesign efforts. Under great pressure to meet deadlines and minimize costs, information systems staffs may resort to workarounds that could ultimately introduce major vulnerabilities

At the operational level, it is not clear that the industry will be able to maintain the principles and procedures that have guided it for the past 30 years. Today, utilities resolve imbalances of generation, load, and transmission system capacity on a relatively informal basis, relying on phone coordination and recognized rules of conduct. In the new OASIS environment, this arrangement may not suffice, especially when transmission system operators may begin driving their lines further towards capacity.

At the industry level, these rulemakings will certainly lead to a major restructuring, as vertically integrated utilities spin off functional elements and a new set of players—power marketers, independent system operators, derivatives traders, retail power resellers—develops. The interactions of these businesses create new and unforeseen tensions, motivations, and risks. With vertically integrated utilities, the responsibility for the reliability of electric power was clear. The responsibility for reliability in a restructured industry is, for the moment, largely theoretical.

In sum, these trends suggest that, in the future, the electric power industry and its infrastructure will become more complex, and networks and information systems will play a major role in how individual utilities deal with the new business environment. As a result, electric power control networks will be exposed to a considerably wider range of attacks and potential attackers. Although the probability of a nationwide disruption of electric power through electronic intrusion will remain extremely low for any but a major structured attack, short-term disruptions up to the regional level may become easier to achieve—unless appropriate precautions are taken.

9.0 RECOMMENDATIONS

The recommendations of this study are directed toward three different groups—the President, the power industry, and the NSTAC. Each set of recommendations is further organized into three categories that reflect increasing levels of maturity in a program of information assurance:

- Awareness
- Information sharing
- Mechanisms for prevention, detection, response, and restoration.

Before effective mechanisms for coordinating information assurance activities between Government and industry can be established, there must be a consensus on the threats, risks, technical issues, business considerations, legal constraints, and other factors involved. This consensus cannot be established if the two parties disagree on whether a problem exists in the first place. For that reason, the recommendations aimed at increasing awareness of network and information systems security should be given first priority.

9.1 RECOMMENDATIONS TO THE PRESIDENT

9.1.1 Awareness

The President should consider assigning to the appropriate Department or Agency the mission to develop and conduct an ongoing program within the electric power industry to identify the threat and increase the awareness of vulnerabilities and available or emerging solutions. The program should be coordinated with other Departments, Agencies and advisory groups as appropriate to insure completeness and to maximize effectiveness.

9.1.2 Information Sharing

The President should consider establishing an NSTAC-like advisory committee to enhance industry-Government cooperation in light of significant regulatory changes affecting power generation, transmission, and distribution and the critical importance of electric power to National and Economic security, the government, and its citizenry. The committee should advise the head of the Department or Agency assigned the lead role for National Security and Emergency Preparedness (NS/EP) protection of the national electric power infrastructure. Such an advisory committee could perform a number of functions, to include the following:

- Provide information on factors affecting the reliability of the electric power infrastructure

- Provide the means for sharing information between Government and industry on potential electric power system faults, vulnerabilities and protection measures

- Provide a forum for recommending Government support activities to help ensure a highly reliable and available nationwide electric power capability

- Review existing or proposed legislation and advise the Government on the potential NS/EP implications for the electric power infrastructure.

9.1.3 Mechanisms for Prevention, Detection, Response, and Restoration

The Government should provide threat information and consider providing incentives for industry to work with government to develop and deploy appropriate security features for the electric power industry.

9.2 RECOMMENDATIONS TO THE POWER INDUSTRY

9.2.1 Awareness

Electric power associations, executive bodies, and individual organizations need to promote information systems security within the industry as a whole. With industry restructuring, and the interoperability of systems and networks, a lack of security in one element of the electric power industry could likely impact other providers or power transporters.

9.2.2 Information Sharing

Electric power associations should establish procedures for sharing sensitive information among member companies. This sensitive information might include threat and vulnerabilities; data security processes, procedures, tools, and techniques; and lessons learned.

9.2.3 Mechanisms for Prevention, Detection, Response, and Restoration

A secure network communications and computing environment will be important to the continued reliability of the electric power infrastructure. Security needs to be considered in communications and systems architectures and standards; in products that are purchased; and in employee methods, procedures, and training. Additionally, industry should consider establishing an electronic incident reporting and clearing function for electronic intrusions, similar to what is already done for power outages and physical attacks.

9.3 RECOMMENDATIONS TO THE NSTAC

9.3.1 Awareness

The NSTAC should reach out to the electric power industry and offer its support, expertise, and assistance in establishing an NSTAC-like capability. NSTAC should share past reports and recommendations to the President, provide advice on lessons learned throughout its tenure, and perhaps sponsor joint meetings to discuss common concerns.

9.3.2 Information Sharing

The NSTAC should invite representatives of the electric power industry to participate in open activities of the Network Security Information Exchange and appropriate meetings of the Information Assurance Task Force. In addition, NSTAC should actively foster opportunities for the exchange of information on protection technologies, attack trends, assurance programs, and other aspects of information security with industry associations.

9.3.3 Mechanisms for Prevention, Detection, Response, and Restoration

The NSTAC should consider the needs of the electric power control networks in its investigations of intrusion detection, indications and warnings, coordination mechanisms, and other elements of infrastructure assurance.

Proprietary Information

Telecommunications Infrastructure

An Information Brief to the OSD/NA IW-D

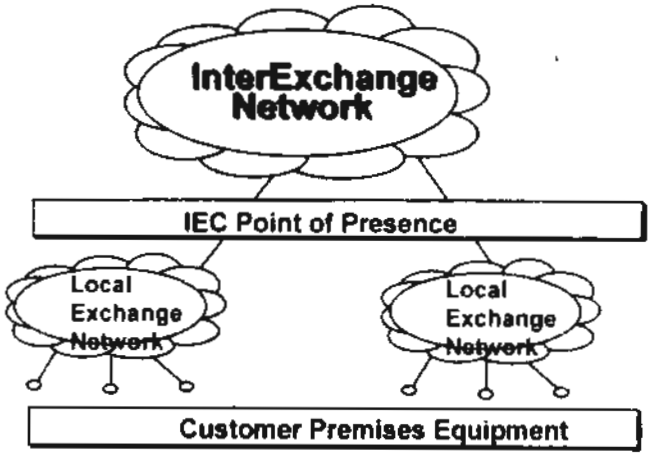
8 April 1997

Booz•Allen & Hamilton Inc.

Purpose

- Provide an understanding of basic telecommunications infrastructure:
  - Establish a common vocabulary
  - Overview system critical dependacies
  - Present an example of critcal node analysis

The Telecommunication System



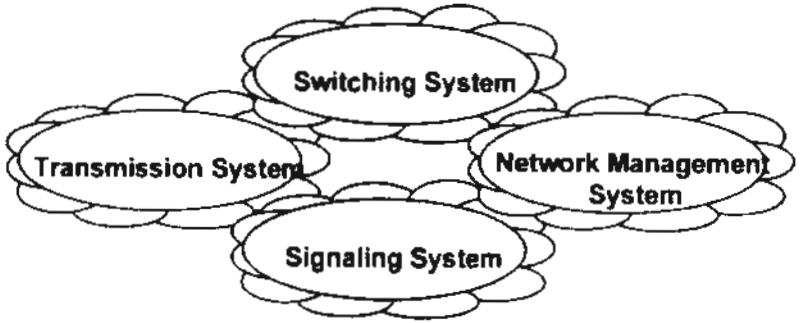
Major InterExchange Carriers:

- AT&T
- MCI
- Sprint
- WilTel

Major Local Exchange Carriers:

- Regional Bell Operating Companies
- GTE
- Independents

Major systems each of the carriers utilize in delivering service to the customers.



Switching Systems

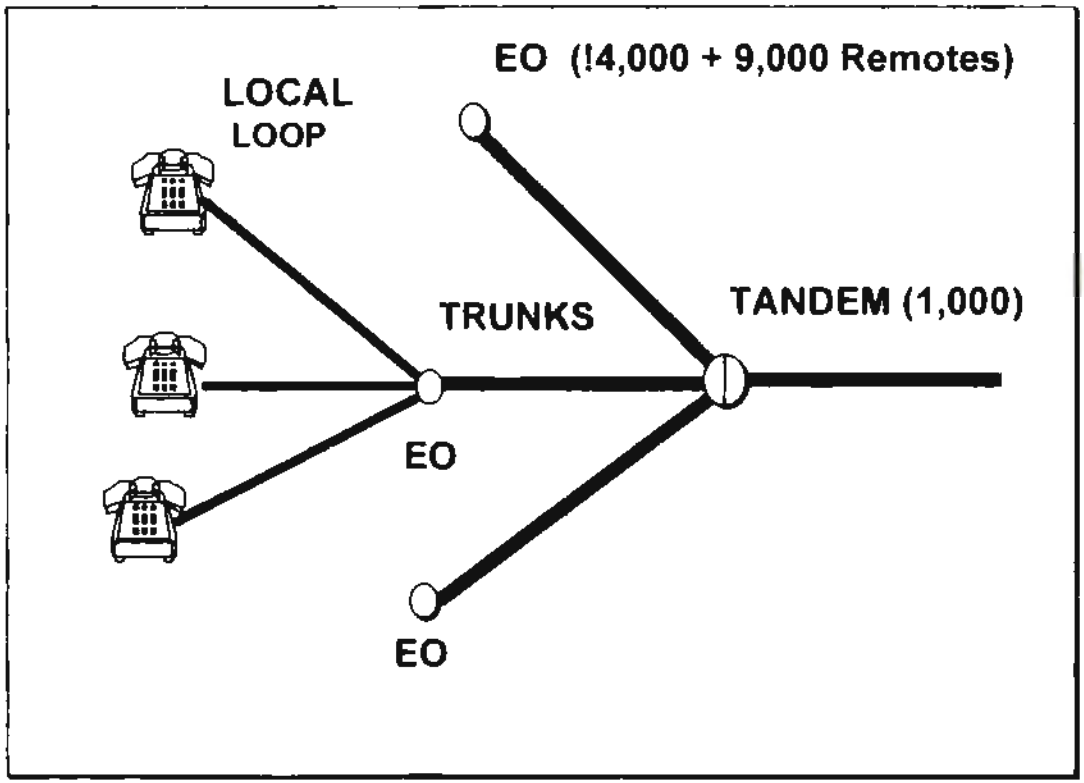
- Switches provide one of three basic functions:
  - Signaling: monitor line activity and send information to control functions
  - Control: process signaling information and set-up connections
  - Switching: make connections between input and output lines

Local Exchange Elements

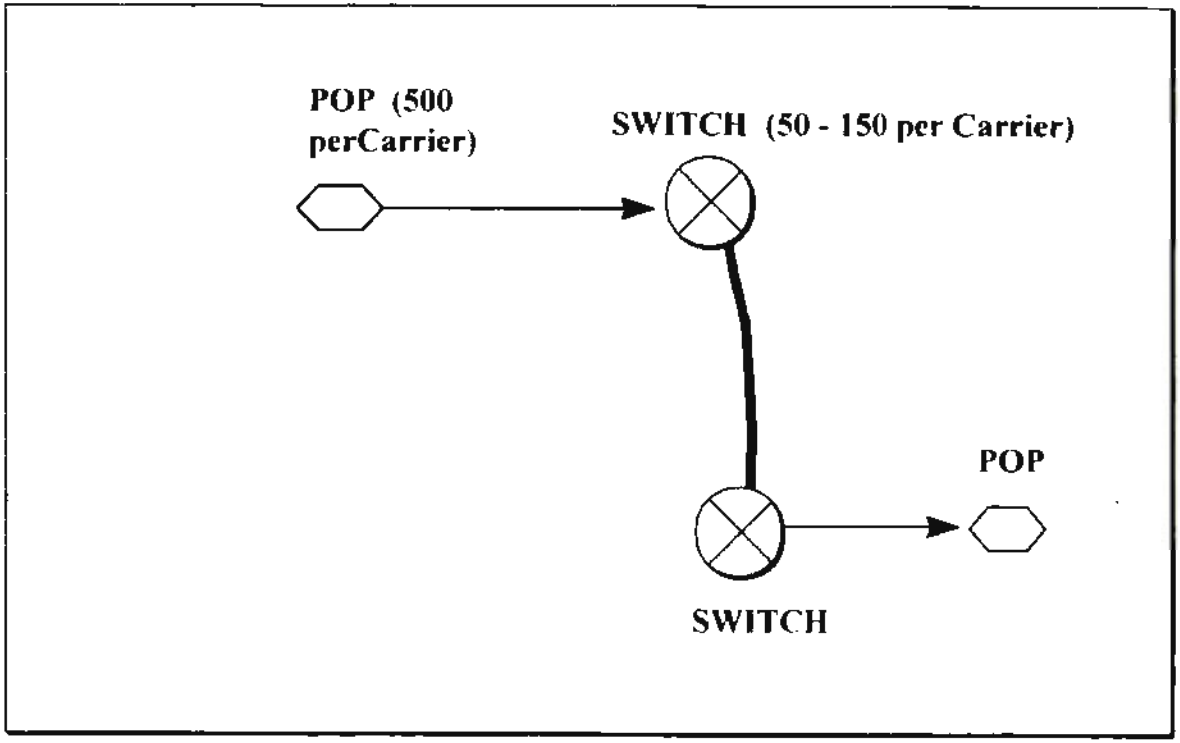
- End offices (EOs):
  - Connect all telephones through local loop
  - Provide dial tone
  - Switch calls between telephones and outgoing trunks
- Trunks:
  - Provide connections between telephone equipment
- Tandems:
  - Switch calls between trunks
  - Telephones can not be directly connected to tandems

Switching Systems...

Local Exchange Equipment



InterExchange Equipment



InterExchange Elements

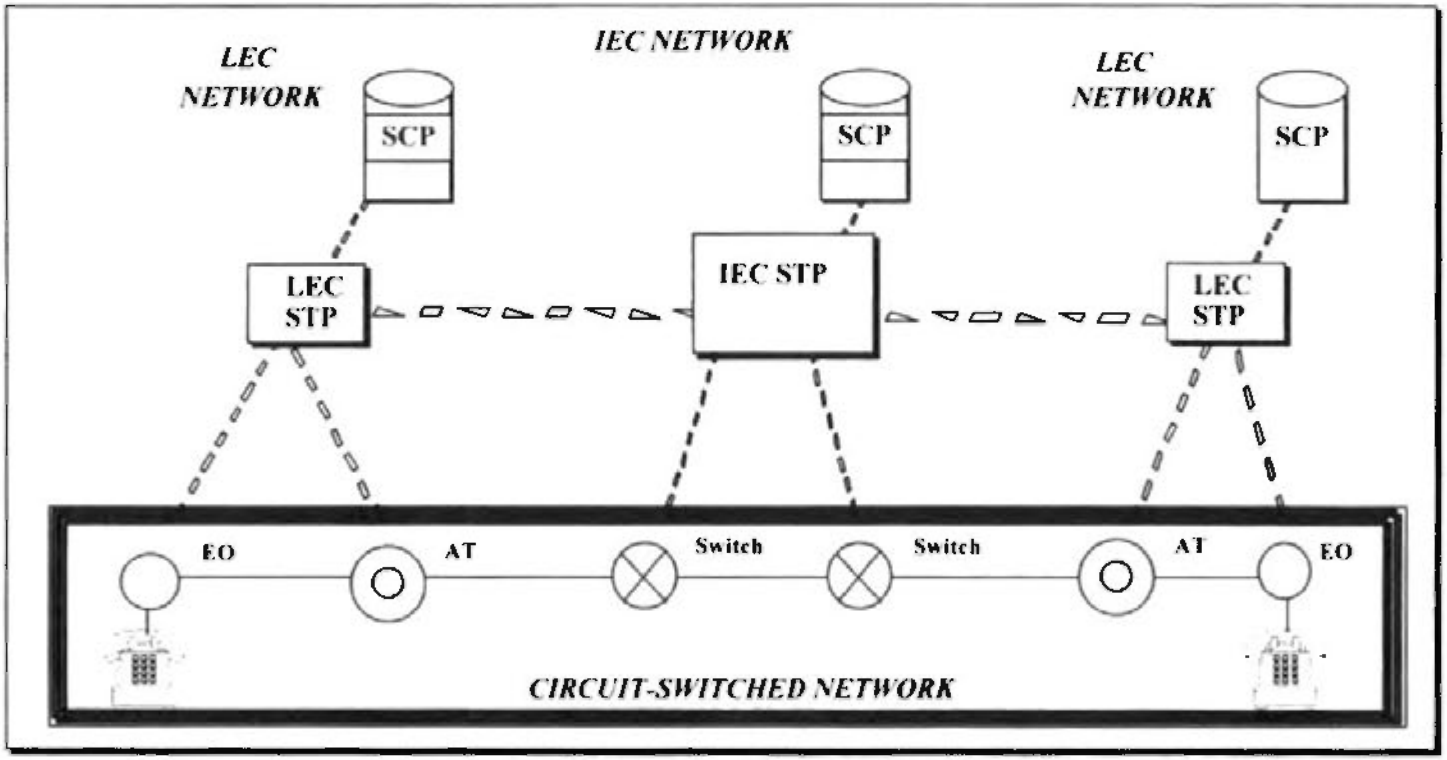
- Points-of-presence (POPs):
  - An IEC facility where traffic is handed off between LECs and IECs
- IEC switch:
  - Routes calls through the IEC network
  - Communicates with other switches (i.e., signaling)
  - Creates billing records
  - Performs customer validation, number translation, and collects statistics

Signaling Functions

- **Supervisory signals — convey status or control network elements**
  - Request for service: *off-hook*
  - Ready to receive address: *dial tone*
  - Call alerting: *ringing*
  - Call termination: *on-hook*
  - Request for operator: *hook flash*
  - Network or called party busy: *busy tone*
- **Information bearing signals**
  - Called party address: *called number*
  - Calling party address: *calling party number*
  - Toll charges
- **There are also supervisory and bearing signals of network control and maintenance:**
  - Maintenance test signals
  - Equipment failures
  - All trunks busy
  - Routing and flow control information

Signaling Systems...

SS7 Network Elements



SS7 Networks

- **SS7 networks are high speed (56 or 64 kbps) packet-switched networks that overlay the carriers' circuit-switched networks**
- **3 types of signaling nodes perform unique functions in the network:**
  - ***Signal transfer point* (STP): Packet switches that route signals through the SS7 network**
  - ***Signal switching point* (SSP): The interface between the circuit-switched and SS7 networks:**
    - Collocated with a circuit-switch
    - Connect to a minimum of 2 STPS
  - ***Signal control point* (SCP): Databases that perform special translation and advanced network services**
- **SS7 networks are engineered to a downtime of no more than 3 minutes per year**

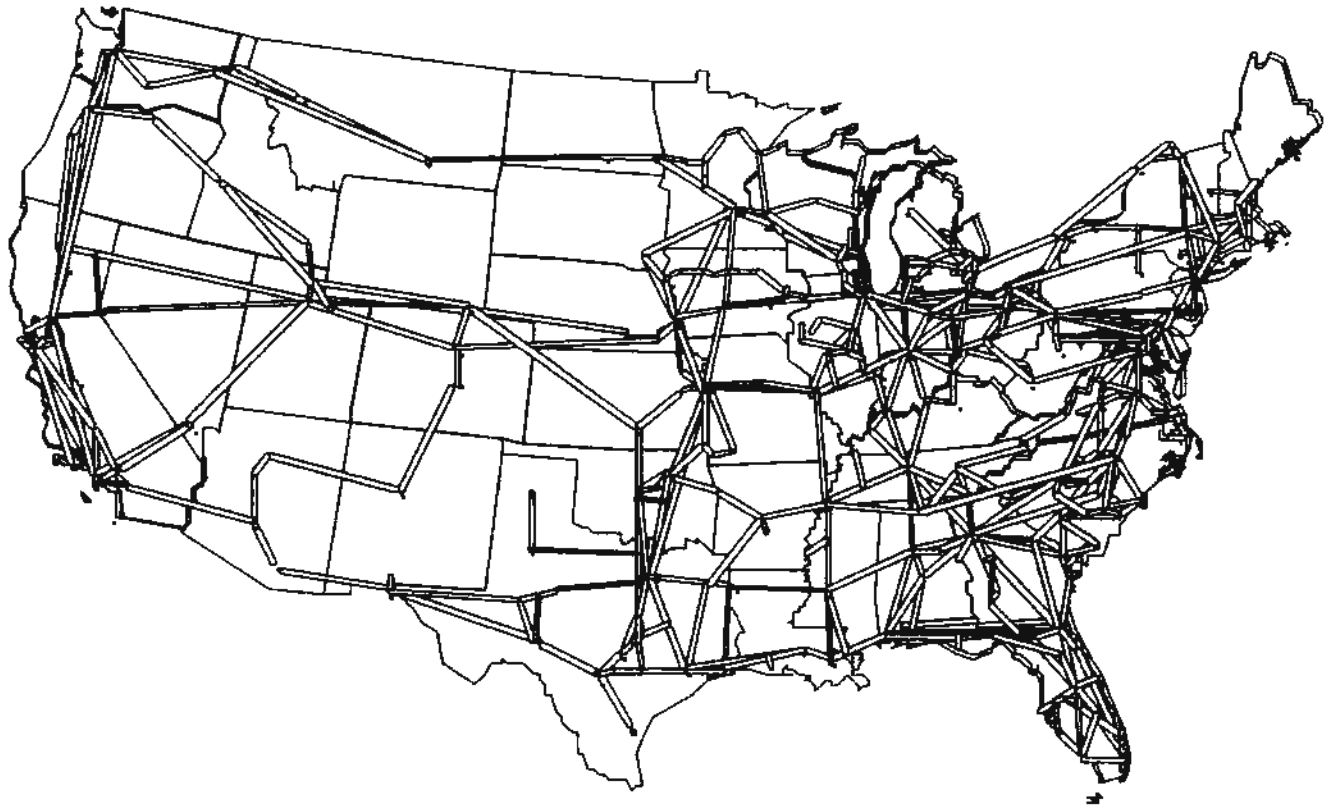
Transmission Systems

- A *link* is a direct physical connection between two nodes using a single propagation medium:
  - The medium may be line-of-sight microwave, satellite, copper cable, or fiber optic cable

- *Routings rules* are the instructions or steps for selecting the optimal circuit path on which to transfer traffic from one destination to another:
  - Routing rules establish "*logical*" paths between network nodes by using one or more nodes in tandem

Transmission Systems...

Long Haul Routes



Network Management

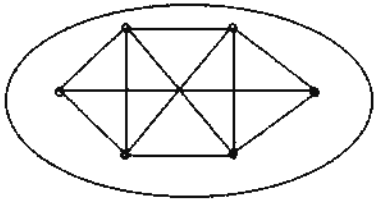
- Network management principles:
  - Keep all circuits filled with successful calls
  - Utilize available circuits
  - Give priority to calls requiring a minimum number of circuits to form a connection, when all circuits are in use
  - Inhibit switching congestion

- Network management controls:
  - Expansive - effect of expanding the network
  - Protective - remove traffic from the network
  - Examples of some control descriptions include

Logical View of the Network

Logical Layer

- Calls and Services

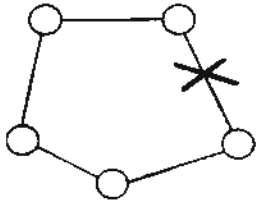


Physical Layer

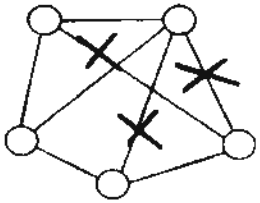
- Transmission and Switching

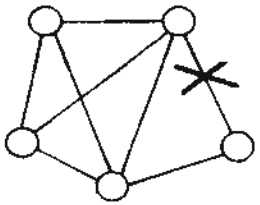
Impact of Facility Failures

Physical Network | Logical Network

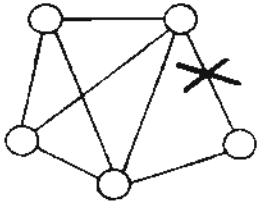


- Low physical connectivity: high impact on the logical network

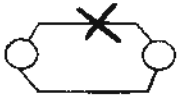


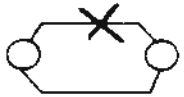


- High physical connectivity : Low impact on the logical network



- Trunk diversity: low impact on the logical network





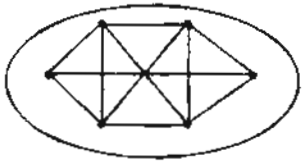
Impact of a physical failure on logical connectivity depends on the underlying architecture.

Techniques Used to Achieve Network Reliability

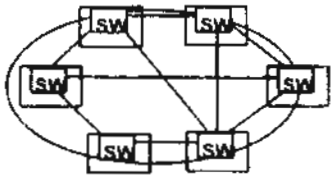
- Automatic Protection Switching
- Dual Homing
- Self-Healing Rings
- Reconfigurable Digital Cross-connects
- Adaptive Bandwidth Management Schemes
  - PSN
  - ATM

Network Management Systems...

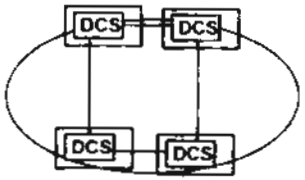
Multiple Layers of Network Reliability



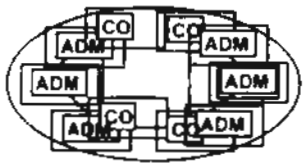
- **Services Layer (Logical)**
  - **Associates resources according to service needs**
  - **Manages congestion/contention among services**



- **Switched Layer**
  - **Reliability achieved by redistributing call flows on trunk capacity**

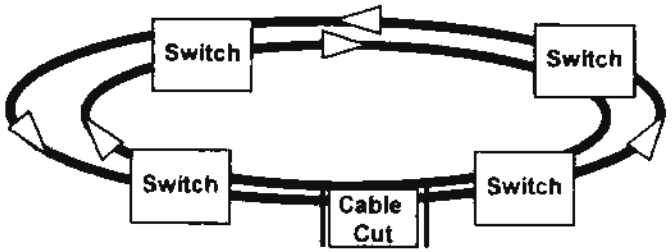
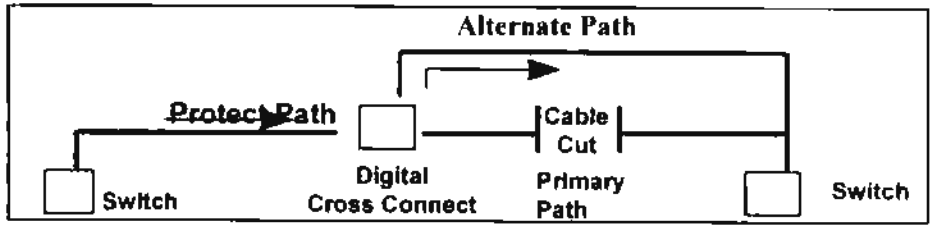
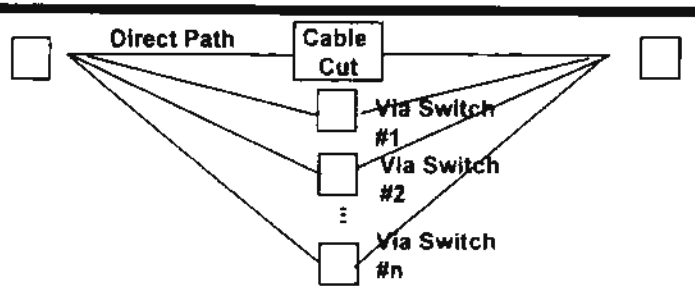


- **Cross-connect Layer (Physical/Logical)**
  - **Reliability achieved by reallocation of spare capacity**



- **Facilities Layer (Physical)**
  - **Reliability achieved by facility diversification and channel Reallocation**

Network Examples

Mechanism	Basis	Description
SONET	Protocol Based	
FASTAR	Physical Based	
RTNR	Switching Based	

Evolution of the PSN

- **The U.S. telecommunications industry has been subject to regulation since its beginning**

- **Government regulations are created and implemented by:**
  - **Federal Communications Commission**
  - **State Public Service Commissions**
  - **Courts and Congress**

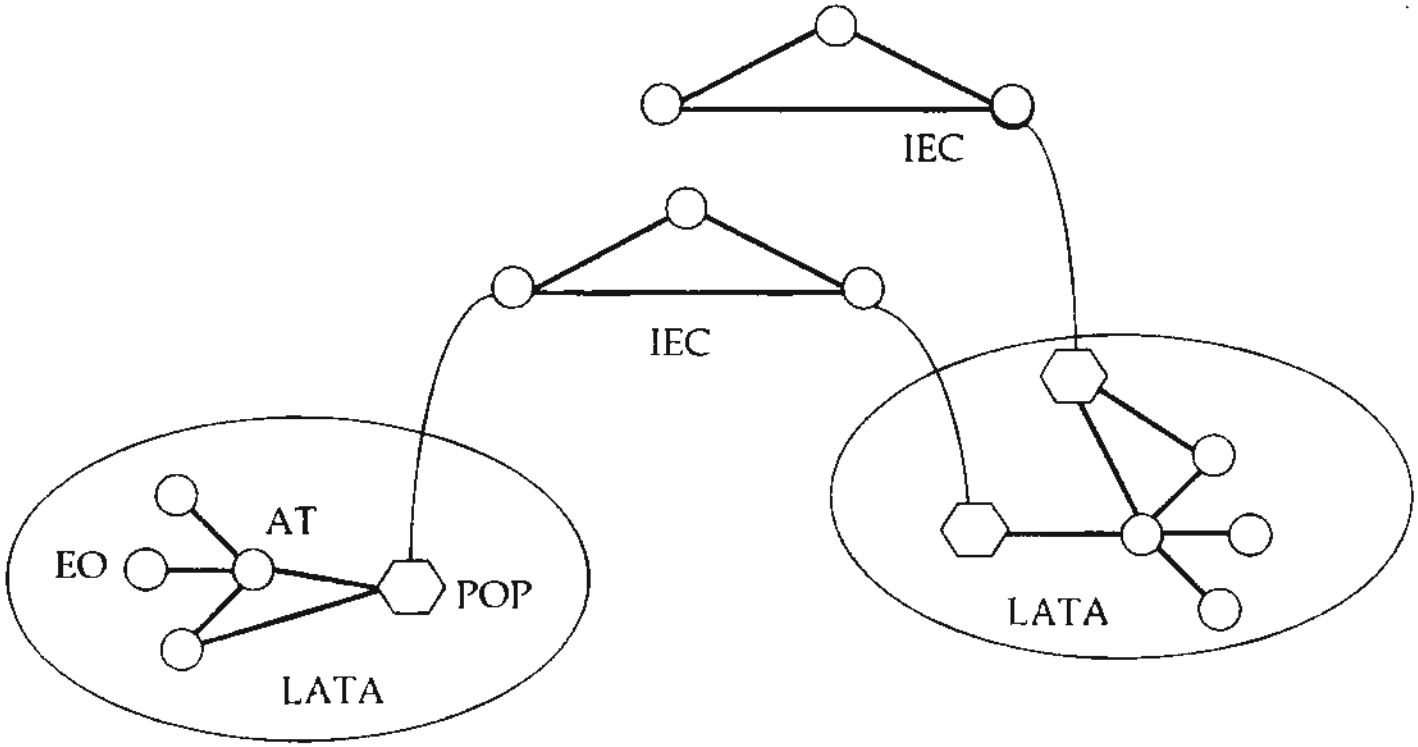
- **The most significant event affecting the current structure of the telecom industry was the Modified Final Judgement (MFJ):**
  - **AT&T was a monopoly that controlled the majority of the local and long distance markets**
  - **Long distance providers and equipment manufacturers demanded changes in the way AT&T did business:**
    - Equal access to the PSN
    - Elimination of monopolistic pricing by AT&T

Post-divestiture PSN

- **The MFJ established rules and regulations concerning deregulation and divestiture of AT&T and the Bell System:**
  - **Created network partitions:**
    - ***Inter-exchange carriers*** (IECs)
    - ***Local exchange carriers*** (LECs)
    - Established *local access and transport areas* (LATAs):
    - LECs carry intra-LATA (within a LATA) traffic
    - IECs carry inter-LATA (between LATA) traffic
  - **Established equal access for all IECs:**
    - Each IEC can have one ***point-of-presence*** (POP) in each LATA
    - Connection for each IEC identical in type, price, and quality
  - **Required that connections between a POP and EO have at most one intermediate switch:**

PSN Structure ...

Post-divestiture PSN Topology

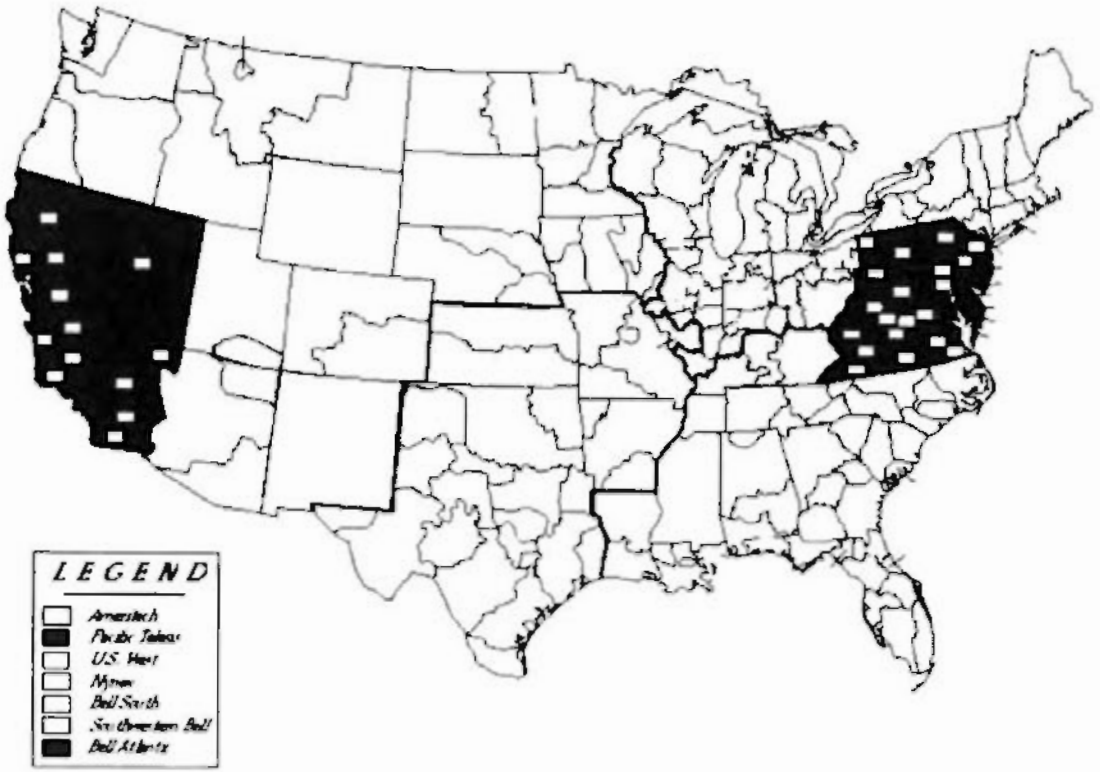


NOTE: POPS are usually collocated with a network element, i.e., EO, AT, or IEC switch

PSN Structure ...

LATA Map

CONUS LATA Map With RBOC Regions



Telecommunications Law of 1996

- The Telecommunications Law of 1996 will change the structure of the telecom industry by allowing more competition and removing regulatory barriers between market segments
- Among its many provisions, the Law will:
  - Allow the RBOCs to enter the long distance market
  - Allow competition in the local exchange
- In anticipation of sweeping telecom reform, many companies have announced plans to merge or divest divisions to become more competitive:
  - AT&T has split into three separate companies
  - Sprint aligned with three cable TV companies to develop a nationwide PCS system, and spun off its cellular holdings
  - US West issued separate classes of stock for its core local exchange business and its media and cellular properties

Analysis Methodology

- To determine critical telcom assets and facilities, two approaches are used:
  - Critical Asset Analysis
  - Coverage Area Analysis
- The critical asset analysis identifies key nodes (i.e. EOs, ATs) that are essential for network connectivity
- The coverage area analysis identifies the regions served by key nodes

Critical Asset Analysis

- Acquire data for telephones at critical location:
  - Area Code (NPA)
  - Exchange (COC)
- Identify the telecommunications facility that serves the critical location:
  - End office (EO) or remote (REM)
- Specify the LEC homing arrangements:
  - Access tandem (AT)

Analysis Methodology ...

Results

Coverage Area Analysis

- Identify AT serving critical EO
- Identify other EOs served by critical AT
- Identify all NPA-COCs served by these EOs
- Plot latitude-longitude coordinates of all customers with these NPA-COCs
- Trace outer perimeter of these points

Results

NATIONAL COMMUNICATIONS SYSTEM
OFFICE OF THE MANAGER
701 SOUTH COURT HOUSE ROAD
ARLINGTON, VIRGINIA 22204-2198

IN REPLY REFER TO

Plans, Customer Service and
Information Assurance Division (N5)

FEB 07 1997

MEMORANDUM FOR NETWORK SECURITY INFORMATION EXCHANGE MEMBERS

SUBJECT: Internet/Public Switched Network (PSN) Interconnectivity and Vulnerability Report

1. The subject document is enclosed for your information and use. The purpose of this report is to provide an understanding of how the Internet uses and relies on the PSN. In addition, a rudimentary analysis was begun to identify key components used for transmitting Internet traffic.

2. The Internet is having a profound impact on how America conducts everyday business in both the public and private sector. The exponential growth in traffic and users has fostered the concept of the Internet as the ubiquitous tool for sharing information. However, the accessibility and availability of the Internet depend on a physical infrastructure of software, routers and transmission media. It is commonly perceived that the Internet and the public telephone networks in the U.S. are two separate and distinct systems. While this is true to a certain extent, most modern data networks, including many leased government Internet Protocol (IP)-based networks, rely on the traditional commercial carriers to transport their traffic.

3. The Office of the Manager, National Communications System (OMNCS), as well as other government organizations, is beginning to assess the impact of the Internet on its operations and planning, particularly as it affects national security and emergency preparedness (NS/EP). This report describes the evolution and current operation of the Internet and begins to evaluate potential vulnerabilities that may hinder Internet reliability, security and availability. The OMNCS will continue to analyze the impact of the Internet on NS/EP telecommunications.

4. Questions or comments on this document should be referred to Mr. James Kerr, NCS Information Assurance Branch, at (703) 607-6133 or through E-mail at "kerrj@ncs.gov."

D. Diane Fountaine

1 Enclosure a/s

D. DIANE FOUNTAINE
Deputy Manager

INTERNET/PSN INTERCONNECTIVITY AND VULNERABILITY REPORT

December 1996

Office of the Manager
National Communications System
701 South Courthouse Road
Arlington, VA 22204-2198

INTERNET/PSN INTERCONNECTIVITY AND VULNERABILITY REPORT

December 1996

Prepared by:
Booz, Allen and Hamilton
8283 Greensboro Drive
McLean, VA 22102

Prepared for:
Office of the Manager,
National Communications System
Under Contract: DCA100-95-C-0113
Optional Task Orders, (NS/EP Telecommunications Performance Analysis Task, Network Security Support)
CDRL Item L001 and DI-MISC-80711

DI-MISC-80711	Internet/PSN Interconnectivity and Vulnerability Report Section
3.2.5 Contents	Table of Contents
3.2.6 Figures and Tables	List of Exhibits
3.2.9 Symbols, Abbreviations, and Acronyms	List of Acronyms
3.3.1 - 3.3.6 Summary and Body	Sections 1 - 5
3.3.7 References	References

TABLE OF CONTENTS

LIST OF EXHIBITS

EXECUTIVE SUMMARY

Background

The Office of the Manager, National Communications System (OMNCS) performs a broad range of activities in fulfilling its mission. These activities include analyzing communications networks that support national security and emergency preparedness (NS/EP) communications. As more businesses, government organizations, and the public use the Internet for their daily activities, it has become more important for the OMNCS and its constituents to understand the operation of the Internet and its dependence on the existing communications infrastructure.

The phenomenal growth of the Internet has been one of the most significant technological events of the last several years. As an instrument for sharing and distributing information, the Internet will be judged one of the major milestones of the latter part of the 20th century. The exponential growth in Internet traffic has fostered the concept of the "Internet" as the ubiquitous tool for sharing information. However, the accessibility and availability of the Internet depend on a physical infrastructure of software, routers, and transmission media. It is commonly perceived that the Internet and the public telephone networks in the United States are two separate and distinct systems. Although this is true to a certain extent, most data networks, including the Internet, rely on the public networks (PN) to transport their traffic.

Internet Definition

At the highest level, the current Internet consists of multiple national and regional Internet Service Providers (ISP) and interconnection points where the ISPs meet and exchange traffic. This infrastructure is similar to that of the old National Science Foundation (NSF) network, NSFNET, which consisted of a three-tier structure:

- Backbone network
- Regional networks
- Local/campus networks.

The NSFNET was decommissioned in 1995. In its place are multiple nationwide networks similar to the original NSFNET backbone network. Regional networks still aggregate their traffic and hand it off to the nationwide backbone networks to which they are connected. Interexchange points (IXP) are located nationwide to facilitate the exchange of traffic between national and regional ISPs.

National Service Providers (NSP) provide national backbone service. This type of service provider owns or leases its own backbone network and has a nationwide customer base. Additionally, NSPs are generally connected to all the major IXPs and

have peering agreements with other major NSPs at these exchange points. Traffic originating with a customer on an NSP that is destined for a customer on another NSP is transferred from the originating NSP's network to the terminating NSP's network at an IXP

Regional Service Providers (RSP) are similar to the NSPs in that they own or lease their backbone network, but they are much smaller in scale. Their networks encompass a single region and usually have a regional customer base. RSPs have peering agreements with NSPs to transfer traffic over the Internet. RSPs either connect directly to the NSP or connect to an IXP where they transfer traffic to the NSP network.

With the dissolution of the NSFNET backbone, the NSF sponsored three primary and one secondary Network Access Points (NAP). The NSF's concern was that without the sponsorship of a core set of exchange points, the commercial backbone providers would set up a conglomeration of bilateral connection points that would potentially result in routing chaos.

Each NAP operator provides the exchange facility while the ISP that connects to the NAP establishes peering agreements with the other ISPs connecting to the same NAP. The purpose of a peering agreement is to ensure that traffic from one ISP can reach all the customers on another ISP by exchanging routing information between the two ISPs.

The current number of IXPs on the Internet far exceeds the original four NAPs sponsored by NSF. The term "NAP" is applied only to the NSF-sponsored IXPs, whereas all IXPs provide the same functionality, which is a common place for ISPs to exchange data.

Analysis

The Internet is a very dynamic entity in that it is constantly evolving and growing. Therefore, it is impossible to accurately identify all components of the current Internet To develop the data for this report, the Internet was analyzed to identify key components used to transmit network traffic across the Internet. To achieve this purpose, a software tool, called the Internet Analysis Tool (IAT) was used to automatically trace the routes used to send traffic between two hosts on the Internet. The IAT collects data from the set of routers an Internet packet traverses on its path from one host to another. The analysis of the routes identified by the IAT yields traffic trends and identifies key components in the Internet infrastructure.

For this analysis, two IAT source sites were chosen:

- Booz•Allen & Hamilton, McLean, Virginia, on the PSINet network
- Proxima, Inc., McLean, Virginia, on the MCI Network.

The tool collected routes from each of these two sites to 105 other sites located across the United States. The type of Web sites chosen for this analysis were the following:

- 23 NCS Member Organizations' Web sites
- 50 State Web sites
- Major university Web sites
- Popular commercial Web sites.

The output from an IAT execution is the set of routers in the path between two hosts. For each router, three datagrams were sent at different times of the day, and the round trip time from the originating host and the router was collected.

Analysis Results

Traces performed throughout the test period indicated high success rates averaging between 87 and 89 percent. Of the unsuccessful trace attempts, most resulted from an unreachable node (i.e., a router or the destination server) in the path that was probably either shut down or incompatible with the IAT software.

Internet use is highest during mid-to-late afternoon business hours. Based on the round trip time for packets to traverse the network, congestion peaks between the hours of 12:00 noon and 4:00 p.m. eastern time.

This analysis indicated that the number of router hops did not vary in accord with the time of day or the day of the week. Thus, the predictability of Internet routing, along with an increasing dependency on this communications medium, renders it vulnerable to targeted and intended network disruptions.

Routers appear to share a somewhat balanced traffic load within the backbone networks (excluding those routers closest to the two sources). As expected, a high number of router "visits" occurred in the initial hops of the traces. These initial routers are critical to the sources; however, they are not necessarily critical to the entire Internet. As the trace moved away from the source and into the backbone networks, the number of visits per router stabilized. Therefore, a single critical router could not be identified, however, it could be determined which networks were more heavily traversed. For this analysis, MCI's network was traversed most frequently and was, therefore, critical to the success of the traces.

Vulnerabilities

The Internet can provide service in a volatile, unreliable network environment. But, like the PN, the Internet has vulnerabilities that can severely degrade its level of service. Because the Internet relies on PN packet and circuit switched networks, it is vulnerable to the same cable cuts and other damage that can affect the PN. In addition, some restoration techniques used by the PN carriers for circuit switched traffic cannot be used on the Internet's packet switched traffic.

National IXPs are critical to the operation of the U.S. portion of the Internet. An IXP failure could greatly reduce the Internet's ability to transport traffic nationwide or even worldwide. Congestion at these IXPs has also convinced ISPs that it is necessary to establish secondary means of interconnecting with one another.

Network routing protocols dictate how traffic is directed through the network in that they determine the paths that should be taken through the network to avoid congestion and network outages. Some Internet routers are vulnerable to "thrashing" – the optimal path through the network changes so frequently that the router spends more time computing these paths than actually routing users' data.

In summary, the initial analysis has determined that the Internet's physical vulnerabilities are consistent with the vulnerabilities of other large communication networks, most notably "last mile" issues and loss of backbone transport. Additional vulnerabilities exist that are distinct to the Internet – congestion (exponential growth in traffic), routing software, and network server management issues.

1. INTRODUCTION

The National Communications System (NCS) is a federation of 23 federal departments, agencies, and organizations that are responsible for the survivability and interoperability of various components of government communications supporting national security and emergency preparedness (NS/EP) activities. The Office of the Manager, National Communications System (OMNCS) is the planning and operational element of the NCS. The OMNCS performs a broad range of initiatives in fulfilling its mission, including analyzing communications networks that support NS/EP communications. The analysis process utilizes a standard OMNCS modeling methodology that incorporates OMNCS and commercial-off-the-shelf models, as well as public and proprietary data.

1.1 BACKGROUND

The phenomenal growth of the Internet has been one of the most significant technological events of the last several years. As a instrument for sharing and distributing information, the Internet will be judged one of the major milestones of the latter part of the 20th century. The introduction of Web browsers, dial-up communications protocols (i.e., Point-to-Point Protocol (PPP), Serial Line Interface Protocol (SLIP), and WinSock), and the increased efficiency of routers have made Internet access possible and cost effective even for small-business and at-home personal computer (PC) users. The exponential increase in Internet traffic has fostered the concept of the "Internet" as the ubiquitous tool for sharing information. However, the accessibility and availability of the Internet depend on a physical infrastructure of software, routers, and transmission media. As more businesses, government organizations, and the public use the Internet for their daily activities, it becomes more important to understand the operation of the Internet and the reliance of the Internet on the existing communications infrastructure.

The infrastructure that supports the Internet has evolved from mainframes and large minicomputers using dedicated transmission lines to low-cost routers and dial-up access from modems on PCs. Additionally, a growing support industry is providing Internet services, software, and content. As the Internet continues to evolve, its users will increasingly be dependent on not only the physical infrastructure but also the supporting services that have allowed the Internet to become an unparalleled information sharing tool.

1.2 SCOPE

This report describes the Internet by tracing its growth and development over the last three decades. It is difficult to provide a detailed, definitive history of the Internet

because much of its history has incorporated computer folklore and anecdotes. However, the major Internet milestones have been captured and serve as a baseline for its future growth. In context of the current description of the Internet and the Public Networks (PN), this document addresses several key vulnerabilities. These vulnerabilities are quantified using a simple route tracing tool that determines the physical path of Internet traffic. The Internet routes are then overlaid onto the PN infrastructure to illustrate the interdependence of the PN and the Internet.

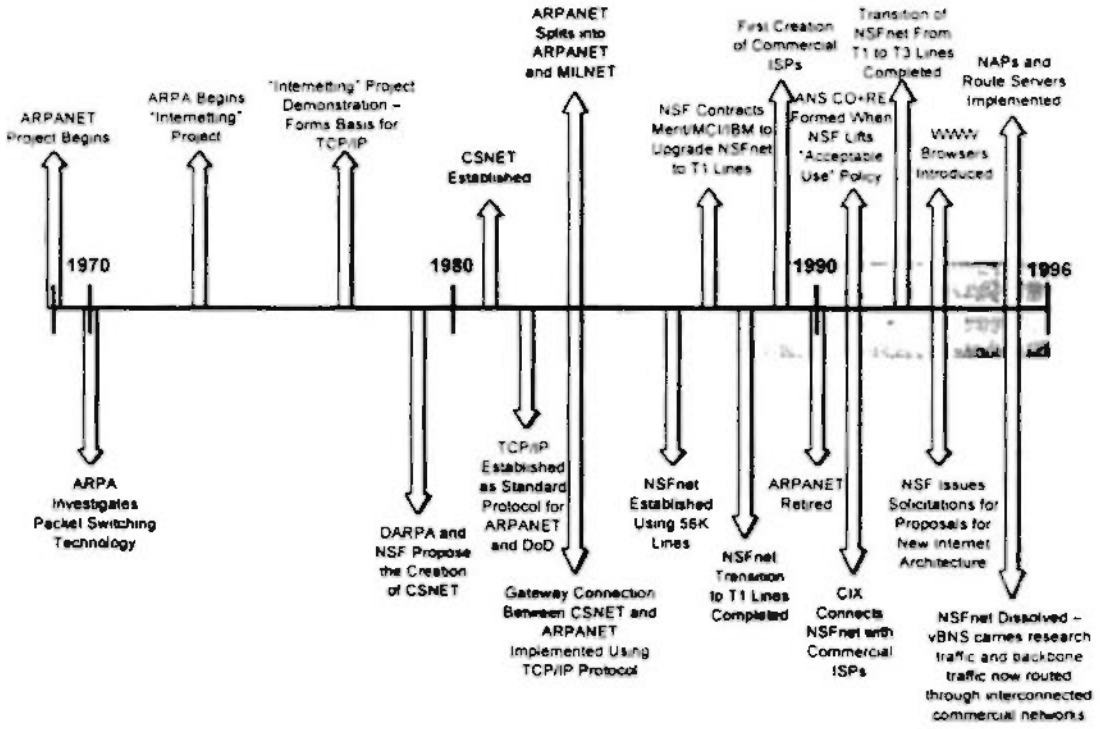
1.3 ORGANIZATION

This document is organized into five sections. Section 1, Introduction, provides the background and scope of the Internet/PSN Interconnectivity and Vulnerability Assessment. Section 2, the History of the Internet, provides a detailed description of the history of the Internet from its earliest inception in 1969 up to the dissolution of the National Science Foundation's (NSF) backbone network in 1995. Section 3, Internet Definition, presents a breakdown of the different types of service providers, a description of the Internet infrastructure at a high level, and a discussion of the relationship of the Internet infrastructure to the PN infrastructure. Section 4, Internet Analysis, describes the Internet Analysis Tool (IAT) functionality and implementation. This section also presents the analysis methodology and results from the IAT. Finally, Section 5, Vulnerabilities, analyzes the current infrastructure of the Internet and discusses its major vulnerabilities.

2. HISTORY OF THE INTERNET

The Internet is a very complex entity of more than 10 million hosts connecting over 95,000 networks. To fully describe what the Internet consists of today, it is necessary to look at how the Internet began and evolved to its current state. The roots of the technology employed by today's Internet are found by analyzing its evolution. This section provides a detailed description of the history of the Internet beginning with the initial work performed by the Defense Advanced Research Projects Agency (DARPA) in 1969 to the recent commercialization of the Internet and the dissolution of the National Science Foundation Network (NSFNET) backbone in 1995. Exhibit 2-1 shows a timeline of the history of the Internet that this section will discuss in detail.

Exhibit 2-1
Internet Timeline



The inception of the Internet can be traced to 1969 when DARPA was commissioned by the United States Department of Defense (DoD) to develop a communications system that would be survivable in the face of enemy attacks including nuclear war. In addition, the network should allow military and academic researchers to collaborate on research projects and share computer processors across the country. In response to this

direction, DARPA, later renamed ARPA, set up a network consisting of the following four nodes:

- University of California at Los Angeles
- Stanford Research Institute
- University of California at Santa Barbara
- University of Utah.

ARPA used this four-node network, referred to as ARPANET, to experiment with the linkage to be used between DoD and military research contractors.

In 1970, ARPA began researching packet switched technology. The goal of this technology was to decentralize the network by giving all nodes on the network equal authority to transmit and receive packets across the network. The route each packet took to its destination was unimportant as long as it reached its destination. Thus, packet switching technology was effective when network connections were unreliable. This packet switching technology, employed by ARPA during the seventies, was known as the Network Control Protocol (NCP). By the end of 1971, there were 15 nodes connecting 23 hosts to ARPANET.

In 1973, ARPA began the "Internetting" project. The goal of this project was to develop a protocol that could seamlessly pass information between different networks. This project culminated in 1977 in a demonstration of networking through various media including satellite, radio, telephone and Ethernet. The protocol developed in this project formed the basis for the Transmission Control Protocol and Internet Protocol (TCP/IP), where IP handles the addressing of the individual packets while TCP coordinates the proper transmission of information.

By the end of 1982, ARPA established TCP/IP as the protocol suite for the ARPANET, requiring that all nodes connecting to ARPANET use TCP/IP. Additionally, DoD declared that TCP/IP was to be its standard protocol. The official cutover from NCP to TCP/IP was executed on January 1, 1983. Aiding this transition was the incorporation of TCP/IP into Version 4.2 of Berkeley Standard Distribution of UNIX. This version of the UNIX operating system was free to anyone who wanted it, thus ensuring a wide deployment for TCP/IP. The marriage of TCP/IP and UNIX began a long-standing affiliation between the Internet and the UNIX operating system that continues today.

Another major event in 1983 was the division of ARPANET into two networks: ARPANET and MILNET. MILNET was to be used for military specific communications, whereas ARPANET was to continue its research and development in networking computers. MILNET was integrated with the Defense Data Network created in 1982. The funding for ARPANET was provided by Defense Advanced

Research Projects Agency (DARPA). By 1984, the number of hosts connecting to the ARPANET was more than 1,000.

While the ARPANET was undergoing major changes, another significant event in the history of the Internet occurred. In 1979, representatives from DARPA and the NSF and computer scientists from several universities met to establish a Computer Science Department research computer network (CSNET). One of the driving forces for the establishment of CSNET was the concern that computing facilities located at universities not connected to ARPANET did not have the same advantages in research and staff and student recruitment as those who were connected. In 1981, CSNET was fully operational through money granted by NSF.

Although designed initially to be a standalone network, CSNET later incorporated a gateway connection to the ARPANET. In the summer of 1980, a DARPA scientist proposed the interconnection of the not yet established CSNET and ARPANET using protocols that would provide services and the seamless transmission of information between users regardless of the type of network. This set of protocols was TCP/IP. The gateway connection between the two networks was established in 1983.

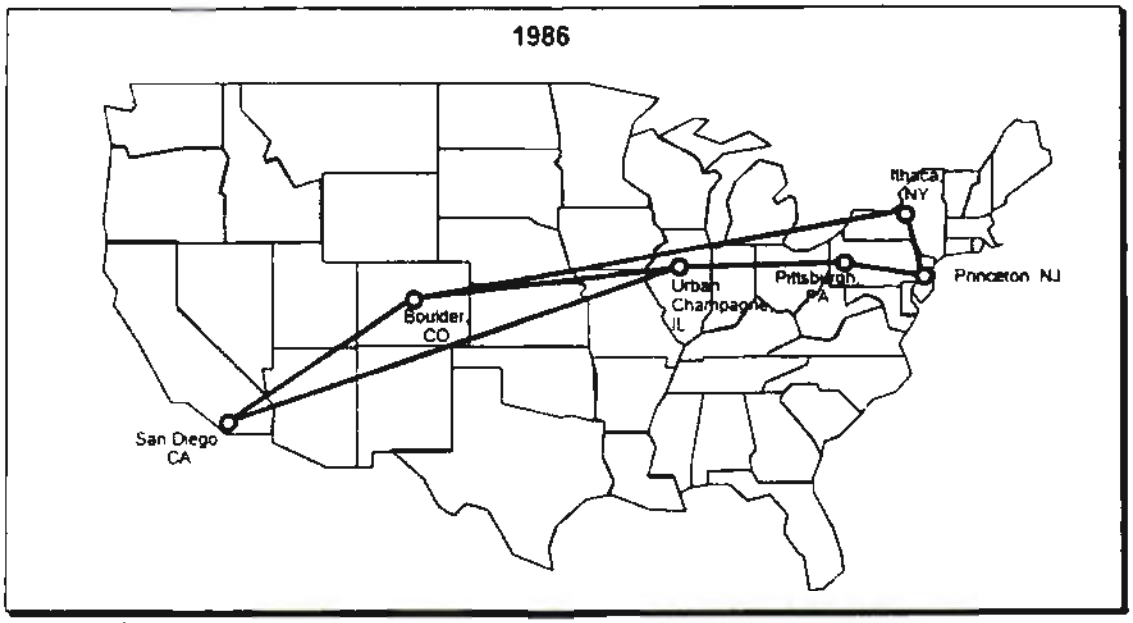
In 1986, the NSF created the NSFNET. The purpose of this network was to provide high-speed communications links between five major supercomputer centers located across the United States. Although ARPANET was flourishing, its 56-Kbps backbone and network topology could not fulfill the demand for high-speed networking required by multiple research projects. The goal of the NSFNET was to provide a reliable environment for the U.S. research and education community and access to the major supercomputing centers. The NSFNET essentially duplicated the functionality of the ARPANET. NSF chose TCP/IP as the standard protocol for its new network. This new network ultimately led to the downfall of ARPANET. In 1990, ARPANET was formally retired.

The infrastructure of the NSFNET was a three-tier hierarchical structure:

- National backbone
- Regional networks
- Local area networks (LAN).

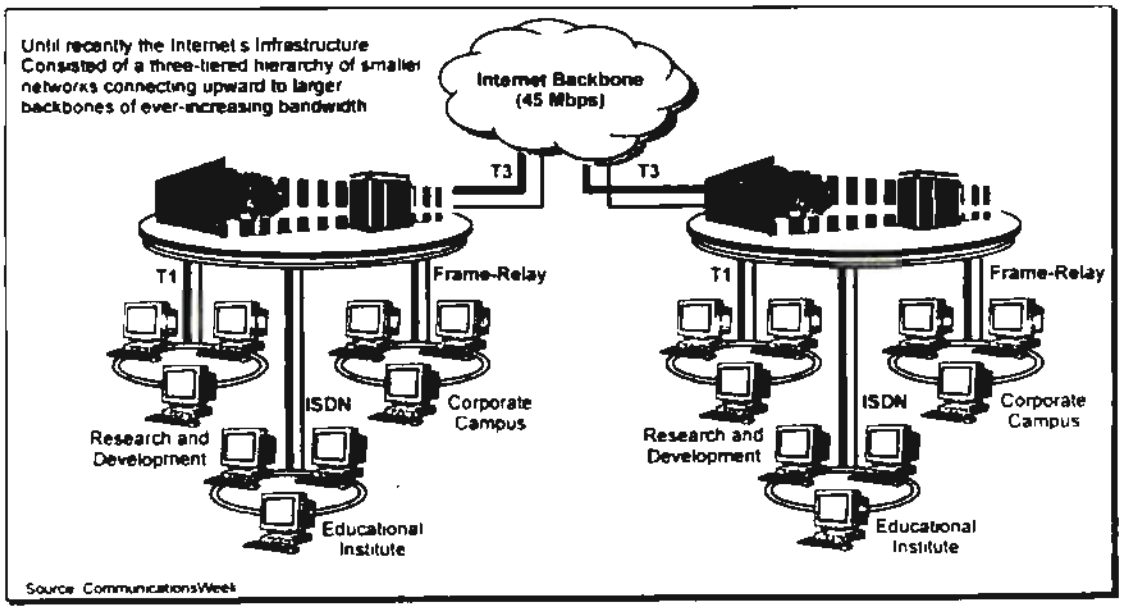
The original backbone of the NSFNET, depicted in Exhibit 2-2, consisted of a 56-Kbps network. This backbone network is considered the basis of what is now called the Internet. Regional networks hung off the backbone network and provided services to LANs at education and research facilities. Universities and research associations combined to form the regional networks, which in turn would aggregate their traffic and "hand it off" to the NSFNET backbone. Exhibit 2-3 depicts the three-tier structure implemented in the NSFNET throughout its existence.

Exhibit 2-2
Original NSFNET Backbone



Source: NSF

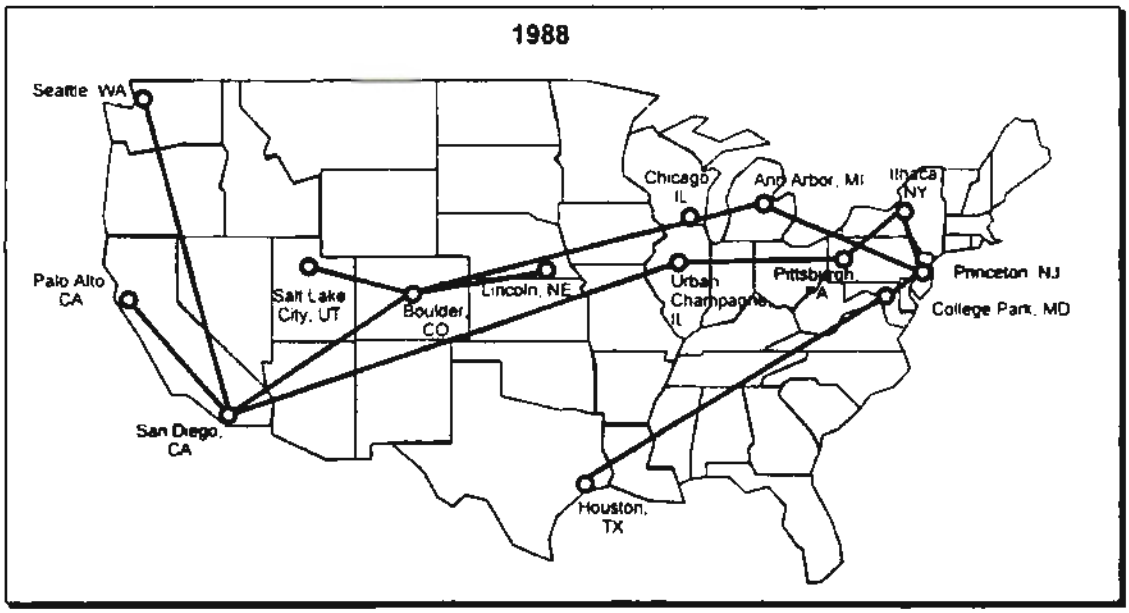
Exhibit 2-3
NSFNET Three Tier Infrastructure (1986 - 1995)



Because NSFNET's primary focus was for nonprofit research and development by universities and research groups, NSF instituted an "acceptable use" policy that restricted the use of the NSFNET to noncommercial activities. Additionally, NSF offered financial help to those regional networks, composed of university and research facility LANs, who wished to connect to the NSFNET backbone.

By 1987, the NSFNET outgrew its existing capacity. NSF awarded a five-year contract to Merit, the Michigan state networking organization, with MCI and IBM. The purpose of this contract was to transition the NSFNET backbone to T1 links and provide several access points around the country. Merit's role was to manage the backbone including routing, whereas IBM provided the routing equipment and MCI provided the trunk lines. The transition to a T1 backbone was completed in 1988. By the end of the 1980s, more than 100,000 hosts from 17 countries worldwide were connecting to the NSFNET. Exhibit 2-4 depicts the T1 backbone of the NSFNET in 1988.

Exhibit 2-4
1988 T1 NSFNET Backbone



Source: NSF

As the NSFNET grew, some organizations realized that providing services and functionality similar to that of the NSFNET without the access restrictions was a golden business opportunity. These organizations, experienced in providing regional network operations, seized the opportunity to set up their own nationwide backbone networks. Thus, the first commercial Internet service providers were created. These providers included Performance Systems (PSINet), and Alternet, which was generated from

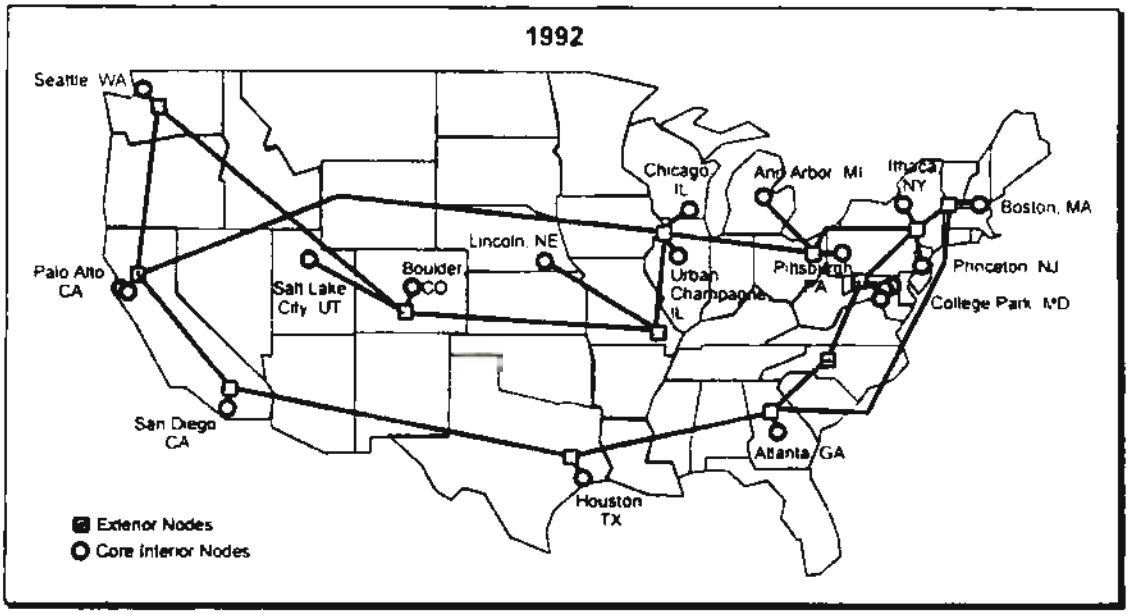
UUNet Technologies. The main focus of these networks was to provide the same functionality as the NSFNET, over their own networks, but without any access restrictions.

In 1991, the fourth year of the five-year contract, Merit, IBM and MCI formed a new nonprofit corporation, Advanced Networks and Services (ANS), which was given the operational responsibilities of the NSFNET. In June 1991, ANS announced it would provide commercial access to the Internet, thus nullifying the acceptable use policy. By broadening access to the Internet, ANS increased its efforts to expand connectivity and make the Internet a more powerful tool. The new evolving private commercial networks were hindering research, forcing researchers to spend time accessing several networks all in the name of science. With expanded commercial providers on the Internet, there was a single common network that increased a researcher's ability to find any information needed and focus on the research at hand. When NSF lifted its access restrictions in 1991, allowing commercial traffic on the NSFNET, ANS formed a for-profit subsidiary, ANS CO+RE (Commercial + Research & Education), to provide full commercial traffic across the backbone. Once the "acceptable use" policy had been abolished, PSINet, UUNet Technologies, and General Atomics (CERFnet) created the Commercial Internet Exchange (CIX). CIX was a traffic exchange point between the NSFNET and the commercial Internet service providers networks.

The other major event that occurred in 1991 was the transition of the NSFNET backbone from T1 links to T3. This transition, like the initial transition from 56-Kbps to T1 links in 1988, was because of the capacity of the backbone network could not meet the traffic loads. Although this transition required new routing equipment and interfaces and, at times, proved to be technically challenging, it was accomplished with relative ease. This was due to the fact that the same organizations who were managing the old T1 backbone were responsible for implementing and overseeing the new T3 backbone network. Additionally, the T1 backbone still existed as a backup if the new network failed. Exhibit 2-5 depicts the T3 NSFNET backbone as of 1992.

In 1992, Vice President Al Gore drafted legislation that proposed a National Research and Education Network (NREN). This new network would consist of T3 links (separate from those making up the NSFNET backbone) and would connect all schools, libraries, etc., for a cost of over $2 billion. Even though the legislation was passed, no new network ever came into existence. The NREN effort did, however, succeed in sparking a greater interest in the Internet.

Exhibit 2-5
1992 T3 NSFNET Backbone



Source: NSF

The new public Internet coincided with the release of the first Microsoft Windows version of Mosaic in 1993. Mosaic, developed by the University of Illinois at Urbana-Champaign, was an X-Windows interface to the World Wide Web (WWW) The concept of the WWW was started in 1989 in Switzerland as a means to easily share information among researchers in high-energy particle physics. In 1991, the first WWW server came into existence, but without any client software. The introduction of the first interface to WWW included the capability to navigate through the Web via the mouse. Today's Web browsers, such as Netscape, include File Transfer Protocol (FTP), E-mail, Telnet, and many more capabilities. The use of a graphical interface to access the Internet has played a significant role in the popularity growth of the network because it allowed access to the Internet without having knowledge or possession of the UNIX operating system.

While the look and feel of the Internet was undergoing changes, NSF, in 1992, began to question its role in the network. NSF observed that its backbone network was operating in conjunction with several commercial nationwide backbone networks. Essentially, NSF was paying for users to access its network, and thus the Internet, whereas the other commercial service providers were being paid for access to theirs. Although in 1991 the NSF had notified the regional networks that they would have to become self-sustaining, it was 1992 before the NSF took action. The NSF began considering ways in which it could successfully pull out of the Internet arena with little

disruption to the Internet while continuing its commitment to the education and research community.

With the five-year contract between the NSF and Merit drawing to a close, Merit was granted an 18-month extension (beyond the original October 1992 expiration date) to allow the NSF time to work out how to transition its backbone network into a new structure. This work culminated in a solicitation for proposals (Solicitation 93-52) in the following four areas that compose the new national Internet structure:

- Network Access Points (NAP)
- Routing Arbiter
- Regional network provider awards
- A very high-speed Backbone Network Service (vBNS).

The NAPs act as interconnection points where commercial Internet service providers can meet and exchange traffic. The NSF believed that without such interconnect points, backbone providers would likely establish their own independent bilateral connect points that would stifle the NSF's plan for full connectivity for the research and education community. The NAP manager contracts were awarded to the following:

- Sprint, for a New York NAP
- Metropolitan Fiber Systems (MFS) Datanet for a Washington DC NAP
- Bellcore and Ameritech for a Chicago NAP
- Bellcore and Pacific Bell for a California NAP.

The Routing Arbiter is an independent group that operates route servers at each NAP. The transfer of traffic among the backbone providers that meet at the NAPs is facilitated by route databases contained in the route servers. These databases contain routing information and policy requirements for each backbone provider and therefore indicate to which provider the incoming information should be sent. This contract was awarded to Merit and the Information Sciences Institute (ISI) at the University of Southern California, which together make up the Routing Arbiter group.

With the dissolution of the NSFNET, and the introduction of NAPs and commercial traffic, access to the Internet by the NSF subsidized regional networks was no longer free. The commercial backbone providers were now paying a fee to interconnect with the NAPs and passing these charges to their users — the regional network providers. Therefore, the NSF decided to create the regional network provider contracts to alleviate the regional networks' initial shock of having to pay for Internet access. The awards provided the regional networks with annual NSF funding, with the funding declining to zero over a four-year period. The regional network providers would use the subsidy to pay the commercial Internet providers who were in turn required to connect to the NAPs. There were 17 contracts awarded to regional network providers for interregional connectivity.

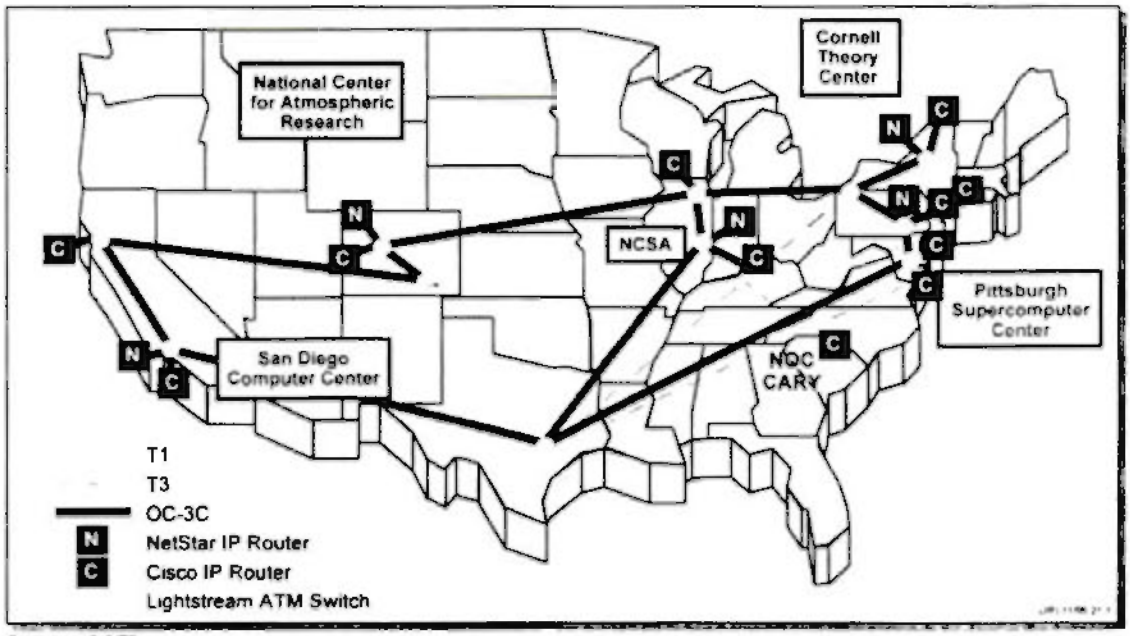
The NSF also proposed to sponsor a new backbone, the vBNS, operating at a minimum speed of OC-3 (155 Mbps), to link the following five NSF supercomputer centers:

- Cornell Theory Center
- National Center for Atmospheric Research
- National Center for Supercomputing Applications
- Pittsburgh Supercomputing Center
- San Diego Supercomputing Center.

Unlike the general purpose NSFNET infrastructure, the vBNS functions as an advanced research laboratory, allowing research, development, and integration of new networking requirements, using technology beyond just IP routing. There is a strict acceptable use policy: the vBNS may only be used for meritorious high-bandwidth research activities and it may not be used for general Internet traffic. NSF entered into a five-year agreement with MCI to provide the vBNS.

During this five-year agreement, MCI is expected to participate in the development and use of advanced Internet routing technologies. At the end of the agreement, it is anticipated that technology will exist that will increase the transmission speeds beyond 2.2 Gbps. Additionally, the vBNS will act as an experimental platform for the development and testing of broadband Internet services and equipment. Exhibit 2-6 depicts the NSF's vBNS network.

Exhibit 2-6
The National Science Foundation vBNS Network



Source: MCI

The result of NSF's solicitation for proposals was a new Internet structure. In April 1995, the NSFNET backbone was formally retired. At that time, 93 countries and more than 50,000 networks were connected by the NSFNET backbone. Exhibit 2-7 details the number of networks, by country, connected to the NSFNET backbone by the end of the project.

NSF's original task was to improve the previous NSFNET backbone, push the technology to new heights, and implement it on a national level. It was hoped that this would place a powerful tool in the hands of the research and education community, and create innovative use and applications. Its goals were accomplished: the NSFNET backbone connected most of the higher research and education community to a robust and reliable high-speed network and it served as the sole player in making the Internet industry.

The NSF's task will continue to evolve in two directions: 1) providing support for the research and education community by guaranteeing the availability of services, resources, and tools to keep the Internet connected, and 2) by continuing to push networking technology using the vBNS.

Exhibit 2-7
Countries and Networks Connected to NSFNET as of April 1995

Country	Total Networks	Country	Total Networks	Country	Total Networks
Algeria	3	Greece	105	Norway	214
Argentina	27	Guam	5	Panama	1
Armenia	3	Hong Kong	95	Peru	44
Australia	1875	Hungary	164	Philippines	46
Austria	408	Iceland	31	Poland	131
Belarus	1	India	13	Portugal	92
Belgium	138	Indonesia	46	Puerto Rico	9
Bermuda	20	Ireland	168	Romania	26
Brazil	165	Israel	217	Russia	405
Bulgaria	9	Italy	506	Senegal	11
Burkina Faso	2	Jamaica	16	Singapore	107
Cameroon	1	Japan	1847	Slovakia	69
Canada	4795	Kazakhstan	2	Slovenia	46
Chile	102	Kenya	1	South Africa	419
China	8	Korea, South	476	Spain	257
Colombia	5	Kuwait	8	Swaziland	1
Costa Rica	6	Latvia	22	Sweden	415
Croatia	31	Lebanon	1	Switzerland	324
Cyprus	25	Liechtenstein	3	Taiwan	575
Czech Rep.	459	Lithuania	1	Thailand	107
Denmark	48	Luxembourg	59	Tunisia	19
Dominican Rep.	1	Macau	1	Turkey	97
Ecuador	85	Malaysia	6	Ukraine	60
Egypt	7	Mexico	126	Unit Arab Emirates	3
Estonia	49	Morocco	1	U. K.	1436
Fiji	1	Mozambique	6	United States	28470
Finland	643	Netherlands	406	Uruguay	1
France	2003	New Caledonia	1	Usbekistan	1
French Polynesia	1	New Zealand	356	Venezuela	11
Germany	1750	Nicaragua	1	Vietnam	1
Ghana	1	Niger	1	Virgin Islands	4

Source: Merit Network, Inc.

3. INTERNET DEFINITION

At the highest level, today's Internet consists of multiple national and regional Internet Service Providers (ISP) and interconnection points where the ISPs meet and exchange traffic. This infrastructure is similar to that of the old NSFNET, which consisted of a three-tier structure:

- Backbone network
- Regional networks
- Local/campus networks.

On the NSFNET, regional networks would aggregate their traffic and "hand it off" to the NSFNET backbone. The regional networks comprised multiple local business and campus networks. Although there were many regional and local networks, there was only one backbone network.

As mentioned in Section 2, the NSFNET has been decommissioned. In its place are multiple nationwide networks, which are similar to the NSFNET backbone network. Regional networks still aggregate their traffic and hand it off to the nationwide backbone network to which they are connected. Interexchange points (IXP) are located around the country where traffic is exchanged between national and regional ISPs. Peering agreements are used between the ISPs connected at an IXP to determine how traffic is routed. These service providers and interexchange centers are the main components of the U.S. Internet. This section will describe different elements of the Internet architecture and the different routing protocols used on today's Internet.

3.1 INTERNET SERVICE PROVIDERS

ISPs are classified according to their network and customer base. The network classification refers to whether or not the ISP owns or leases its network. An ISP that does not own or lease its network is referred to as a reseller. The customer base classification refers to an ISP's type of customers, national or regional. A particular ISP may have national and regional customers, but generally it has more of one type than another. There are three types of ISPs:

- National Service Providers (NSP)
- Regional Service Providers (RSP)
- Resellers.

The following sections provide further detail for each type of ISP.

3.1.1 National Service Providers

The first category of ISPs is NSP, which provide national backbone service. This type of service provider owns or leases its own backbone network and has a nationwide customer base. Additionally, NSPs are generally connected to all the major IXPs and have peering agreements with other major NSPs at these exchange points. Traffic originating with a customer on an NSP that is destined for a customer on another NSP is transferred from the originating NSP's network to the terminating NSP's network at an IXP. The NSPs network infrastructure consists of routers (network layer) and switches (data link layer) that are owned by the NSP. The following are examples of NSPs:

- ANS
- BBN
- MCI
- PSINet
- Sprint
- UUNet.

Of the NSPs, MCI and Sprint are the only two that own their entire network. Other NSPs may own small parts of their networks, but most of their networks consist of circuits leased from the PN providers. Most of these circuits are leased from the large Interexchange Carriers (IEC)[1]. However, some circuits are also leased from the Local Exchange Carriers (LEC) (e.g., Bell Atlantic), Competitive Access Providers (CAP) (e.g., Metropolitan Fiber Systems), and smaller IECs (e.g., LDDS).

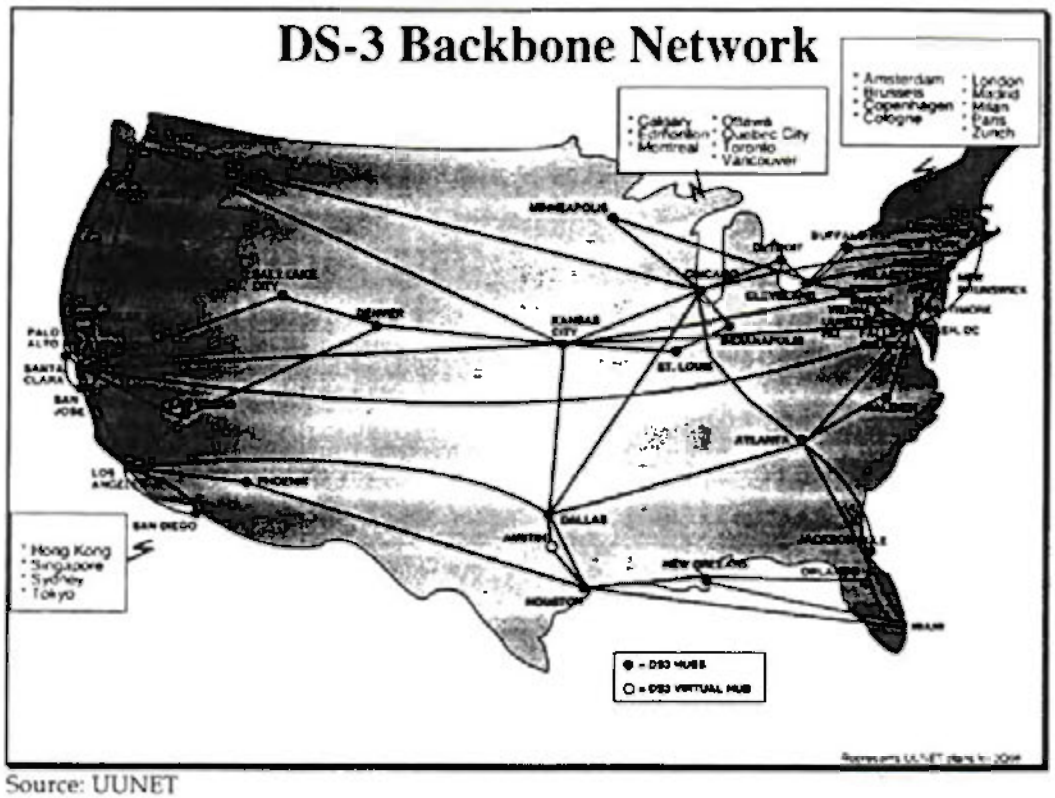
Exhibit 3-1 depicts a representative backbone network for UUNet, one of the NSPs mentioned above. As shown in the exhibit, UUNet (like most NSPs) has redundant connectivity between each switching node on its backbone network.

NSPs rarely sell directly to small consumers (e.g., small businesses and residential customers) because of the added "customer handholding" required by smaller, less experienced users. Instead, NSPs sell their services to large businesses and resellers. Resellers in-turn resell Internet service to small business and residential customers. It is important to note that not all NSPs resell their networks, e.g. PSINet.

The architecture of an NSP's network may be separated into access and transport. Access refers to the customer's connection to the NSP, whereas transport refers to the backbone of the NSP's network. Customers connect to NSPs via leased and dial-up lines. Typical leased lines are 56-Kbps or T1 and usually terminate at an NSP's point of presence (POP).

[1] MCI advertises that 40% of all Internet traffic travels over MCI circuits. This includes traffic on MCI's NSP and traffic on other NSPs that use MCI leased lines.

Exhibit 3-1
Representative NSP Backbone Network



Source: UUNET

For dial-up customers, the NSP usually has digital and/or analog modem banks terminating from its POP into the local central office using T1s. Because NSPs have national presence and reach, once a customer's traffic reaches an NSP's POP, it has essentially reached the Internet. The typical backbone of an NSP comprises routers and switches connected by T1, T3, or even OC-level circuits. These circuits may be leased from one or more IEC. One NSP, PSINet, leases backbone circuits from five different IECs.

The NSP market has not escaped the notice of existing PN providers anxious to get involved in the growth of the Internet. In the short term, PN providers have chosen to partner with NSP providers for Internet backbone transport instead of developing NSP expertise in-house. For example, GTE recently announced a partnership with UUNet to provide Internet access under the GTE name to customers in 46 U.S. states[2]. Cross PN-NSP service agreements also exist between Pacific Bell and America On-Line (which owns ANS), and AT&T and BBN.

[2] Washington Post, July 11, 1996, Page D9.

The recently announced merger between UUNet and MFS may be a harbinger of future mergers between NSPs and PN providers. PN providers own the data links necessary to run an NSP and have the marketing savvy to sell Internet service to business and residential customers. NSPs, on the other hand, have the in-house technical expertise to manage the switches, routers, and interconnection arrangements necessary to make the NSP backbone work.

Other future developments in the NSP market will include service differentiation to target selected customer markets. For example, MCI and BBN have announced services that provide a higher quality of service to business customers who subscribe to their NSP. BBN provides priority treatment to business customers through Internet Protocol version 6 (IPv6) priority service protocols. MCI provides a separate network for its business subscribers' Internet traffic. This separate network includes locally hosted mirror sites from popular Web sites on other NSP networks and in the future will include IPv6 priority treatment.

3.1.2 Regional Service Providers

The second category of ISPs are the RSPs. These service providers are similar to the NSPs in that they own or lease their backbone network but are much smaller in scale. Their networks encompass a single region and usually have a regional customer base. RSPs have peering agreements with NSPs to transfer traffic over the Internet.

RSPs either connect directly to the NSP or connect to an IXP where they transfer traffic to the NSP network. NorthWestNet is an example of an RSP that connects directly to an NSP. NorthWestNet, which provides service to customers in Washington, Oregon, and Idaho, has direct connections to both MCI and Sprint's NSP networks. Erols is an example of a network with a direct connection to an IXP. Erols, which provides service to customers in the metropolitan Washington, DC area, is connected to the Metropolitan Area Ethernet-East (MAE-EAST) IXP where it can transfer traffic to most of the larger NSPs and several smaller RSPs.

RSP service is an attractive option for residential and small business customers. Because of the small customer base, RSPs can offer more "hands-on" assistance in the form of customer training and help desk operators trained to assist less knowledgeable users.

Like NSP networks, the RSP's network architecture may be separated into access and transport portions, though with different meanings. In the RSP scenario, access refers not only to the customer connecting to the RSP but also the RSP connecting, if at all, to the Internet. Transport refers to the backbone of the RSP's network. As in the NSP scenario, customers connect to RSPs via leased and dial-up lines. Typical leased lines are 56-Kbps or T1 and usually terminate at an RSP's POP. For dial-up customers, the

RSP usually has digital and/or analog modem banks terminating from its POP into the local central office using T1s.

An RSP's backbone is typically restricted to a region, as opposed to NSPs who have a national presence and whose backbone spans the entire United States. Transport on an RSP's network, or backbone, comprises T1 and T3 circuits that connect their POPs and customers in a particular region. These circuits are leased from LECs, CAPs, and IECs. As noted above, RSPs' customers are primarily small business and residential subscribers. In the coming years, new companies will enter this market. Most notable are the Internet service offerings from the IECs and the Region Bell Operating Companies (RBOC). This increased competition may cause some consolidation of the RSP market when smaller RSPs go out of business or are bought out by larger firms. The remaining RSPs will survive by targeting market niches, such as high volume residential users or businesses new to the Internet.

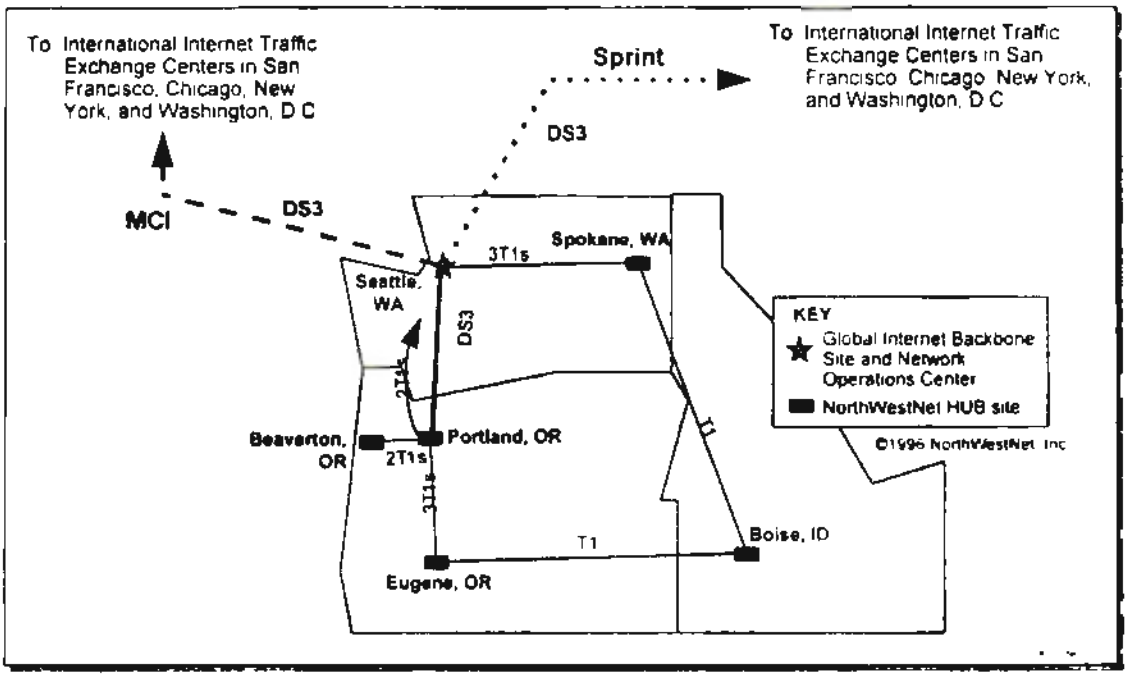
The exhibits below show two example RSP network backbones. Exhibit 3-2 shows NorthWestNet's backbone and Exhibit 3-3 shows CERFnet's backbone. Note that NorthWestNet has redundant connections to Sprint and MCI to transfer traffic, whereas CERFnet connects directly to NAPs to share traffic.

3.1.3 Resellers

Resellers are another member of the Internet provider family. Resellers purchase service from NSPs or RSPs and resell this service to small business and residential customers. Resellers are differentiated from RSP because resellers do not own or lease a network infrastructure. Instead resellers typically operate out of a single site with a modem bank for customer access and a T1 connection to transfer traffic to the NSP/RSP network.

There are approximately 1,400 Internet resellers in the United States, most of which base their business on monthly subscriptions to Internet service. As the Internet market matures, monthly Internet service is becoming a commodity. This trend has been furthered by the entry of the RBOCs and IECs into the residential Internet service market. Typically, unlimited access is provided on a monthly basis for a flat-rate fee or a combination of flat-rate and usage-based pricing.

Exhibit 3-2
NorthWestNet Backbone Network



Source: NorthWestNet, Inc

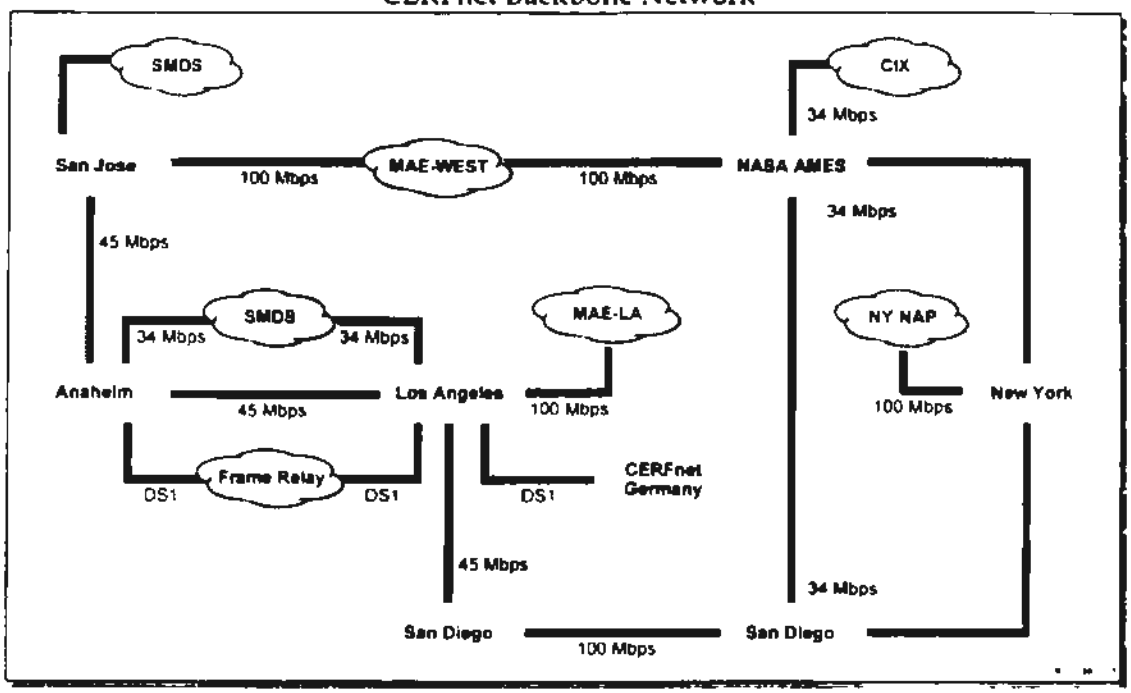
Because Internet service has significant economies of scale, the market favors the larger providers who can spread their fixed costs over a larger customer base. Because of this, many experts predict that the number of Internet resellers will decrease dramatically in the next few years. The Yankee Group predicts that there will only by 200 resellers left in business by 2000.

The remaining resellers may survive by looking for market niches. For example, instead of simply providing monthly Internet subscriptions, resellers are already starting to provide value-added services such as Web page hosting, Web page development, security management, and electronic commerce consulting. In these areas, a reseller may be able to provide better service to small businesses than a larger NSP or RSP company.

3.2 INTEREXCHANGE POINTS

With the dissolution of the NSFNET backbone, the NSF was concerned with maintaining connectivity between the commercial ISP networks and the research and education community. To address this issue, the NSF sponsored three primary and one secondary NAPs. Without the sponsorship of a core set of exchange points, the NSF feared that the commercial backbone providers would likely setup a hodgepodge of bilateral connect points potentially resulting in routing chaos.

Exhibit 3-3
CERFnet Backbone Network



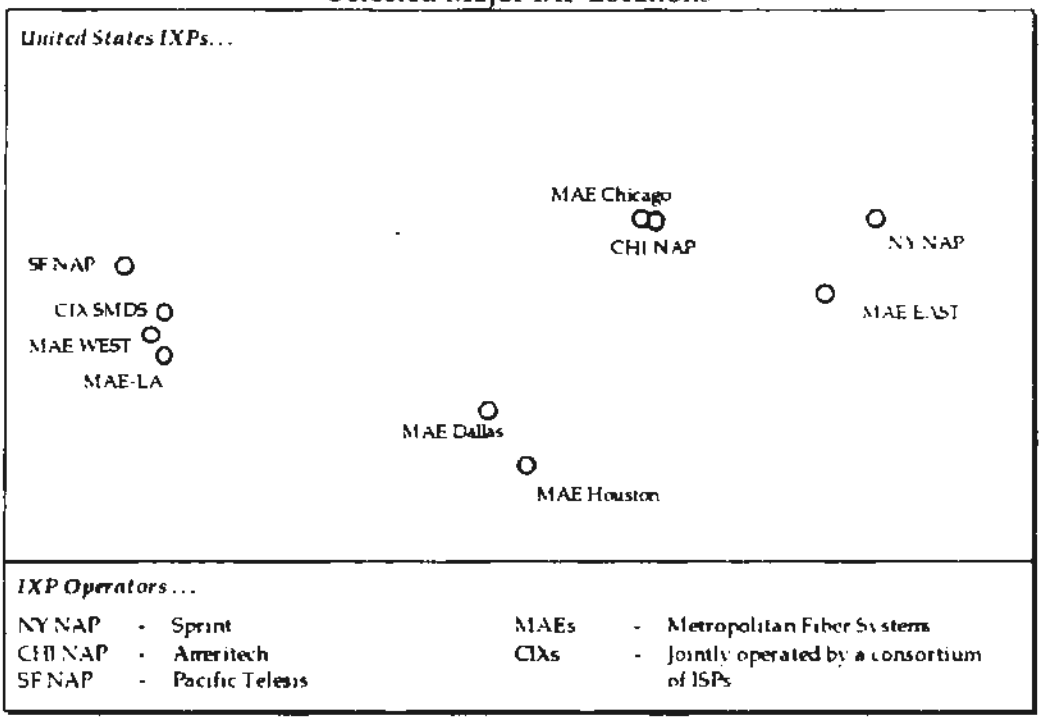
Source: CERFnet

Under the NSF model, each NAP operator provides the exchange facility while the ISP that connects to the NAP establishes the exchange agreements, also known as peering agreements, with the other ISPs connecting to the same NAP. The purpose of a peering agreement is to ensure that traffic from one ISP can reach all the customers on another ISP by exchanging routing information of the two ISPs.

Today there are many more IXP centers on the Internet other than the original four sponsored by NSF. The term NAP is applied only to the NSF sponsored IXPs, whereas all IXPs provide the same functionality, a common place for ISPs to exchange data. Various cities and organizations have used different names for the exchange point, e.g., NAP, MAE, CIX, Federal Internet Exchange (FIX). Exhibit 3-4 presents a snapshot of several of the larger IXPs in the United States.

It is important to note that an IXP does not have to serve the national ISPs. There are metropolitan exchange points (MXP) used today, which are similar in structure to the NAPs, but service only local and regional traffic. This means that traffic originating and terminating in a single region would not traverse any of the national ISPs' backbones, thus removing some of the burden on these networks. The remainder of this section describes the structure of an IXP and details the different types of peering agreements used by the ISPs at an IXP.

Exhibit 3-4
Selected Major IXP Locations



3.2.1 IXP Functionality and Architecture

The large, national-scope IXPs, such as the NAPs or MAEs, interconnect numerous national ISPs and may exchange data requiring large amounts of bandwidth. The smaller regional or metropolitan IXPs will have fewer interconnects and require much less bandwidth. The IXP structure is similar regardless of the size of the IXP or the technical architecture used to exchange the traffic.

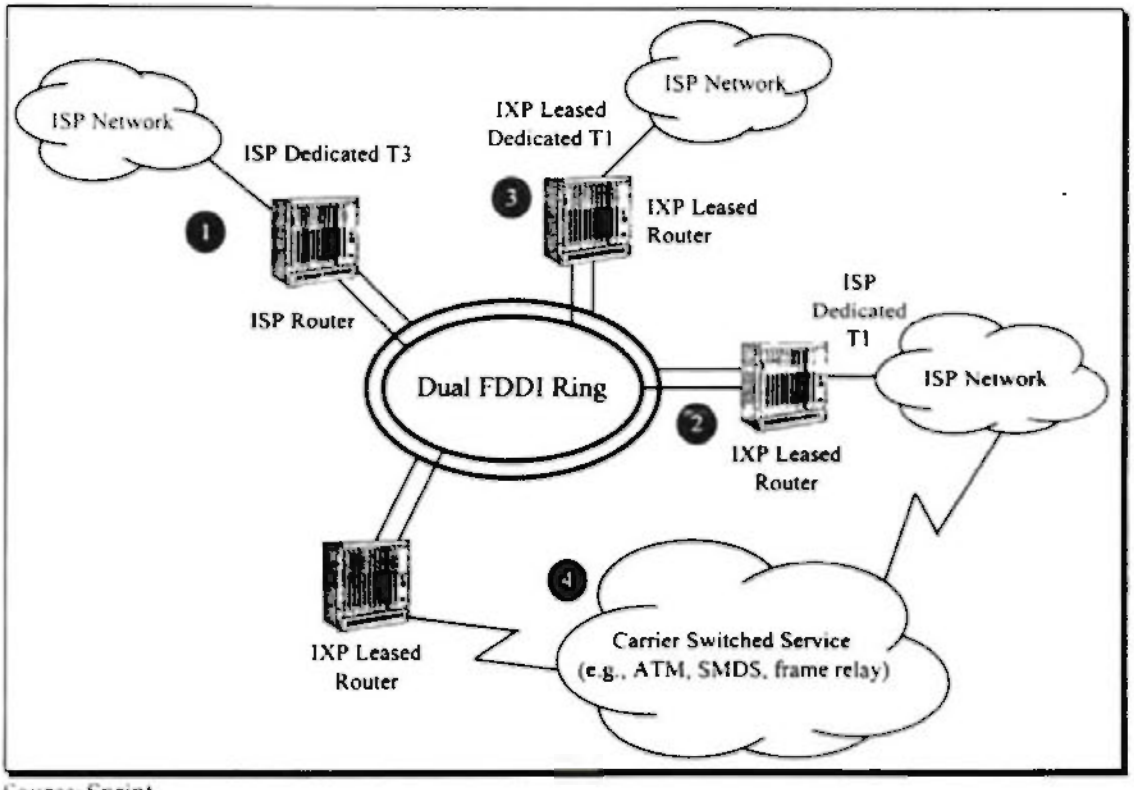
IXP facilities generally consist of a high-speed LAN or metropolitan area network (MAN) architecture capable of interconnecting various wide area network (WAN) technologies. ISPs connect to the IXP LAN via either a high-speed router or an asynchronous transfer mode (ATM) switch capable of connecting to the IXP architecture. Each of the connecting ISPs must negotiate bilateral or multilateral peering agreements with other ISPs interconnecting at the IXP. The Routing Arbiter administers the traffic routing resulting from these peering agreements. This traffic routing and addressing information is provided to each ISP's router by a route server within the IXP LAN. Incoming packets are routed to the high-speed LAN ring where the route server indicates the possible routes available to the packet.

The most common NAP architecture is a Fiber Distributed Data Interface (FDDI) dual ring backbone LAN running at 100 Mbps. Routers for each ISP are homed to the dual ring bus in the various access configurations discussed below:

1. The ISP provides and manages its own router collocated at the IXP facility. The ISP would have dedicated access to this router via its own dedicated line (typically a T1 or T3). This option may not be available at all IXPs because of space limitations.
2. The ISP leases an IXP provided router located at the IXP. The ISP has dedicated access to the IXP router via its own dedicated line.
3. The ISP leases the dedicated connection and the router from the IXP.
4. The ISP leases switched access service to the IXP facility from the IXP or another provider. Switched access may include ATM, Switched Multimegabit Data Service (SMDS), and frame relay.

These access configurations are shown in Exhibit 3-5. For each of the access configurations, all equipment is located in a single facility.

Exhibit 3-5
Typical National-scope IXP Configurations



Source: Sprint

Other IXP architectures that have been used include SMDS and ATM networks. Lower bandwidth solutions such as SMDS may be more commonplace in regional or metropolitan IXPs.

All IXPs are privately owned and administered by IECs, Incumbent Local Exchange Carriers (ILEC), Competitive Local Exchange Carriers (CLEC), or ISPs. The four NSF-sponsored NAPs are owned by Sprint, MFS, Pacific Bell, and Ameritech. Regional and metropolitan IXPs may also be owned by ISPs, e.g., the SMDS Washington Area Bypass (SWAB) is operated by PSINet. The IXPs normally charge flat interconnection fees and usage based fees to the interconnecting ISPs.

Large IECs, ILECs, and CLECs can provide network management for their IXPs from their PN network management centers. Most IXP operators will ensure reliability of service and mean time to repair, and provide maintenance for collocated equipment. The dual ring FDDI buses used in many large IXPs are also very robust to a single line fiber cut. A single dedicated connection from the ISP network to the IXP router will pose the greatest vulnerability in the IXP architecture. Redundant connections to the IXP should be used by regional ISPs that do not have presence at multiple IXPs.

3.2.2 IXP Peering Agreements

The policies for data exchange at an IXP are set forth by the parties involved. Just because an ISP connects to a particular IXP does not guarantee that that ISP can exchange traffic with every other ISP connected to that exchange point. Agreements that specify how traffic is carried and transferred, and how billing is handled have to be established and maintained between the ISPs on an IXP. Any ISP can connect to an IXP as long as the ISP agrees to the predefined policies. Currently, there are three different types of exchange policies:

- Bilateral
- Multilateral
- Multi-party bilateral.

A bilateral agreement is between only two ISPs at an exchange center. A multilateral agreement is between many ISPs at an exchange center. A multi-party bilateral agreement is between a small ISP and a large ISP to carry the small ISP's traffic to other ISPs. The more IXPs a single ISP connects to the better the performance and reliability of the ISP's service. Each IXP has its own procedures for establishing peering agreements among the IXP-attached ISPs.

A peering agreement is defined as the advertising of routes via a routing protocol for customers of the IXP participants. Specifically, the ISP is obligated to advertise all its customer's routes to all other participating ISPs and accept routes from the customer's

routes advertised by the ISP. ISPs are required to peer with the IXP's route server which facilitates the routing exchange between the ISPs routers. The route server gathers the routing information from each ISP's router, processes the information based on the ISP's routing policy requirements, and passes the processed routing information to each of the IXP-attached ISPs. Currently, ISI handles the work done on the routing management system, while Merit implements and maintains the route servers and route server databases.

3.2.3 National-scope IXP Architecture Example

Pacific Bell's NAP, located in San Francisco, California, is fairly typical of national-scope IXPs. PacBell's NAP is an ATM/FDDI hybrid LAN, whereas other national-scope IXPs may be straight FDDI design or an FDDI/Ethernet hybrid. PacBell's use of ATM makes it one of the fastest IXPs, capable of up to 139 Mbps for OC-3 access. PacBell's FasTrak℠ ATM Cell Relay Service offering is being rolled out in phases, first utilizing Permanent Virtual Circuits (PVC) and in the future, Switched Virtual Circuits (SVC). As the ATM technology matures and becomes more of an industry and user standard, PacBell and other IXP operators will migrate to fully switched ATM IXP backbones.

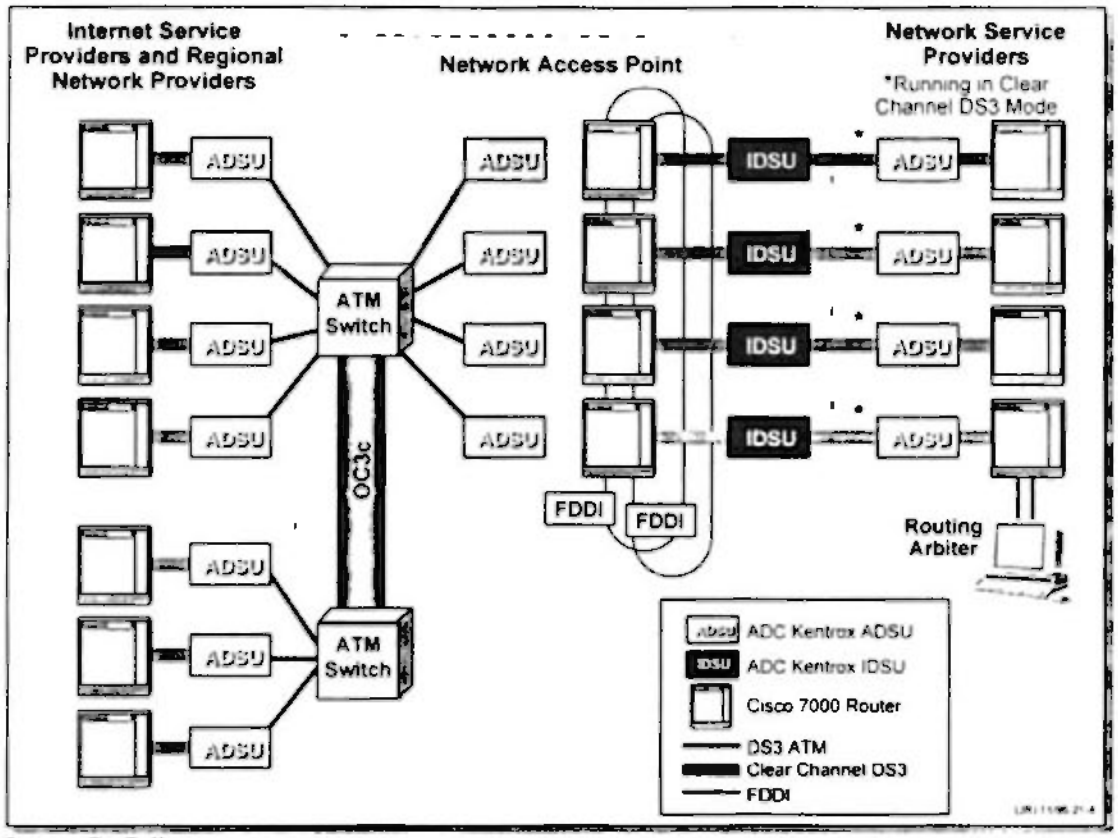
SF NAP consists of ATM switching sites in the San Francisco area connected by OC-3 Synchronous Optical Network (SONET) links. Participants can access the NAP network using an ADC Kentrox ADSU and a Cisco 7000 or 7010 router. Access speeds reach 36.8 Mbps for DS-3 access and 139 Mbps for OC-3 access.

In addition to the ATM network, the NAP includes an interconnected FDDI dual-ring LAN. The FDDI LAN provides service to customers that require bandwidth less than 30 Mbps. The FDDI LAN was added when PacBell tests indicated that the ATM network was dropping cells at speeds between 20 Mbps and 30 Mbps. ISPs provide or lease dedicated T1 or T3 connections to PacBell DSUs and Cisco 7000 routers connected to the FDDI backbone. Exhibit 3-6 depicts PacBell's San Francisco NAP ATM/FDDI hybrid network architecture.

3.2.3.1 Routing

Each participating ISP must negotiate bilateral peering agreements with other ISPs before connecting with PacBell's San Francisco NAP. Routing on the FDDI ring is accomplished via the route server database maintained by the Routing Arbiter. On request, PacBell will provide NAP clients with a PVC to the Routing Arbiter route server database to receive and provide routing updates. Routing among peered ISPs may also be accomplished by direct PVC connections between the ISPs at the NAP, without regards to the route server database.

Exhibit 3-6
PacBell San Francisco NAP ATM/FDDI Hybrid Architecture



Source: PacBell

3.2.3.2 National ISP Clients

The San Francisco NAP interconnects numerous national and regional ISPs. National ISPs include ANS, MCI, and Sprint.

3.2.4 Metropolitan IXP Architecture Example

PSI, Inc. manages a metropolitan IXP in the Washington, DC area. PSI established the SWAB as an alternative IXP to the MAE-EAST NAP. SWAB operates nearly identically to the national-scope IXPs, requiring participating ISPs to negotiate peering agreements. Unlike the NAPs, the SWAB network is not facilities-based. Instead, each interconnecting ISP subscribes to Bell Atlantic's SMDS service over which the TCP/IP is routed.

Each participating ISP must subscribe to Bell Atlantic's SMDS service at a specified access class (speed). SMDS may be accessed at up to 34 Mbps, making it a lower bandwidth solution than FDDI or ATM. The ISP must supply its own dedicated access (either T1 or T3) to the SMDS service. To route TCP/IP over SMDS, the ISP must also provide an SMDS capable CSU/DSU and an IP router that supports SMDS encapsulation at the SWAB interface.

SWAB provides broadcast capabilities by use of SMDS address groups. The SWAB participants can have their SMDS address included in the SWAB SMDS address group for broadcast purposes.

3.2.4.1 Routing

The functionality of the Routing Arbiter's route server database is provided using SMDS address screening. Address screening is used to filter out SMDS addresses from the SMDS connection, analogous to how the SS7 network can screen calls from a voice line. An ISP's screen accepts packets from peered ISPs, while refusing packets from other ISPs. Each ISP must request that Bell Atlantic screen SMDS addresses from their SWAB interface.

3.2.4.2 National ISP Clients

Currently, PSINet and UUNet are the only national ISPs interconnected at the SWAB.

3.3 INTERNET ROUTING PROTOCOLS

The Internet, as previously described, is a collection of networks that allows communications between research institutions, universities, and many other organizations worldwide. These networks are connected by routers. A router is connected to two or more networks, appearing to each of these networks as a connected host. Forwarding an IP datagram generally requires the router to choose the address of the next router in the path or, for the final hop, the destination host. This choice, called routing, depends on a routing database located within the router. The routing database is also known as a routing table or forwarding table. The routing database should be maintained dynamically to reflect the current topology of the Internet. A router normally accomplishes this by participating in distributed routing and least-cost routing algorithms with other routers.

Routers within the Internet are organized hierarchically. Some routers are used to move information through one particular group of networks under the same administrative authority and control, known as an autonomous system (AS). Routers used for this purpose are called interior routers and they use a variety of Interior

Gateway Protocols (IGP). Routers that move information between ASs are called exterior routers and they use Exterior Gateway Protocols (EGP).

There is no standard protocol for either IGP or EGP. However, there are three protocols that are used by the ISPs and at the IXPs on the Internet. Generally, ISPs use the Routing Information Protocol (RIP) or the Open Shortest Path First (OSPF) protocol.

Most IXPs use the Border Gateway Protocol Version 4 (BGP4) as their routing protocol. All three protocols are dynamic in that the routers interact with adjacent routers to learn which networks each router is currently connected. The IGP protocols, RIP and OSPF, are detailed in Section 3.3.1 and 3.3.2, respectively. BGP4 is presented in Section 3.3.3.

3.3.1 Routing Information Protocol

RIP was developed by the Xerox Corporation in the early 1980s for use in Xerox Network Systems (XNS) networks. RIP is a dynamic protocol that continually updates its routing table based on information received from its adjacent routers. RIP is a distance-vector protocol, meaning that each router maintains a table of distances (hop counts) from itself to each other router in the system. These routing tables are updated based on RIP messages from adjacent routers.

RIP performs five basic operations:

- Initialization
- Request received
- Response received
- Regular routing updates
- Triggered updates.

On execution, RIP determines which of the routers interfaces are up and sends a request packet out on each interface. The purpose of this request packet is to ask each of its adjacent routers for their entire routing table.

A request received operation occurs when a router receives a packet from one of its adjacent routers asking for all or part of the router's routing table. The router will process the request and reply by sending the requested data.

A response received operation occurs when a router receives a response to its request for all or part of its adjacent routers' routing table. When a response is received, the router must validate the response and update its routing table.

Regular routing updates occur every 30 seconds. A router sends either all or part of its routing table to all of its adjacent routers. This ensures that each router on the network consistently has an accurate routing table.
Finally, a triggered update occurs when a router notices that one of its routes has changed. The router sends all routes from its routing table which are affected by the changed route, which may or may not be the entire table.

Although RIP appears to be a very simple protocol, it does have serious limitations. First, as shown by the series of operations in RIP, the protocol propagates either all or part of a router's routing table every 30 seconds in addition to any triggered updates. Subsequently, the protocol is very slow to stabilize when network failures or routing errors occur.

Second, RIP limits the number of hops between any two hosts on the network to 16. This means that hosts that are more than 15 hops apart within a single AS will not be able to communicate with one another. As a result, RIP is not well suited for large internetworks and works best in small environments.

Finally, when faced with multiple routes between a router and a network, RIP always chooses the path with smallest number of hops. This choice does not consider other cost factors such as line speed and line utilization, which are important when choosing a path between two nodes. Although RIP is still a very popular protocol, many companies are moving toward its replacement, OSPF.

3.3.2 Open Shortest Path First

OSPF was developed by the Internet Engineering Task Force (IETF) as a replacement for RIP. OSPF is designed to overcome the limitations of RIP and is supported by all major routing vendors. OSPF uses IP and its own protocol and the transport layer, not UDP or TCP. OSPF is a dynamic link-state protocol, unlike RIP, which is a distance-vector protocol. In a link-state protocol, a router does not exchange distances with its neighbors. Instead, each router tests the status of its links with its neighbors and sends this information to each adjacent router. Routers using OSPF are able to build an entire routing table based on the link-state information received from each of its neighbors.

In contrast to RIP, OSPF does not make its routing decisions based on the number of hops to a destination. Instead, OSPF assigns a dimensionless cost to each of interfaces of the router. This cost is not based on hop count, but on throughput, round trip time, reliability, etc. When the router is faced with multiple paths for a particular route, the routing decision is made using this cost. If two routes exist with the same cost, OSPF distributes the traffic equally among the routes. Additionally, OSPF allows multiple routes to a destination based on the IP type of service, e.g., Telnet, FTP, SMTP. This

means that a router can chose the best route for outgoing packets based on the type of traffic contained within the packet.

As described in Section 3.3.1, RIP is not well suited for larger internetworks because of its functionality. OSPF however, is designed for larger networks and stabilizes much faster when network failures or routing errors occur. OSPF also does not impose limitations on the number of hops between any two hosts because it does not use this metric when making routing decisions. Although RIP is still very popular, OSPF will ultimately replace RIP as the Internet grows.

3.3.3 Border Gateway Protocol Version 4

The primary routing protocol used on the Internet is BGP4. This protocol is used on Internet core (high level) routers to dynamically learn network reachability, respond to outages, and avoid routing loops in interconnected networks. Although RIP and OSPF are IGPs, BGP4 is an EGP used to pass traffic between different autonomous systems. BGP4 uses the TCP protocol to communicate routing information with its BGP4 peers.

Routers using BGP4 classify traffic as either local traffic or transit traffic. Local traffic is traffic that either originates or terminates in the router's AS. All other traffic is classified as transit traffic. The goal of BGP4 is to reduce the amount of transit traffic on the Internet.

The BGP4 system exchanges network reachability information with other BGP4 systems. This information includes the full path of autonomous systems that traffic must transit to reach the destination. The network reachability information is used by the router to construct a graph of AS connectivity. Once constructed, routing loops can be removed from the AS connectivity graph and routing policy decisions can be enforced.

BGP4 peers initially exchange their full routing tables. From then on incremental updates are sent as the routing tables change. BGP4 assigns a version number to the routing table and all adjacent routers will have the same version number for their routing tables. This version number changes whenever the routing table is updated as a result of routing information changes. To ensure that the each adjacent router is alive, keepalive[3] packets are sent between BGP4 peers whereas notification packets are sent in response to errors or other special conditions.

After a router using BGP4 receives routing updates, the protocol decides which paths to choose to reach a specific destination. Like RIP, BGP4 is a distance-vector protocol that allows only a single path to a destination. However, BGP4 does not impose a limit on the number of hops between two hosts and stabilizes quickly after network failures or

[3] The BGP4 keepalive operation is independent from the TCP version of keepalive.

telephone lines. However, ISDN is gaining popularity with residential users as ISDN equipment and service prices drop. Both ISDN and analog modem connections use PN switched connections. The characteristics of analog modem and ISDN connections are described in Exhibit 3-7 below.

The bandwidth allocation for ISDN and analog modems is symmetric, meaning that there is an equal amount of inbound and outbound bandwidth. Unfortunately, many traffic applications are asymmetric, whereby the user receives far more inbound traffic than he or she generates. Examples of asymmetric applications include video-on-demand (small request to access a movie results in many gigabits of high resolution video) and Internet access (small request to access a Web page results in many megabits of text and images from the Web page).

Exhibit 3-7
Analog Modem and ISDN Characteristics

Characteristics	Analog Modem	ISDN
Speed	2.4 to 33.6 Kbps	64 to 128 Kbps
Equipment Cost	$100 to $150	$300 to $400
Representative Service Cost[4]	Flat Rate Monthly ($40/month)	Monthly Plus Usage ($100/month + $0.02/minute)

ILECs, cable companies, and direct satellite companies are testing and deploying several asymmetric access technologies (see Exhibit 3-8 below). These technologies have up to 30 Mbps of inbound bandwidth and up to 2 Mbps of outbound bandwidth.

Exhibit 3-8
Asymmetric Internet Access Characteristics

Characteristics	Direct Broadcast Satellite	ADSL	Cable Modems
Service Provider	DirecTV Satellite	ILECs	Cable Companies
Inbound Speed	400 Kbps	1.544 to 6 Mbps	10 to 30 Mbps
Outbound Speed	28.8 Kbps (over analog phone lines)	16 to 512 Kbps	768 Kbps to 2 Mbps
Equipment Cost	$1,700	$1,000	$500
Service Cost	$40/month	$60 to $100/month	$40/month
Status	Deployed	In trial	In trial

[4] Includes the cost of service from the LEC and the cost of access from the ISP.

routing errors occur. The decision process is based on different factors, including next hop, path length, route origin, local preference. BGP4 always propagates the best path to its adjacent routers. Currently, BGP4 is used by most IXPs on the Internet but is not defined as the standard EGP.

3.4 INTERNET ACCESS

The last (and in some ways the most vulnerable) component of the Internet architecture is the link between the service provider and customer. This access connection is typically a single dedicated or switched line over PN facilities.

Because access is provided over a single PN line, the connection is vulnerable to outages. This situation is identical to the "last mile" vulnerability of the PN architecture. Most other parts of the Internet architecture can use redundant links to route around outages. However, the access link is typically a single point of failure for an end user's connection to the Internet.

Internet access can be divided into two broad categories: business access and residential access. These categories are described separately below.

3.4.1 Business Access

Large and medium-size businesses use dedicated lines to connect their enterprise LAN/WAN to the Internet. These lines are either bundled with the ISP's service or leased separately by the company. In either case, the connection travels over PN facilities.

Most large businesses use T1 (1.544 Mbps) or higher connection speeds. Medium-size businesses use T1 or fractional T1 speeds (i.e., 128 Kbps to 768 Kbps) depending on their traffic requirements. Small businesses (10 to 50 employee sites) may be able to get by with a 56 Kbps leased line or a 128 Kbps Integrated Services Digital Network (ISDN) connection.

Leased line connections are available from ILECs and in metropolitan areas from CLECs. Today, CLEC companies include CAPs (e.g., Metropolitan Fiber Systems, Teleport Communications Group) and in many cases, IECs (e.g., LDDS, AT&T, MCIMetro). As legislation opens the local exchange to increased competition, leased lines may be available from utility companies, cable companies, or other providers.

3.4.2 Residential Access

Residential access connects a single user's computer to an ISP, reseller, or on-line provider. Most residential access is through modem connections over a LEC analog

The direct broadcast satellite offering is the only one of the three that is currently in widespread distribution. Direct broadcast satellite allows a user to receive inbound traffic over a 1-meter satellite dish and transmit outbound traffic over a standard analog modem line.

Asymmetric Digital Subscriber Line (ADSL) is a technology developed by the RBOCs to provide high bandwidth asymmetric connections over standard copper twisted pair wire. ADSL was originally developed exclusively for the home entertainment market (e.g., video-on-demand, interactive cable). However, as residential Internet access has grown in popularity, the LECs have added Internet access to their ADSL marketing efforts. ADSL is popular with LECs because copper cable is the basis for almost every residential phone installation. ADSL has a head start over its rival technologies because of the widespread deployment of copper wire (which reaches 98 percent of U.S. homes compared to 60 percent for cable). However, ADSL does have several drawbacks:

- Installation costs are high to upgrade existing copper cable to carry ADSL signals.
- Subscribers must be within 10,000 feet of the central office to reliably receive ADSL signals.
- Strong local AM stations can interfere with ADSL signals.
- The bandwidth available for communication is far less than the bandwidth available over cable modems.

Cable modems have the highest inbound and outbound bandwidth, but also have the most obstacles to widespread deployment. Cable modems depend on a two-way communication path between the cable operator and the subscriber. Almost every cable installation is designed to provide only a one-way path for video. To facilitate Internet access over cable plant, cable operators must upgrade their coaxial cable networks to two-way operation. Once upgraded, cable operators may have additional problems with the reliability of their plant, e.g., cable wires are installed only several inches below ground level and are highly susceptible to outages due to unintentional cable cuts. Once these issues are addressed, cable modems may easily fill a niche in the new market of Internet-enabled television (i.e., WebTV). Currently, access for these devices is provided using analog modems over dial-up lines.

4. INTERNET ANALYSIS

As described in Section 3, the Internet can be viewed as an interconnection of national and regional networks, end-users and organizations, and interexchange points. The Internet is a very dynamic entity that is constantly evolving and growing. Therefore, it is impossible to identify all of the components of today's Internet. For this report, the Internet is analyzed to identify key components used to transmit network traffic across the Internet. To achieve this purpose, a software tool, referred to as the IAT, was used to automatically trace the routes used to send traffic between two hosts on the Internet. The tool collects the set of routers an IP packet traverses on its path from one host to another. The analysis of these routes will identify traffic trends and key components in the Internet infrastructure.

This section provides an in-depth description of the IAT and analysis results. Section 4.1 details the functionality of the IAT. Section 4.2 details the implementation of the tool, including the set of hosts that was analyzed. Section 4.3 presents the analysis methodology and the results of the analysis.

4.1 INTERNET ANALYSIS TOOL FUNCTIONALITY

The purpose of the IAT is to collect the routes traveled by IP packets from one host to another. Because it is impossible to collect and analyze routes between every host on the Internet, a subset was chosen to provide an accurate sample of U.S. Internet traffic. Section 4.2 details the sites chosen for this analysis.

The IAT utilizes a UNIX utility, *traceroute*, to record the different routers a packet traverses once it is sent from the originating host to the destination host. The *traceroute* application is available with all UNIX and UNIX-variation operating systems. *traceroute* uses the Time To Live (TTL) field in the IP packet header to determine the routers in a particular path. The purpose of the TTL field is to ensure that packets do not stay on the Internet for an infinite amount of time (e.g., as a result of a routing loop). Each router that receives an IP packet is required to decrement the TTL field in the IP header by the number of seconds the router holds onto the datagram. Because most routers process a datagram in less than one second, the TTL field effectively becomes a hop counter that is decremented by one by each router.

IP packets are usually transmitted with a TTL of 60 by the originating host. When a router has an IP datagram with a TTL of one, the router decrements the TTL to zero, discards the packet, and returns an error message to the originating host. This error message is an Internet Control Message Protocol (ICMP) packet

that identifies the router that sent the error message and indicates that the time has been exceeded on the datagram.

The basic operation of the IAT is to send out *traceroute* IP datagrams beginning with a TTL of one, then a TTL of two, and so on, until the entire route between two hosts is determined. The router receiving the first IP datagram with a TTL of one will decrement the TTL and return an ICMP message to the originating host. This identifies the first router in the path. The IAT will then send out a second *traceroute* IP datagram with a TTL of two. The first router decrements the TTL to one, and sends the datagram to the next router in the path. The second router will decrement the TTL to zero and return the ICMP message. This continues until enough datagrams have been sent to have one of them reach the destination host. The destination will not discard the *traceroute* IP datagram, even though it will have a TTL of one because the datagram is addressed to that host.

For the IAT to determine that a datagram has reached its destination (because it has not received the final ICMP message), the IAT sends UDP datagrams to the destination host using a very high destination port number. The destination host will not respond to incoming packets on this port number; thus, the destination host will send back an ICMP "port unreachable" error to the IAT. The IAT differentiates between the time exceeded and port unreachable errors to determine when the route has been fully traced.

The output from an IAT execution is the set of routers in the path between two hosts. For each router, three datagrams are sent, and the round trip time from the originating host and the router is collected. Exhibit 4-1 depicts the sample output from a source host to the destination, www.disa.mil.

Exhibit 4-1
Sample Output From the IAT

Traceroute to www.disa.mil
1 Cisco-AGS.dcmetro.bah.com (156.80.1.1) 2 ms 2 ms 2 ms
2 fr.herndon.va.psi.net (38.2.104.1) 128 ms 227 ms 47 ms
3 38.1.2.19 (38.1.2.19) 45 ms 77 ms 138 ms
4 mae-east.ddn.mil (192.41.177.130) 68 ms 54 ms 41 ms
5 137.209.1.2 (137.209.1.2) 176 ms 168 ms 204 ms
6 198.26.127.10 (198.26.127.10) 179 ms 132 ms 114 ms
7 164.117.2.13 (164.117.2.13) 134 ms 127 ms 134 ms
8 164.117.1.1 (164.117.1.1) 143 ms 135 ms 125 ms
9 www.disa.mil (164.117.147.116) 135 ms 147 ms 176 ms

4.2 INTERNET ANALYSIS TOOL IMPLEMENTATION

This section details the implementation of the IAT described in Section 4.1. For this analysis, two sites were chosen as source sites:

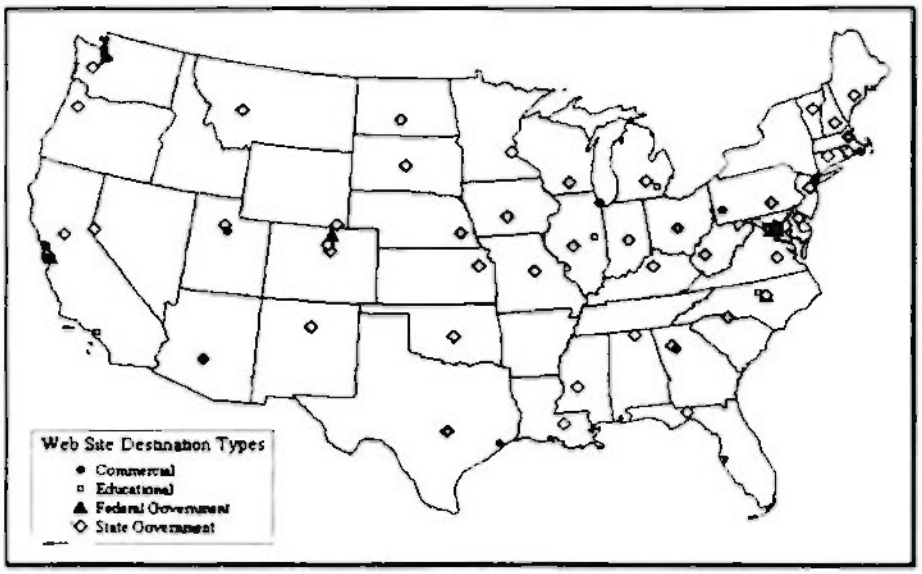
- Booz·Allen & Hamilton, McLean, Virginia, on the PSINet network
- Proxima, Inc., McLean, Virginia, on the MCI Network.

The tool collected routes from each of these two sites to 105 other sites located across the United States. The Web sites chosen for this analysis included the following:

- 23 NCS Member Organizations Web sites
- 50 State Web sites
- Major university Web sites
- Popular commercial Web sites.

Appendix A provides the entire list of Web sites used in this analysis. Exhibit 4-2 also shows the geographic locations of these sites. The IAT, which collects the routes from the two source locations to all 105 sites, is executed six times daily, every four hours beginning at midnight. This results in a sample of Internet traffic throughout the day. The output from this tool is formatted and loaded into an Oracle database where the analysis on the collection of routes is performed. Section 4.3 presents the analysis methodology followed by the IAT study.

Exhibit 4-2
IAT Site Locations



4.3 INTERNET ANALYSIS RESULTS

The data collected using the IAT represents a general picture of Internet connectivity. The destination Web sites used in the analysis were selected to provide both a United States and NCS specific view of the Internet's topology.

4.3.1 Internet Analysis Methodology

An in-depth analysis of the physical topology of the Internet would be an incredibly complex and difficult task. Because of the number of national backbones and regional distribution networks spanning multiple carriers, the Internet's topology is an amalgamation of CLEC, ILEC, and IEC networks. Determining the entire physical topology of the Internet may well be impossible without the cooperation of these PN carriers.

An analysis methodology was developed to provide the most complete and valuable view of the Internet and its topology. The methodology defines the steps used to evaluate the data obtained from the IAT. A description of the methodology is presented below.

- *Identify Scope of Analysis.* Although the Internet is too large and complex to be handled in its entirety, the scope of the analysis was selected to provide a representative view of the Internet. The IAT is most useful in analyzing single, specific routes, not large network topologies. Given enough representative routes, the collective results of the IAT can provide a view of portions of the larger Internet. By collecting data at various times of day from multiple routes, the IAT provides a representative set of data. The originating and destination sites selected for this analysis provide a distribution of sites across the United States. The inclusion of the NCS Member Organizations provides a capability to capture and analyze data specifically for the NCS community.

- *Identify Pertinent Data.* The data used in the analysis must provide a complete and accurate picture of how IP packet traffic will be routed over the Internet. Variables such as the distance traveled, number of networks traversed, and the congestion of the network will affect how packets traverse the network. The IAT provides a host of data that is used to analyze our representative Internet routes. The data used in this analysis includes the following:

  - Origin to destination route
  - Physical distance of route in air-miles
  - Time of day

- Round trip time
- Number of hops in route
- Routers in route
- Networks in route.

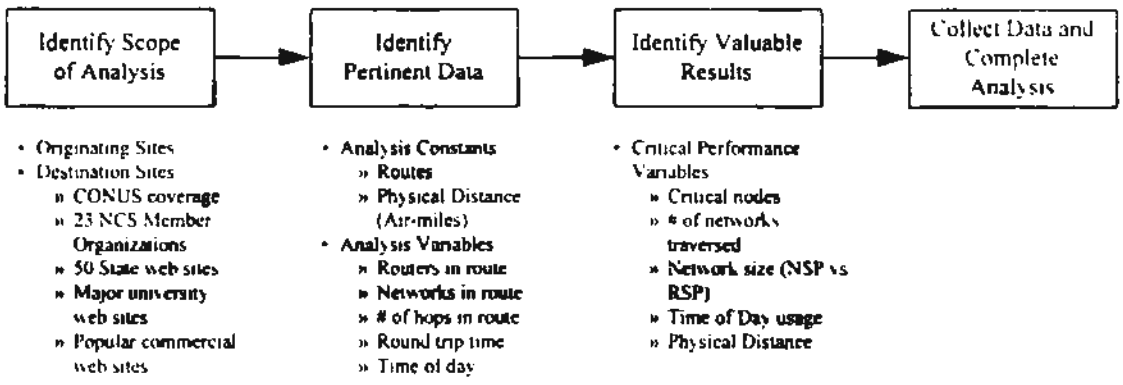
- *Identify Valuable Results*. The purpose of the analysis is to identify the discriminating variables that affect the Internet's performance. Using the available data (i.e., round trip time and number of hops in route), the analysis should indicate differences in performance based on the following variables:

  - Critical nodes
  - Physical distance between hosts
  - Time of day congestion
  - Number of networks traversed
  - Relative size of networks traversed (NSP versus RSP).

  These results will provide input to the analysis of the vulnerabilities of the Internet. They may also identify how the OMNCS and NCS Member Organizations can improve Internet reliability by choosing certain ISPs, mirroring important Web sites, or performing downloads in off-peak hours.

Exhibit 4-3 illustrates the Internet analysis methodology.

Exhibit 4-3
Internet Analysis Methodology



4.3.2 Internet Analysis Results

The IAT analysis focuses on identifying the path that is critical for transmitting data across the Internet's regional and national backbone networks. The data provided by the IAT was analyzed to trace the paths through the Internet and to identify how Internet data traffic is affected by daily traffic surges and congestion and network outages. This analysis is intended to provide an estimate of the performance characteristics of a portion of the U.S.-based Internet. However, the results presented here cannot be assumed to represent the entire Internet, or even the entire U.S.-based network. This is because of the limited scope of the data, and the sheer size of the Internet in terms of routers and hosts. More thorough analyses of the entire Internet are planned as a follow-up to this initial analysis. We chose to use two source hosts for this analysis, one based on Booz•Allen & Hamilton's network and the other on Proxima, Inc.'s network. Booz•Allen and Proxima, Inc. receive Internet service from two of the six NSPs, PSINet and MCI, respectively. Therefore, this analysis may primarily represent the characteristics of these two networks.

The data provided by the IAT traces is the basis of a statistical analysis of the number of hops and round trip time for the 210 source and destination pairs (2 sources and 105 destinations). Traces were given a status of either "successful" or "unsuccessful." A successful trace was one in which the IAT packets generated reached the destination router address and an unsuccessful trace was one in which they did not. Exhibit 4-4 shows the number of successful traces per source and the percentage of the total traces performed.

Exhibit 4-4
Status of IAT Traces

Source	*Total Traces*	*Successful Traces*	*Unsuccessful Traces*
Booz•Allen	5134	4468 (87 %)	666 (13 %)
Proxima, Inc.	9128	8098 (88.7 %)	1030 (11.3 %)

A small percentage of the traces for both sources was determined unsuccessful. An unsuccessful trace could typically be attributed to one of the following reasons:

- The destination name server entry could not be resolved and therefore the trace never began
- An initial router of the ISP could not be reached
- A router or gateway in the path of the trace was unreachable

- The destination server was unreachable, most likely due to it being shut down
- The host's network might use code that is incompatible with the IAT testing protocol. That might have resulted in a router not returning the ICMP messages required for the operation of the IAT.

Exhibit 4-5 illustrates an approximate categorization of reasons why traces were unsuccessful. The percentages of those due to an unreachable path router, an unreachable destination server, or incompatible network code were combined. A hop-by-hop analysis of all unsuccessful traces, comprising nearly 45,000 hops, would be required to determine the component percentages.

Exhibit 4-5
Categorization of Unsuccessful IAT Traces

	Booz•Allen	Proxima
Unresolved host name:	2.6 %	0 %
ISP unreachable:	0.2 %	0.8 %
Router or destination machine unavailable:	10.2 %	10.5 %
Total Unsuccessful:	13.0 %	11.3 %

The results described in the remainder of this analysis are solely based on successful traces.

4.3.2.1 Traffic Congestion

Internet traffic encounters congestion due to surges in its use in daylight hours. Traffic surges occur during working hours, and most notably between noon and 6:00 p.m. Weekend traffic should not be as susceptible to Internet congestion because of the reduced number of business users. Our analysis assumes the effects of congestion will become manifest in the response time for data traveling over the Internet.

The IAT collects the round trip time for a single datagram to travel to and from each of the destinations. For each destination, three datagrams are sent, and the total travel time is recorded for each. The average travel time versus time of day for these datagrams is shown in Exhibit 4-6. As expected, these results appear to coincide with traffic patterns for a typical east coast IXP, MFS's MAE-EAST. The additional traffic on the Internet results in a proportional increase in the delay time. Representative weekday and weekend data for MAE-EAST and MAE-WEST are shown in Exhibit 4-7 and Exhibit 4-8, respectively. The traffic

increase between 12:00 noon and 4:00 p.m. shown in the MAE-EAST traffic profile is similar to that of our round trip time results. Note that traffic on MAE-EAST, located in Washington, DC, and MAE-WEST, located in San Jose, CA, are nearly identical for the time of day, based on eastern standard time (EST). Because of the large amount of traffic traveling between the east and west coasts, these two IXPs are interdependent. The traffic generated on the east coast between 12:00 noon and 4:00 p.m. eastern time affects the west coast traffic patterns between 9:00 a.m. and 1:00 p.m. Pacific time.

Exhibit 4-6
Average Round Trip Time Versus Time of Day

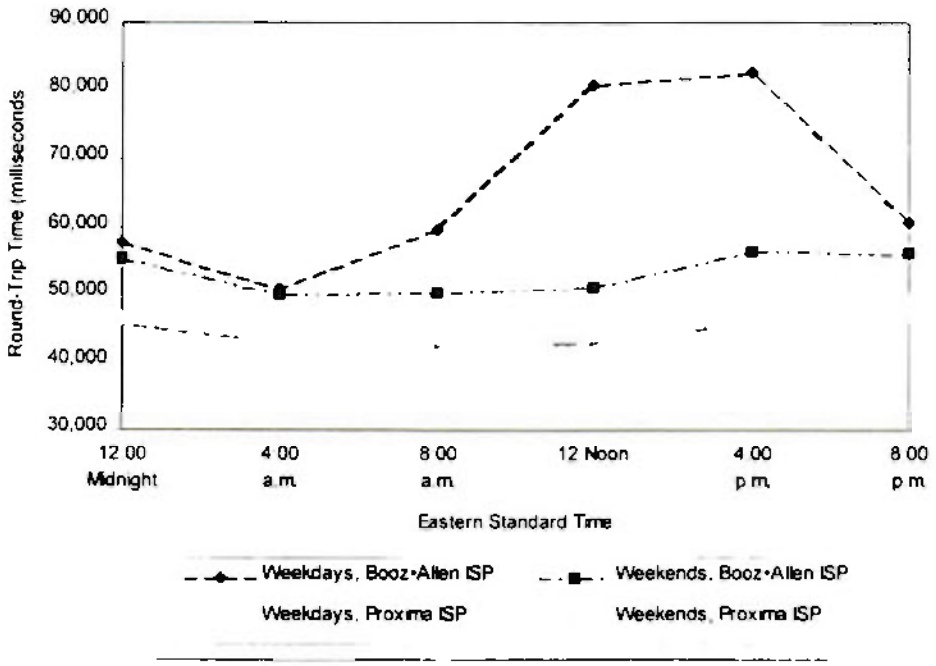
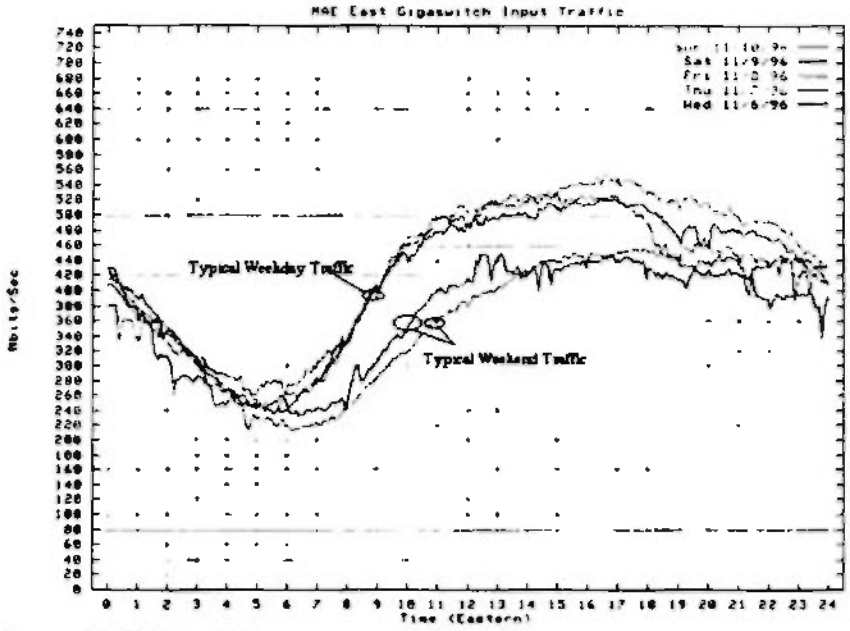
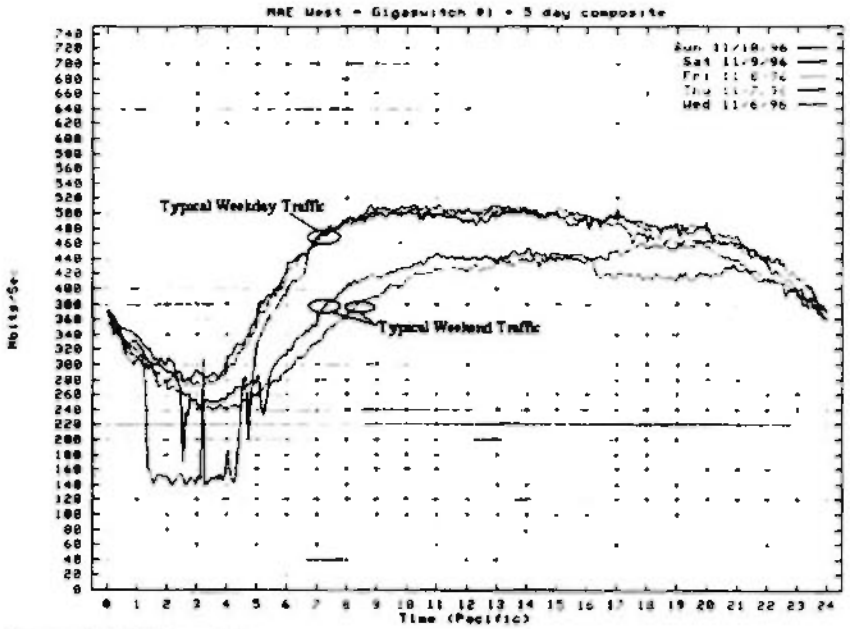


Exhibit 4-7
Typical Traffic Patterns at MAE-EAST



Source: MFS Datanet, Inc.

Exhibit 4-8
Typical Traffic Patterns at MAE-WEST



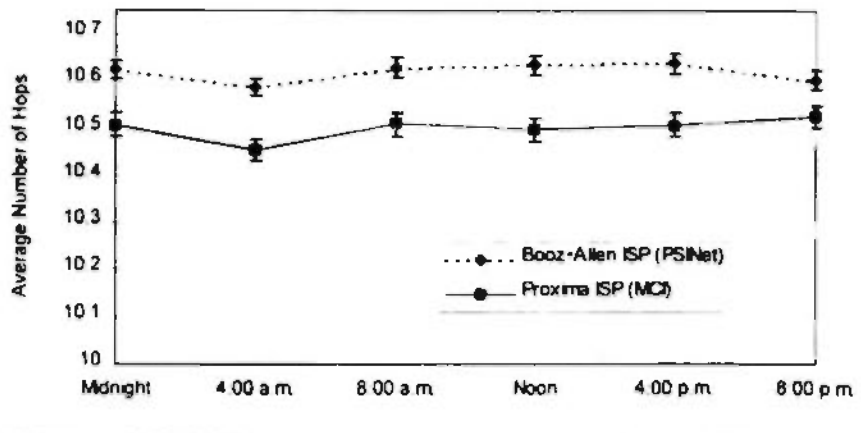
Source: MFS Datanet, Inc.

4.3.2.2 Network Outages

Network outages are the most disruptive of the Internet's vulnerabilities. In the case of critical nodes, a network outage can preclude access or egress from the network (as in the case of an isolated regional or local network) or severely hamper the flow of traffic (as in the case of a NAP or IXP failure). Network outages will occur with much less frequency than network congestion, but they may result in a significant reduction of network capacity and availability depending on their severity.

We determined the number of hops in each successful IAT trace from source to destination. Exhibit 4-9 compares the average number of hops with the time of day for each source network. It is clear that the number of hops does not depend on the time of day. This indicates that the path taken from source to destination does not change frequently due to outages or routing around network congestion. This is because Internet routing tables are generally static. Routing tables are meant to change during a disruption in service and in the event of network congestion. Although some routing algorithms will route around link congestion, this analysis indicates this is uncommon, because the number of hops does not depend on the time of day, while congestion does. Creating large Internet routing tables requires expensive processing power. This process can result in more route "thrashing" than actual routing. In fact, routing tables will normally only be recreated when links become disrupted, or when a network administrator manually replaces the routing table.

Exhibit 4-9
Average Number of Hops Versus Time of Day



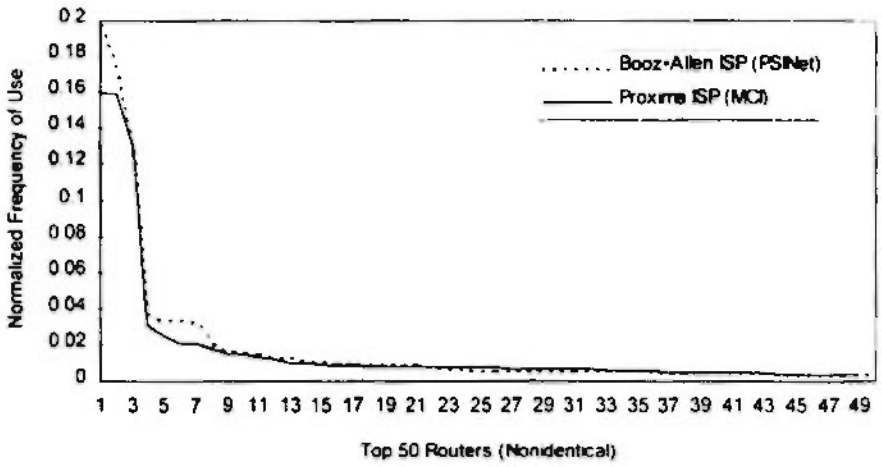
We hypothesize that an outage in a critical network node, such as a national IXP, would greatly reduce, but not eliminate, the ability of the Internet to route traffic quickly nationwide.

4.3.2.3 Critical Network Nodes

As explained in Section 3.2, the Internet relies primarily on the national IXPs to route and exchange traffic. Exhibit 3-4 shows the locations of the major IXPs across the United States. These high-speed LANs provide the majority of the routing among the backbone NSPs and the RSPs. Additionally, traffic is exchanged at private direct connects between ISPs' networks. Private direct connect exchange points of this kind are becoming more common due to congestion at the IXPs. ISPs are establishing private direct connects to avoid congestion problems and improve routing redundancy.

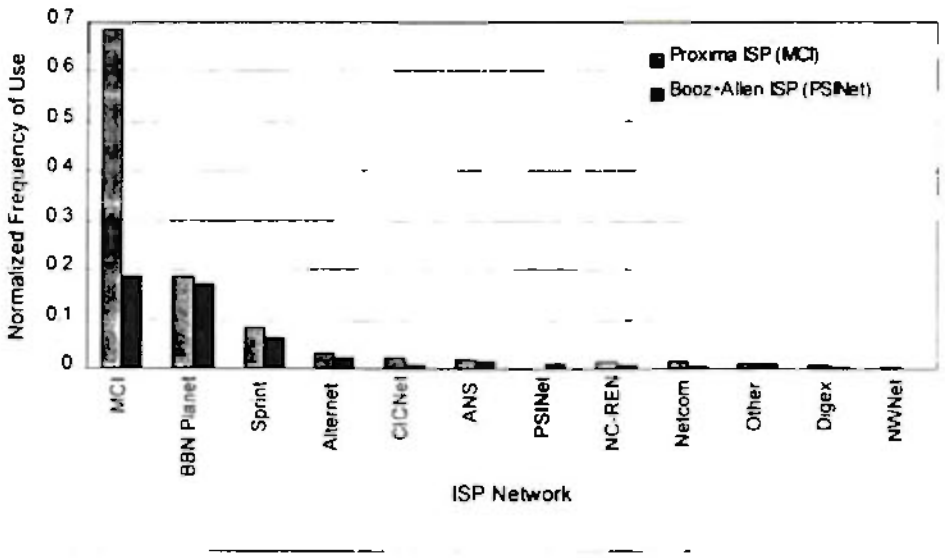
The IAT output provides the IP address of each of the routers traversed in the Internet traces. Using this data, we compiled lists of the most commonly visited routers for our two source networks. Exhibit 4-10 shows the distribution of the normalized frequency of use for the top 50 routers for both sources. The normalized frequency was obtained by dividing the number of hits on any router by the total number of hits recorded by the IAT for that source. This allows a direct comparison between the two sources. The first, second, and third router in each trace is considered to be specific to the source. These three routers show a very high frequency of use for our sources, and they are therefore critical to these sources, but do not fairly represent the remainder of the Internet. These three routers have been eliminated from the remainder of the analysis.

Exhibit 4-10
Top 50 Routers' Normalized Frequency of Use



The network domain names provided by the IAT output identify the router's owner. Using these domain names, we identified the relative importance of ISP networks to the two sources. The normalized frequency of use for each network is shown in Exhibit 4-11. "Other" networks were those networks that did not individually represent a large portion of the total frequency of use or that were not identified by a domain name.

Exhibit 4-11
Normalized Frequency of ISP Network Use



The critical network nodes had the highest frequency of use. Network nodes were considered critical if:

- They had a high frequency of use
- They were not too specific to the source routes, i.e., the top three routers
- They were not too specific to the destination routes.

All routers with normalized frequency greater than 0.004 were considered critical. Each of the sources shows a dependence on multiple critical network routers to trace a path to the destinations. Exhibits 4-12 and 4-13 show the critical ISP networks for the Booz•Allen and Proxima ISPs, respectively.

Exhibit 4-12
Booz • Allen's Critical ISP Networks

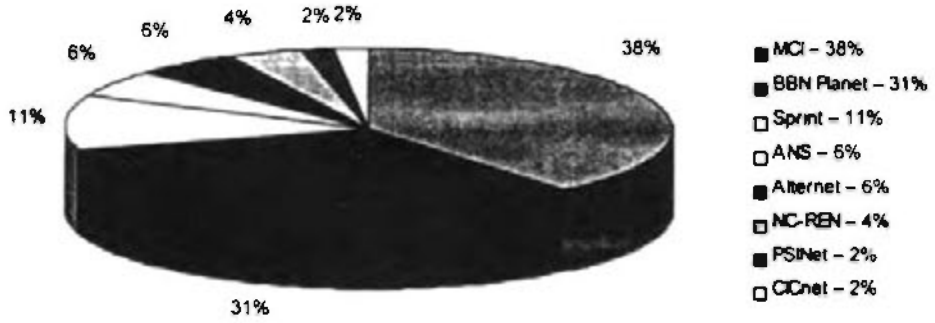
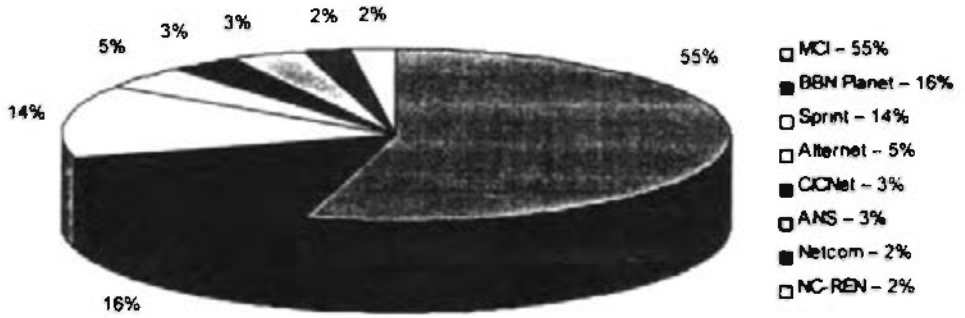
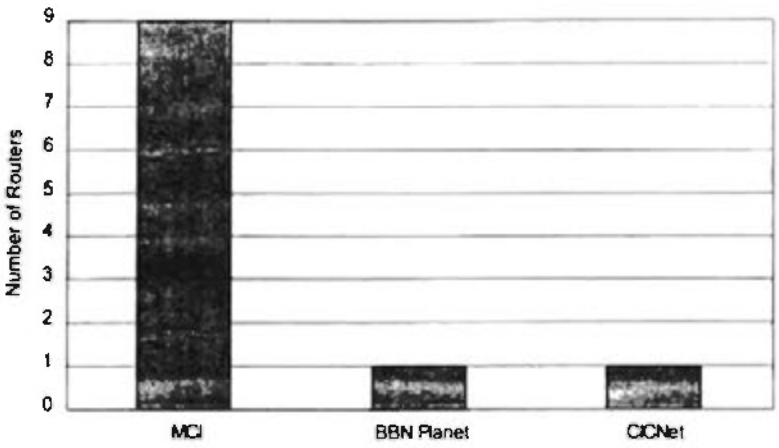


Exhibit 4-13
Proxima's Critical ISP Networks



Some of the critical nodes for one source were also critical to the other source. These nodes become our most critical nodes, which we can then identify as critical to the Internet based on our study. Exhibit 4-14 shows the distribution of these critical nodes to ISP networks.

Exhibit 4-14
Shared Critical Nodes



4.3.2.4 Conclusions

Traces performed throughout the test period indicated high success rates averaging between 87 and 89 percent. Of the unsuccessful trace attempts, most were due to an unreachable node (i.e., a router or the destination server) in the path that was probably either shutdown or incompatible with the IAT software.

Internet use is highest during mid-to-late afternoon business hours. Based on the round trip time for packets to traverse the network, congestion peaks between the hours of 12:00 noon and 4:00 p.m. eastern time. However, the dependence of businesses on the Internet could not be determined, i.e., the analysis did not determine whether the Internet was used to conduct critical business communications and research, or simply for personal use.

This analysis indicated that the number of hops did not depend on the time of day or the day of the week. Generally, routing tables are rarely modified to route around network congestion. Unlike switched traffic, the routes of Internet connections were somewhat "predictable." Therefore, the predictability of Internet routing, along with an increasing dependency on this communications media, renders it vulnerable to targeted and intended network disruptions.

Routers appear to share a somewhat balanced traffic load within the backbone networks (excluding those routers closest to the two sources). As expected, a high number of router "visits" occurred in the initial hops of the traces. These initial routers are critical to the sources, however, they are not necessarily critical to the entire Internet. As the trace moved away from the source and into the

backbone networks, the number of visits per router stabilized. Therefore, a single critical router could not be identified, however, it could be determined which networks were more heavily traversed. For this analysis, MCI's network was traversed most frequently and was therefore critical to the success of the traces.

5. VULNERABILITIES

This section addresses connectivity vulnerabilities that are inherent in the architecture of the Internet. These systemic vulnerabilities result from the utilization of the current PN infrastructure by the Internet composite networks. The vulnerabilities include second order effects such as availability and reliability due to outages on critical links and routing database errors. Security issues and vulnerabilities from outside influences, such as hackers, are not addressed. Internet vulnerabilities from hackers are addressed in the *Electronic Threat Intrusion Report*. The vulnerabilities associated with the ISPs, IXPs and Internet access connections are discussed below.

5.1 INTERNET SERVICE PROVIDERS

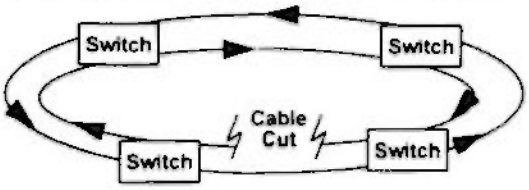
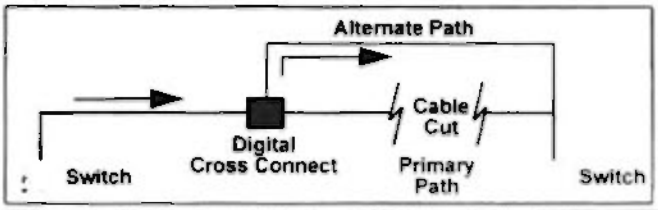
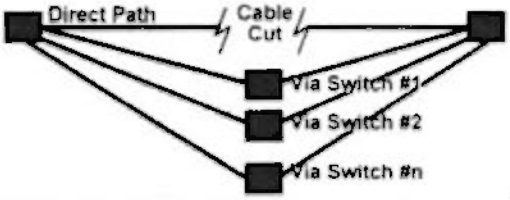
As introduced in previous sections, the ISPs provide the basic backbone architecture of the Internet. The ISPs can be divided into three categories: NSPs, RSPs, and resellers. Internet vulnerabilities that are unique to each category are detailed in the following sections.

5.1.1 National Service Providers

The majority of the NSP links travel over dedicated lines leased from the PN carriers. PN dedicated lines travel in the same conduit as other switched PN lines. Thus, the NSP links have a physical reliability comparable to that of the carrier's network. The IEC maintain their high reliability standards through a three tier restoration architecture. This architecture is based on protocols, physical diversity, and switching algorithms. Figure 5-1 details this tiered architecture.

The PN providers' current restoration techniques for cable cuts, the most frequent cause of outages, are not available for the dedicated lines used in the Internet. The switched-based mechanisms are not available because of the fundamental differences between switched voice and data communications. The protocol- and physical-based restoration mechanisms, however, could be employed for dedicated line failures. Each NSP needs to work closely with the PN providers to ensure that their dedicated lines are afforded these restoration techniques. For example, SONET rings are currently being deployed to increase the reliability of communications links. Traffic on a SONET ring automatically reverses its direction as a result of a cable cut. However, a PN provider may impose additional charges to add dedicated lines to a SONET ring if there are unused non-SONET protected lines available. Thus, the primary alternate routing schemes used to ensure connectivity is dependent on the NSP's routers, routing protocol, and restoration plans.

Exhibit 5-1
PN Three Tier Restoration Architecture

Mechanism	Basis	Description
SONET	Protocol Based	
Digital Cross Connects	Physical Based	
Dynamically Controlled Routing	Switching Based	

NSPs connect to multiple IXPs nationwide. Typically, an NSP's connection at each of these IXPs is non-redundant. If this connection is lost, the NSP will lose its connectivity to the IXP and the ability to exchange traffic with the other interconnected NSPs. However, if the NSP has connections to other IXPs, either regional or national, the NSP can still exchange traffic with the IXP-attached NSPs. The loss of the connection between an NSP and an IXP is critical only if the NSP does not have connections to multiple IXPs.

NSP networks are also susceptible to routing problems, such as slow convergence and routing loops. The three routing protocols discussed – BGP4, OSPF, and RIP – can affect routing within and between ISP networks. Because BGP4 is an external protocol, it can affect routing between ISPs. RIP and OSPF, which are internal protocols, will only affect an ISP's internal network.

RIP, the oldest of the three routing protocols discussed, has particular vulnerabilities that have been addressed by the newer protocols. RIP is a distance vector protocol based on hop count to the destination node. RIP routing tables contain only the single best route from origin to destination; when a better route is present, it replaces the old

route. When determining the best route available, RIP only considers the hop count and not other important factors such as bandwidth and line utilization.

Additionally, RIP is very slow to converge after a network failure or routing error has occurred. If a link in the route path is disrupted, RIP may not settle on the new best route for several minutes. During those minutes, service between those particular nodes is disrupted.

RIP is also susceptible to routing loops. In the minutes that it takes RIP to converge after a failure, routing loops may develop that will cause packets to route endlessly over the network until their TTL expires. Although there are modifications to the implementation of the RIP protocol that will help to avoid routing loops, they are subtle and may not be present in every network using RIP.

Finally, because RIP propagates its routing table to each of its neighbors every 30 seconds, RIP networks that are already congested by user traffic will be congested further by these routing tables.

The OSPF routing protocol overcomes RIP's shortfalls. The link state vector characteristic of OSPF allows each router in the network to have complete routing tables with multiple paths to destination. This greatly improves convergence time during a network failure and eliminates the chance of routing loops. OSPF routinely propagates route advertisements every half hour. OSPF also uses IP's multicasting capability to reduce the bandwidth requirement for these advertisements. This reduces the overall bandwidth overhead on the network attributed to the routing protocol. In time, OSPF will replace RIP as the standard internal routing protocol on the Internet.

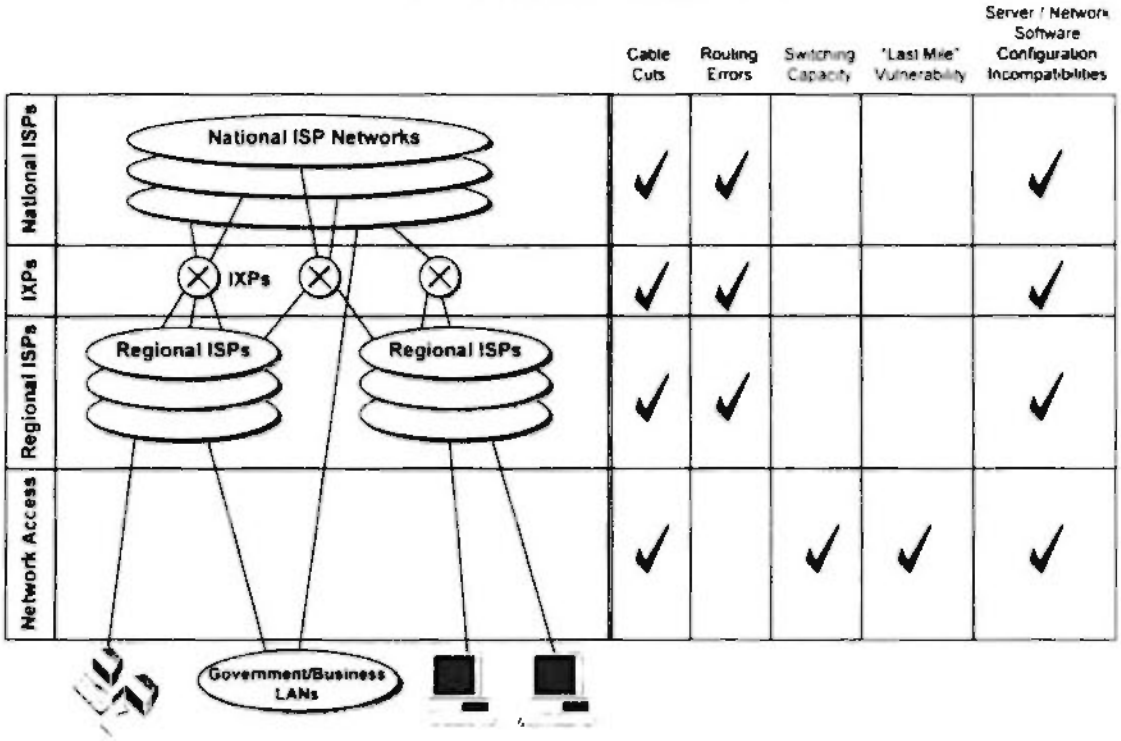
Exhibit 5-2 summarizes the vulnerabilities of the NSP networks, RSP networks, IXPs, and the access portion of the Internet architecture. These vulnerabilities are described in greater detail in the following sections.

5.1.2 Regional Service Providers

RSPs have similar vulnerabilities to those of the NSPs. These vulnerabilities may be compounded since RSP's smaller geographic scale limits the availability of physical diverse paths and their choice of a PN provider. This increases the possibility of isolation of the RSPs.

RSPs usually have fewer connections to IXPs. These connections may also be limited to the region that the RSP services. If one or more of an RSP's IXP connections is disrupted, the RSP's service will suffer greater degradation than an NSP. RSP service could be seriously affected by a regional natural or man-made disaster.

Exhibit 5-2
Internet Architecture Vulnerabilities



Because of an RSP's smaller geographic coverage, traffic will be carried over fewer links. If a major link fails because of a cable cut, it can have a large effect on the traffic within the RSP's network. For example, in NorthWestNet's backbone shown in Exhibit 3-2, the DS-3 circuit between Seattle, WA, and Portland, OR, is a critical high-bandwidth link. If that link fails, Portland's bandwidth to the national Internet connectivity provided at Seattle will fall from DS-3 (45 Mbps) to 2 T1s (3.088 Mbps) — a possible 93 percent drop in speed and bandwidth.

Since RSPs have smaller networks, much of their traffic is transmitted over other ISP's networks. Thus the effect of EGP routing, the IXP connection, and bilateral NSP network connection failures are more pronounced in an RSP's network. The RSP's traffic will also encounter the vulnerabilities of the NSP network carrying its traffic, including the reliability problems encountered due to routing errors.

5.1.3 Resellers

Resellers depend on their "host" ISP network to provide reliable and responsive service. Resellers typically have a single dedicated connection between their distribution facilities and its ISP. This connection typically travels over PN dedicated

lines. A failure in the dedicated line will result in a loss of service for the users homed to that distribution facility.

A reseller's network may become a congestion bottleneck when multiple customers access a single distribution facility with dedicated lines. If a reseller has not engineered the network connection for sufficient bandwidth to support dedicated and dial-up users, congestion may occur. This problem may occur in some reseller networks more than others.

Network availability is also a concern for dial-up customers of reseller networks. The ratio of customers to reseller modems may vary from 5 to more than 15. During high congestion periods, customers may be unable to gain access to the Internet. Higher ratio resellers have a greater potential for customer blocking.

5.2 INTEREXCHANGE POINTS

The interexchange point is the central location where ISPs meet to exchange network traffic. Recall from section 3, that all the necessary switching and routing equipment for all IXP-attached ISPs and for the IXP are physically located within a single facility. Subsequently, any disruption or disaster encountered at that facility could result in the loss of service at the IXP. For most NSPs the loss of one IXPs is not critical because NSPs generally have connections to multiple IXPs nationwide. However, for RSPs, the loss of an IXP is more critical, specifically if the RSP is connected to a single IXP.

In addition to the physical vulnerabilities, IXPs are susceptible to routing problems between the various interconnected ISPs. Routing problems could come from EGP protocol faults or invalid IXP routing tables. IXPs operators attempt to eliminate routing problems by requiring a single EGP protocol at the IXP.

5.3 INTERNET ACCESS

The Internet access connection is the most vulnerable aspect of the Internet with respect to business and residential end users. Business connections are typically single, non-redundant connections from the business' LAN to the ISP. Like all critical single lines, if the connection is lost, the company loses Internet connectivity. Large companies with advanced nationwide WANs (e.g., GE, IBM, and Boeing) may employ redundant connections to the Internet for reliability. A business' Web page will also be vulnerable to a cut in the Internet access link. However, businesses may have their Web pages hosted on an ISP Web server instead of hosting them on their own network. This practice reduces LAN traffic and provides those Web pages with the additional reliability provided by the ISP network.

Residential access to the Internet is provided almost exclusively through analog modem or ISDN dial-up access. Both connections are over single connections and are a single point of failure for the residential connection. However, overall reliability of the PN remains very high. Reliability will drop when users access the Internet using alternate schemes, such as cable, which are not built to telephone industry standards.

Flat-rate pricing for Internet service has also introduced new availability issues for LEC PN networks. These networks' demand and pricing models were designed based on a 5-minute voice call, whereas Internet data calls can last hours. During times of crisis when voice and Internet traffic surge, long dial-up data calls may reduce the availability of the voice network using the same end-office switching capacity. Continued growth in the use of alternative access techniques such as cable modems and DirectPC satellites should eventually reduce these switching issues in PN carrier networks.

Some Internet users connect over direct broadcast satellite services, such as DirecPC. DirecPC uses an inbound satellite connection over a 1-meter dish and an outbound connection over an analog modem. If either leg of this connection fails, the entire connection will be lost. The reliability of the analog modem link will be the same as described above. The reliability of the satellite link will depend on the satellite terminal at the residential location and the satellite company's downlink location.

ADSL will be comparable is reliability to other LEC access technologies (e.g., analog modem, and ISDN). However, ADSL has limitations to where it can be installed. ADSL cannot be installed near a strong AM radio station because of AM frequency interference on the ADSL signal. Additionally, only homes within 10,000 feet of the LEC central office may be serviced by ADSL.

In the short term, cable modem reliability is close to that of the cable television provider. Cable modem service poses special reliability concerns because the cable industry, unlike the voice telephone industry, has not been required or expected to have the degree of reliability of phone service because it is not considered essential to public welfare (e.g., 911 emergency access). Typically, the cable has not been installed to telephone industry standards and has been installed in shallow trenches (typically less than 6 inches deep). Additionally, cable providers do not employ the restoration mechanisms of the traditional carriers. These factors make the cable facility, and ultimately the cable modem connection, very vulnerable to cable cuts and outages.

APPENDIX A
INTERNET ANALYSIS TOOL SITES

Organization	Web Site
Central Intelligence Agency	www.odci.gov
Department of Commerce	www.doc.gov
Department of Defense	www.dtic.dla.mil
Department of Health and Human Services	www.dhhs.gov
Department of Energy	www.doe.gov
Department of the Interior	www.doi.gov
Department of Justice	www.usdoj.gov
Department of State	www.state.gov
Department of Transportation	www.dot.gov
Department of the Treasury	www.ustreas.gov
Department of Veteran Affairs	www.va.gov
Federal Communications Commission	www.fcc.gov
Federal Emergency Management Agency	www.fema.gov
General Services Administration	www.gsa.gov
Joint Staff	www.dtic.dla.mil
National Aeronautics and Space Administration	www.nasa.gov
National Communication System	www.disa.mil
Nuclear Regulatory Commission	www.nrc.gov
United States Department of Agriculture	www.usda.gov
United States Information Agency	www.usia.gov
United States Postal Service	www.usps.gov
FedWorld Information Network	www.fedworld.gov
Library of Congress	www.loc.gov
Alabama	www.asc.edu
Alaska	www.state.ak.us
Arizona	www.state.az.us
Arkansas	www.state.ar.us
California	www.state.ca.us
Colorado	www.state.co.us
Connecticut	www.state.ct.us
Delaware	www.state.de.us
Florida	ww.state.fl.us
Georgia	www.state.ga.us
Hawaii	www.hawaii.gov
Idaho	www.state.id.us
Illinois	www.state.il.us
Indiana	www.state.in.us
Iowa	www.state.ia.us

Kansas	www.state.ks.us
Kentucky	www.state.ky.us
Louisiana	www.state.la.us
Maine	www.state.me.us
Maryland	www.mdarchives.state.md.us
Massachusetts	www.state.ma.us
Michigan	www.state.mi.us
Minnesota	www.state.mn.us
Mississippi	www.state.ms.us
Missouri	www.state.mo.us
Montana	nris.mls.mt.gov
Nebraska	www.state.ne.us
Nevada	www.state.nv.us
New Hampshire	www.state.nh.us
New Jersey	www-ns.rutgers.edu
New Mexico	www.state.nm.us
New York	www.state.ny.us
North Carolina	www.state.nc.us
North Dakota	www.state.nd.us
Ohio	www.ohio.gov
Oklahoma	www.oklaosf.state.ok.us
Oregon	www.state.or.us
Pennsylvania	www.state.pa.us
Rhode Island	www.state.ri.us
South Carolina	www.state.sc.us
South Dakota	www.state.sd.us
Tennessee	www.state.tn.us
Texas	www.texas.gov
Utah	www state.ut.us
Vermont	www.state.vt.us
Virginia	www.state.va.us
Washington	www.wa.gov
West Virginia	www.state.wv.us
Wisconsin	www.state.wi.us
Wyoming	www.state.wy.us
Alta Vista	altavista.digital.com
America Online	www.aol.com
Apple Computer, Inc.	www.apple.com
Computer Network (cnet)	www.cnet.com
CNN	www.cnn.com
CompuServe	www.compuserve.com
Digex (ISP)	www.digex.com
Interport (ISP)	www.interport.com

Lycos, Inc.	www.lycos.com
Macro Computer Systems, Inc. (ISP)	www.mcs.com
Microsoft, Inc.	www.microsoft.com
MTV	www.mtv.com
NetCom (ISP)	www.netcom.com
Netscape	www.netscape.com
Olympics	www.atlanta.olympic.org
Oracle Corporation	www.oracle.com
Primenet (ISP)	www.primenet.com
Sun Microsystems, Inc.	www.sun.com
USA Today	www.usatoday.com
WebCrawler	www.webcrawler.com
Windows95 Home Page	www.windows95.com
Word Magazine (on-line)	www.word.com
World Wide Web Consortium	www.w3.com
Yahoo	www.yahoo.com
Massachusetts Institute of Technology	www.mit.edu
Ohio State University	www.osu.edu
Stanford University	www.standford.edu
University of California, Los Angeles	www.ucla.edu
University of Illinois, Urbana-Champaign	www.uiuc.edu
University of Michigan	www.umich.edu
University of North Carolina	www.unc.edu
University of Texas	www.utexas.edu

sl-dc-8-F0/0.sprintlink.net	186	(144.228.20.8)	Sprint
borderx1-fddi-1.WillowSprings.mci.net	180	(204.70.104.52)	MCI
core1.SanFrancisco.mci.net	176	(204.70.4.169)	MCI
ntis.bbnplanet.net	174	(192.221.253.22)	BBN Planet
Fddi0-0.CR2.DCA1.Alter.Net	173	(137.39.33.131)	Alternet
border2-fddi-0.Boston.mci.net	172	(204.70.3.34)	MCI
rtp1-gw.ncren.net	172	(128.109.70.248)	NC-REN
border1-fddi-0.Greensboro.mci.net	171	(204.70.80.18)	MCI
nc-research-net.Greensboro.mci.net	171	(204.70.81.6)	MCI
atlanta2-cr99.bbnplanet.net	170	(192.221.25.1)	BBN Planet
t3-2.was-dc-gw1.netcom.net	170	(163.179.220.181)	Netcom
rtp5-gw.ncren.net	170	(128.109.32.2)	NC-REN
mae-east.digex.net	170	(192.41.177.115)	Digex
fddi.mae-east.netcom.net	170	(192.41.177.210)	Netcom
f0.cnss61.Washington-DC.t3.ans.net	170	(140.222.56.197)	ANS
core1-aip-4.Greensboro.mci.net	170	(204.70.1.21)	MCI
border2-fddi-0.Denver.mci.net	170	(204.70.3.114)	MCI
atlanta2-cr99.bbnplanet.net	170	(192.221.25.230)	BBN Planet
atlanta3-cr1.bbnplanet.net	164	(192.221.42.1)	BBN Planet
border1-fddi-0.KansasCity.mci.net	163	(204.70.2.66)	MCI
midnet.KansasCity.mci.net	163	(204.70.40.6)	MCI
StLouis-StLouis2-f30.gi.net	162	(192.35.171.35)	Other
ut8-h1-0.the.net	162	(129.117.16.241)	Other
borderx1-fddi-0.WillowSprings.mci.net	161	(204.70.104.20)	MCI
cambridge2-cr3.bbnplanet.net	160	(192.233.33.10)	BBN Planet
cambridge1-cr1.bbnplanet.net	154	(192.233.149.201)	BBN Planet
cambridge2-cr2.bbnplanet.net	154	(192.233.33.2)	BBN Planet
cambridge2-cr2.bbnplanet.net	154	(199.92.129.2)	BBN Planet
sl-chi-15-H2/0-T3.sprintlink.net	153	(144.228.10.69)	Sprint
sl-kc-2-F0/0.sprintlink.net	152	(144.224.20.2)	Sprint
jackson-cr1.bbnplanet.net	148	(192.221.5.17)	BBN Planet
border1-fddi-0.Chicago.mci.net	147	(204.70.2.82)	MCI
merit-michnet-ds3.Chicago.mci.net	146	(204.70.24.6)	MCI
Hssi2-0.Vienna6.VA.Alter.Net	136	(137.39.100.78)	Alternet
sprint-nap.WestOrange.mci.net	135	(204.70.1.210)	MCI
Fddi0-0.SR1.TCO1.ALTER.NET	132	(137.39.11.22)	Alternet
borderx2-fddi-1.Seattle.mci.net	127	(204.70.203.68)	MCI
seabr1-gw.nwnet.net	127	(192.147.179.5)	NWNet
nwnet.Seattle.mci.net	127	(204.70.203.118)	MCI
core2.Seattle.mci.net	126	(204.70.4.33)	MCI
144.228.135.34	123	(144.228.135.34)	Sprint
core-hssi-3.Boston.mci.net	122	(204.70.1.2)	MCI
sl-atl-1-F0/0.sprintlink.net	119	(144.228.80.1)	Sprint
sl-fw-6-H3/0-T3.sprintlink.net	119	(144.228.10.86)	Sprint
dgc-fddi5-0.chicago.cic.net	118	(131.103.1.18)	CICNet
sl-fw-15-F0/0.sprintlink.net	116	(144.228.30.15)	Sprint
dgb-fddi5-0.chicago.cic.net	106	(131.103.1.17)	CICNet
f1-0.t56-0.Washington-DC.t3.ans.net	97	(140.222.56.66)	ANS

LIST OF ACRONYMS

ADSL	Asymmetric Digital Subscriber Line
ANS	Advanced Networks and Services
ANS CO+RE	ANS Commercial + Research and Education
ARPA	Advanced Research Projects Agency
AS	Autonomous System
ATM	Asynchronous Transfer Mode
BGP4	Border Gateway Protocol Version 4
CAP	Competitive Access Provider
CIX	Commercial Internet Exchange
CLEC	Competitive Local Exchange Carrier
DARPA	Defense Advanced Research Projects Agency
DoD	Department Of Defense
EGP	Exterior Gateway Protocol
EST	Eastern Standard Time
FDDI	Fiber Distributed Data Interface
FIX	Federal Internet Exchange
FTP	File Transfer Protocol
IAT	Internet Analysis Tool
ICMP	Internet Control Message Protocol
IEC	Interexchange Carrier
IETF	Internet Engineering Task Force
IGP	Interior Gateway Protocol
ILEC	Incumbent Local Exchange Carrier
IPv6	Internet Protocol Version Six
ISDN	Integrated Services Digital Network
ISI	Information Sciences Institute
ISP	Internet Service Provider
IXP	Interexchange Point
LAN	Local Area Network
LEC	Local Exchange Carrier
MAE	Metropolitan Area Ethernet
MAN	Metropolitan Area Network
MFS	Metropolitan Fiber Systems
MXP	Metropolitan Exchange Point
NAP	Network Access Point
NCP	Network Control Protocol
NCS	National Communication System
NREN	National Research and Education Network
NS/EP	National Security Emergency Preparedness
NSF	National Science Foundation
NSFNET	National Science Foundation Network

NSP	National Service Provider
OMNCS	Office of the Manager, NCS
OSPF	Open Shortest Path First
PC	Personal Computer
PN	Public Network
POP	Point of Presence
PPP	Point-to-Point Protocol
PVC	Permanent Virtual Circuit
RBOC	Regional Bell Operating Company
RIP	Routing Information Protocol
RSP	Regional Service Provider
SLIP	Serial Line Interface Protocol
SMDS	Switched Multimegabit Data Service
SONET	Synchronous Optical Network
SVC	Switched Virtual Circuit
SWAB	SMDS Washington Area Bypass
TCP/IP	Transmission Control Protocol/Internet Protocol
TTL	Time To Live
UDP	User Datagram Protocol
vBNS	Very High Speed Backbone Network Service
WAN	Wide Area Network
WWW	World Wide Web
XNS	Xerox Network Systems

SECTION 2 REFERENCES

1. Cerf, Vinton G., "Computer Networking: Global Infrastructure for the 21st Century," World Wide Web, www.cs.washington.edu/cra/networks.html, 1995.

2. CERFnet, "Network Service Provider Interconnections and Exchange Points," World Wide Web, www.cerf.net/cerfnet/interconnects.html

3. Cooper, Lane F., "The Commercialization of the Internet," *Communications Week*, April 1, 1996, pp. 135-139.

4. Fazio, Dennis, "Hang Onto Your Packets: The Information Super Highway Heads to Valleyfair or Building a High Performance Computer System Without Reading the Instructions," World Wide Web, www.mr.net/announcements/valleyfair.html, March 14, 1995.

5. Frazer, Karen D., "The NSFNET Phenomenon," World Wide Web, www.merit.edu/nsfnet/final.report/phenom.html.

6. Hardy, Henry Edward, "A Short History of the Net," World Wide Web, www.ocean.ic.net/ftp/doc/snethisthew.html, 1995.

7. MCI Telecommunications Corporation, "The vBNS Network," World Wide Web, www.government.com/vBNS/network_map.html, 1995.

8. Merit Network, Inc., "NSFNET: Transition to T3," World Wide Web, www.merit.edu/nsfnet/final.report/transition.html.

9. Merit Network, Inc., "Router Server Technical Overview," World Wide Web, www.ra.net.routing.arbiter/RA/.rs.overview.html.

10. National Laboratory for Applied Network Research, "Background Information," World Wide Web, www.nlanr.net/VBNS/background.html.

11. National Laboratory for Applied Network Research, "Collaboration on the Very High Speed Backbone Network Services (vBNS)," World Wide Web, www.nlanr.net/VBNS.

12. National Laboratory for Applied Network Research, "NSFNET -- The National Science Foundation Network," World Wide Web, www.nlanr.net/INFRA/NSFNET.html, November 23, 1995.

13. National Science Foundation, "NSF 93-52 - Network Access Point Manager, Routing Arbiter, Regional Network Providers, and Very High Speed Backbone Network Services Provider for NSFNET and the NREN(SM) Program - Program Solicitation," May 6, 1993.

14. Quarterman, John, "What is the Internet Anyway?," World Wide Web, gopher.tic.com/00/matrix/news/v4/what .408, 1994.

15. Rietz, Randy, Lewis, Will, "History of the Internet," World Wide Web, falcon.cc.ukans.edu/~wlewis'project/history.html, July 31, 1995.

16. Sprint, "Network Access Point Handbook," October 25, 1994.

17. Sprint, "SprintLink Customer Handbook 2.1," Sprint Document #5953-2, October 11, 1995.

18. Zakon, Robert Hobbes, "Hobbes' Internet Timeline v2.4a," World Wide Web, info.isoc.org/guest/zakon/Internet/History/HIT.html, 1996

SECTION 3 REFERENCES

1. Ameritech, "The Chicago NAP," World Wide Web, www.ameritech.com/products/data/map/The_Chicago_NAP.html, 1995.

2. Associated Press, "Computer Network Weathers Big Jolt: Internet Users Swap News, Worries After Quake Hits," Associated Press, January 18, 1994.

3. Bickel, Robert, "Building Intranets," *Internet World*, March 1996, p. 73.

4. CERFnet, "CERFnet T3 Backbone and Interconnectivity," World Wide Web, www.cerf.net/cerfnet/about/T3-map.html, June 7, 1996.

5. Cisco Systems, "BGP4 Case Studies Tutorial Section 1," World Wide Web, ciso.cisco.com/warp/public/459/13.html.

6. Cisco Systems, "Protocol Brief," 1994.

7. Cortese, Amy, "Here Comes the Intranet," Business Week, February 26, 1996, p. 76.

8. Coy, Peter, Judge, Paul, "Limo Service for Cruising the Net: MCI and BT Will Help Business Surfers Go First Class—for a Price," *Business Week*, June 24, 1996, p. 46.

9. Detroit MXP, "What is an MXP?," World Wide Web, www.mai.net/mxp/detroit/bckgrnd.htm.

10. Eng, Paul M, "War of the Web: Commercial Online Service Providers, Upstart Companies and Telecommunications Companies All Fighting for Internet Market," *Business Week*, March 4, 1996, p. 71.

11. Finneran, Michael, "Cable Modem Madness," *Business Communications Review*, March 1996, p. 68.

12. Holmes, Allan, "Flood Data Rides Internet Wave," *Federal Computer Week*, February 5, 1996, p. 1.

13. IITF, Reliability and Vulnerability of the National Information Infrastructure (NII), Information Infrastructure Task Force (IITF), August 17, 1995.

14. Loeb, Larry, "The Stage is SET: The SET Agreement Between MasterCard and Visa Could Pave the Way for Widespread E-commerce," *Internet World*, August 1996, p. 54.

15. MacKie-Mason, Jeffrey, Varian, Hal R., "Pricing the Internet," World Wide Web, gopher.econ.lsa.mich.edu, April 1993.

16. MacKie-Mason, Jeffrey, Varian, Hal R., "Economic FAQs About the Internet," World Wide Web, gopher.econ.lsa.umich.edu, August 21, 1994.

17. MacKie-Mason, Jeffrey, Varian, Hal R., "Some FAQs About Usage-Based Pricing," World Wide Web, gopher.econ.lsa.umich.edu, November 4, 1994.

18. Mendes, Gerald H, "Next-Generation IP Takes Shape," *Business Communications Review*, March 1996, p. 49.

19. Mills, Mike, "MCI Offers Customers Free Internet Access," *The Washington Post*, March 19, 1996, p. C1.

20. Netscape, "Netscape Announces New Real-time Audio and Video Framework for Internet Applications," Netscape Press Release, January 31, 1996,

21. Pacific Bell, "Multi-Lateral Peering Agreements Pacific Bell Network Access Point," World Wide Web, www.pacbell.com/Products/NAP/mlpa.html, August 14, 1995.

22. Pacific Bell, "Pacific Bell Network Access Point," World Wide Web, www.pacbell.com/products/business/fastrak/networking/nap/features.html.

23. *PC Week*, "UUNet puts ADSL on trial," *PC Week*, June 17, 1996, p. 3.

24. PSINet, "PSINet Technology and Infrastructure," World Wide Web, www.psi.new/psi-tech/psi-tech.shtml, 1995.

25. PSINet, "SWAB - SMDS Washington Area Bypass," World Wide Web, www.psi.net:80/misc/swab.html.

26. PSINet, "Typical POP Design," World Wide Web, www.psi.net/psi-tech/pop.hmtl

27. Reilly, Patrick, "More Publishers Charging for Web Services," *Wall Street Journal*, May 8, 1996, p. B8.

28. Rigdon, Joan E, "Blurring the Line: New Technology Aims to Make the Web Look and Act More Like Television," *Wall Street Journal*, March 28, 1996, p. R5.

29. Sandberg, Jared, "Making the Sale: The Allure of On-Line Commerce, Its Proponents Argue, Will Eventually Prove Overwhelming," *Wall Street Journal*, June 17, 1996, p. R6.

30. Scott, D.F., "The Underground Internet: Through the MBONE, the Internet May Become the World's Largest Broadcast Service," *Computer Shopper*, March 1996, p. 548.

31. Sprint, "Network Access Point Handbook," October 25, 1994.

32. Stevens, Richard, "TCP/IP Illustrated Volume 1, The Protocols," Addison-Wesley Publishing, 1994, Chapter 10, pp. 97-110.

33. Swisher, Kara, "By the Sweat of Their Browser: District Entrepreneurs Turn a Web Search Idea Into a $38 Million Deal," *The Washington Post*, June 4, 1996, p. C1.

34. Vaughan-Nichols, Steven J, "Radio Comes to Cyberspace," *Byte*, October 1995, p. 46.

35. Verity, John W., "Invoice, What's An Invoice: Electronic Commerce Will Soon Radically Alter the Way Business Buys and Sells," *Business Week*, June 10, 1996, p. 110.

36. Wingfield, Nick, "RSA to Connect Virtual Private Networks," *InfoWorld*, January 15, 1996, p. 47.

37. UUNET, "The UUNET Network Backbone," World Wide Web, www.uu.net.bbone.html.

38. Ziegler, Bart, "Up and Running: Why Did the Web Replace Interactive TV as the New Mantra? A Simple Reason: It's Here," *Wall Street Journal*, March 28, 1996, p. R6.

SECTION 4 REFERENCES

1. Asif, "U.S. Federal and State Government WWW Sites," World Wide Web, www.ilinks.net/~ace/html/government/html#sh6.

2. Bruno, Charles, "Internet Health Report: Condition Serious," Network World, September 16, 1996, pp. 1, 104-111.

3. InterNIC, "InterNIC Whois Service," World Wide Web, www.internic.net/wp/whois.html.

4. MFS Datanet, "MAE East Statistics," World Wide Web, ext2.mfsdatanet.com/MAE/east.stats.html.

5. MFS Datanet, "MAE West Statistics," World Wide Web, ext2.mfsdatanet.com/MAE/west.stats.html.

6. University of Illinois at Urbana-Champaign, "Host Name to Latitude/Longitude," World Wide Web, cello.cs.uiuc.edu/cgi-bin/slamm/ip2ll, June 19, 1995.

7. Stevens, Richard, "TCP/IP Illustrated Volume 1, The Protocols," Addison-Wesley Publishing, 1994, Chapter 10, pp. 97-110.

AN ASSESSMENT OF THE RISK

TO THE SECURITY OF

PUBLIC NETWORKS

NOT TO BE FURTHER DISTRIBUTED WITHOUT PERMISSION OF THE

DEPUTY MANAGER, NCS

Prepared by the U.S. Government and
National Security Telecommunications Advisory Committee (NSTAC)
Network Security Information Exchanges (NSIE)

DECEMBER 12, 1995

TABLE OF CONTENTS

TABLE OF CONTENTS
(Continued)

PREFACE

This report assesses the risk to public networks from electronic intruders and software-based attacks This assessment is based primarily on the knowledge and day-to-day observations of the United States Government and National Security Telecommunications Advisory Committee (NSTAC) Network Security Information Exchange (NSIE) representatives in the performance of their jobs It reflects a consensus among the representatives on the threats, deterrents, vulnerabilities, and protection mechanisms that affect the public networks

By its nature, network security is continually evolving Therefore, this document presents a snapshot of the current state of security in the Nation's public networks and should be viewed as a work in progress

EXECUTIVE SUMMARY

Since early 1990, the United States Government and the President's National Security Telecommunications Advisory Committee (NSTAC) have been working together to address network security issues. Central to this process are separate, but closely coordinated, Government and NSTAC Network Security Information Exchanges (NSIEs). The NSIEs provide a forum to identify issues involving penetration or manipulation of software and databases affecting national security and emergency preparedness (NS/EP) telecommunications. The attached report documents a risk assessment the NSIEs prepared in 1995.

This risk assessment focuses on the current and near-term Public Network (PN)[1], taking into account the security of new technologies for which implementation has begun or is planned. It recognizes that far-reaching changes are occurring in communications structure, technology, and regulation, and addresses the concomitant NS/EP implications. The assessment was based primarily on the knowledge and day-to-day observations of both the Government and the NSTAC NSIE representatives in the performance of their jobs.

The complexity of the PN is increasing and securing it is very difficult. Industry has been factoring network security risk factors and overall network reliability into their decision processes and have been reasonably effective to date in mitigating serious intrusions. The last NSIE risk assessment in 1993 concluded that the risk to the Public Switched Network (PSN) from electronic intrusions was a serious concern. The NSIE representatives believe that in 1995 the overall risk to the PN from electronic intrusions is greater than that reported in the 1993 risk assessment, on the basis that threats are outpacing our deterrents while vulnerabilities are outpacing the implementation of protection measures. The NSIE representatives based their observations on the following:

- ***Computer intruders are using increasingly advanced software tools and techniques to attack the PN.*** They are motivated by financial gain and there are troubling indications of links to organized crime and foreign intelligence services.

- ***The PN is the means for providing access to other desirable targets.*** In some cases, disruption of the PN may be the end goal for some of our adversaries.

- ***Interconnection between different technologies is proliferating rapidly (e.g., the Internet to the PN).*** The potential impact of a single intrusion incident is becoming greater as new nationwide National Information Infrastructure (NII) services are rolled out and as network elements serve wider geographical areas.

[1] The PN includes any switching system or voice, data, or video transmission system used to provide communications services to the public (e.g., public switched networks, public data networks, private line services, wireless systems, and signaling networks).

- *Although the effectiveness of our deterrents will never be as great as we may wish, NSIE representatives believe deterrent activities are focused on the correct objectives and progress is being made.*

- ***Known security vulnerabilities persist, despite aggressive efforts to eliminate them, and new technologies bring with them new vulnerabilities.*** Greater focus on security and vigorous efforts to provide it would lessen the security impacts

- ***Changes in the business environment often affect network security, reliability, and quality.*** Increasing competitive pressures on all aspects of the industry require high levels of attention to network security investments

- ***The interconnection of new PN service providers into the voice and data communications market brings additional security concerns.***

- ***The PN is rapidly evolving to incorporate many different emerging technologies and services, and additional security standards are needed.*** A single, consistent set of security standards for open systems and networks should be a near-term goal

The protection of the PN is important to maintaining our national security posture, supporting emergency preparedness activities, realizing the capabilities and services offered by the emerging NII, ensuring our economic security and effectively competing in a global marketplace. Network and systems security is everyone's job:

- ***Service providers*** must ensure the reliability and assurance of network services and capabilities

- ***Manufacturers*** must ensure that the security capabilities of their goods and services adequately reflect the needs of the marketplace

- ***Users*** must subscribe to and pay for appropriate levels of privacy and security, and

- ***The Federal Government*** must support the needs of industry by supporting research and development, and developing laws to enable prosecution of offenders

Representatives from each of these four sectors have contributed to NSIE deliberations in the past years. The NSIE process has proven to be effective for exchanging information on threats, vulnerabilities, and mitigation strategies related to NS/EP telecommunications and should continue

1. INTRODUCTION

1.1 Background

In recent years, telecommunications services provided by the public network (PN)[2] have expanded at an astonishing rate, in both degree of sophistication and availability. Advances in new computer software and hardware technologies are allowing the United States telecommunications industry to provide innovative and robust new services and to automate the PN's operations, administration, maintenance, and provisioning (OAM&P) functions to reduce costs. The public and private sectors increasingly depend on these new telecommunications systems capabilities and services, and this dependency can be expected to grow as new technology initiatives are developed as part of the National Information Infrastructure (NII). Both sectors are concerned, however, about the threats posed to the system by computer intruders.

The PN, and the services on which the public and private sectors depend, rely heavily on the security of the PN's software; consequently, the security of this software is of vital interest to the Government. A software attack on the PN's computer systems could have a significant impact on end users, including national security and emergency preparedness (NS/EP)[3] telecommunications services users.

In April 1990, the Chairman of the National Security Council (NSC) Policy Coordinating Committee for National Security Telecommunications and Information Systems (PCC-NSTIS) requested that the Manager, National Communications System (NCS), identify what actions Government and industry should take to protect critical national security telecommunications from the threat from computer intruders. Working together, the Manager and the President's National Security Telecommunications Advisory Committee (NSTAC) established a structure and a process for addressing network security issues. Central to this process are separate, but closely coordinated, Government and NSTAC Network Security Information Exchange (NSIE) groups. Government member organizations include departments and agencies that are major telecommunications services users, represent law enforcement, or have information about the network security threat. Industry member organizations include telecommunications service providers, equipment vendors, and major users. NSIE representatives are individuals who are engaged in the prevention, detection, and/or investigation of telecommunications network software penetrations. Both Government and NSTAC NSIE representatives are subject matter experts in their fields.

---

[2] Although earlier Network Security Information Exchange (NSIE) documents have used the term "Public Switched Network (PSN)," the NSIEs' efforts have not been limited to switched voice networks, which this term connotes in scope. They have focused on a broader range of communications services including data and signaling networks. The NSIEs determined that the term "Public Network (PN)" better portrays this broader focus. The PN includes any switching system or voice, data, or video transmission system that is used to provide communications services to the public (e.g., public switched networks, public data networks, private line services, wireless systems, and signaling networks).

[3] "NS/EP telecommunications services" are the telecommunications services used to maintain a state of readiness or to respond to and manage any event or crisis (local, national, or international) that does or could cause injury or harm to the population, cause damage to or loss of property, or degrade or threaten the NS/EP posture of the United States. National Communications System Manual 3-1-1, *Telecommunications Service Priority (TSP) System for National Security Emergency Preparedness (NS/EP) Service User Manual*, National Communications System, Washington, DC, July 9, 1990.

The NSIEs provide a forum to identify issues involving penetration or manipulation of software and databases affecting NS/EP telecommunications. The NSIEs' focus is to (1) exchange information and views on threats, incidents, and vulnerabilities affecting the PN's software and (2) identify actions to mitigate their impact, thereby raising the effectiveness of all participants Periodically, the NSIEs also assess the risks to the PN from computer intruders The last risk assessment was completed in 1993

1.2 Value of the Public Network

The PN is an essential element of our country's communications and economic infrastructure, on which all sectors of our society depend. The PN's value can be viewed from the three perspectives Government, business, and the individual

GOVERNMENT

The PN provides more than 90 percent of the Federal Government's communications capabilities, ranging from day-to-day business activities to handling crisis situations such as natural disasters (e g , hurricanes, earthquakes, and floods) and national security crises at home (e.g., the bombing in Oklahoma City) and abroad (e.g., Desert Shield/Desert Storm) State and local governments also depend on the PN to conduct business, provide basic and essential community services (e.g , library telephone reference assistance and emergency-911 [E-911] service), and respond to emergencies which impact the community, such as natural or manmade disasters (e.g., floods or major fires)

BUSINESS

Businesses depend on communications capabilities to provide products and services to their customers and manage their internal operations Communications capabilities enable businesses to reduce operating costs through practices such as maintaining "just-in-time" inventory, and to generate revenue The Administration's NII initiative is intended to strengthen the economy by taking advantage of advances in information services and communications technologies to create business opportunities and new jobs; central to this undertaking is a reliable and robust PN

INDIVIDUALS

Individuals depend on communications capabilities in many different ways, ranging from E-911 service in life-threatening situations to their role in supporting infrastructure activities, (e.g., transportation, utilities, and finance) to keeping in touch with family members The public's confidence in the PN's availability and reliability is high, and must remain so if citizens are expected to increase the use of NII services

1.3 Scope

The PN is a network of networks composed of complex, interconnected communications systems that rely on computer-based, software-controlled network elements This architecture allows great flexibility for both service providers and end users to establish or modify network features and

services Remote access allows these activities to occur from centralized centers or from customer premises Internal telecommunications company data networks are used extensively to control remote services to network elements These internal networks, often called corporate networks, support billing, service provisioning, engineering, maintenance, switching, network management, and administrative systems, databases, signaling control, signaling transfer, and service control points, and transport elements These networks provide remote access to network elements and enable legitimate users to perform their work functions expeditiously and cost effectively More network control elements are interconnected and integrated with corporate networks that use industry standard protocols such as X.25, Common Channel Signalling (CCS) and Transmission Control Protocol/Internet Protocol (TCP/IP) If these networks are then interconnected to the Internet, the potential for intrusions increases.

The activities of the Government and NSTAC NSIEs focus on issues of unauthorized penetration or manipulation of PN software and databases affecting NS/EP telecommunications. Their primary concerns are the identification and mitigation of vulnerabilities that could be exploited by computer intruders and result in denial of service or extraction of sensitive NS/EP information. Although there are other threats to the PN, such as breaches in physical security, this risk assessment addresses them only as much as they relate to electronic intrusions For example, computer intruders sometimes exploit vulnerabilities in physical security to obtain knowledge, tools, or access to systems that enable them to attack the PN's software

Previous risk assessments focused narrowly on network elements and their supporting systems, such as their OAM&P systems, and addressed how computer intruders' exploitation of software vulnerabilities affected the risk to NS/EP telecommunications services. The NSIEs recognized, however, that the nature of the PN was changing rapidly, not only in the technology, but also in the convergence of telecommunications and information services Because these changes will affect the security of the PN, the NSIEs have included in the risk assessment factors such as Internet connectivity, open protocols, industry restructuring, and the changing business environment The NSIEs continue to assess how these factors affect the risk to the PN

This risk assessment focuses on the current and near-term state of security of the PN It represents three changes from previous risk assessments: (1) it includes the security of new technologies (e.g., Synchronous Optical Network [SONET], Asynchronous Transfer Mode [ATM]) for which implementation has begun or is planned; (2) it recognizes that significant changes are occurring in the service provider community, and (3) to a limited degree, it also deals with certain aspects of the Internet, addressing risks shared by both the Internet and the PN, such as vulnerabilities in TCP/IP, and risks to elements of the PN that result from its connection to the Internet. This risk assessment does not address access risks of the Internet itself

1.4 Methodology

This assessment is based primarily on the knowledge and day-to-day observations of the Government and NSTAC NSIE representatives in the performance of their jobs It reflects a consensus among the representatives on the threats, deterrents, vulnerabilities, and protection mechanisms that affect the PN Analysis of the NSIE Vulnerability Database was used to validate the observations of the

NSIEs However, there are no nationwide statistics or measurements to quantify the problem As a result, this document contains few statements of quantification

The risk assessment in this document comprises four elements **threats**, which are mitigated by **deterrents**, and **vulnerabilities**, which are mitigated by **protection measures**. This document describes each of these elements and concludes with an assessment of the consequent risk to the PN

An important factor affecting the risk to the PN is the **changing business environment** Because threats, deterrents, vulnerabilities, and protection measures can best be understood within the context of this environment, it is discussed in Section 2.

2. CHANGING BUSINESS ENVIRONMENT

Both the public and private sectors are changing the way they do business, to reduce expenses, increase revenue, and compete in the global marketplace At the same time, rapid advances in technology allow businesses to "do more with less " These factors may make good security more difficult to achieve For example, business decisions to outsource work or engage in joint ventures without a carefully thought out security plan can affect a company's security by making the company vulnerable to its vendors and partners. This makes it essential to define and implement security policies and procedures that will explicitly define access privileges granted to contractors or business partners

Three major factors influencing the business environment are (1) the need to reduce expenses, (2) the pressure to increase revenue, and (3) where and how people work. Each factor presents challenges to the security of any corporation and its ability to compete in a global marketplace.

2.1 Reducing Expenses

The following efforts to control expenses and improve profitability bring with them new challenges to maintaining secure networks.

- **Corporate Re-engineering**: Corporate process re-engineering reduces the number of employees and increases empowerment for those who remain. Terminated employees often have the knowledge and skills to exploit the vulnerabilities of their former employers' networks and some could be thus motivated. Remaining employees feel less secure in their jobs, may be required to carry a greater workload, and may generally feel less loyal to their employer. They could exploit their increased access to commit fraud as a source of financial security or they may simply be less diligent in their duties All of these factors affect security Security administration is often considered a support function and downsizing generally hits support functions the hardest. Without high-level attention, downsizing could exacerbate the situation more people are capable of doing harm to the network, and fewer people are dedicated to protecting it.

- **Outsourcing**: Both the public and private sectors use outsourcing to reduce expenses and increase flexibility in meeting staffing requirements. Institutions which outsource can be at risk from the inadequate security measures of their vendors unless strong security controls are adopted Without these controls, proprietary information could be at risk. Outsourcing also could be a path for introducing malicious code

- **Software patches**: Because of the resources used in patching software to fix vulnerabilities, and the reduced time between major software releases (less than 18 months), software vendors may be reluctant to issue interim patches to fix software vulnerabilities. This reluctance may give computer intruders a greater "window of opportunity" to exploit vulnerabilities Often patches are not entirely effective, they may work in the laboratory, but function much differently in the real world, where feature interactions affect their operation

2.2 Increasing Revenue

Efforts to increase revenue and profitability bring with them new challenges to maintaining secure networks

- **Joint ventures** Joint ventures affect security much the same way outsourcing does Since joint ventures generally include companies with expertise in different technologies or business areas, each company may be unaware of security requirements peculiar to the other's specialty and may not adapt appropriate practices Again, security should be included in joint venture planning

- **Foreign ownership**: U.S. companies are pursuing business opportunities in foreign markets, to obtain foreign approvals, the U.S. frequently allows foreign companies to do business in the U.S. The security implications of this trend are similar to those of outsourcing and joint ventures. Also, there are security implications from the availability and transfer of U S technology to foreign entities

- **Competition** As competition increases, the pressure to get new products into the market place also increases Security matters need to be preplanned early in the product development cycle. Because efforts to implement adequate security may delay product delivery, the need to meet a market window may override the need to include a complete suite of security features This situation extends into product implementation as well; customers may choose not to implement security features if it will delay implementation and operation of the product and/or increase its cost.

- **Nondiscriminatory access** Open competition is one of the main tenets of the Government's initiative for the NII. The Government believes that open competition will drive the development of new tools, products, and services required to ensure that the U.S continues to be a major force in the Information Age. To that end, legislation has been drafted to give third-party service providers nondiscriminatory access to elements of the telecommunications infrastructure to create and deliver services This nondiscriminatory access to the physical infrastructure as well as access to databases and associated signaling elements necessary for call routing and completion multiplies the number of service providers connected to the network and the number of potentially exploitable access points Perhaps more importantly, many third-party providers will be start-up companies, operating with minimal resources and security experience

2.3 Changes in How and Where People Work

Technology has made possible changes in how and where people perform their work

- **Telecommuting**. Working at home or at a shared work station is attractive to many employees and diminishes the requirement for office space and the concomitant expense. The additional connectivity required for telecommuting can create additional opportunities for intruders to gain access to resources, or for employees to inadvertently transfer malicious code into the company's systems. Whether the employee works from a home or from a shared workstation, the terminal the employee uses effectively becomes another node in the company network, with the potential for anyone accessing that node to obtain corporate access. Physical security of a telecommuting location therefore becomes an important consideration in preventing unwanted access.

- **Laptops**. Laptop computers provide more connectivity options than telecommuting from limited locations, and their portability exposes them to a danger of being stolen or lost. The consequences of losing a laptop extend beyond the loss of computer and the proprietary or confidential information stored on the hard disk. If the laptop is used for access to a mainframe or the network, and the owner uses script files to store logon-id or password information, anyone who has the laptop can access the same applications and functions as the laptop's owner, unless additional, strong authentication mechanisms are used.

- **Upgrades and equipment leasing**. With rapidly escalating capabilities, and the desire to keep up with technology, more people are trading in their computers for ones with higher capacity. There is also a growing trend to lease equipment rather than buy it, giving users the flexibility to respond to changing requirements. When users upgrade their equipment or return leased equipment, they must take specific precautions to thoroughly erase their hard drives to prevent making all information and capabilities on them available to others.

- **Migration from the mainframe environment**. Many applications are migrating from mainframes to PCs but mainframe security features (e.g., password strength, password aging) do not migrate. This change is likely to be transparent to end users, who may assume they have the same level of security with their personal computer (PC) application as they had when it was on the mainframe (e.g., without being prompted, they may never change their passwords).

- **Customer Premise Equipment (CPE)**. End users are migrating more communications functions to their own equipment such as private branch exchanges (PBXs), and have greater access to telecommunications logic, as in CCS interconnections and Intelligent Network (IN) services. This access places control of and responsibility for applications security in the hands of customers, who may not be as knowledgeable of the equipment's vulnerabilities, and consequently may not take necessary installation and operations precautions. This makes it important for service providers to configure their networks to control access to system software to overcome CPE security deficiencies.

- **Communications:** Many organizations desire to be connected to the Internet to gain access to information or obtain services such as electronic mail. This desire leads to many security concerns because internal networks are exposed to the vulnerabilities associated with Internet connectivity. Frequently, these vulnerabilities are not well understood.

The changing business environment is a security challenge taxing the capabilities of system security features, especially as new applications are introduced. Corporate reengineering usually defines the business process first, and information systems and security are secondary. Last to be considered is how to create a secure environment for legacy systems. It often is a great challenge just to get things working, let alone implement a strong security plan.

3. THREAT

The PN is an attractive target for computer intruders

- ***The cost to the attacker is low*** Computer intruders have acquired technical skills and knowledge through easily accessible publications and electronic bulletin boards These resources provide accurate, detailed information and instructions to exploit the vulnerabilities of automated information systems and networks The equipment intruders need is affordable and readily available, and most of it, or its components, can be purchased in the retail market Intruders often avoid telecommunications costs through fraudulent activities with dialup access and/or Internet connectivity, and hide their identities

- ***The risk of getting caught is low.*** Computer intruders can attack from almost anywhere, and easily disguise their location so the chances of being caught are minimized Even if they are caught, the chances of being prosecuted by the Federal Government are low, since intent to do damage is currently required for a felony conviction, and the evidence required to prove intent is difficult to obtain Intrusions without intent to do damage are misdemeanors and are generally deemed not worth the effort required for prosecution Historically, the chances of being convicted have also been low; and even if intruders are convicted, sentences have tended to be short, although more recent cases show the courts are beginning to hand down longer sentences than in the past.

- ***The return is high.*** The PN itself is an interesting target, and some computer intruders have found markets to sell information obtained from PN databases It can also offer access to other desirable targets such as financial support systems, public utility systems, and law enforcement databases unless the targets have been properly secured. Information carried by the PN may also be of considerable value, e.g., credit card information

Computer intrusions are not bound by political or geographic boundaries They come from both domestic and foreign sources, and foreign attacks come from both friendly and hostile nations Intruders use the PN for toll fraud and to illegally monitor or divert calls, often as an aid to commit other crimes Intruders also use the PN to penetrate attached systems to commit industrial espionage. Some foreign intelligence services (FIS) are able to use these same techniques for similar purposes, to acquire information and potentially cause denial or degradation of service The effects of such actions could be exacerbated during war, natural disasters, or other emergencies Dishonest and disgruntled insiders are also a concern, and have more ready access to these systems with less likelihood of being detected

3.1 Motivation

Traditionally, computer intruders have been viewed as young, amateur computer enthusiasts motivated primarily by curiosity and technical challenge Analysis of computer intrusions in recent years, however, indicates that there is now an older generation of computer intruders for which financial gain is a more prominent motivator In addition to accessing telecommunications systems

for personal use, these older intruders are willing to sell their skills for industrial espionage, and there are troubling indications of their collusion with organized crime and FISs Law enforcement has seen evidence of such activities

Society has viewed computer intruders as lacking intent to destroy or disrupt the network This paradigm may be changing Because of some of the more recent intrusion activities, some in the telecommunications community are coming to believe that breaking into computers is passe, the new target may be the network itself [4] Although most intruders appear to target the PN to access other systems or avoid toll charges, software time bombs planted in network elements in Denver, Atlanta, and New Jersey in 1990 indicate denial of service could also be an objective [5]

INSIDERS

The primary insider motivation to exploit the PN still appears to be financial gain or revenge Insiders can be employees, contractors, alternate service providers, or anyone else with legitimate access to the PN's components, systems, and/or premises Increasingly, insiders also include the customers of service providers because new services give them access to PN software and databases to directly control their own telecommunications services Insiders are usually granted varying degrees of physical access, administrative access or both to the PN's software and databases and may use legitimately or surreptitiously acquired computer access privileges to compromise them, or inhibit access by others They know the security of the system and raise no alarm by their presence For these reasons, insiders acting in collusion with an outside threat (e.g., a competitor, criminal organization, or elements of a foreign country) could provide targeted access to software and databases to meet specific requirements of their outside accomplices. In 1994, an insider provided thousands of calling card numbers to an outsider who then sold them to foreign computer intruders

FOREIGN GOVERNMENTS

FISs and other foreign government agencies may be interested in major telecommunications systems and software within the U.S to assess whether they could be used to provide information and services, and act as conduits to other targeted systems supporting the national infrastructure To support national interests, many countries have developed strong relationships between government and business entities in the collection of economic intelligence, scientific and technological intelligence or both. For some countries, intelligence collection is often an expedient, cost-effective way to upgrade and modernize Even technologically developed countries are known to target both types of intelligence for competitive purposes The traditional line between hostile and friendly nations has become blurred Information gathered by intruders from abroad could be used in intrusions against systems in the U.S. Because many U.S companies do not fully document, report, or share their intrusion experiences, it is difficult to estimate the true magnitude of foreign government sponsored activity

---

[4] Steve Bellovin of Bell Labs, as noted in "A Rogue's Routing", *Scientific American*, May 1995, page 31

[5] *The Electronic Intrusion Threat to National Security and Emergency Preparedness Telecommunications An Awareness Document*, Second Edition, December 5, 1994, Office of the Manager, National Communications System, page 2-5

The reasons given for attacking the PN are as varied as the types of intruders conducting these attacks. Systems have been attacked for national interests, financial gain, power, revenge, prestige, ideology, and simple curiosity.

3.2 Techniques and Tools

Intruders have demonstrated their ability to effectively and systematically exploit PN software. Intruders' skills appear to be increasing, and the most skillful intruders are adept at eluding detection. In the past, attacks were laborious and time consuming and used social engineering and other techniques that took advantage of poor password management and other security weaknesses. Although computer intruders continue to exploit some of these same vulnerabilities, they also use increasingly advanced software tools and networking techniques. At first, software tools were used just to gain access to network elements and hosts, now malicious code can be attached to intrusion tools, allowing intruders to use one tool to simultaneously gain access to and steal, damage, or destroy software and databases. They use customized software programs to target specific types of computers, networks, or network elements, e.g., malicious code designed to attack a specific software vendor's product, or viruses to target antivirus software.

NEW TOOLS

Intruders often obtain system administrator utility programs and electronic intrusion detection tools from the Internet and bulletin board systems and use them to attack network hosts. They even create tutorials on bulletin board systems so others can use these tools. To rapidly share these tools with one another, intruders make them readily available across international networks. In one case, an attack program was posted on a bulletin board, and in less than 2 hours, numerous computer intruders used the program to break into systems. Unfortunately, vendors usually cannot respond with fixes in a similar time. Cooperation among computer intruders goes beyond merely sharing their tools and techniques—they have launched coordinated attacks involving collusion between domestic and foreign computer intruders.

Because these tools enable amateurs to use techniques previously employed only by more experienced intruders, they upgrade the amateurs' capabilities. Also, within the same amount of time it used to take to conduct a single attack manually, the automated tools can exploit data networks to attack many systems at various levels. Automation of attacks masks the number and identities of intruders attacking the PN, so it is unclear whether one or several intruders cause multiple attacks. It is also difficult to determine whether a series of intrusion incidents reflects an organized effort to attack a specific target for a particular purpose, or whether the series is simply unrelated activities without any specific target or purpose. It is possible that *some* of these incidents *may* be part of a coordinated effort to achieve a particular goal, but the general profusion of intrusion attempts would obscure these organized activities.

DETECTION

It is increasingly more difficult to detect intruders. The existing and growing connections between the PN and the Internet offer intruders an avenue of attack, making it easier for them to disguise their

initial point of access and weave through the network. Intruders use cellular telephones to make it more difficult to determine where attacks originate. The PN's software and databases are sizable and technically complex, it is becoming more difficult to find malicious code.

Automated tools also prevent law enforcement from distinguishing intruders from one another by their individualized attack methods. With the use of programmed attacks, it is difficult for law enforcement to identify individual intruders by their characteristic techniques or signatures. Programmed attacks can make an investigation more difficult.

In the late 1980s and early 1990s, intruders began to systematically map the internal networks they were exploring. Today, some intruders are analyzing these maps and planting programs that capture and store logon-ids, passwords (password "sniffers") and other information-gathering programs at key network hosts where they can be used most effectively.

SPOOFING

The initial IP "spoofing" attacks reported in January 1995, are an example of intruders' skills and interests. "Spoofing" is creating packets and making them appear to be coming from a trusted source. This new form of automated attack exploits improperly configured firewalls. Firewalls should be configured to recognize and block externally originating packets if they have not been authenticated or are not received from a trusted source address from within the network. Some firewalls are not. Although the vulnerability of this form of attack exploits is not new[6], the concern is that recently automated tools have been developed to exploit the vulnerability. This attack would have previously required an intruder with advanced skills, willing to devote a significant amount of time to this endeavor, with the automated tool, a novice can now exploit this vulnerability quickly and easily. NSIE member companies and agencies are reporting an increasing number of attacks against their TCP/IP-based networks. This increase probably results from the availability of automated intrusion tools and their ease of use.

NETWORK SCANNING TOOLS

Another indication of the increased sophistication of intrusion tools is the emerging use of graphical user interfaces (GUIs), or icon-driven interfaces. In the past, accessing network systems took some level of skill, which reduced the likelihood that intruders would arrive at a point in the system where they could accidentally damage it. Lowering the skill required to access critical network elements to a "point-and-click" level allows individuals with minimal skills to access them, increasing the potential for unintentional or malicious damage. One example of a tool featuring a GUI is the Security Administrator Tool for Analyzing Networks (SATAN), which was made available to the public in April 1995. SATAN scans systems to find several common networking-related security problems, and reports whether the vulnerabilities exist on a tested system without actually exploiting

---

[6] See Robert T. Morris, "A Weakness in the 4.2BSD UNIX TCP/IP Software", 1985, *Computing Science Technical Report No. 117*, AT&T Bell Laboratories, Murray Hill, NJ., and Steve Bellovin, "Security Problems in the TCP/IP Protocol Suite", published in *Computer Communication Review*, Vol 19, No. 2 April 1989, pages 32 - 48.

them Although systems administrators can use SATAN to analyze their networks, intruders could just as easily use this tool to identify vulnerabilities to enable attacks on the network

Rootkit is a relatively new set of tools that hackers use to mask computer intrusions Often, even skilled systems administrators using available state-of-the-art auditing tools will not be aware when this set of tools is being used Although Rootkit has many different capabilities, it can falsify data provided by the device itself (e.g., reported file sizes, dates and checksums not changing even though they have been modified through hacker activities such as planting Trojan horses, modifying permission tables, or granting access privileges) Only now are researchers working on a tool to overcome the effects of Rootkit; no proven products are on the shelf

It is easy for intruders to set up their equipment (e.g., a PC, phone and modem) almost anywhere such as a hotel room, or even at a pay telephone in an isolated area, and launch an automated attack program. The automated tools reduce the amount of time intruders require to access the targeted system, and the portability of their equipment diminishes their chances of being caught Intruders are increasingly using cellular phones.

TRADITIONAL HACKER ACTIVITIES

Dumpster diving and social engineering are time-proven techniques that intruders continue to use effectively Dumpster divers sort through an organization's trash to obtain information to help in electronic intrusion Social engineers impersonate a telecommunications company employee, customer, or vendor, and persuade a legitimate employee to divulge information, such as logon IDs and passwords. Social engineering takes advantage of a company's lack of security training and its emphasis on customer service

Reports by NSIE representatives of attempts at social engineering are also increasing The implications of this increase are unclear it could signal an increase in attempted attacks, it could mean that employees are more aware of social engineering attempts and are more diligent about reporting them, or it could be an indication of activities as yet unknown. It could also indicate more effective security controls which would drive intruders to use social engineering techniques to gain access they used to be able to achieve on their own by using tools such as default passwords or password "crackers."

Fraud and theft of services must also be considered as serious threats in commercial ventures therefore special consideration must be given to these problems These activities may be useful barometers of more destructive intruder activities—an intruder detected stealing services may also be engaged in more destructive undetected activities

3.3 Overall Threat

NSIE representatives believe the electronic intrusion threat to the PN is greater than it was during the last risk assessment in 1993, primarily because of the increasing sophistication of the intruders and the more advanced methods of attack. Increasingly, intruders are more experienced and motivated by financial gain, as shown by the increasing indications of links between computer

intruders, organized crime and FISs. There is more evidence of coordinated attacks, including collusion between domestic and foreign intruders. Traditional intelligence methods do not provide sufficient detail on the role that foreign governments play in these coordinated activities. The threat can no longer be characterized as coming from a group of adolescents trying to gain a few hours of free telephone service or satisfying their curiosity. The threat now includes more purposeful adults with increasingly malevolent objectives.

The tools available to intruders are increasingly automated, easy to use, and effective. Those who have no interest in spending long hours to become technically proficient now have tools to achieve their objectives. Use of these tools has two consequences: the number of individuals *capable* of attacking the PN increases as the required level of skill decreases, and less-skilled individuals can gain access to systems about which they know very little, increasing the likelihood that they could damage them, even accidentally.

The determination of the intruders, the growing ease with which they can attack the PN, the difficulty in detecting their activities, and the increasing complexity of recovering systems are all reasons for serious concern. Further, intruders have the skill to access and damage the PN, and can cause significant denial and degradation of service. The NSIEs are concerned that the intruders may choose to do so.

4. DETERRENTS

One important agent of deterrence is law enforcement. Equipment and software vendors, service providers, and their customers must work in a partnership with law enforcement to report intrusions, help identify intruders, cooperate in investigations, and help prosecute computer intruders who attack PN elements. Although the number of computer intrusions reported to law enforcement has increased, victims (telecommunications equipment vendors, service providers, and their customers) continually need to report incidents of network intrusions. Law enforcement and the private sector also need to continue cooperating in activities such as joint investigations, training, and exchanging technical information.

Sometimes, victim companies may need to maintain the exploited vulnerabilities while evidence is collected to enable a successful prosecution. This problem may put the company at risk for some time and be very costly. It will continue even if the law is changed, as discussed in the next section

4.1 Law Enforcement

Law enforcement is aggressively pursuing PN intrusions and has expanded its focus on this area of criminal activity as follows.

- It has increased training efforts to improve the technical expertise of agents and prosecutors assigned to these types of cases.
- The Department of Justice (DOJ) has established the Computer Telecommunications Coordinator (CTC) program to ensure every U.S. Attorney's office has at least one trained prosecutor to advise on technical issues and coordinate multidistrict cases
- State and local law enforcement investigative abilities are improving. Coordination between local agencies and Federal authorities has also increased and should continue to be emphasized
- Interaction between U.S. and international law enforcement entities has increased and is becoming more important, although more needs to be done.

As their investigative abilities improve, Federal, State, and local law enforcement communities are prosecuting more cases. The number of convictions is increasing, and judges are beginning to impose longer sentences.

There are certain constraints on the ability of law enforcement to deter intruders. Limits on funds affect the number of offices assigned to computer crime and how much money can be spent on training and equipment. Intruders can commit crimes against victims in the United States from anywhere in the world. In many cases, U.S. law enforcement officials cannot pursue them, either because the laws of the intruder's country do not consider these activities a crime or law enforcement in that country does not have the resources to pursue such activities

Even within the U.S , investigation and prosecution of computer intrusion cases can be complicated by the different laws and resources of the various jurisdictions involved (i e , Federal, State, and local) The Federal government is fragmented on addressing computer intruders, and no focal point has been empowered to bring together all the information and activities for computer intrusions Although cooperation among different jurisdictions is improving, some fragmentation will no doubt continue

4.2 Legislation

The NSIE groups have been concerned about deficiencies in Federal computer crime laws Recently, DOJ proposed several improvements to these laws that will be helpful if enacted The three changes that will have the greatest impact on the ability to prosecute computer intruders who attack the PN are the following

- Upgrading a class of intrusions from misdemeanors to felonies, increasing the likelihood of prosecution and the severity of the sentences,
- Revising the definition of "Federal interest computers" to include those used in interstate commerce and communications, thereby expanding the law's applicability to most computers that are part of the PN, and
- Expanding the definition of "damage" to include any impairment of data integrity or availability that threatens public health and safety

In addition, DOJ is proposing changes in sentencing guidelines to encourage judges to consider factors beyond economic loss to the victim when determining the severity of an intruder's sentence The extent to which the intruder violated the victim's privacy is an example of one such factor The Office of Management and Budget (OMB) approved DOJ's proposal, and these changes are reflected in the NII Protection Act of 1995 (S982)[7], introduced into the Senate on June 29, 1995 The NSIEs support DOJ's proposed changes

4.3 Education and Awareness

Education and awareness programs are another form of deterrence They can help deter young people from getting involved in computer crime by making them aware of the consequences of these intrusions, both for the individual (i.e., prosecution) and for society (e.g , disrupting E-911 service) Since intruders may begin their activities early in life, education and awareness programs should be targeted at school-aged children in the hope of discouraging intrusion activities Young people can often be deterred by warnings, promotional efforts, and diversions that give them opportunities to develop and exercise their computer skills in a more acceptable way

[7] This act proposes revisions to the Federal criminal code provisions for fraud and related activity on computers

Some companies have developed videos with teacher's guides and student materials, which they provide free to public schools Also, industry and law enforcement professionals may reach this target audience through youth groups (e.g., Boy Scouts), parents' organizations, teachers' associations, computer game companies, TV, radio, newspapers, magazines, or computer users' groups

A single effort to educate young people on this issue cannot be measurably effective on its own The message must be sent from many sources—home, school, work, government, the media—with persistence. Efforts to change behavior do not generally produce rapid and dramatic changes and are difficult to justify in the short term

4.4 Overall Deterrents

By its nature, deterrence always lags behind the threat. Legislation tends to be focused on "righting a wrong" rather than preventing it, law enforcement officials deal with intruders after they have broken the law. The first line of defense must be to protect the PN by taking full advantage of the security measures available Law enforcement must be prepared to deal with intruders and victims must be vigilant to detect computer crime and prepared to report intrusions and work with law enforcement

The law enforcement community currently operates within many restrictions, ranging from resource limitations, a changing and challenging technical environment, and the difficulty of pursuing computer criminals across local, state, and national boundaries The law enforcement community is working to address these challenges.

The effectiveness of deterrents may be limited, but deterrent capabilities within the U.S are among the best in the world, and are improving:

- DOJ is addressing legislative issues
- Law enforcement capabilities are improving.
- Prosecutions and convictions are increasing
- Judges are ordering more lengthy sentences.

The increase in efforts to deter young people from becoming involved in computer crime is encouraging Although the progress is difficult to assess, it is important to continue these efforts

Although the effectiveness of our deterrents will never be as great as we may wish, NSIE representatives believe deterrent activities are properly focused and progress is being made

5. VULNERABILITIES

Vulnerabilities are flaws in the PN's fabric that allow intruders to enter its computerized elements This section addresses eight areas known vulnerabilities (i e , vulnerabilities that have been well-known for some time and for which remedies are available), firewalls, Internet connectivity, centralized control centers, open protocols, standards, new technologies, and industry restructuring Section 6, Protection, identifies actions being taken to address vulnerabilities

5.1 Known Vulnerabilities

In recent years, PN service providers and equipment vendors have become more aware of the vulnerabilities that affect their systems. Security audits, information sharing activities (e.g., NSIEs), and incident response teams (e.g., Forum of Incident Response Security Teams [FIRST]) have revealed many vulnerabilities Many computer owners have taken steps to mitigate these vulnerabilities; others have not The potential impact of these known vulnerabilities on the PN has increased because the size and functionality of modern switching elements and support systems have grown over the years The compromise of certain switching elements or operations support systems can have much more widespread consequences than in the past Although many different techniques for mitigating these vulnerabilities have been well-known and documented for years, in some cases systems administrators have not chosen to close particular vulnerabilities or have not implemented fixes correctly or consistently. One example is the sendmail vulnerability in Unix which has resulted in intrusions to thousands of computer systems.

Another example is unprotected dial-up modems. Despite exhaustive efforts to eliminate unprotected dial-up modems, security audits continue to reveal new dial-up modems that employees have installed, often without knowledge of management. Modems serve an important need, and as long as the need persists and other approaches are not available, dial-up modems will continue to be used However, protection is often a missing key element.

The failure to change default passwords on systems is also a well-known vulnerability Another common vulnerability, the use of weak and easily guessed passwords, can be mitigated somewhat by the migration to token-based access and one time passwords, but it will be some time before every system has these access methods. Finally, new software releases can reintroduce old vulnerabilities if the patches that fixed those vulnerabilities are not incorporated into the new release Users often assume that known vulnerabilities have been fixed when a new version of software is released, and are unaware that they need to address it again

5.2 Firewalls

There is a growing trend by organizations to address network security by isolating their systems with firewalls Although firewalls can be effective if implemented properly, several factors need to be considered Router configurations, if not carefully designed and maintained, can introduce vulnerabilities to spoofing attacks (Section 3.2) and other intrusion techniques Routers themselves are increasingly targeted by intruders seeking to bypass firewalls If systems administrators do not

properly implement a router's security features, some users may be allowed to obtain more privileges than warranted In addition, seldom-used features, if left enabled, could become entry points for intruders This is an acute problem for organizations with a high turnover of systems administrators and users The Computer Emergency Response Team (CERT) Coordination Center has stated that although the current number of attacks on the Internet backbone infrastructure remains low, there is a huge potential for intruders to attack routers at the network provider level and reconfigure them

Firewalls should be viewed as one component of comprehensive security programs—not as a panacea The false sense of security provided by firewalls has caused many systems administrators to decrease their reliance on traditional systems security methods As a result, many systems have become more vulnerable to intrusion attacks This fact is borne out in recent IP spoofing attacks against poorly configured firewalls

5.3 Internet Connectivity

Connections to the Internet are increasing, and while many service providers have exercised due care in isolating critical network systems and components from more open-enterprise data networks and the Internet, there may still be potentially exploitable connectivity, such as through a restrictive router or firewall An error in the design, configuration, or implementation of such a protective barrier could lead to compromise of critical systems from anywhere in the world For example, a firewall that recognizes trust relationships between nodes within a network but does not restrict internal network addresses originating from outside the protected network may be susceptible to an attack by an intruder outside the network impersonating one of the trusted sites (as demonstrated by the IP spoofing attack in Section 3).

5.4 Centralized Control Centers

Many service providers have centralized OAM&P functions to control their networks from a single location This centralization has advantages from a security perspective, for example, it is potentially easier to secure a single logical access point with uniform access control than to secure multiple access points with diverse or idiosyncratic access control systems However, a compromise of a system serving one of these centralized centers would affect communications over a wider area than 5 or 10 years ago The same is true of switching and signaling elements, since modern network elements serve many more subscribers over more widely distributed geographical areas

5.5 Open Protocols

Migration to open protocols such as TCP/IP for network management systems renders those systems more vulnerable to compromise, since the community at large understands these protocols and their associated vulnerabilities better than earlier proprietary systems Several carriers presently offer access to CCS-based customers through dedicated TCP/IP links from UNIX-based workstations Although these TCP/IP links are dedicated lines, intruders could exploit TCP/IP vulnerabilities and may be able to access the carriers' CCS networks if they can intrude through the customer's gateway In fact, NSIE companies and agencies are reporting an increase in the number of such vulnerabilities with potential impact on the PN As seen in the Internet community, the results of TCP/IP attacks

can lead to disruption or degradation of service and disclosure or modification of data Some operating systems are being preloaded with software that provides TCP/IP connectivity capability Customers may not be aware of this software, further, even if they are aware of it, they may not know how to enable security precautions necessary to prevent computer intruders from using Internet connectivity to access their systems and networks

5.6 Standards

Additional security standards are needed for telecommunications networks NSTAC's Network Security Standards Oversight Group (NSSOG) examined this issue and in its October 1994 report identified 12 major issues in security standards that need to be addressed Efforts are now underway to alert standards bodies to the security issues associated with telecommunications networks so that network security standards can be developed as appropriate The issue of standards will be further complicated as more entities such as Cable Television (CATV) and wireless communications service providers become involved in the process, bringing their own perspectives and approaches to integrating their services and technologies with those of the traditional telecommunications service providers

5.7 New Technologies

In addition to known vulnerabilities of mature, well-established PN's, there is rising concern about the lack of security in emerging and future technologies New technologies supporting the NII are expected to bring with them new vulnerabilities—computer intruders have exploited existing technologies and there is every reason to expect them to develop new approaches New technologies, and new releases of existing network element software may not always include adequate security features Products lacking security features are brought to market before security problems are known or can be resolved Sometimes, solutions to security problems in older technologies are not carried forward to the new technology. For example, as more applications are migrated from mainframes to PCs, many of the well-established security features have been left behind (e.g., password strength, password aging). New telecommunications features such as remote call forwarding and selective call forwarding create new vulnerabilities unique to each feature Furthermore, vulnerabilities result from feature interaction. When two or more features are used together, they can produce unintended results Also, as customers gain more direct control over their services, the PN is potentially exposed to additional vulnerabilities through the interaction with end user systems and CPE

New technologies are in various stages of implementation throughout the PN, examples include the IN, CCS, ATM, SONET, and Integrated Services Digital Network (ISDN) CCS technology is of particular concern There is a need for cross-industry creation and implementation of a baseline level of security requirements for the CCS network elements, their support systems, and network protocols Also, CCS applications developers should determine the level of security an application requires, assess whether the baseline security on the CCS platform will provide that level, and develop and deploy any incremental security required if baseline security is inadequate for the application

New technologies are expected to make the PN more vulnerable because of the following reasons

- The ability provided by the new technologies to change the way the network reacts to subscribers' calls makes them a potential liability if components are spoofed, misprogrammed, altered, or corrupted Because new service logic is written in well-known programming languages rather than proprietary code, intruders can understand it and manipulate it more easily

- New technologies will undoubtedly be supporting NS/EP telecommunications in the future Their ability to support sensitive government telecommunications may make these technologies targets of foreign governments and terrorists, who could attack vital services as a prelude to, or as integral part of, an attack on the Nation.

- Advanced technologies will require more sophisticated troubleshooting and maintenance tools and expertise Because the development of such tools and expertise may lag behind the implementation of the new technologies, troubleshooting and maintenance may be more difficult, initially.

- Because control of the technology will be more widely dispersed, the number of people who have access to network components and operations systems will increase. This increase in users means a larger potential threat from insiders (with a corresponding increase in the potential for wrongdoers to masquerade as real workers).

- Expected open access to nontraditional third-party service providers will further increase the number of access points to the network, and a corresponding increase in the potential for abuse by authorized and unauthorized persons.

Appendices A and B provide detailed discussions of SONET and ATM vulnerabilities.

5.8 Industry Restructuring

New service providers (e.g., CATV providers) are entering into the voice and data communications market and will require interconnection with more traditional service providers. This entry of new providers raises concern over the impact on PN security. CATV was initially intended to provide one-way communications, primarily for entertainment and education. It was not generally considered an essential service, and outages have been frequent The CATV industry's primary security concerns in the past have been loss of revenue resulting from theft, degradation and disruption of service, and security measures have been implemented to deal with these problems Providers implemented security measures appropriate to its initial functionality However, CATV functionality is now changing to include two-way or interactive services Security which is adequate to protect against theft of service or interruption of programming is not sufficient to ensure the level of reliability necessary for essential telecommunications service or to provide privacy

While wireless communications technology provides an effective and flexible communications alternative, it also brings additional vulnerabilities It requires more nodes in its configuration and is

characterized by more opportunities for intrusion In addition, wireless vulnerabilities may be compounded by wireless interconnection with CCS networks Digital wireless services, such as personal communications systems (PCS), will rely heavily on the CCS network, and therefore will be subject to the combined vulnerabilities of both technologies Another new network service, Cellular Digital Packet Data (CDPD), is also a concern CDPD will be implemented by installing data switches (mobile data intermediate systems [MD-IS]) in cellular networks These MD-ISs will be interconnected through public packet-switched networks such as the Internet, thereby interconnecting PN switching equipment and the Internet Current Internet protection strategies such as firewalls will not protect MD-ISs Firewalls are designed to restrict the types of traffic allowed from external networks to internal systems, but a CDPD MD-IS is specifically required to route all types of traffic to and from mobile terminals Thus, an MD-IS is conceptually similar to an Internet router, rather than an Internet host system, and current firewall technology is not designed to protect intermediate systems or routers [6]

5.9 Overall Vulnerability

The overall vulnerability of the PN is an increasing concern Many of the old vulnerabilities are still there and new ones are being created Computer intruders continue to exploit vulnerabilities that have been well known for years, despite the existence of tools to help security administrators identify and fix holes. New technologies and the restructuring of the industry will introduce new vulnerabilities Regardless of the technology involved, data and services, testing and maintenance features, administrative services (including security administration), and communications interfaces to operations systems and other network components are considered potential points of vulnerability The level of concern is increased even more by the rapid proliferation of interconnectivity among all these technologies, and the degree to which the vulnerabilities extant in one technology are expected to compound those in another Another aspect of this concern is that because of the degree of interconnectivity and the capabilities of the new technologies, the potential impact of a single intrusion incident is becoming greater. For example, an intruder intent on disrupting telecommunications service in a large area could accomplish that objective by disabling a mated pair of CCS signaling transfer points (STPs) Causing equivalent damage in a non-CCS network would require much more effort, because the intruder would have to disable many more network elements to achieve the same widespread effect Further, advanced technologies will require more sophisticated troubleshooting and maintenance tools and expertise whose development may lag Therefore troubleshooting and maintenance may be more difficult As NSIE representatives become increasingly knowledgeable about existing and potential vulnerabilities in the PN, their level of concern grows.

[6] *The Electronic Intrusion Threat to National Security and Emergency Preparedness Telecommunications An Awareness Document*, Second Edition Office of the Manager, National Communications System, December 5, 1994, pages 3 - 6

6. PROTECTION MEASURES

Telecommunications service providers and their hardware and software vendors are the first line of defense to protect the PN from computer intruders, and the maximum benefit to secure the PN can be derived by taking full advantage of the tools and techniques available As customers gain increasing degrees of control of their services, they must also assume their share of responsibility for security.

6.1 Current Protection Mechanisms

In the 1990 NSTAC Network Security Task Force report, several rational and prudent steps were identified to protect the PN These techniques are still valid and apply equally to service providers, their vendors, and their customers Actions to produce near-term results include the following

- Conducting intensive security evaluations and audits
- Ensuring dial access control (i.e., modem security).
- Using existing security features.
- Eliminating security holes.
- Evaluating and deploying new security technologies
- Controlling proprietary information (e.g., documentation storage and disposal)
- Improving skills of the security staff.
- Establishing security awareness programs.

Over the past few years, the telecommunications industry has responded to perceived risks from electronic intrusions by implementing network security plans and programs. Examples of these kinds of activities include.

- **Firewalls:** There is a growing business need to connect with the Internet and other TCP/IP networks. Implementation of these requirements brings new threats and vulnerabilities Firewall technology has rapidly evolved to address this exposure. In only the past 2 years, the number of vendor products has grown substantially and numerous features and architectures are available. The telecommunications service providers have been analyzing their needs and deploying firewall products at their Internet access points. In addition, to detect and react to unauthorized use, network management has extended to the firewall with various degrees of effectiveness However, as noted in Section 5.2, firewalls must be properly configured to be effective.

- **Internal network partitioning**. Historically, security has been focused on controlling external access to networks. Recently, more emphasis has been placed on developing partitioning strategies to control access from internal users. Internal network partitions also help contain intrusions, recover from attacks, and define network management domains for security Firewall techniques are being analyzed and implemented to secure critical networks (e.g , those that directly support OAM&P of network elements) from other corporate network applications

Additionally, more attention is being given to assigning users to the appropriate privilege classes restricting access to root privileges

- **Strong authentication** The deployment of advanced authentication mechanisms such as one-time passwords has increased dramatically, especially for users with unrestricted work access Administrative and maintenance-level access to network elements and OAM&P systems has been a high-profile target for electronic intruders in recent years One-time password technology, while dramatically reducing the effectiveness of hacker tools such as sniffers, is still evolving to meet the network security requirements

- **Security policies** Telecommunications service providers are constantly modifying policies to address security issues arising from new technologies, services, and operations architectures Policies are being constantly refined and expanded to give direction to internal users and telecommunications vendors Strong security policies are the cornerstone of an effective network security program, especially in light of changing business environments discussed in Section 2

- **Security training and awareness:** Good security administration is one of the keys to effective network security. The quality of awareness and technology training has improved over the past few years, enabling staff members to more readily identify unauthorized activity and alert systems administrators Real security exposures and experiences integrated into hands-on training are increasingly available both within telecommunications organizations and from outside consultants In many organizations, this training has been expanded to include systems administrators, security personnel, vendors and users.

- **Security standards**: The industry is addressing security on various levels—protocols, applications, and architectures for existing and emerging technologies and services More resources are needed to identify issues, propose technical solutions, and prototype and deploy security enhanced capabilities. Also, more attention should be directed toward streamlining security administration and managing security features (e.g., Simple Network Management Protocol and the Telecommunications Management Network), which will lead to more consistent, cost-effective, interoperable, and widely deployed security features

6.2 Security Research and Development

Both Government and industry are engaging in security research and development (R&D) The National Security Agency (NSA) and the National Institute of Standards and Technology (NIST) have programs to make the results of their R&D available to industry. Products resulting from R&D in the private sector may be used exclusively within the company where they were developed, or may be made available to other companies through the marketplace As the public becomes more aware of the security issues associated with the NII, demand for security products is likely to foster even more security R&D

Besides the mechanisms just mentioned, the telecommunications industry has contributed to the development of security requirements for evolving network components, high-speed encryption, security-enhanced commercial protocols, and security architectures using security servers

6.3 Risk Management

Although it is not feasible for organizations to prevent all intrusions from both internal and external sources, they can operate within acceptable levels of risk. Risk management principles suggest that organizations focus on spending resources to deploy safeguards to protect themselves against intrusions that could cause the greatest amount of damage, but be prepared to react to intrusions with lesser risk as needed. Organizations must be able to detect and react to intrusions Current capabilities do not always detect intrusions, detection is the key to mitigation Many companies are slow to buy technological capabilities and adequate security tools and provide sufficient numbers of trained system security administrators to do an effective security job, because the perceived risks are low

Awareness of the risks to the network and the implementation of prudent actions are critical steps enabling cost effective and sound security programs. Exchanging information on threats, vulnerabilities, and remedies, as done in the NSIE groups, helps improve understanding. Similarly, through symposia and documents such as this one, the NSIE groups can help increase awareness of network security issues throughout a broader segment of the industry. Increased awareness facilitates increased reporting, elevates management awareness, and results in more support of security activities

Increased awareness and security programs have reduced the opportunity for intruders to gain access by using easily detected methods (e.g., modem access, default passwords, and social engineering) However, eternal vigilance in the form of good security management and information exchange, a sustained level of technical and procedural improvement, and a program to continue monitoring network security and eliminating identified vulnerabilities will be required. Further, security and security awareness efforts in a company need to include the company's contractors, customers, and partners in joint ventures.

6.4 Overall Protection

Government and industry recognizes the importance of protecting the PN from electronic intrusions, and are continuing to work together toward that goal. A great deal has been done and additional initiatives are underway to continue to improve security methods and tools, including implementing firewalls, both external and internal to the network, using strong authentication such as one-time token-based passwords, developing security standards and R&D programs, establishing strong security policies; and implementing security awareness and training programs Resources, competition, cost, and convenience may constrain an organization's decisions on security tools and techniques The industry is applying the principles of risk management in making these security decisions

7. CONSEQUENT RISK

NSIE representatives believe the overall risk to the PN is greater today than it was perceived to be during the last formal risk assessment in 1993 No specific metrics are available to quantify this assertion, instead it is based on conclusions from industry and government security professionals participating in the NSIE process Perhaps in the future this type of data will be available

For some time, **the PN has been one of our Nation's most critical infrastructures, providing routine and essential communications capabilities locally, nationally, and globally** Other key infrastructures—such as transportation, utilities, and banking—depend on the PN for reliable communications to fulfill their missions As the NII continues to evolve, new applications and services will require even more capabilities and capacity from the Nation's communications infrastructure. These new applications and services are expected to create economic growth vital to national and economic security Risks to the PN are a concern because they pose a risk to these other infrastructures, our economic health and ultimately, our national security

The current trend toward increased network interconnection has profound implications for all networks. Security programs are often widely inconsistent both within and across network domains—allowing attacks to propagate to networks with relatively solid security postures Therefore, weak security programs in one network can often increase risks in other interconnected networks

Government and industry have taken actions, both independently and jointly, to make the PN more secure. The NSIE process is a major effort through which Government and industry, through NSTAC, are addressing network security As a consequence, they have come to realize the following facts.

- **Technology alone will not solve the problem**. To a great extent, security is a people problem, requiring both full attention and support of management and the continued vigilance of systems users and administrators
- **There is no silver bullet.**
- **Protecting the PN is a continuous, dynamic, and growing process** Measures such as training and audits are not one-time efforts, and there is no guarantee that past measures will continue to be effective in the future
- **Security is everybody's problem** Service providers and equipment vendors are responsible for protecting the network components over which they have control However, as customers gain access to network components that allow them to have greater control over their own services, they must also take responsibility for protecting those network components
- **The changing business environment should prompt periodic reviews of security programs** Efforts to reduce operating expenses frequently entail workforce reductions

Terminated employees have the knowledge and may have the motivation to attack the resources of their former employers, retained employees may become disgruntled or may simply be unable to devote as much time and attention to security-related activities as is needed Companies that outsource their work or embark on joint ventures may be exposed to the vulnerabilities of their vendors and partners Changes in how people do their work, such as telecommuting and the increasing use of laptops, create new vulnerabilities

The threat to the PN is increasing Today's computer intruders are older and more purposeful, often motivated by financial gain, and armed with effective automated tools that facilitate software attacks on the PN. There is considerable concern about the ability and motivation of computer intruders to seriously damage the PN itself. Today's intruders share their knowledge and skills and coordinate activities to achieve their objectives. Increasingly user-friendly intrusion tools intensify the threat by lowering the skills required to attack the PN, and their widespread availability increases the number of users who have access to them. Evidence gained in criminal prosecutions continues to substantiate this change in the nature of the threat.

The deterrent capabilities in the U.S. are among the best in the world and are improving DOJ is addressing legislative issues that have hampered the ability of law enforcement to prosecute computer intruders. The increasing numbers of prosecutions and successful convictions, in combination with longer sentences, demonstrate that the law enforcement community is increasing its capabilities to investigate and successfully prosecute crimes of this nature

Public education to increase awareness of the consequences of attacks on the PN, both for the individual and for society overall, is just now beginning to emerge, and it is too soon to assess its effectiveness. Although such efforts are needed, they do not generally produce rapid and dramatic changes Deterrents are usually a reactionary step taken to address a threat; therefore they cannot be expected to keep pace with the level of the threat, particularly because of the rate at which the threat is growing

The vulnerability of the PN is also increasing. Old vulnerabilities are still being exploited, despite readily-available tools and techniques to eliminate them. New technologies such as IN, ATM, and SONET, are bringing new vulnerabilities into the PN, as are new telecommunications service providers. Because of the increased capabilities and interconnectivity of new technologies, the impact of a single intrusion incident has the potential to be more widespread and severe than with the older technology. **Although progress has been made in developing tools to protect the PN, these protection measures have not kept pace with the vulnerabilities, nor have they been ubiquitously applied**

Government and industry recognize the importance of protecting the PN, particularly as society moves towards using capabilities and services offered by the emerging NII Consequently, they are taking advantage of available protection measures and continuing research into improved methods and tools to strengthen PN security. In addition to the tried and true methods (e.g., intensive security evaluations and audits, improving skills of the security staff, and controlling proprietary information), Government and industry are pursuing new tools, such as advanced authentication

mechanisms and internal network partitioning However, just as the threat is outpacing the deterrents, the vulnerabilities are outpacing the protection measures

The bottom line of this risk assessment is the following

- Reliance on the PN is growing
- Complexity of the network and its technology, interfaces, and vulnerabilities is growing
- Deterrent capabilities are improving and require continued commitments of resources, and industry and government coordinated efforts
- Protection mechanisms are improving, but have not kept pace with new and emerging vulnerabilities

In conclusion, the NSIE subject matter experts feel that while a great deal has been accomplished, much remains to be done

APPENDIX A

The Risks to Synchronous Optical Networks (SONET) from Electronic Intrusion

SONET, an industry standard for high-speed transmission over optical fiber, is a transport vehicle capable of delivering bandwidth in the gigabit-per-second range SONET technology will form the foundation for future telecommunications transmission networks. Inter-exchange and local exchange carriers, as well as many private network operators are deploying SONET widely Virtually all new fiber optic installations by commercial carriers are currently being configured as SONET networks Because of SONET technology's rapid penetration in the commercial carrier networks, security is important to address. SONET security issues can be grouped into three areas described below information security management functions, SONET network element security, and SONET network configuration and operation.

1. Information Security Management Functions

The SONET protocol under development since 1985, provides many advantages over existing transmission facilities, including flexible bandwidth and network element management Many in the standards community believe that security concerns were not adequately addressed during the protocol's development. Currently, the SONET protocol, as defined in the International Telecommunications Union Telecommunications Standardization Sector (ITU-TSS) M.30 recommendation, allows four basic management levels in the network network element management, network management, service management, and business level management. Within these four levels are embedded a series of management functions that provide basic processes to operate SONET networks

The SONET architecture does not specifically address security as a management function in the SONET hierarchy. The information security management function has been introduced to the standards community to provide a generalized way for network operators to control the information made visible across a network interface. Information security management has received very little attention to date from the standards community. The security function is considered a very general aspect of management, and because the other protocols traversing SONET networks provide their own security functions, SONET-specific security functions are unlikely to be developed. However, the SONET Interoperability Forum has recently begun to address aspects of the SONET management functions

Other management functions also have a bearing on information security in SONET networks The *network element management level* provides functions such as configuration management, alarm reporting, performance reporting, and cross-connection The *network management level* provides functions such as event management, performance management, fault correlation, and dynamic trail control The *service management level* provides functions such as billing management, quality of service tracking, customer service packaging, and service contract details. The *business management level* is not well defined yet, but it is expected to provide functions such as service

design and planning, inventory control, network design and planning. All of these functions could severely affect the performance of a SONET network if compromised.

The SONET protocol defines a 192K-bits per second (bps) section-layer data communications channel (DCC) that functions as an embedded message-based operations channel. The section-layer DCC is reserved for operations, administration, maintenance, and provisioning (OAM&P) messages transmitted by network elements, operations support systems, and network management systems. SONET also defines a 576K-bps line-layer data communications channel. The line-layer DCC is reserved for OAM&P between line termination equipment, such as add/drop multiplexers (ADMs). Access to these DCCs can be restricted to authorized users, but adequate security measures have not been designed to effectively protect these channels from electronic exploitation. An intruder who has broken into a DCC could compromise SONET network elements or read, modify, or delete other users' traffic. Until security mechanisms have been designed and implemented for SONET DCCs, they should be considered highly vulnerable.

2. SONET Network Element Security

SONET is identified not only by its protocol, but by the hardware and software that comprise the structure of installed SONET rings. These network elements fall into three basic categories: access, switching, and transport. Specific network elements include ADMs, broadband and wideband digital cross-connects (DCS), digital loop carriers, regenerators, broadband switches, terminal multiplexers, and switch interfaces.

ADMs are the primary building blocks of SONET networks—they serve the important function of adding and dropping traffic from the SONET ring. They are unique to the SONET architecture, and are equivalent to the M13 multiplexers found in DS-3 networks. Since each access point on a SONET ring has an ADM, information on the ring traverses through each ADM. Proper precautions are needed to physically protect the ADMs, to electronically protect the information traversing them, and to ensure that information is not improperly disclosed or monitored.

Other network elements such as switch interfaces, digital loop carriers, DCSs, broadband switches, terminal multiplexers, and fiber signal repeater stations need to be considered in a SONET vulnerability analysis as well. Most of these devices can be electronically accessed for many different purposes including operations, administration, maintenance, provisioning, and testing. Any element used as part of a SONET system should be considered vulnerable to electronic and physical attack.

3. SONET Network Configuration and Operation

Controlling access to the information transmitted across a SONET network is an important concern because of the security issues identified in this assessment. Because of the lack of built-in security features, the security of a SONET network depends largely on its configuration and operation.

Because SONET is a relatively new protocol that is just now being implemented widely, security has not been fully analyzed in SONET networks installed by telecommunications service providers. Security is especially important because SONET network elements such as ADMs are being

managed remotely through packet data network connections Thus, SONET network elements are vulnerable to electronic intrusions on carriers' internal corporate networks If these corporate networks are not adequately protected with advanced authentication, firewalls, and other security mechanisms, SONET network elements could be exposed to substantial risks

Another important implementation issue is related to the interconnection of SONET networks SONET was originally designed to connect major trunking facilities in telecommunications transmission networks. However, as SONET became more widely accepted in the industry, it evolved into a complete transmission architecture supporting carriers, end users, service providers and other entities. This evolution has created security issues because SONET does not provide standardized firewall or gateway network elements. Therefore, there is no mechanism to filter or restrict traffic traveling between SONET networks and crossing administrative domains Filtering traffic is especially important in relation to the DCCs mentioned earlier Since access to DCCs cannot be effectively restricted, many service providers are completely disabling the DCCs because they fear the DCCs may be abused by intruders from other interconnected networks.

In commercial SONET installations, network operators normally protect their network elements with a goal of providing an acceptable level of security that balances perceived risk with the cost of mitigating this risk. The differences between this industry security approach and the Government's national security and emergency preparedness approach may cause some concern in the Government because both the industry and Government have a great deal of experience with electronic intrusions However, industry is working to resolve these issues and build security into off-the-shelf SONET products.

APPENDIX B

The Risks to Asynchronous Transfer Mode (ATM) from Electronic Intrusion

ATM is an emerging packet-based switching and multiplexing communications technology. ATM will integrate many different traffic types (i.e., voice, data, video, etc.) on a single physical network. ATM was designed to use fiber-optic transmission media and support very high transmission speeds (up to gigabits per second). It can also operate at lower speeds over copper and wireless communications links. ATM can be used for local area networks, with a single protocol, and to interconnect many different higher-layer network protocols and traffic types. Together, ATM and SONET form the foundation of the Broadband Integrated Services Digital Network (B-ISDN).

ATM's role as a major interworking protocol make the security aspects of this technology critical. Three specific risk areas are discussed below: information security, network element security, and network and security management.

1. Information Security

One of the biggest risks in any network is the monitoring or modification of user information by unauthorized individuals. Protecting this information from unintended exposure is referred to as confidentiality. Encryption is increasingly providing confidentiality of communications. Encryption can negatively affect network performance by causing added information transmission delays while data is encrypted. If encryption is implemented at the ATM layer, the encryption mechanisms must introduce as little delay as possible. ATM encryption will require the use of a cryptographic key distribution and management scheme that is designed to support network speeds and high-speed applications that run on ATM networks. In certain circumstances, implementing encryption at higher layers may be preferable. Several ATM encryption products are currently being developed.

Preventing disclosure of user traffic to unauthorized individuals is referred to as traffic confidentiality protection. ATM transfers information using fixed packets called cells that uniquely identify the switching route within a network element. Since each value is unique only within a network element, each switching element along a network path must be capable of reading the value and changing this address for the next network element. This vulnerability makes it very difficult to protect cell destination information from disclosure during transmission. Without traffic confidentiality protection, an eavesdropper could observe where particular traffic is going simply by looking at the values. A related vulnerability is that a malicious party who has access to a switch could modify the values, and traffic would be rerouted on an unintended network path.

Protecting user information against modification is referred to as integrity protection. The ATM cell payload does not provide an integrity service. As a result, a higher layer protocol must provide integrity. Integrity is typically provided using some type of cryptographic checksum mechanism. As with cryptographic confidentiality protection, this mechanism may introduce unwanted delays, it requires a key management and distribution system. A cryptographic system may provide both the confidentiality and integrity services simultaneously.

2. Network Element Security

ATM network elements include switches, workstation adapter equipment, routers, hubs, and other related equipment. These elements will be in many different places, from private corporations and private service locations to public network service providers and government locations. A wide variety of network elements could handle information traveling across an ATM network. The degree of security inherent in each of these intermediate elements may vary greatly, and some of them may not meet the user's requirements for security. Consequently, the end user should not send sensitive information without some assurance that the information is protected. This assurance may be achieved through mechanisms the end user controls (e.g., confidentiality provided above the ATM layer) or by confirming that intermediate network elements have adequate security.

Also, ATM switches are designed to be fast and simple to support the low latency switching and transmission speeds required for ATM networks. Adding security features may impede this fast transmission. As a result, many overhead services, such as security, are being performed outside the ATM network through adjunct devices such as security servers.

3. Network Management and Security Management

Management of ATM networks is a developing area. Standards and interoperability groups such as the ATM Forum are developing network management solutions. However, security and security management are just beginning to be addressed. Network management solutions using the Simple Network Management Protocol (SNMP) and the Common Management Interface Protocol (CMIP) are being considered, but neither protocol is considered to have robust security features. The risk of exposing network management information is expected to help motivate ATM service providers to develop and implement security measures.

As a developing technology, other aspects of ATM are still evolving that may pose risks that have not yet been identified. Examples include the following:

Traffic management, involves definition of traffic contracts, different levels of quality of service, and congestion control mechanisms. Many items published in open literature indicate that there are still significant theoretical problems in these areas. The security risks cannot be clearly identified and remedied until solutions to traffic management issues are developed and adopted.

Denial of service, a condition in which authorized users cannot obtain the network services they require. In ATM networks, conditions exist where a rogue network user could flood a network with unauthorized traffic, thereby preventing legitimate users from obtaining services. Developments in traffic management should prevent denial-of-service attacks.

Increased use of switched virtual circuits, on-demand (versus dedicated) network connections logically equivalent to our use of the telephone system today. Initial tests of ATM networks involve mostly permanent virtual circuits that are dedicated, manually configured connections.

4. Summary

In general, the ATM development community acknowledges that security issues need to be addressed. Because the technology is new, largely untested, with features developing rapidly, security risks continue to be indeterminate. As an interworking protocol, ATM could serve as the convergence point for networks of many different protocol types. As a result, the security and availability of ATM networks become critical issues that may affect many diverse networks and applications.

Although this appendix provides a high-level view of the risks of ATM, it should not be considered a comprehensive treatment of the security issues surrounding ATM. The most thorough means of evaluating security will include assessment of specific applications and systems.

APPENDIX C
ACRONYM LIST

ADM	Add/Drop Multiplexer
ATM	Asynchronous Transfer Mode
B-ISDN	Broadband Integrated Services Digital Network
BPS	Bits per second
CATV	Cable Television
CCS	Common Channel Signaling
CDPD	Cellular Digital Packet Data
CERT	Computer Emergency Response Team
CMIP	Common Management Interface Protocol
CPE	Customer Premise Equipment
CTC	Computer Telecommunications Coordinator
DCC	Data Communications Channel
DCS	Digital Cross-connect
DOJ	Department of Justice
E-911	Emergency 911
FIRST	Forum of Incident Response Security Teams
FIS	Foreign Intelligence Service
GUI	Graphical User Interface
IN	Intelligent Network
IP	Internet Protocol
ISDN	Integrated Services Digital Network
ITU-TSS	International Telecommunications Union Telecommunications Standardization Section
MD-IS	Mobile Data Intermediate System
NCS	National Communications System
NII	National Information Infrastructure
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NSC	National Security Council
NS/EP	National Security and Emergency Preparedness
NSIE	Network Security Information Exchange

ACRONYM LIST
(Continued)

NSSOG	Network Security Standards Oversight Group
NSTAC	National Security Telecommunications Advisory Committee
OAM&P	Operations, Administration, Maintenance, and Provisioning
OMB	Office of Management and Budget
OMNCS	Office of the Manager, National Communications System
PBX	Private Branch Exchange
PC	Personal Computer
PCC-NSTIS	Policy Coordinating Committee for National Security Telecommunications and Information Systems
PCS	Personal Communications Systems
PN	Public Network
PSN	Public Switched Network
R&D	Research and Development
SATAN	Security Administrator Tool for Analyzing Networks
SNMP	Simple Network Management Protocol
SONET	Synchronous Optical Network
STP	Signaling Transfer Point
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
TSP	Telecommunications Service Priority

APPENDIX D
REFERENCES

Initial Tasking Document

Memorandum to the Manager, National Communications System (Subject: Public Switched Network Action Plan) from the Chairman of the National Security Council Policy Coordinating Committee for National Security Telecommunications and Information Systems. April 23, 1990

Previous Status Reports

Manager, National Communications System. *Security of the Public Switched Network: A Status Report to the Chairman, Policy Coordinating Committee, National Security Telecommunications and Information Systems*. August 1991

Manager, National Communications System. *Security of the Public Switched Network: The Second Status Report to the Chairman, Policy Coordinating Committee, National Security Telecommunications and Information Systems*. July 1992.

Manager, National Communications System, *Status Report on Security of the Public Switched Network: Report to the Assistant to the President for National Security Affairs*. December 1993

Manager, National Communications System, *Status Report on Security of the Public Switched Network: Report to the Assistant to the President for National Security Affairs*. January 1995.

National Security Telecommunications Advisory Committee (NSTAC) Documents

- Network Security Task Force Reports
  - *Final Report of the Network Security Task Force*. June 1992.
  - *Report of the Network Security Task Force*. November 1990.
  - *Status Report of the Network Security Task Force for NSTAC XIII*. August 1991
  - *National Information Infrastructure (NII) Task Force Report to NSTAC XVII*. January 1995
- NSTAC's Network Security Standards Oversight Group (NSSOG)
  - *Network Security Standards for the Public Switched Network: Issues and Recommendations*. October 13, 1994

NSIE Charters

Charter for the Federal Government Network Security Information Exchange, June 25, 1991

National Security Telecommunications Advisory Committee (NSTAC) Network Security Information Exchange (NSIE) Charter, May 1991

NSIE Products

Digital Cross-connect System (DCS) Security Evaluation Aid Consists of three parts a DCS Configuration Profile, a DCS Security Checklist, and an Operations Support (OS) Security Checklist Used in combination, these three tools will enable organizations with DCSs to perform rigorous assessments of the security of their DCSs The *DCS Evaluation Aid* has been provided to the FCC's Network Reliability Council for dissemination to the broader telecommunications audience. [1993]

Proceedings: Network Security Symposium. The Office of the Manager, National Communications System, and the President's National Security Telecommunications Advisory Committee co-sponsored this symposium, which took place February 6 - 8, 1994, in Reston, VA The proceedings were published and distributed in August 1994

Proceedings: Workshop on Network Firewalls for NS/EP Communications The NSTAC and Government NSIEs cosponsored this symposium, which took place on June 28, 1994, in McLean, VA The proceedings were published and distributed in August 1994

OFFICE OF THE MANAGER, NATIONAL COMMUNICATIONS SYSTEM (OMNCS) - Sponsored Documents

National Communications System Manual 3-1-1, *Telecommunications Service Priority (TSP) System for National Security Emergency preparedness (NS/EP) Service User Manual*, National Communications System, Washington, DC. July 9, 1990

The Electronic Intrusion Threat to National Security and Emergency Preparedness (NS/EP) Telecommunications: An Awareness Document Office of the Manager, National Communications System, September 30, 1993

The Electronic Intrusion Threat to National Security and Emergency Preparedness (NS/EP) Telecommunications: An Awareness Document Office of the Manager, National Communications System, October 31, 1994

Security in Open Systems, NIST Special Publication 800-7, Computer System Laboratory, Computer Systems Laboratory, National Institute of Standards and Technology, Gaithersburg, MD July 1994

SRI International *Vulnerabilities of the PSN, Volume I: Conclusions and Recommendations*, Menlo Park, CA January 1993. [Client Private. Prepared for OMNCS, Arlington, VA; may not be distributed without the consent of the Government and NSTAC Network Security Information Exchanges.]

SRI International. *Vulnerabilities of the PSN, Volume II: Findings*, Menlo Park, CA January 1993 [Client Private: Prepared for OMNCS, Arlington, VA. not be distributed without the consent of the Government and NSTAC Network Security Information Exchanges.]

SRI International *1993 Research on the Vulnerabilities of the PSN, Volume I: Conclusions and Recommendations*, Menlo Park, CA. March 1994 [Client Private Prepared for OMNCS, Arlington, VA, may not be distributed without the consent of the Government and NSTAC Network Security Information Exchanges.]

SRI International *1993 Research on the Vulnerabilities of the PSN, Volume II: Detailed Findings: Working Notes from the Field and Remote Interviews*, Menlo Park, CA March 1994 [Client Private. Prepared for OMNCS, Arlington, VA, may not be distributed without the consent of the Government and NSTAC Network Security Information Exchanges.]

Other

"A Rogue's Routing," *Scientific American*, May 1995, page 31

Bellovin, Steve, "Security Problems in the TCP/IP Protocol Suite," *Computer Communication Review*, Vol 19, No. 2 (April 1989), pages 32 - 48.

Clinton, William J. and Albert Gore, Jr. Technology for America's Economic Growth, A New Direction to Build Economic Strength February 22, 1993.

Morris, Robert T., "A Weakness in the 4.2BSD UNIX TCP/IP Software," *Computing Science Technical Report No. 117*, AT&T Bell Laboratories, Murray Hill, NJ 1985

National Research Council *Growing Vulnerability of the Public Switched Networks: Implications for National Security Emergency Preparedness*, Washington, DC National Academy Press Spring 1989

REFERENCES (Concluded)

National Research Council *Computers at Risk: Safe Computing in the Information Age*. Washington, DC National Academy Press 1991

Private Branch Exchange (PBX) Security Guideline, National Institute of Standards and Technology Computer Systems Laboratory, Open Telecommunications Security Project, Integrated OSI, ISDN, and Security Program NIST Government Contractor Report, NIST/GCR-93-635, September 1993

The Information Infrastructure: Agenda for Action, September 15, 1993

U.S. Office of Technology Assessment. *Information Security and Privacy in Network Environments*, OTA-TCT-606. Washington, DC U.S. Government Printing Office, September 1994

Proprietary Information

SYSTEM SECURITY AND INFORMATION WARFARE:

NETWORKS AT RISK

TED PHILLIPS
BOOZ·ALLEN & HAMILTON INC

April 1997

Today's Agenda

- System Security Issues -- Understanding The Risks
  - Telecommunications Industry Trends
  - Network Vulnerabilities
- Threats And Case Histories
- Strategies To Reduce Your Risk Exposure

This Briefing Is Based On Entirely On Unclassified And Open Source Information.

SYSTEM SECURITY ISSUES: UNDERSTANDING THE RISKS

Understanding the Risks

Electronic Intruders Are Targeting Core Communications Technologies

Networks Are Highly Interconnected And International. . .

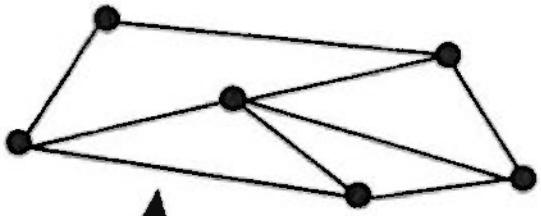
They Are Very Attractive Targets For Electronic Intruders. . .

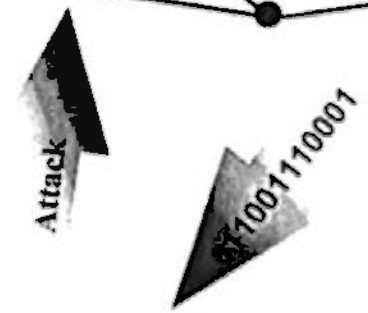
Understanding the Risks

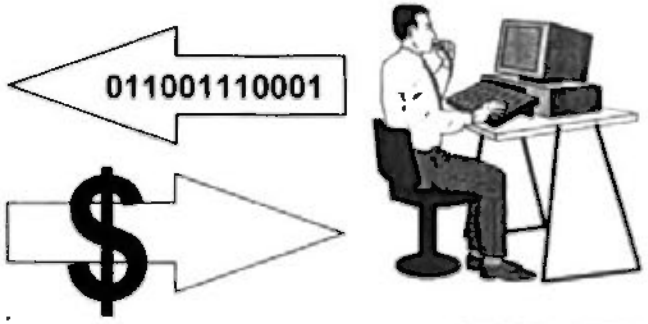
Financial Gain Is A Strong Motivator

Foreign Intelligence Services
Organized Crime
Terrorist Organizations
Industrial Espionage Agents
Private Investigators
Information Brokers

Many groups have a high level of interest in electronic intrusion skills







Understanding the Risks

During The Past 3 Years. . .

Network Attacks Have *Increased Significantly*

Intruders Have Attacked
All Major Categories Of Network Elements

Intruders Have Attacked
A Wide Variety Of End User Systems

Intruders Have Attacked
All Major U.S. Telecommunications Carriers

Intruders Have Attacked
Many Major International PTT Networks

Intruders Have Attacked
All Major Internet Service Providers

Telecommunications Industry Trends

Industry Trends Will Increase Risk

Industry Competitive Issues

Privacy And Confidentiality Trends

Architectural Trends

Technology Trends

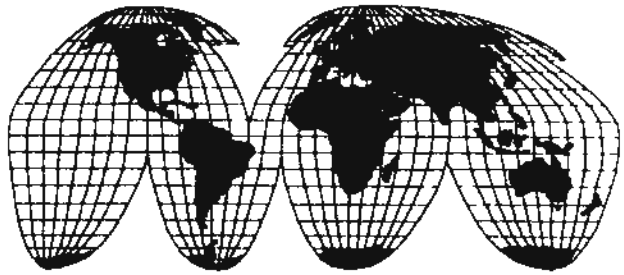
Industry Competitive Issues

- Financial Pressures Reduce Security's Priority
- Metrics To Conduct Security Cost/Benefit Analyses Not Fully Developed
- Downsizing Reduces Worker Loyalty And Creates Disgruntled Ex-Employees

Privacy And Confidentiality Trends

- Sensitive Customer and Network Information Is Created And Stored On Network Elements
- Sensitive Information Is Openly Exchanged Among Network Elements
- End User Systems Are Directly Connected To Public Networks

Architectural Trends



- Network Administration Is Increasingly Shared Between Carriers, Service Providers, And Users
- Customer Premise Equipment (CPE) Is More Interconnected With Public Network Elements
- Public Network Elements Are Richly Interconnected, Creating Extremely Complex Network Structures
- The Communications Industry Is Moving Toward A Cell-Switched Architecture

Technology Trends

- Public Network Elements Are Virtually All Computerized And Software-Controlled
- Network elements are increasingly complex and difficult to securely administer
- Wireless Technology Will Be Important For End-User Network Access

New Technologies Will Increase Risk

- Synchronous Optical Networks (SONET)
- Asynchronous Transfer Mode (ATM) Networks
- Internet Protocol, version 6 (IPv6)
- Digital Subscriber Line Technologies (xDSL)
- Advanced Intelligent Networks (AIN)
- Integrated Services Digital Network (ISDN)
- Wireless Local Loop Technologies
- Wireless Data Networks (CDPD, PCS)

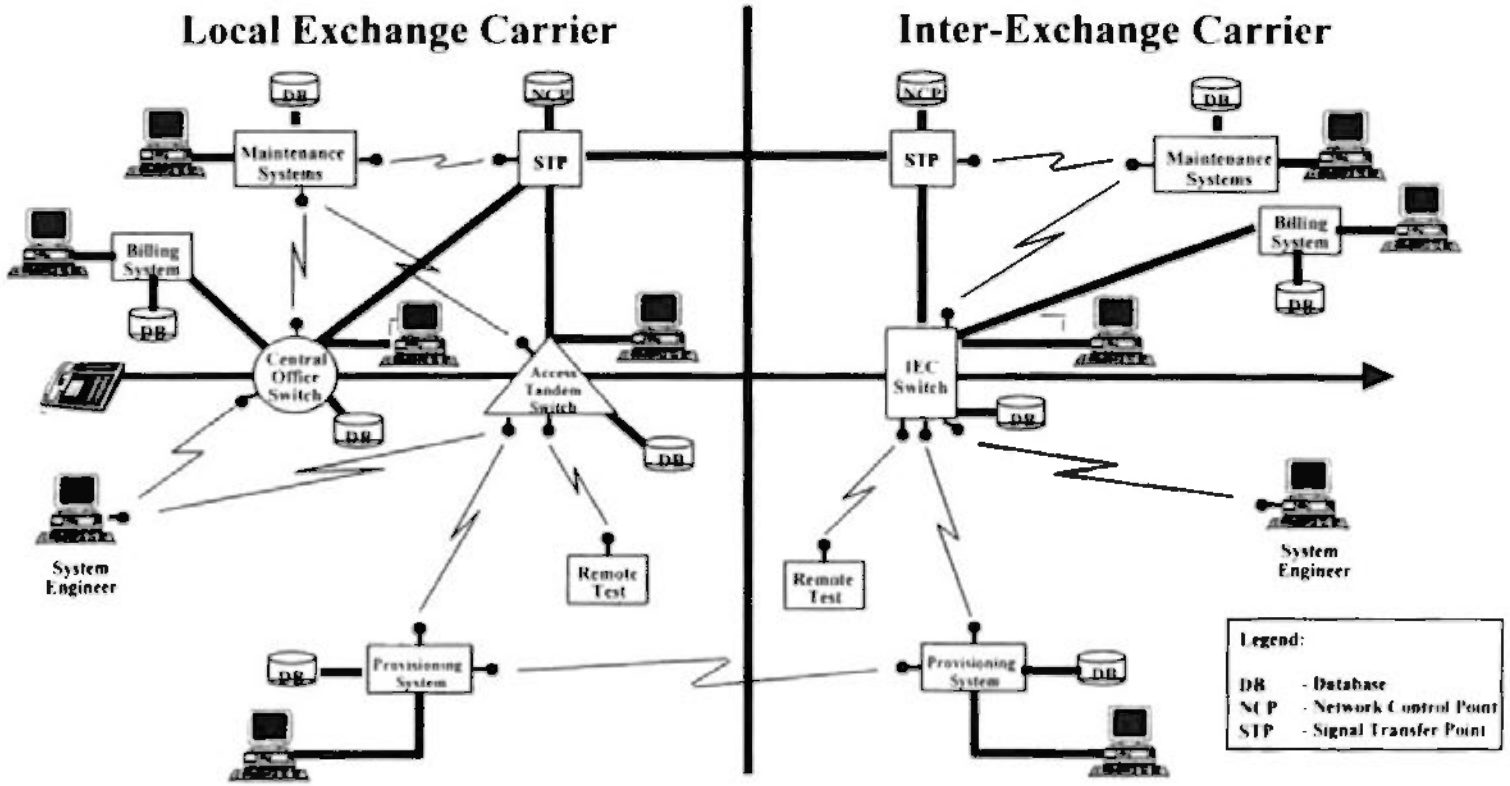
⇨ ***Electronic Intruders Are Developing Techniques To Attack Each Of These Technologies***

Network Vulnerabilities

Understanding the Risks

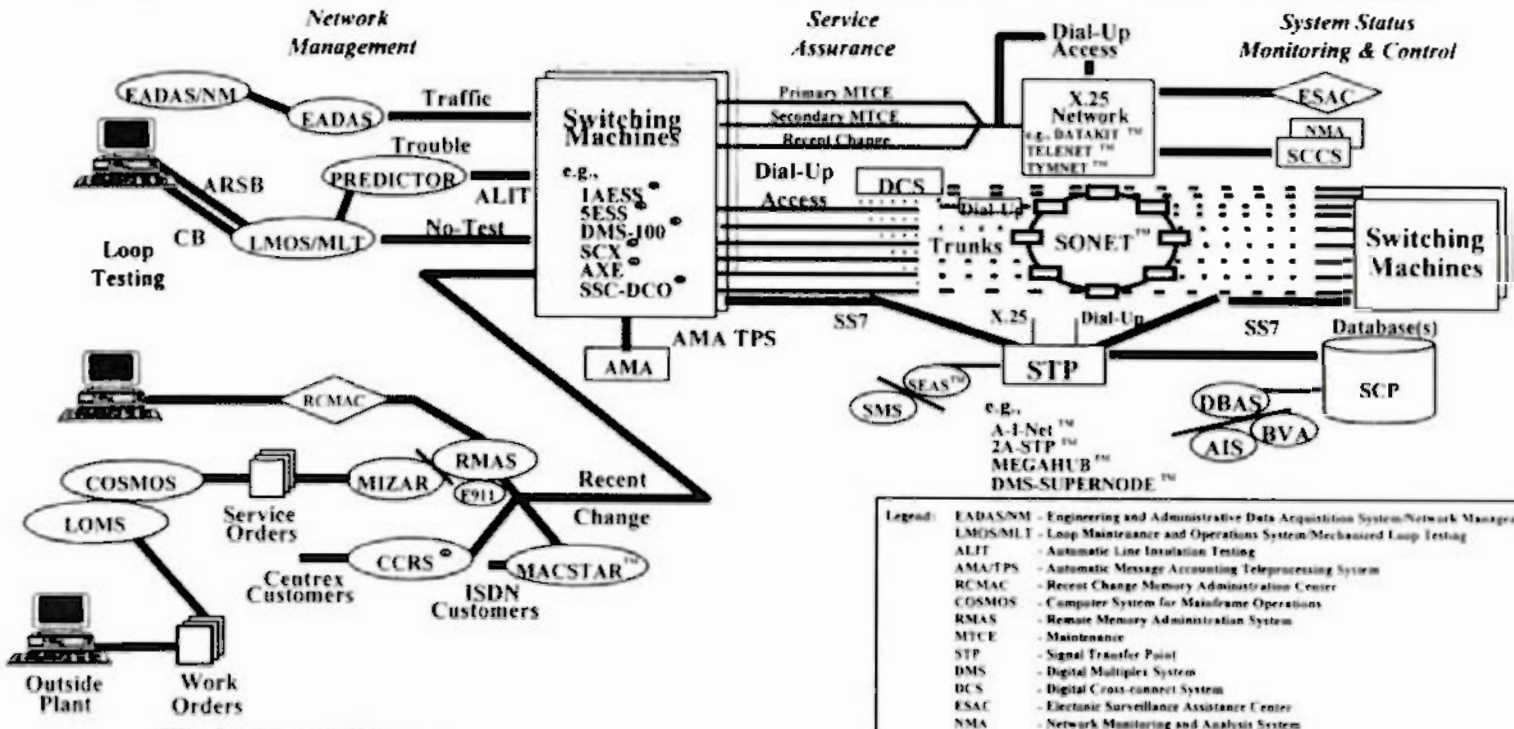
Network Vulnerabilities

All Systems On This Diagram Have Been Penetrated At Least Once In The Past 3 Years



Understanding the Risks

Network Vulnerabilities (cont.)

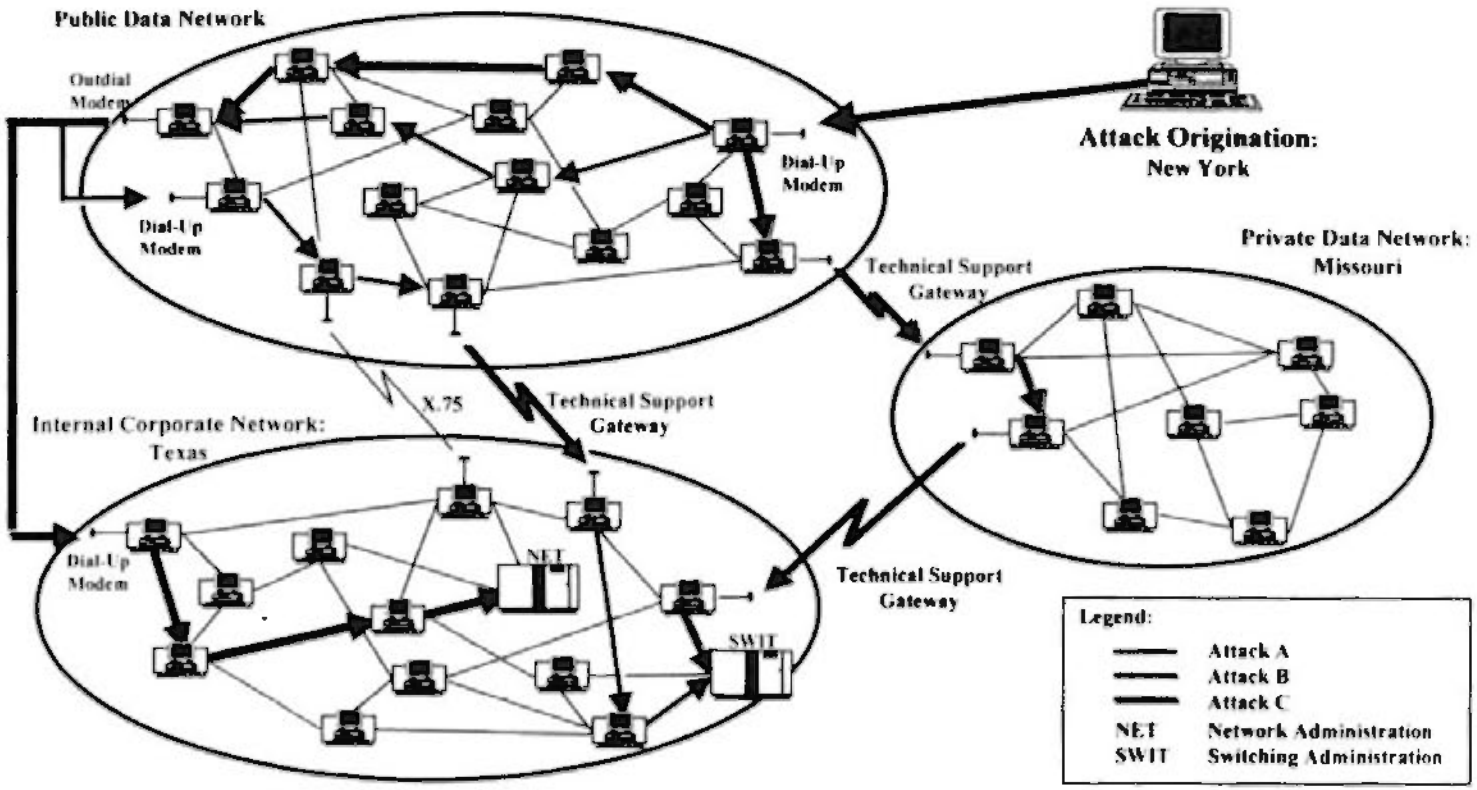


CCRS is a Registered Service Mark of Bellcore
SONET and SEAS are Registered Trademarks of Bellcore
1AESS, 5ESS, A-1 Net, 2A-STP, DATAKIT, and MACSTAR are Registered Trademarks of AT&T
DMS is a Registered Trademark of Northern Telecom
SCX is a Registered Trademark of Rockwell
TELENET is a Registered Trademark of Sprint
TYMNET is a Registered Trademark of British Telecom
MEGAHUB is a Registered Trademark of DSC Communications
AXE is a Registered Trademark of Ericsson
SSC-DCO is a Registered Trademark of Siemens Stromberg Carlson

Legend:	EADAS/NM - Engineering and Administrative Data Acquisition System/Network Management
	LMOS/MLT - Loop Maintenance and Operations System/Mechanized Loop Testing
	ALIT - Automatic Line Insulation Testing
	AMA/TPS - Automatic Message Accounting Teleprocessing System
	RCMAC - Recent Change Memory Administration Center
	COSMOS - Computer System for Mainframe Operations
	RMAS - Remote Memory Administration System
	MTCE - Maintenance
	STP - Signal Transfer Point
	DMS - Digital Multiplex System
	DCS - Digital Cross-connect System
	ESAC - Electronic Surveillance Assistance Center
	NMA - Network Monitoring and Analysis System
	SCCS - Switching Control Center System
	SCP - Signal Control Point
	SEAS - Signaling Engineering and Administration System
	SMS - Service Management System
	AIS - Automatic Intercept System
	BVA - Billing Validation Application
	DBAS - Database Administration System

Understanding the Risks

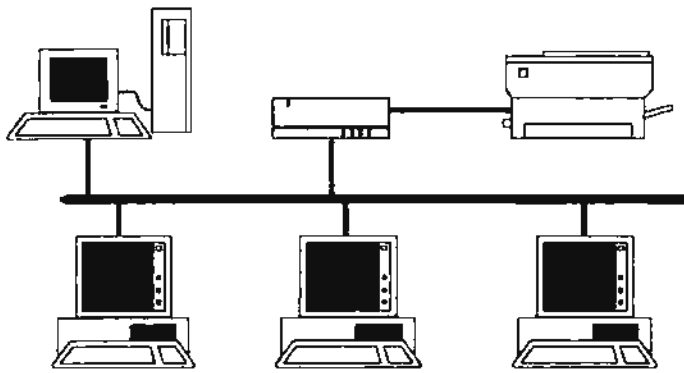
Data Network Vulnerabilities:
Attack Scenario



Understanding the Risks

Computer Networks Have A Long History Of Intrusions

⇨ *The Computer Emergency Response Team (CERT) And Other Similar Bodies Have Averaged 3 Advisories A Month For The Past 8 Years. . .*



CA-94:15 NFS Vulnerabilities
VB-94:02 ULTRIX OSF/1 Vulnerabilities
CA-94:12 Sendmail Vulnerabilities
F-06 Novell UnixWare Vulnerabilities
VB-94:01 SCO System Software Vulnerabilities
F-07 New & Revised HP Bulletins
D-04 SunOS Security Patches
93-29 Sendmail Exploitation
CA-92-14 Altered System Binaries
92-07 Attempts to Steal Passwords
92-09 Automated TFTP Probes
92-53 UNIX System V Security Problem
92-70 Cisco Access List Vulnerability
CA-92:19 Keystroke Logging Banner
CA-92:16 VMS Monitor Vulnerability
DDN05 ULTRIX 3.0 BREAK-IN
CA-91:14 SGI "IRIX" Vulnerability
C-21 AIX REXD Daemon Vulnerability
A-1 UNIX TFTP Attacks
A-22 Hacker/Cracker Attacks

Understanding the Risks

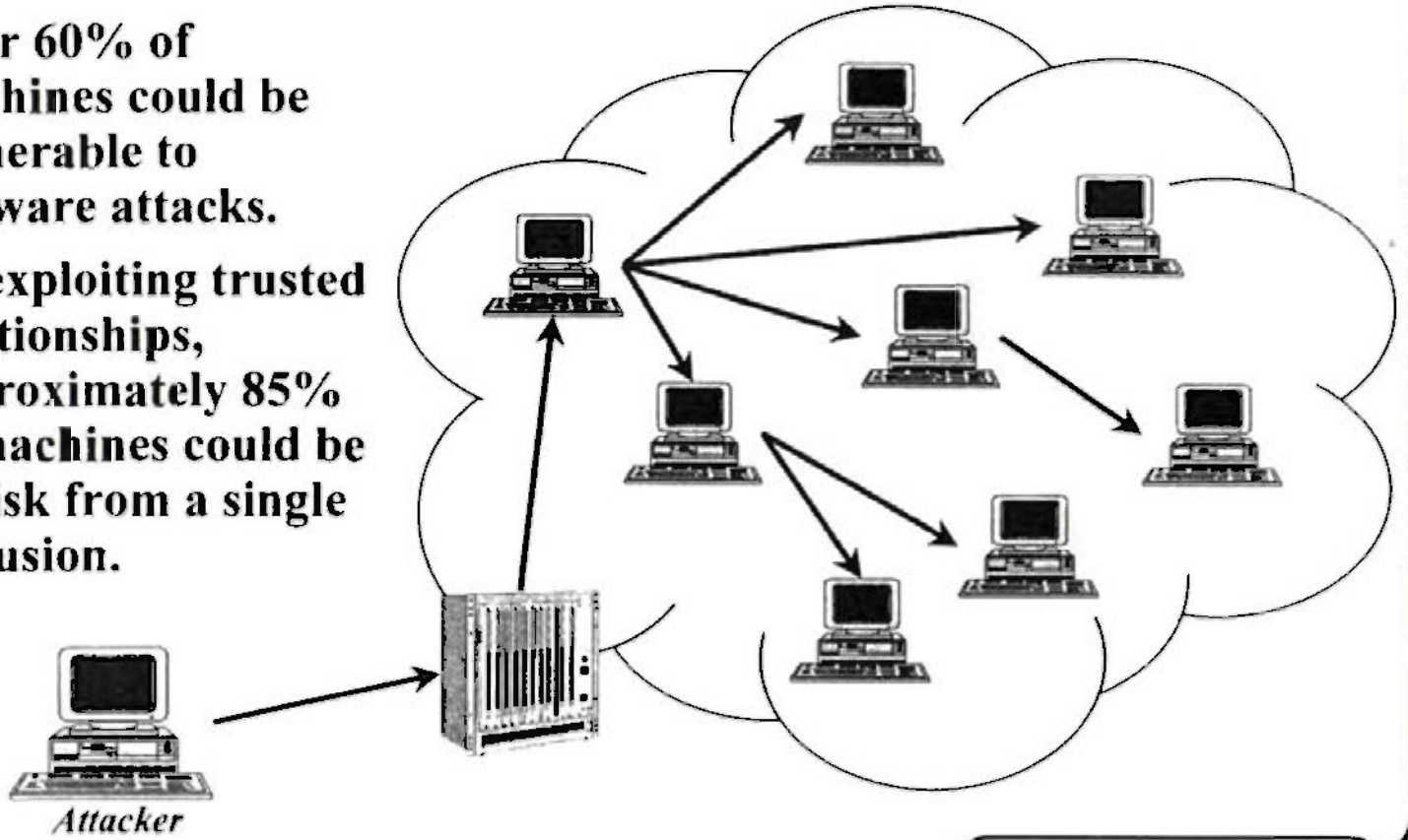
The Internet Security "Dirty Dozen"

• Trusted Host Relationships	"+" in .hostequiv file
• Network File System	World readable/writable
• Xwindows Vulnerabilities	Keystroke capture
• Rexec/Rexecd	Remote execution without authentication
• TFTP	Access without authentication
• FTP Servers	Default login/password on PCs, Macs, Novell
• Anonymous FTP	Check for writable areas, encrypted password file
• Ybind/Ypserv	Domain name server weaknesses
• Default Logins	bin, lp, guest, sysadm, demo, ftp, root, field
• Weak/Null Passwords	Easily guessable, null passwords
• CGI Script Vulnerabilities	Web server vulnerabilities
• Sendmail	A new vulnerability every week!

Understanding the Risks

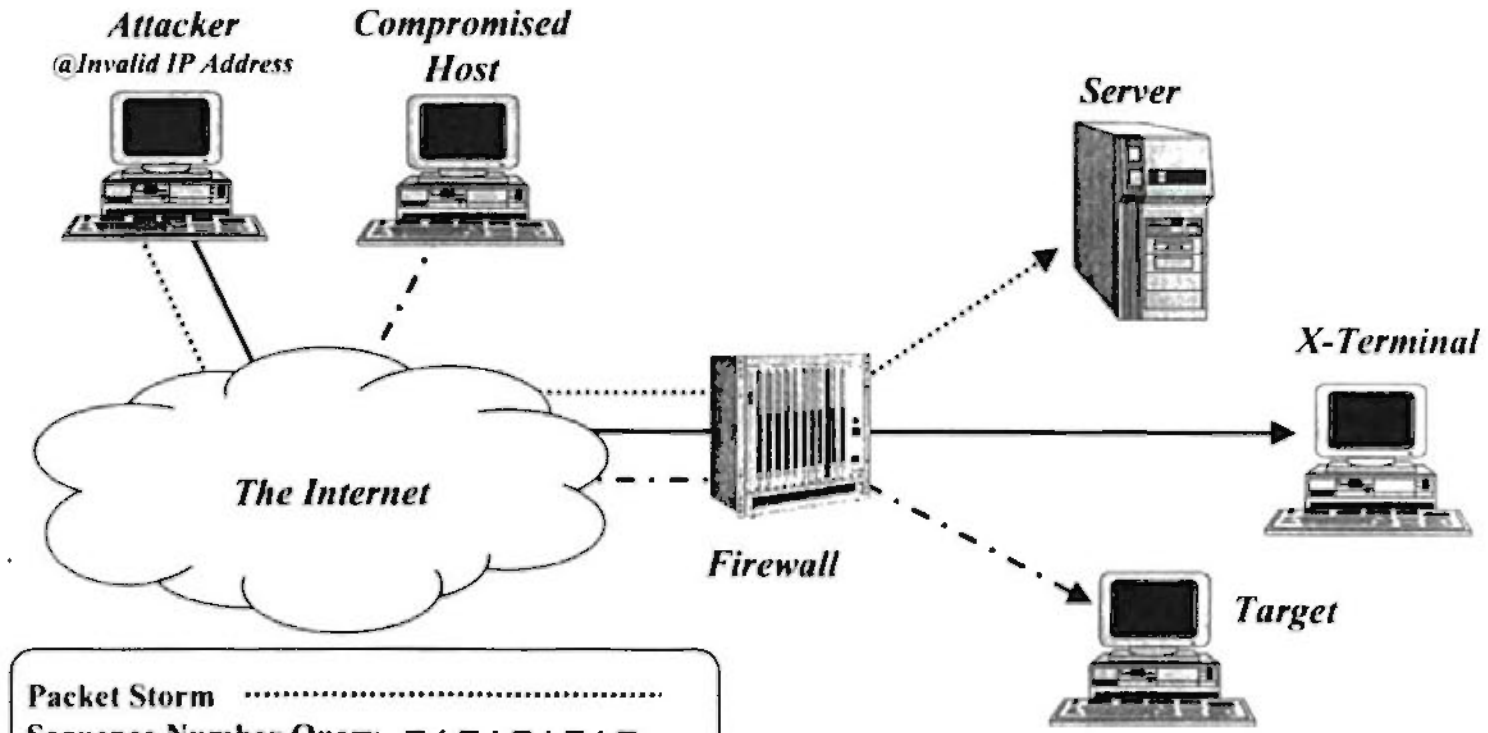
Exploitation Of Trusted Relationships

- Over 60% of machines could be vulnerable to software attacks.
- By exploiting trusted relationships, approximately 85% of machines could be at risk from a single intrusion.



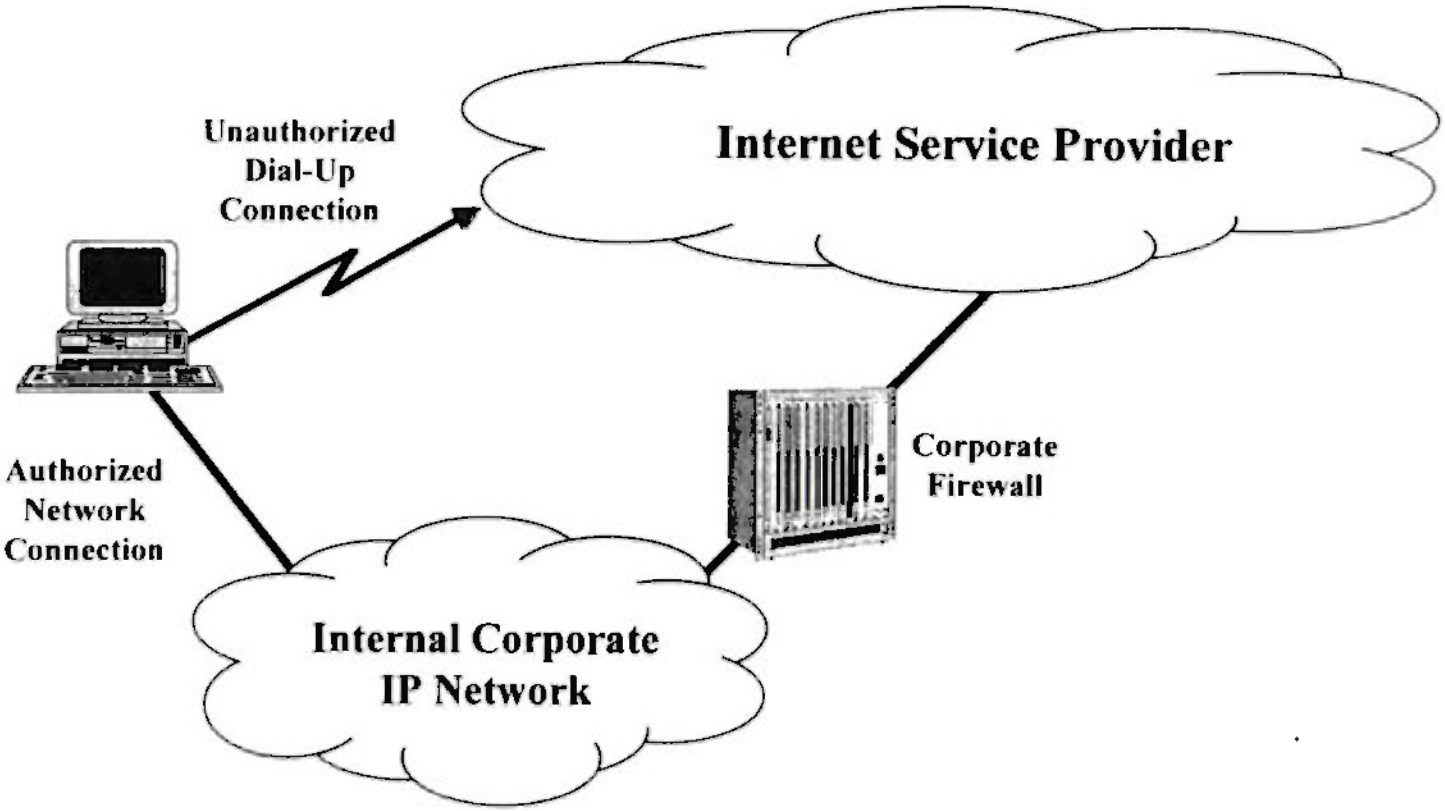
Understanding the Risks

The IP Spoofing Attack



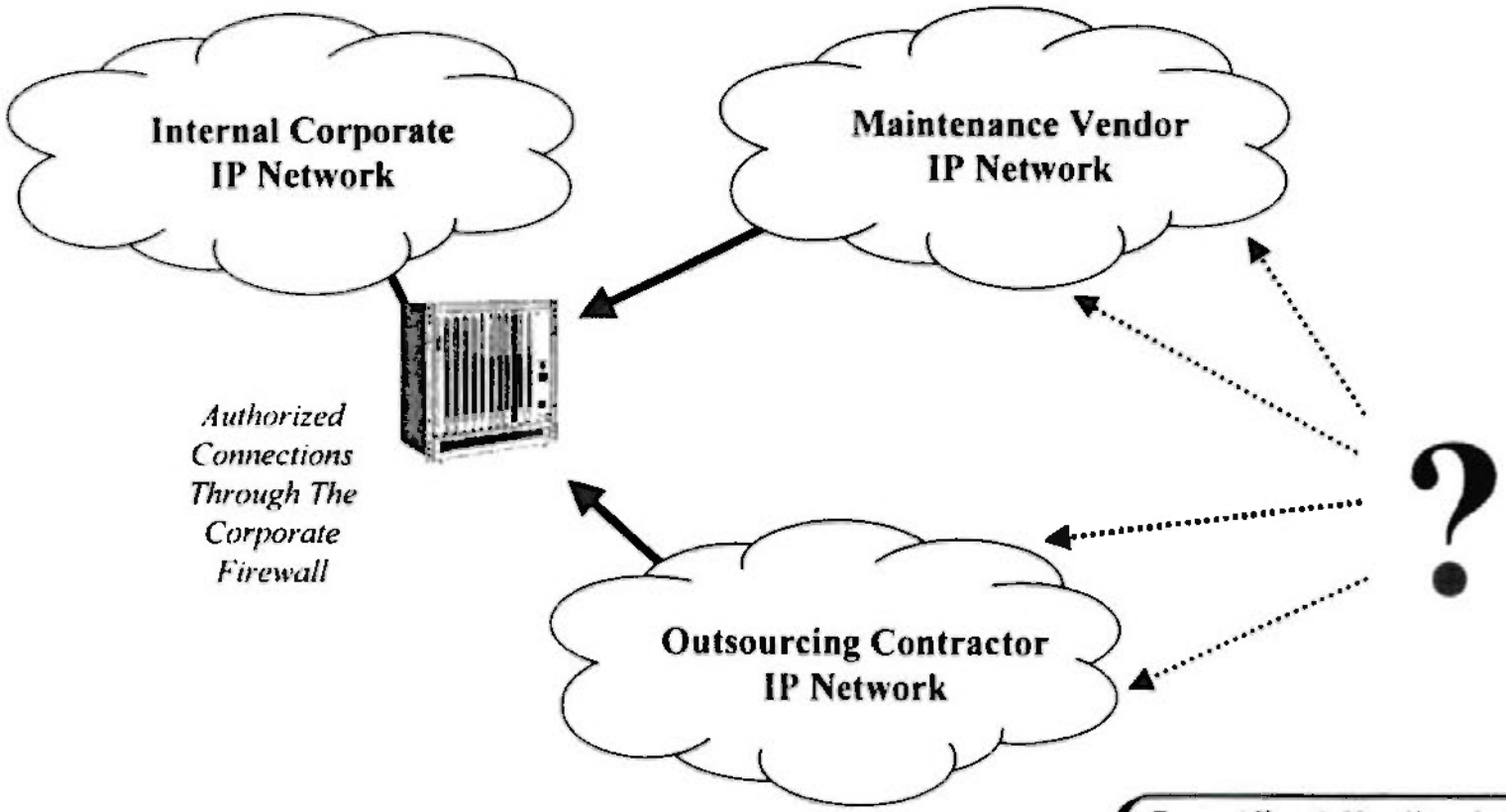
Understanding the Risks

Network Configuration Issues

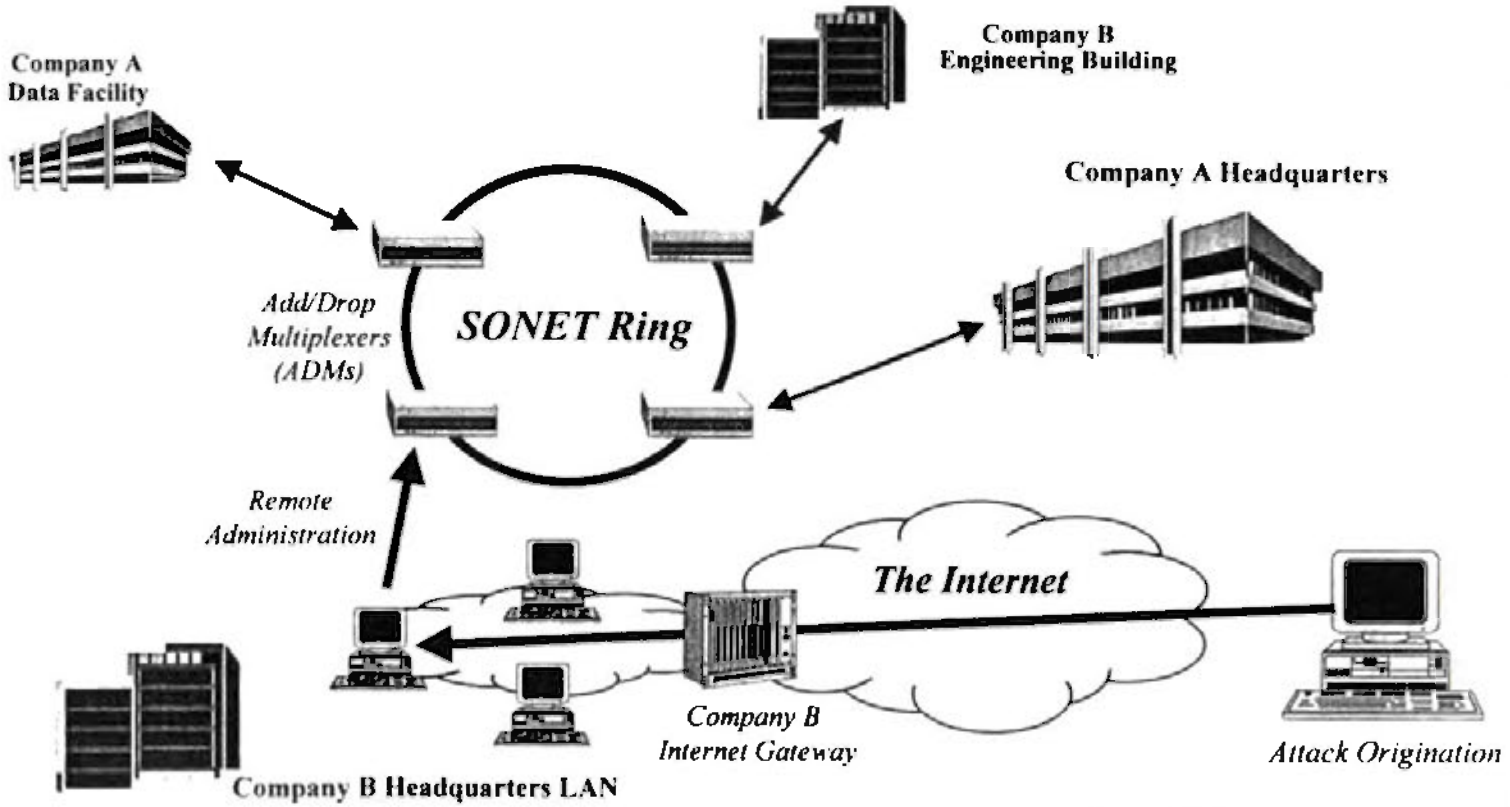


Understanding the Risks

Outsourcing And Vendor Issues

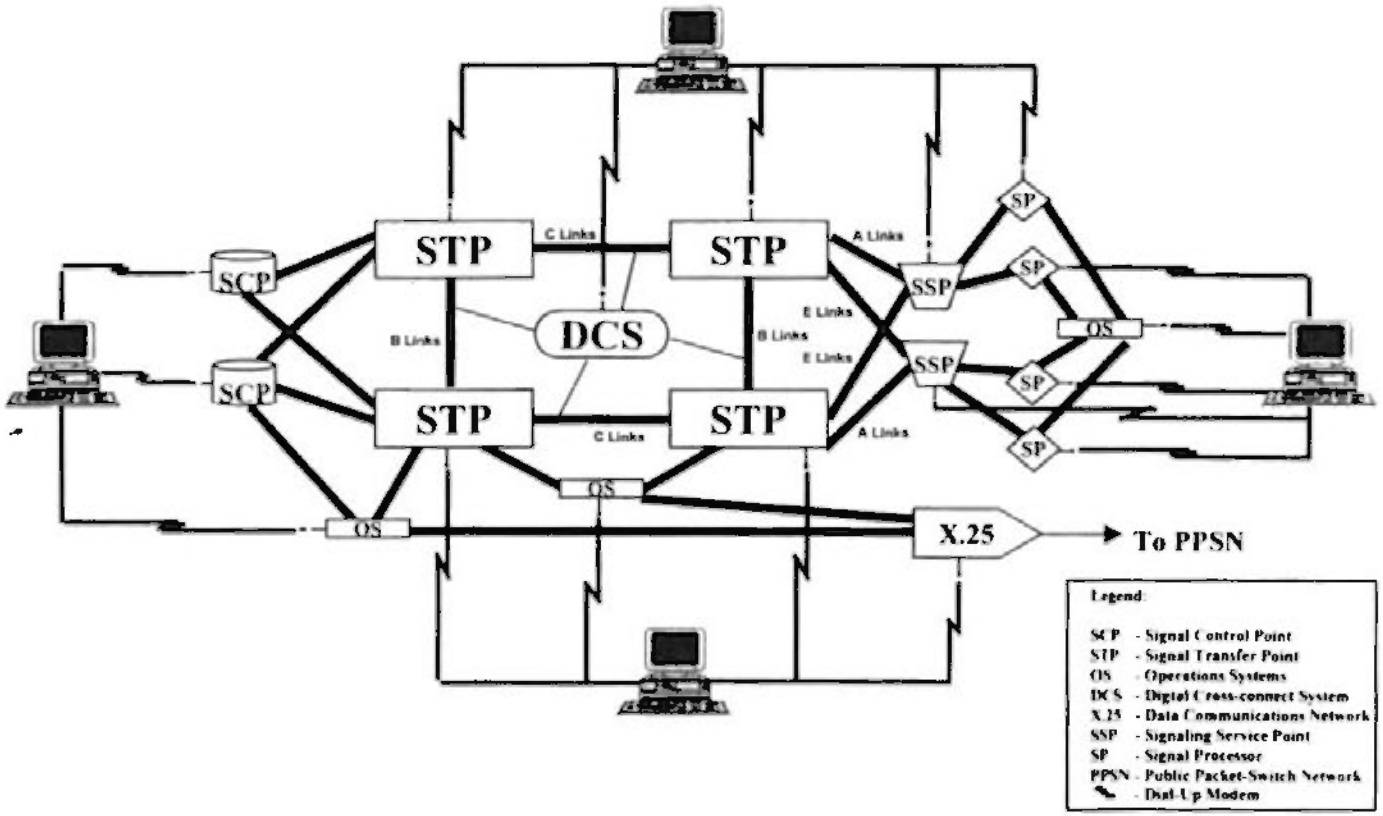


SONET Vulnerabilities



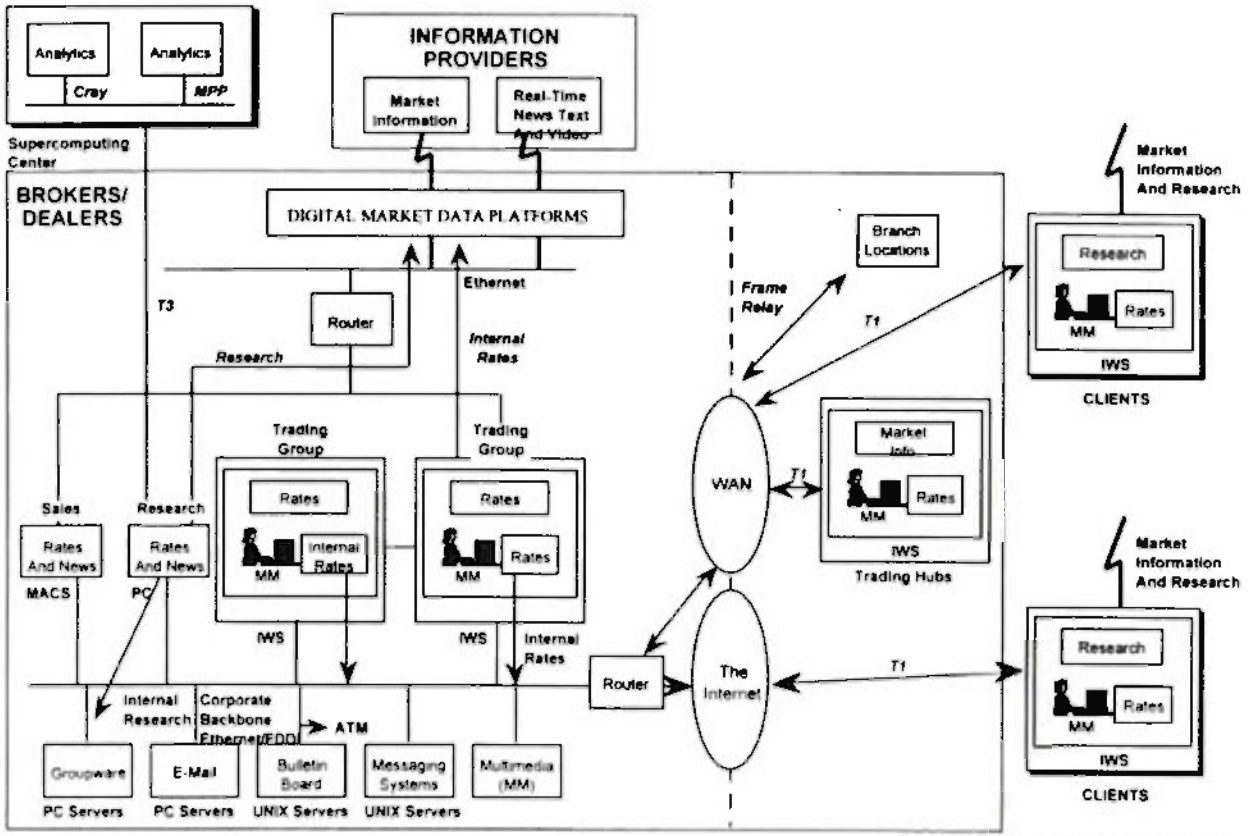
Understanding the Risks

Signaling System 7 (SS7) And Intelligent Network Vulnerabilities



Understanding the Risks

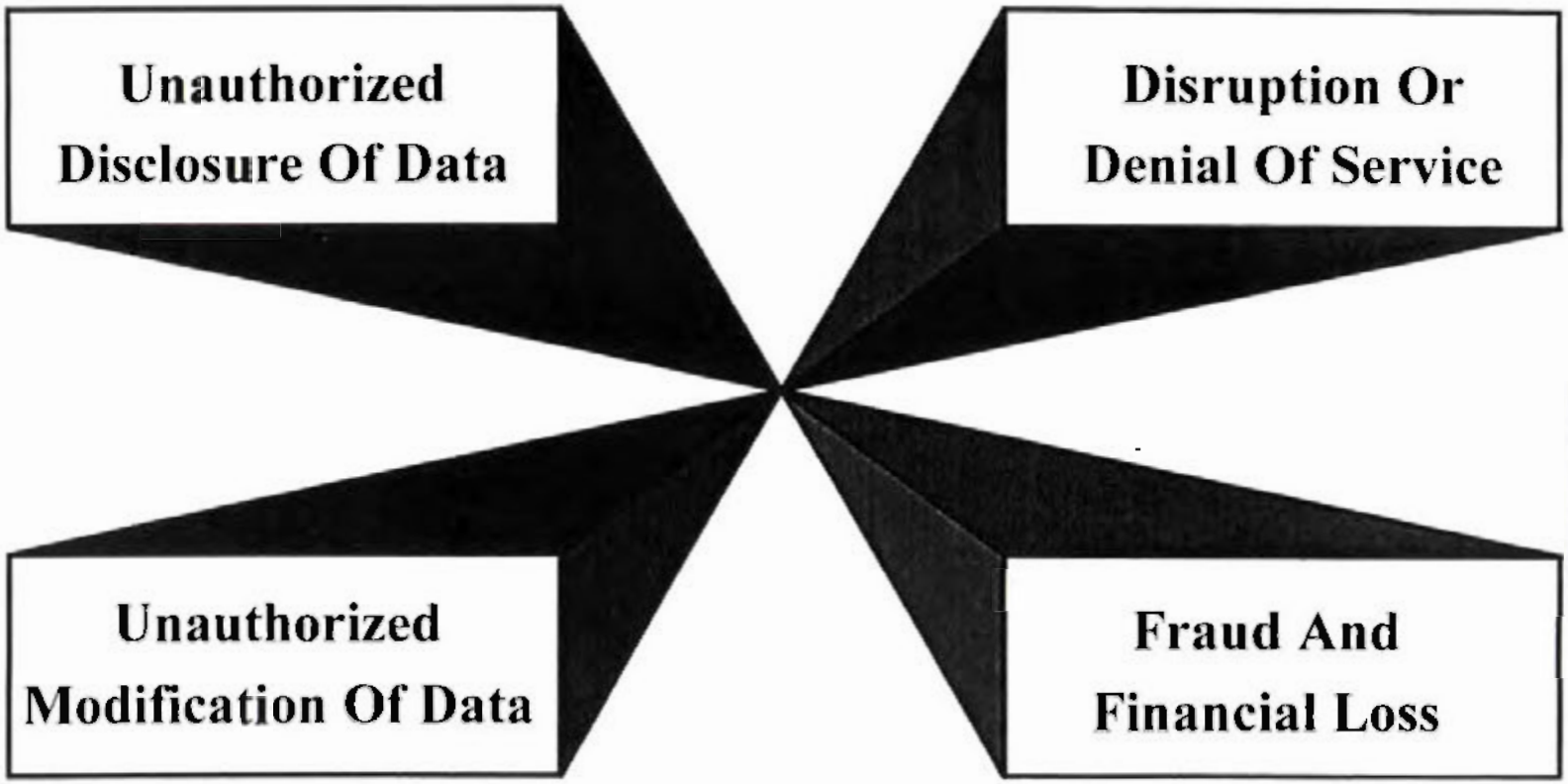
Financial Systems Are Completely Dependent On Networks



THREATS AND CASE HISTORIES

Threats And Case Histories

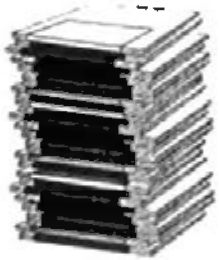
The Primary Threats To Network Technologies



Hacker Toolkits

Include:

- Highly targeted, custom scripted attacks
- Automated attack tools
- Sophisticated surveillance & data gathering tools
- Offensive use of network management tools
- Complex stealth & evasion techniques
- Password cracking tools
- Network element attack techniques



Case Histories

- Masters Of Deception (MOD)
- Kevin Poulsen
- Kevin Mitnick
- Legion Of Doom (LOD)
- The Posse And Internet Attacks
- Shadowhawk

+ Countries With Significant Hacker Activity

Masters Of Deception (MOD)

- Developed And Unleashed "Programmed Attacks" On Telephone Company Computers
- Monitored Data Transmissions On Packet Data Networks
- Created New Telephone Circuits And Add Services With No Billing Records
- Changed An Adversary's Long Distance Carrier To Illegally Obtain Calling Records
- Sold Passwords, Access Codes, and Other Illegally-Obtained Information
- Destroyed Data In Computer Systems

Threats And Case Histories

Kevin Poulsen

aka "Dark Dante"

Allegedly. . .

- **Hacked Into Phone Company Computers Hundreds Of Times**
- **Used Stolen Access Codes To Access Government Information And Sold Access Codes For Money**
- **Compromised Several Ongoing Law Enforcement Investigations**
- **Eavesdropped On Telephone Company Investigators**
- **Sold Untraceable, Unbilled Circuits To Criminals**
- **Illegally Entered Telephone Company Offices And Stole Data And Equipment**

Threats And Case Histories

Kevin Mitnick

aka "Condor"

Allegedly. . .

- **Attacked Telephone Central Offices**
- **Stole Telco Equipment & Manuals**
- **Attacked DEC's Software Development ComputerAnd Copied Proprietary Source Code Programs For The VAX/VMS Operating System**
- **Modified This Stolen Source Code To Introduce A "Trap Door"**
- **Compromised Cellular Telephone Network Equipment**
- **Implemented IP Spoofing Attack**

Legion Of Doom (LOD)

- Planted Software Time Bombs In Telephone Switching Centers
- Corrupted Pointer Tables In Signaling Switches

- Changed Circuit Routing Tables In Traffic Switches
- Electronically Eavesdropped On Telephone Conversations
- Traded Stolen Credit Card Numbers, Calling Card Numbers, And Computer System Information

The Posse And Internet Attacks

Allegedly. . .

- **Attacked Internet With "Sniffer" Programs Designed To Record Login IDs and Passwords**
- **Penetrated The Primary Internet Backbone Networks**
- **In First 6 Months, Sniffer Programs Were Discovered On Over 500,000 Internet Hosts—The Number May Now Be Over 1 Million**
- **Individual Sniffer Programs Have Captured Over 40,000 Passwords Per Day**
- **The Sniffer Is Now Part Of The Standard Hacker Toolkit, Along With Scanner Programs And The "Rootkit" Software**

Shadowhawk

- Illegally Copied The 5ESS Switching System Source Code Valued Between $28,000 And $40,000
- Illegally Copied Source Code Files Worth Over $1 Million
- Attacked A Telephone Carrier's Computers And Installed A "Trap Door" Password Allowing SysAdmin Access
- Accessed A Military Computer And Destroyed Diagnostic Files Reflecting The Operation Of The Military Base's Communication System
- Published Entry Codes To 27 Computers As Well As Legitimate Names, Telephone Numbers, Account Names, And Passwords

Threats And Case Histories

Countries With Significant Hacker Activity *

- Netherlands
- England
- Germany
- Belgium
- France
- Austria
- Sweden
- Switzerland
- Malaysia
- South Africa
- United States
- Canada
- Brazil
- Israel
- Australia
- Italy
- Greece
- Korea
- PRC
- Japan
- Hungary
- Czech Republic
- Bulgaria
- Russia
- Belarus
- Turkmenistan
- South Africa
- Spain
- Philippines
- Argentina

* Based On Unclassified Open Source Information

STRATEGIES TO REDUCE YOUR RISK EXPOSURE

Conclusions

- → All Aspects Of Worldwide Communications Networks Are At Risk From Electronic Intruders
- → Electronic Intrusions Are Escalating In Frequency & Severity
- → New Technologies And Other Industry Trends Are Increasing Risks To Both End Users And System Operators

Risk Management

- **Risk Can Not Be Eliminated Entirely, But It Can Be *Effectively Managed***
- **Your Risk Exposure Can Be Dramatically Reduced By Developing and Implementing An *Organizational Security Strategy***
  - **Organizational Security Policy**
  - **System Specific Security Policies**
  - **Detailed Seeurity Procedures**

- **Your Security Posture Should Reflect Management's Position On Security *Costs and Benefits.***

Risk Can Be Reduced By Implementing New Procedures

- Establish Security Awareness Programs
- Improve Security Staff Skills
- Perform Regular Security Audits
- Control Proprietary Information
- Use Existing Security Features In Equipment
- Implement Dial Access Control
- Identify and Close Security "Holes"
- Design & Implement A Security Architecture
- Implement Advanced Security Technologies

Less Complex

More Complex

Inventing an Experimental System for National Level Indications and Warning for Information Warfare

Presented By

LT Sean Heritage, USN, JCS/J-2J

8 April 1997

A Notional System

"The following is an editorial program. The opinions expressed herein are not necessarily those of J2, DIA or the Joint Staff."

"The following broadcast is not to be used for commercial purposes without the express written permission of the Baltimore Orioles and Major League Baseball."

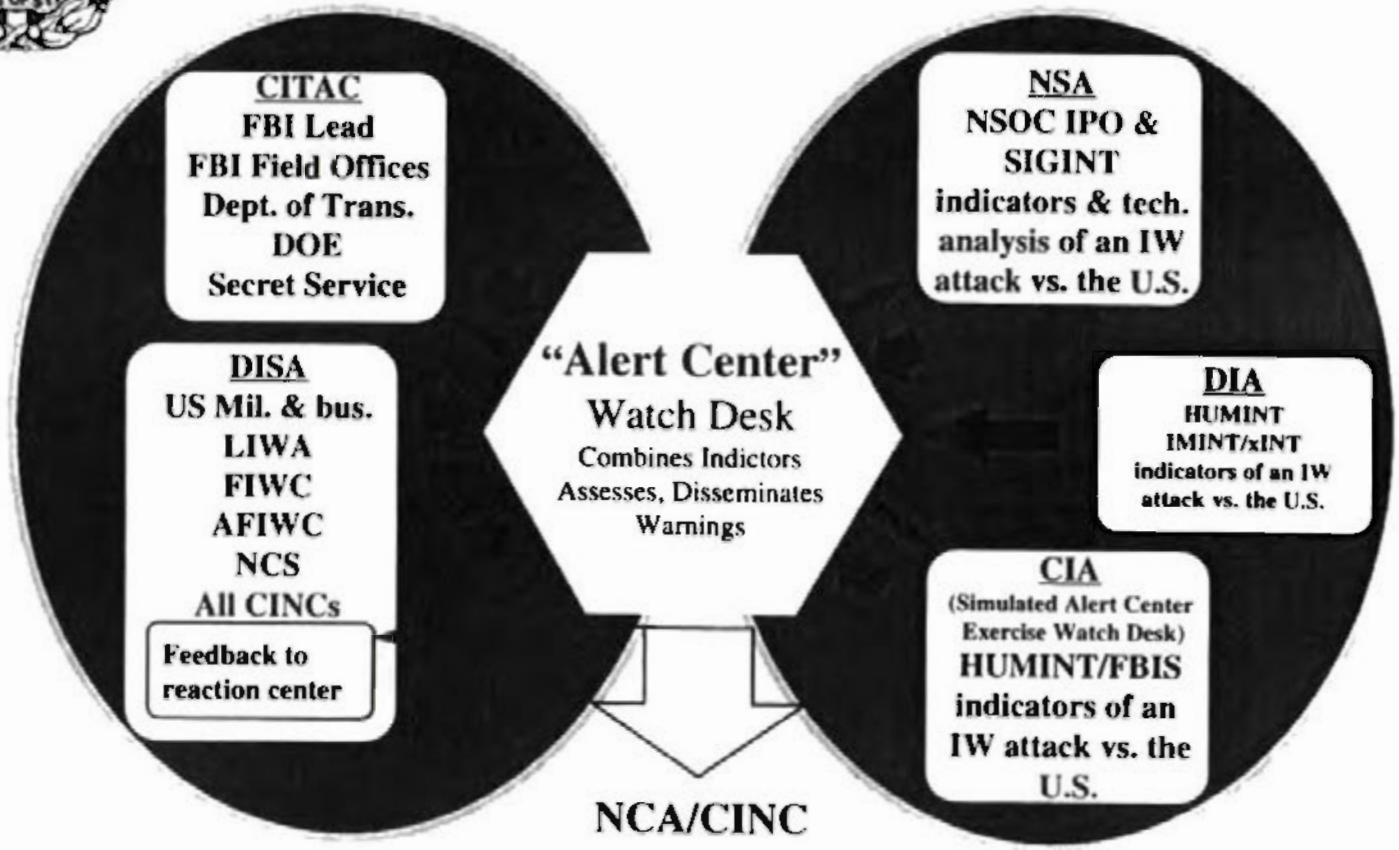
CONOPS for War Game

- **Identified as shortcoming for ES-96**
- **Requested by ACOM/J-38 for ES-97**
- **Must cover all areas of IW**
  - **Network Attack**
  - **C2W: PSYOP, Deception, OPSEC, EW, Kill**
- **Neither IW nor I&W**
- **Indications of Attack**
  - **Piecemeal**
  - **After-the-fact**

Sources & Models

- OSD I&W for IW Study
- DSB Study
- NSR Study for NCS
- Interviews with existing agencies
- Terrorism desk in JCS Alert Center
- NORAD, USSPACECOM SPADOC

I&W for IW Attack
Experimental Construct for EW-97



I&W for IW Products

- **IW Indicators List**
  - **Country & threat specific**
  - **A tickler list based on threat nation capabilities**
- **Threatcons**
  - **Estimate of foreign-based threat**
  - **Uses six classes of IW attack**
  - **Modeled after Terrorism and I&W Lists**
- **Country Specific Threat Library**

I&W for IW Output

- Summary of key events
- Status of the infrastructure
- Fusion of pieces
  - Disparate
  - Inner-look sources from CONUS
  - Outer-look sources from military intelligence
- Threatcons
  - Advanced warning
  - Evaluate size & intent
  - Evaluate country of origin

Information Warfare - Defense

Incident Classifications

and

Watch Conditions (WATCHCONs)

Class I IW Incidents - Privacy Invasion

Class I IW incidents are characterized by computer intrusions and attempted intrusions from a variety of sources which essentially invade the privacy of individual or organizational computer users of non-classified networks. Class I incidents do not include any evidence of intent to cause damage to the data or networks accessed. This could also be characterized as low-level computer, "hacking." These incidents could come from either domestic or foreign sources.

Class II IW Incidents - Commercial/Industrial Espionage

Class II IW incidents are characterized by concerted attempts or actual penetrations of commercial computer systems to gain unauthorized access to specifically targeted or sensitive information for the purposes of obtaining that information. Class II incidents do not include any evidence of intent to cause damage to the data or networks accessed. These incidents could come from either domestic or foreign sources.

Class III IW Incidents - Military/Government Espionage

Class III IW incidents are characterized by concerted attempts to penetrate, or actual penetrations of military or government computer systems to gain access to and/or steal classified information. Class II incidents do not include any evidence of intent to cause damage to the data or networks accessed. These incidents could come from either domestic or foreign sources Intrusions into unclassified government networks containing sensitive data falls under this category when evidence of foreign involvement or specific targeting is present.

Class IV IW Incidents - Low Level PSYOP/Deception Programs

Class IV IW incidents are characterized by persistent, long term, low level PSYOP or Deception programs which occur at times of mildly increased tension between the United States and an adversary. Typically they include the increase in news items which are favorable to the adversary nations. The original source of these news items may be very difficult to determine

Class V IW Incidents - Commercial Terrorism

Class V IW incidents are characterized by penetrations or concerted attempts to penetrate the computer systems of commercial businesses in an attempt to electronically destroy or degrade those systems or to threaten to destroy computer systems in order to extort money. These incidents could come from either domestic or foreign sources.

Class VI IW Incidents - Civilian and Governmental Infrastructure Terrorism and Attack

Class VI incidents usually occur during a time of impending or ongoing crisis with a foreign power. They can include foreign, state-sponsored PSYOP, Deception, Electronic Warfare against and physical sabotage (destruction) of non-military U.S. government information systems. Class V incidents may also include attacks against the computer systems of key civilian or non-DoD governmental organizations which operate critical elements of the U.S. infrastructure. Those computer attacks may include destructive or degrading electronic codes and viruses or the insertion of false data.

Class VII IW Incidents - Military Infrastructure Terrorism & Attack

Class VII incidents usually occur during a time of impending or ongoing crisis with a foreign power. They can include confirmed foreign, state-sponsored PSYOP, Deception, Electronic Warfare against and physical attack or sabotage (destruction) of U.S. military information systems. Class VII incidents also may include attacks against the computer systems of military organizations which operate critical elements of the U.S. military support structure. Those computer attacks may include destructive or degrading electronic codes and viruses or the insertion of false data.

WATCHCON 5 - Operations Normal

No significant IW events. No significant rise in the numbers of small, isolated IW events. May be characterized by a normal level of Class I events.

WATCHCON 4 - Slight Rise In IW Events.

A slightly larger than normal number of IW events have occurred. No significant events which cause major system damage, outages or losses. No correlation of IW events to foreign governments. Characterized by a statistically significant rise in the overall number of Class I events. May also be characterized by suspected Class IV PSYOP or deception events.

OR

A significant IW event has occurred, but purposeful intent vice accidental happenstance cannot be confirmed. May be characterized by a Class II event or events.

WATCHCON 3 - Significant Increase In IW Events.

A significant, confirmed IW event has occurred which causes or has the potential to cause major damage, outages or losses to the U.S. government, military or business. May or may not be accompanied by a slight increase in the number of IW events. No correlation of this major IW event to foreign governments. May be characterized by a rise in the number of Class II, Class III, Class IV or Class V events

WATCHCON 2 - Significant Increase In Attributable IW Events.

A significant, confirmed IW event/s has/have occurred which causes or has the potential to cause major damage, outages or losses to the U.S. government, military or business. This event or events are possibly, or probably correlated to the purposeful activity of a foreign government The overall number of attributable and non-attributable IW events have increased. Characterized by an increase in the number of Class III, Class IV and Class V events. Also characterized by the confirmation of initial Class VI and/or Class VII events being launched by a foreign power. May also be characterized by an increase in the number of Class III and Class IV events.

WATCHCON 1 - Broad Scale, Attributable IW Attacks.

Significant, confirmed IW events have occurred and are occurring. A number of the events are attributable to a hostile, foreign power. The foreign power initiating the events is also involved in hostilities or crisis confrontation with the United States in other political, international or military arenas. Characterized by a large number of Class IV, Class V, Class VI and/or Class VII events.

Key Definitions

Command and Control Warfare: The integrated use of operations security (OPSEC), military deception, psychological operations (PSYOP), electronic warfare (EW), and physical destruction, mutually supported by intelligence, to deny information to, influence, degrade, or destroy adversary command and control capabilities, while protecting friendly command and control capabilities against such actions. Command and control warfare applies across the operational continuum and all levels of conflict.

C^2 Attack: Prevent effective C^2 of adversary forces by denying information to, influencing, degrading or destroying the adversary C^2 system.

C^2 Protect: Maintain effective command and control of own forces by turning to friendly advantage or negating adversary efforts to deny information to, influence, degrade, or destroy the friendly C^2 system.

Command and Control: The exercise of authority and direction by a properly designated commander over assigned forces in the accomplishment of the mission.

Computer Network Attack (CNA): Operations to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves.

Counterinformation: Action dedicated to controlling the information realm.

Defense Information Infrastructure (DII): Is the shared or interconnected system of computers, communications, data applications, security, people, training, and other support structures serving DOD's local, national, and world-wide information needs. The DII connects DOD mission support, C^2, and intelligence computers through voice, telecommunications, imagery, video-and multi-media services.

Defensive Counterinformation: Actions protecting our military information functions from the adversary.

Global Information Infrastructure (GII): An interconnection of communications networks, computers, databases, and consumer electronics that makes vast amounts of information available to users. It encompasses a wide range of equipment including cameras, scanners, keyboards, fax machines, computers, switches, compact disks, video and audio tape, cable, wire, satellites, optical fiber transmission lines, microwave, nets, switches, televisions, monitors, printers, etc. The GII includes more than the physical facilities used to store, process, and

display voice data, it also includes the personnel who operate and consume the transmitted data.

Information: Facts, data or instructions in any medium or form.

Information Assurance: IO that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.

Information Attack: Directly corrupting information without visibly changing the physical entity within which it resides.

Information Environment: The aggregate of individuals, organizations, or systems that collect, process or disseminate information, also included is the information itself.

Information Function: Any activity involving the acquisition, transmission, storage, or transformation of information.

Information Operations: Actions taken to affect adversary information and information systems while defending one's own information and information systems.

Information Superiority: The capability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same.

Information System: The entire infrastructure, organization, personnel, and components that collect, process, store, transmit, display, disseminate, and act on information.

Information Warfare: Information Operations (IO) conducted during time of crisis or conflict to achieve or promote specific objectives against a specific adversary or adversaries.

Information Warfare - Defense: Protecting the National Information Infrastructure and the Defense Information Infrastructure and interrelated CONUS infrastructures against physical and electronic attacks and ensuring the availability of those infrastructures for commercial and military use.

Military Information Function: Any information function supporting and enhancing the employment of military forces.

National Information Infrastructure (NII): The NII mirrors the GII but is focused on national instead of global networks and systems.

Offensive Counterinformation: Actions against the adversary's information functions.

Special Information Operations (SIO): Information Operations that by their sensitive nature, due to their potential effect or impact, security requirements, or risk to the national security of the U.S., require a special review and approval process.

INFORMATION SECURITY TECHNOLOGY AND TRENDS

presented to

The National Commission on Restructuring the Internal Revenue Service

March 13, 1997

prepared by

Joseph Mahaffee
Booz·Allen & Hamilton Inc.
8283 Greensboro Drive
McLean, VA 22102

Edward Rothenheber
Booz·Allen & Hamilton Inc.
8283 Greensboro Drive
McLean, VA 22102

Acknowledgments

Special thanks to:

Armando Gomez and Chuck Lacijan for providing Booz·Allen & Hamilton Inc. the opportunity to brief The National Commission on Restructuring the Internal Revenue Service

Melissa Hathaway for establishing contact with the information security staff at Booz·Allen & Hamilton Inc. and facilitating the opportunity for the authors to present their views on information security technology and trends

Deborah Banning, Rich Dean, Joanne Evans, Dale Hapeman, Stuart Moore, Mike Otten, and Tom Russell for their technical contributions

INFORMATION SECURITY TECHNOLOGY AND TRENDS

BACKGROUND

More than ever, the national security departments and agencies, are being challenged to provide affordable, interoperable, and evolutionary network security solutions in a timely manner. Over the last few years, they have recognized the dramatic benefits offered by the highly interconnected information systems as illustrated by our nation's dependence on them in all facets of society. However, they also recognize that these systems have the effect of exposing our national information systems to the borderless threat of Information Warfare (IW). So while changes in the political climate have reduced some mission threats, new threats are emerging within the networked world.

Over the past year, it has become a weekly or even daily routine to hear about successful attempts of hackers to break into networks from around the world with the intent of eavesdropping, modifying, spoofing, or disrupting the information systems and/or the information that they process and store. Of course, for any Department of Defense (DoD), Federal, or commercial security system, the ultimate objective is to prevent unauthorized disclosure or undetected modification of user information and system resources while ensuring the availability of the system to authorized users. Typically, the national security departments and agencies use six security services, as shown below, to achieve this objective:

- **Confidentiality** - Ensures the privacy of the information and prevents an unauthorized third party from reading the data.
- **Integrity** - Ensures that the system configuration, application software, and associated data have not be modified or destroyed.
- **Authentication** - Ensures that the person or system with whom you are exchanging information, is in fact the person or system they claimed to be.
- **Non-repudiation** - Provides positive confirmation that an action took place.
- **Access control** - Limits access to the system and its data to those who are authorized.
- **Availability** - Ensures the system or information is available when needed.

Any of these services may be implemented by physical, administrative, procedural or electronic mechanisms. Often, a combination is employed. From a practical perspective, many of the security services can be implemented with cryptographic products. In fact, the same cryptographic product can be used to encrypt the data, authenticate the user, maintain data integrity with digital signatures, and support system availability. Trusted security products can also support many of the security services, except for confidentiality. However, trusted security products are more expensive and trusted technology is relatively immature. Given cryptographic products are more readily

available and inexpensive than trusted products, they appear to offer a more reasonable set of solutions for the IRS and other Federal communities.

The assurance provided by any of the security services previously mentioned can be ascertained by determining the strength and correctness of the mechanism that provides the service. For physical, administrative, and procedural mechanisms, the assurance level is determined by reviewing the processes that are implemented. For electronic mechanisms, empirical or exhaustive techniques are generally used. In recent weeks, the news media reported that a high school student required only three hours to successfully "break" a 40-bit code cryptographic algorithm. For cryptographic devices, the assurance level or strength is largely dependent on the length of the codes used in the algorithm. In national security applications, where classified information is processed, or in Federal and Commercial applications where privacy is a major concern, higher assurances levels are required, which necessitates the use of longer codes.

The successful application of security services and mechanisms requires security management support for the overall operational environment. Specifically, security management includes the distribution, collection, and analysis of management information (e.g., cryptographic keys, audit data, registration data) for the security services and mechanisms. One of the primary issues noted with the implementation of security management functions concerns the distribution of security management responsibilities across multiple security administrators. For example, one person may be responsible for monitoring the firewall and a second may be responsible for administering the web site. Case studies have shown that hackers often attempt to penetrate multiple points in a network. Unfortunately, news of a potential attack at one point is not always communicated to the other system administrators whose systems may also be under attack. This example highlights the need for the IRS and all defense, civil, and commercial organizations to implement a coordinated security management approach.

TRENDS AND TECHNOLOGIES

From the perspective of the national security departments and agencies, it is obvious that the "groundrules" have changed dramatically over the past decade with respect to defining and fielding security solutions. These changes are being driven by several major paradigm shifts in the public and private networking world, and within the DoD and Intelligence communities as shown below:

- Rapid evolution of information technology and systems
- Explosive growth of the Internet
- Evolution from "stovepipe" to open, integrated, multimedia systems
- Increasing public and commercial awareness and concern over network and information security
- Increasing availability and compatibility of commercial network products and solutions

- Transformation from requirements driven to market driven solutions
- Evolution from risk avoidance (absolute security) to risk management (adequate or appropriate security)
- Migration from standalone "Black Boxes" to integrated system security solutions
- Transformation from product development to customer service orientation
- Migration from stand-alone systems connected by point-to-point links to networked systems
- New emphasis on security for "sensitive but unclassified (SBU)" applications, in addition to classified applications
- Unprecedented downsizing, staff turnover, and budget reduction

Two obvious challenges that the national security departments and agencies are facing as a result of these paradigm shifts are: 1) keeping pace with rapidly evolving technology and a rapidly emerging network security market in which future directions are sometimes unclear, and 2) continuing to improve system security processes and procedures that reflect more of a commercial orientation.

In general, the national security departments and agencies are responding to these changes by placing more emphasis on:

- Establishing new policies, procedures, and criteria that will adequately address the changing threat environment and yield consistent and reliable security solutions
- Developing security architectures and generic security solutions that may be tailored to meet specific applications
- Defining security standards and protocols that can be integrated into commercial standards and protocols
- Fielding currently available security products and tools that will help them "close the front doors" to their networks and optimize system performance
- Evaluating and using commercial off-the-shelf (COTS) products and systems

In the following paragraphs, we will discuss the efforts being pursued and how they may be applied to the IRS applications.

DEFINING POLICIES, PROCEDURES AND CRITERIA: In the post-cold war environment, defense budgets have continued to decline. As such, the notion of perfect security is being replaced with that of affordable security and user assumed risk. This change, more than any other, is driving the security analysts to develop and apply improved security analysis procedures, tools, and methodologies that can effectively deal with the complexity of modern information systems and provide balanced, cost-effective security solutions.

One of the biggest challenges for the defense, civil, and commercial communities is to develop and implement policies and business processes that are in many ways equivalent or better than existing processes. In general, security technology is available or

will be available in the very near future. The real challenge is to integrate those technologies in the context of the business processes. To do this, most effectively, the IRS will have to examine their current policies and processes from an information perspective, define a set of security policies and requirements based on the information content, develop a security strategy that takes into account their existing system architecture and their desired system capabilities, and define a migration plan given the current and future availability of security technology. Achieving a common view on security as it relates to the IRS business processes will be paramount, particularly when considering taxpayer trust and acceptance.

Information engineering will be the key for successful integration of security services into any information system. In this process, it is most important for the "owners" of the information to establish the system requirements, including general requirements for security. The security analyst can then work with the system designers and administrators to define the appropriate security solutions, based on information content and business practices.

DEVELOPING SECURITY ARCHITECTURES: A system security architecture is a means for describing the structure and organization of the security aspects of an information technology system or application. It provides a conceptual means to grasp how a large, complex system will be made secure without unduly constraining the actual implementation. By defining the security services and functions that must be provided and the relationship between these security services and functions, the system security architecture provides a foundation for designing and building systems within common structures, using consistent standards. This approach promotes interoperability, commonality of security solutions, and a thorough understanding of how system security is being provided. The DoD has successfully applied this approach in the development of their security architectures (e.g., Defense Message System and the Defense Information System Network).

As the IRS systems and networks continue to evolve, it will be important that a comprehensive information technology and security strategy be developed from which a system security architecture could be defined. Additionally, it will be increasingly important to model the system architecture in an effort to predict performance issues associated with integrating security services into the network and scaling the network size to meet user (i.e., the taxpayer) demands. Developing and modeling the security architecture will allow the IRS to focus on the information content and consistently implement security solutions throughout the networks and systems. The IRS should leverage the results of current security architectures (e.g., Target Security Architecture for the Defense Information Infrastructure [DII]) developed for the DoD, as appropriate. Doing so will promote compatibility between the Defense Information Infrastructure and the National Information Infrastructure.

DEFINING SECURITY STANDARDS AND PROTOCOLS: The national security organizations have made a conscious decision to limit the development of

custom products and systems, in favor of using commercial off-the-shelf (COTS) hardware and software. To ensure the COTS products incorporate appropriate security services that meet their needs, the Government is placing a significant amount of energy into the definition and development of security standards and protocols. Specifically, the DoD is working directly with the national and international standards bodies, such as the Internet Engineering Task Force (IETF) to influence future standards and protocols, with respect to key management and other security services. Additionally, they are working with several product vendors and service providers, such as RSA, Netscape, and Microsoft to name but a few, to collaborate on the development of security protocols that will be implemented in their respective offerings. By doing so, they have taken the burden off the Government to supply their customers with specific security products. Instead, they have created a market that will promote interoperability and competition for security products and services that may be employed in IRS and other Federal applications.

FIELDING PRODUCTS AND TOOLS: Many security products have been developed to provide security services and to meet threats to information systems and data. These products range from those narrowly designed to provide a specific service, such as encryptors, to more general products, such as firewalls, which can be configured to provide a variety of services. The products themselves can be loosely grouped into the following classes:

- **Firewall:** A firewall is used to protect a network from another untrusted network (e.g., Internet). Its main purpose is to control access to or from a protected network. Firewalls shield a network from protocols and application services that can be abused from hosts outside the shielded network. Firewalls can generally be configured to meet a user's specific requirements. For example, many firewalls maintain access control lists to identify users who are allowed to enter or exit through the firewall. The range of capabilities of firewalls varies by product and user needs, so care must be taken to select a firewall that meets the operational requirements. Organizations throughout the Department of Defense (DoD) are deploying firewalls to protect their enclaves from attacks launched from the Internet and even from their connections to the Defense Information System Network (DISN). For IRS applications, where users and third parties login and access the IRS Web site, it may be appropriate to consider implementing multiple firewalls or a single firewall with multiple ports that will permit the establishment of public and private (IRS) information domains. Most organizations implement a single firewall, which provides some inherent protection. However, if a hacker is able to penetrate the firewall, the hacker in this scenario would have access to the private information.

- **Secure Application Packages:** Many software developers are including security features directly into their applications (e.g., e-mail, web browsers, database). For example, every computer user is familiar with being prompted to enter a

password. These application packages make good use of the network environment by distributing information repositories and allowing multiple users to access and share information. These very capabilities raise specific security concerns with respect to maintaining the confidentiality and integrity of information as it moves through the network and ensuring only authorized users have access to the information. Additionally, with recent developments in the web environment, users are downloading and executing software onto their machines without any assurance in the source or integrity of the software. This capability while facilitating the transfer of information creates additional security concerns (e.g., viruses, trojan horses). The security being integrated into these application packages presumably addresses these concerns, but the degree of protection varies from product to product. As subsequently discussed in the section concerning "Evaluating COTS Products", it would be beneficial to have an independent agent, similar to Underwriters Laboratory, evaluate and disseminate information regarding the security actually provided by a given product in a specific environment.

- **Public Key Infrastructure:** The public key infrastructure (PKI) supports public key cryptography. Public key cryptography is a special class of encryption algorithms that rely on the exchange of private and public keys between two users on a network. The private and public keys are used to generate the secret code that in turn is used to encrypt the data exchanges between the two network users. These algorithms provide inherent benefits associated with minimizing the logistical burden of having to physically distribute keys to all potential users prior to them being used. With the exception of a few secure voice applications, most of the encryption algorithms used in national security applications today do not make use of public key cryptography, simply because the technology was not available when the systems were developed. However, public key cryptography is clearly the preferred choice for future security applications, particularly given newer versions of public key algorithms will support higher transmission speeds, provide greater protection, and be more efficient.

- **Certificate Authority:** The certificate authority supports public key cryptography. The certificate authority is responsible for registering end users, defining their security privileges, and providing them with certificates that are used to support cryptographic functions. In many ways an analogy can be drawn between the PKI and acquiring a driver's license. Specifically, a driver's license is the certificate a user presents to authenticate his right to operate a car and a PKI certificate is a mechanism that can be used to authenticate a user to access and "operate" a remote computer. Carrying the analogy one step further, the Motor Vehicle Administration is responsible for verifying a driver's information, determining his/her rights to operate different vehicles (e.g., cars, motorcycles, or tractor trailers), and issuing the license. The certificate authority performs a similar operation for the user's PKI certificate.

In general, the technology associated with the certificate authority is available today, but the specific policies and procedures are still being defined and implemented by industry. Potential organizations being considered as the certificate authorities include the U.S. Postal Service and banking institutions. Assuming the IRS moves forward with a plan to implement a public key infrastructure, decisions will have to be made as to whether the IRS should use the Federal-wide certificate authority or one unique to the IRS.

- **Secure Tokens:** The most common means of identificating and authenticating a source is to use passwords. However, significant vulnerabilities have been identified with the use of passwords. Secure tokens have been developed to combat this vulnerability and to provide a more secure means of identifying and authenticating users. The most common form of a token is a card that contains information specific to a user. For example, the card can contain the user's private key, which in public key cryptography allows the user to authenticate themselves or establish a cryptographically protected communication connection across the network. The private sector and the national security communities have developed secure token systems. These systems are expected to be used more frequently for commercial and Government applications. However, the IRS will have to decide if a common token may be used for multiple applications (e.g., filing tax returns, trading stock) or if an IRS unique token would be required.

- **Network Intrusion Devices:** Network intrusion devices monitor the operation of the user's networks. For example, a network intrusion device will look at the unsuccessful login attempts. These attempts could signify that a hacker is trying to penetrate the network. Additionally, these devices can monitor the flow of information and compare it to normal operations to detect unusual activities. State-of-the-art intrusion detection devices use smart technology to analyze information exchanges in real-time and cut-off the communications link when unusual activity is detected.

EVALUATING COTS PRODUCTS: With the Government emphasizing the use of COTS products to satisfy the majority of their future needs, it is extremely important to have an understanding of all the products that are on the market and determine if the products perform as advertised. Unfortunately, most users of information technology products are unable to keep up with the multitude of security products hitting the market each day. Furthermore, the users generally do not understand the technical details with respect to how the products are configured and operated. They can only rely on information they read in brochures and journals, which often advertise the individual product capabilities, as opposed to examining the product in a system context. Evaluating security products from a system perspective is very difficult, particularly when considering the way systems and networks are customized to meet business objectives. The national security community has established programs and

initiatives to monitor the availability of COTS products, evaluate their capabilities, and make smart decisions relative to their potential system applications. A similar effort to evaluate COTS products for a broader community (i.e., Federal and commercial) would be beneficial.

SUMMARY

Once again, the basic set of security products and technologies are available or will be available in the very near future to support most known information applications. The real challenges lie in the areas of defining the policies and the business processes to take advantage of the security products and services. As appropriate, the business processes will have to change to accommodate the technologies or in some cases it may be necessary to develop a whole new set of processes. However, as with any system that attempts to automate existing business processes, the real success will be determined by the degree of trust and comfort established with the end users (i.e., taxpayers).

IW Defense Seminar - Participants

NAME	ORGANIZATION	ADDRESS	CITY	STATE	ZIP	TELEPHONE
Bigelow, Brad Mr	NCS/N53	701 S Courthouse Rd	Arlington	VA	22204-2198	703-607-6211
Blair, Randy Mr	Department of Defense Attn: C44 Suite 6704	9800 Savage Road	Ft Meade	MD	20755	410-859-6529
Boot, Brad Mr	CIA	PO Box 1925	Wash	DC	20505	703-874-0187
Callahan, Roger	ASD(C3I) (Information Assurance)	Pentagon, Room 1E151	Wash	DC	20301-6000	703-695-8705
Christy, James Mr	FBI/IPTF	9th St & Penn Ave NW	Wash	DC	20535	202-324-0345
Curtin, Mary Ms	DIA-Clarendon	3100 Clarendon	Arlington	VA	22201	703-907-1586
Dowd, Thomas Major	JC2WC	2 Hall Blvd	San Antonio	TX	78243	210-977-4715
Ducharme, Lee CDR	NDU	Marshall Hall, Room #212, Ft McNair	Wash	DC	20319-5066	202-685-2174
Falvey, Thomas Mr	PCCIP - Transportation	P O Box 46258	Wash	DC	20050-6258	703-696-9395
Fuhrman, Tom Mr	OSTP	Washington, DC 20319-5066	Wash	DC	20504	202-456-6057
Garvey, Tom Mr	DARPA	3701 N Fairfax Drive	Arlington	VA	22203-1714	703-696-7460
Greene, Brent Mr	PCCIP	P O Box 46258	Wash	DC	20050-6258	703-696-9395
Gustanane, Gary Mr	Infrastructure Policy Directorate	5109 Leesburg Pike Suite 304	Falls Church	VA	22041	703-681-5650
Heritage, Sean LT	JCS/J2	Pentagon Room 1F935	Wash	DC	20301-2900	703-695-4742
Hudson, Susan Ms	JPO - Special Technical Countermeasures	Mail Code J07, NSWC Dahlgren Division	Dahlgren	VA	22448-5000	540-653-8730
Kerr, James Mr	NCS-OMNCS/N5	701 S Courthouse Rd	Arlington	VA	22204-2198	703-607-6133
King, Fred Mr	DIA/TWE-3	DIAC, Bldg 6000	Bolling AFB	DC	20340-5100	202-231-2335
Ladig, Alan Mr	NSA	9800 Savage Road	Ft Meade	MD	20755	301-688-2072
Mahoney, Steve LtCol	ASD(C3I)	Pentagon, Room 3D200	Wash	DC	20301-6000	703-614-0622
Maleski, Mark Mr	CIA	PO Box 1925	Wash	DC	20505	703-874-5199
Mays, Sharon Ms	FBI-CITAC	9th St & Penn Ave NW	Wash	DC	20535	202-324-0353
McChesney, Tim Mr	Commander, SPAWAR Attn: PD16	2451 Crystal Drive	Arlington	VA	22245-5200	703-602-8238
Penrosa, Martin D LtCol	JCS/J7 JETD	Pentagon, Room 2B857	Wash	DC	20318-7000	703-695-3226
Phillips, Deborah Ms	DISA/D2 - Info Assurance Division	5113 Leesburg Pike Suite 400	Falls Church	VA	22041	703-681-6960
Roberts, Andrew Mr	Asst DIO, Military Forces	Pentagon, Room 2D241	Wash	DC	20340	703-697-3107
Rodgers, James LtCol	AF/XOMP	Pentagon, Room 1D373	Wash	DC	20330-1480	703-697-9390
Rona, Thomas Dr	Consultant to OSD/NA	8104 Hamilton Spring Road	Bethesda	MD	20817	301-299-1777
Roth, Alan Mr	ASD(C3I)	Pentagon, Room 3D200	Wash	DC	20301-6000	703-614-0625
Rowell, Scott COL	OSD/Net Assessment	Pentagon Room 3A930	Wash	DC	20301-2950	703-697-1312
Russell, Matthew Mr	ASD/S&R	Pentagon, Room 4B724	Wash	DC	20310	703-697-0209
Saydjari, Sami Mr	DARPA	3701 N Fairfax Dr	Arlington	VA	22203-1714	703-696-2231
Sinck, Ronald Mr	JWAC	18385 Frontage Road	Dahlgren	VA	22448	540-653-5053
Snowden, Ben LtCol	TRANSCOM	402 Scott Dr Unit 1L8	Scott AFB	IL	62225	618-256-3344
Spies, Harry Col	ASD/S&R	Pentagon, Room 4B926	Wash	DC	20310	703-697-9478
Turney, Maureen Ms	FBI-CITAC	9th St & Penn Ave NW	Wash	DC	20535	202-324-0325
Walsh, Buzz Major	JCS/J6	Pentagon, Room1C826	Wash	DC	20318-6000	703-614-2403
Bolish, Steve Mr	Booz Allen & Hamilton Inc	8284 Greensboro Drive	McLean	VA	22102	703-917-2612
DeMoss, Dan Mr	Booz Allen & Hamilton Inc	8284 Greensboro Drive	McLean	VA	22102	703-902-4711
Gladstone, Tom Mr	Booz Allen & Hamilton Inc	8284 Greensboro Drive	McLean	VA	22102	703-902-5826
Hathaway, Melissa Ms	Booz Allen & Hamilton Inc	8283 Greensboro Drive	McLean	VA	22102	703-902-4844
Herman, Mark Mr	Booz Allen & Hamilton Inc	8291 Greensboro Drive	McLean	VA	22102	703-902-5986
Jacobsohn, Mark Mr	Booz Allen & Hamilton Inc	8285 Greensboro Drive	McLean	VA	22102	703-902-5290
Leven, Barry Mr	Booz Allen & Hamilton Inc	8289 Greensboro Drive	McLean	VA	22102	410-684-6456
Phares, Richard Mr	Booz Allen & Hamilton Inc	8286 Greensboro Drive	McLean	VA	22102	703-902-5245
Phillips, Ted Mr	Booz Allen & Hamilton Inc	8288 Greensboro Drive	McLean	VA	22102	703-902-5420
Skordas, John Mr	Booz Allen & Hamilton Inc	8290 Greensboro Drive	McLean	VA	22102	410-684-6231
Sobotka, Mel Mr	Booz Allen & Hamilton Inc	8287 Greensboro Drive	McLean	VA	22102	703-902-5430