



## ANNEXES

The opinions expressed in this Study are those of the authors and do not necessarily reflect the views of the European Commission.  
© ECSC – EC – EAEC, Brussels – Luxembourg 2007

This page is intentionally left blank

## A. KEY FINDINGS MATRIX

Each of the 100 Key Findings identified in Section 3 is associated with one or more of the “eight ingredients” that comprise the communications infrastructure. This association is shown with colour coded boxes in Section 3 beside each Key Finding and is shown in the table.

Table A-1: Key Findings Matrix

Key Finding	Power	Environment	Software	Hardware	Payload	Network	Human	Policy
1	X					X	X	
2					X	X		
3	X	X				X		
4	X	X				X		X
5								X
6					X			X
7						X		X
8	X	X		X				
9	X	X						
10	X	X					X	
11			X	X		X		
12					X	X	X	
13			X			X		
14	X	X					X	X
15					X	X		
16		X		X	X	X		
17			X					
18	X	X				X	X	X
19							X	X
20		X		X		X	X	X
21								X
22			X	X		X		
23								X
24								X
25	X	X	X	X	X	X	X	X
26								X
27	X	X				X	X	X
28					X	X		
29						X		X
30						X		X

Key Finding	Power	Environment	Software	Hardware	Payload	Network	Human	Policy
31			X			X	X	X
32								X
33			X	X				
34			X	X	X	X		X
35							X	X
36							X	
37			X		X	X		
38	X	X						X
39			X	X		X	X	
40					X	X		X
41					X	X		X
42	X	X	X	X	X	X	X	X
43			X	X		X	X	
44					X	X		
45			X	X		X		
46			X			X	X	
47			X	X		X		X
48			X	X		X		X
49			X	X		X		
50			X	X		X		
51					X			X
52	X	X	X	X	X	X	X	X
53	X	X	X	X	X	X	X	X
54							X	X
55					X			X
56					X	X		X
57					X	X		
58	X			X		X	X	X
59	X	X				X		X
60	X	X				X	X	X
61			X		X	X	X	X
62						X		X
63			X		X	X		X
64					X	X		X
65			X			X	X	
66			X	X			X	
67			X		X	X		
68					X	X		X
69							X	X
70								X

Key Finding	Power	Environment	Software	Hardware	Payload	Network	Human	Policy
71					X	X	X	X
72			X		X			
73							X	
74					X			X
75					X	X	X	
76			X	X			X	
77			X	X			X	
78			X		X	X		
79			X		X	X	X	
80			X	X		X		
81					X			
82					X	X		X
83			X	X	X	X	X	X
84	X					X	X	X
85					X	X		
86					X	X		X
87					X	X		X
88								X
89								X
90	X	X					X	X
91					X	X		X
92							X	X
93					X	X		
94					X	X		
95					X	X		
96			X		X	X		X
97								X
98								X
99					X	X		
100			X			X		
<b>TOTALS</b>	<b>19</b>	<b>18</b>	<b>34</b>	<b>24</b>	<b>43</b>	<b>65</b>	<b>35</b>	<b>57</b>

This page is intentionally left blank

## B. COMMUNICATIONS INFRASTRUCTURE VULNERABILITIES

### The Eight Ingredient Framework<sup>1</sup>

The eight ingredients, introduced in Section 2.2, provide a comprehensive framework that can be used to improve the network reliability and security of the communications network. Figure B-1 depicts these eight ingredients.

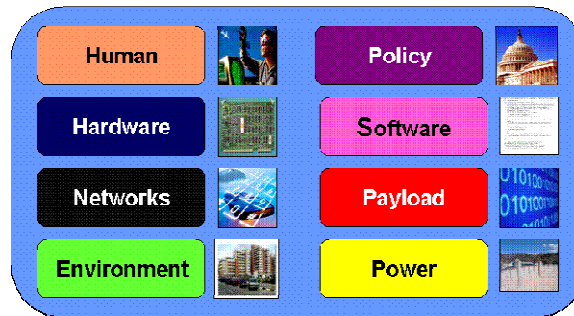


Figure B-1: Eight Ingredients of Communications Infrastructure

This eight ingredient framework has been used extensively by key industry-government-academic forums,<sup>2</sup> and has enabled subject matter experts to conduct complete analyses, assessments and reviews of complex communications systems. This eight ingredient framework also provides the needed structure for conducting a complete vulnerability analysis of the communications network. The definition for each of the eight ingredients is provided in Section 2.2.

### Vulnerability Analysis Using the Eight Ingredients

Vulnerability analysis is a distinct approach to protecting a system from unknown threats. Rather than simply reacting to previously seen attacks or trying to anticipate new attacks, as is done with a “threat-based” approach, a vulnerability analysis looks at the characteristics of the communications infrastructure. To understand the two approaches, two terms must first be defined. *Vulnerabilities* are intrinsic weaknesses of a system that render it susceptible to damage. As shown in the figures below, each of the eight ingredients has a finite number of vulnerabilities. *Threats* are attempts to exploit one or more vulnerabilities (as shown below), that can, if successful, result in damage to communications services. Threats are not limited to terrorism or other intentional attacks. Natural disasters (e.g., hurricanes)<sup>3</sup> as well as unintentional human errors continue to attack networks in unforeseen ways. There are an infinite number of threats that can attempt to exploit a single vulnerability.

<sup>1</sup> Bell Labs Technical Journal 11(3), 73-81 (2006) ©2006 Lucent Technologies Inc. Published by Wiley Periodicals, Inc.

<sup>2</sup> The 8 Ingredient Framework was first used by the IEEE Technical Committee on Communications Quality and Reliability (CQR) to anticipate the challenges of emerging technologies. It has also been used by the FCC Network Reliability and Interoperability Council (NRIC) toward the development of vulnerability-based best practices, by the ATIS Network Reliability Steering Committee (NRSC) to identify possible influencing factors driving observed improvements, and by the President’s National Security Telecommunications Advisory Committee (NSTAC) to prepare for next-generation networks.

<sup>3</sup> B. L. Malone III, “Wireless Search and Rescue: Concepts for Improved Capabilities,” Bell Labs Tech. J., 9:2 (2004), 34–49;

United States, Office of Homeland Security, National Strategy for Homeland Security, July 2002, pp. vii–viii, <[www.dhs.gov/interweb/assetlibrary/nat\\_strat\\_hls.pdf](http://www.dhs.gov/interweb/assetlibrary/nat_strat_hls.pdf)>.

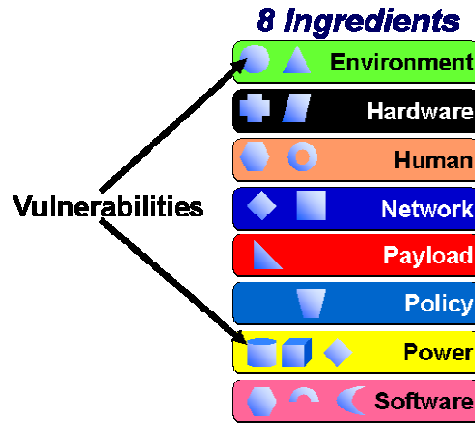


Figure B-2: Vulnerabilities in the Eight Ingredients

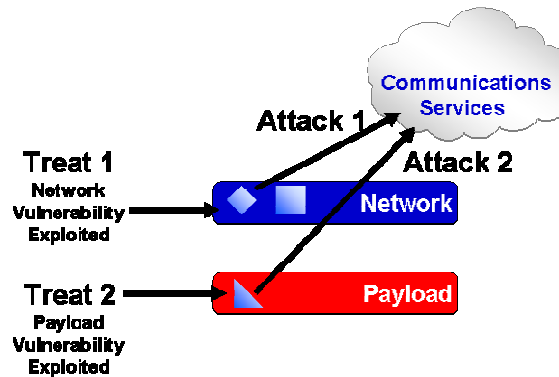


Figure B-3: Threats exploiting vulnerabilities

### Threats Analysis

Threat analysis supports decisions involving setting defence priorities based on the likelihood of a specific threat occurring. A security plan based on threat knowledge is very efficient when the likelihood of having a commanding knowledge of all possible threats is high, but is ineffective if the knowledge of possible threats is less certain. The fundamental weakness of threat analysis is that it is based on hard to obtain intelligence or simply tries to react to previously seen attacks, and generally leaves its user one step behind the creative attacker.

### Vulnerability Analysis

Threats are not effective unless they exploit a vulnerability. The people who design, build, and maintain communication systems and networks know the points at which they are vulnerable. By systematically addressing these vulnerabilities, the communications industry can defend against known and unknown threats.

Identifying and addressing the vulnerabilities of a communications system can protect it from attack or exploitation. This is especially essential for future networks, which are only now being defined and created. Their open architecture exposes them to a myriad of threats, originating from multiple access points, which cannot be predicted. Only by identifying and protecting the intrinsic vulnerabilities can future network owners hope to provide reliable and secure networks.

The primary objectives in assessing vulnerabilities are:

- *Be complete*, do not overlook anything.
- *Master knowledge*, understand the nature of each vulnerabilities fully.
- *Recognise distribution*, capture all instances of a vulnerabilities' presence.
- *Understand dependencies*, anticipate the impact and consider coordinated and blended attacks.<sup>4</sup>

When completed properly, this analysis will result in the identification of a complete and finite number of vulnerabilities for each of the eight ingredients, and therefore for the system as a whole.

### Using the Eight Ingredients

As cited earlier, the communications industry utilises the framework of eight ingredients to provide a structure with which to systematically manage the identification of vulnerabilities. Industry experts identify areas of concern and categorise then using the eight ingredients. These are analyzed by individuals with expertise in each of the specific ingredients to develop a finite but comprehensive list of vulnerabilities.<sup>5</sup>

By systematically addressing the vulnerabilities of a system, protection can be developed for general classes of problems independent of knowing what the specific threat may be. Because threats are constantly changing, and are limited only by the imagination of the attacker, addressing classes of problems by closing know vulnerabilities is the only hope of staying ahead of the attackers. As shown in the following figure, the implementation of best practices eliminates or disables the vulnerability, thereby rendering ineffective the threats attempting to exercise that vulnerability.

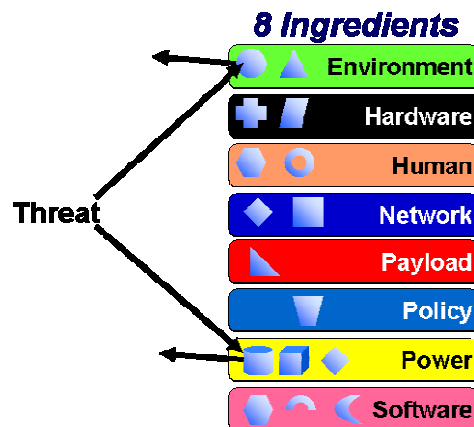


Figure B-4: Threats nullified by vulnerability removal

The vulnerability-based approach is not an exclusive strategy. Known threats should still be responded to in a timely fashion, but such responses are no substitute for the proactive, systematic coverage which vulnerability analysis can provide. The need to proactively address vulnerabilities rather than just focusing on previously seen

<sup>4</sup> Federal Communications Commission, "Report and Order and Further Notice of Proposed Rulemaking, Revision of the Commission's Rules to Ensure Compatibility With Enhanced 911 Emergency Calling Systems," FCC 96-264, adopted June 12, 1996, p. 8.

<sup>5</sup> Network Reliability and Interoperability Council VI, Homeland Security – Physical Security (Focus Group 1A) – Final Report, Issue 3, Dec. 2003, <[www.nric.org/fg/nricvifg.html](http://www.nric.org/fg/nricvifg.html)>.

attacks is clearly demonstrated in security, a unique area of reliability. While reliability was once only measured in terms of the availability of a network and the ability of information to traverse a network successfully, the openness of future networks puts even the reliability of the transmitted information at risk. Security is difficult to measure since network administrators may not even be aware that an attack is underway or has occurred previously. Undetected attacks may steal information or gain access to networks. Protecting against only previously seen attacks would not help protect against undetected attacks. Analyzing and addressing system vulnerabilities would close holes that undetected attacks may be exploiting.

### **Intrinsic Vulnerabilities of the Eight Ingredients**

The vulnerabilities of future networks were studied systematically to determine the vulnerabilities of each of the eight ingredients. This Study included:<sup>6</sup>

- A suitable framework for vulnerability assessment
- A comprehensive list of intrinsic vulnerabilities of the eight ingredients for future networks
- Relevant trends that affect the exposure of the vulnerabilities
- Evaluation of significance of each vulnerability for future networks

The vulnerabilities listed below are a comprehensive set of vulnerabilities for each of the eight ingredients.

---

<sup>6</sup> The President's National Security Telecommunications Advisory Committee (NSTAC) Next Generation Networks Task Force Report, March 28, 2006, *Background and Charge, Appendix G*.

## ENVIRONMENT

The Environment ingredient includes buildings, trenches where cables are buried, space where satellites orbit, locations of microwave towers and cell sites, and the ocean where submarine cables reside.

ENVIRONMENT VULNERABILITY
accessible
exposed to elements
dependence on other infrastructures
contaminate-able
Subject to surveillance
continuously being altered
identifiable
remotely managed
non-compliance with established protocols and procedures

## POWER

The Power ingredient includes the internal power infrastructure, batteries, grounding, high voltage and other cabling, fuses, back-up emergency generators and fuel.

POWER VULNERABILITY
uncontrolled fuel combustion
fuel contamination
fuel dependency
battery combustion
battery limitations
battery duration
Maintenance dependency
require manual operation
power limitations
frequency limitations
Susceptibility to spikes
physical destruction

## HARDWARE

The Hardware ingredient includes the hardware frames, electronic circuit packs and cards, and metallic and fibre optic transmission cables and semiconductor chips.

HARDWARE VULNERABILITY
chemical (corrosive gas, humidity, temperature, contamination)
electric (conductive microfibre particles – carbon bombs)
radiological contamination
physical (shock, vibration, strains, torque)
electromagnetic energy (EMI, EMC, ESD, RF, EMP, HEMP, IR)
Environment (temperature, humidity, dust, sunlight, flooding)

life cycle (sparing, equipment replacement, ability to repair, aging)
logical (design error, access to, self test, self shut off)

## SOFTWARE

The Software ingredient includes the physical storage of software releases, development and test loads, version control and management, and software delivery controls.

SOFTWARE VULNERABILITY
ability to control (render a system in an undesirable state, e.g., confused, busy)
accessibility during development (including unsegregated networks)
accessible distribution channels (interception)
accessibility of rootkit to control kernel/core
developer loyalties
errors in coding logic
complexity of programs
discoverability of intelligence (reverse engineer, exploitable code disclosure)
mutability of deployed code (patches)
incompatibility (with hardware, with other software)

## NETWORK

The Network ingredient includes the configuration of nodes and their interconnection, network topologies and architectures, various types of networks, technology, synchronisation, redundancy, and physical and logical diversity, and network design, operation and maintenance.

NETWORK VULNERABILITY
capacity limits
points or modes of failure
points of concentration (congestion)
complexity
dependence on synchronisation
interconnection (interoperability, interdependence, conflict)
uniqueness of mated pairs
need for upgrades and new technology
automated control (via software)
accessibility (air, space or metallic or fibre)
border crossing exposures

## PAYLOAD

The Payload ingredient includes the information transported across the infrastructure, traffic patterns and statistics, information interception, and information corruption. It includes both normal and signalling and control traffic.

PAYLOAD VULNERABILITY
unpredictable variation
extremes in load
corruption
interception
emulation
encapsulation of malicious content
authentication (mis-authentication)
insufficient inventory of critical components
encryption (prevents observability)

## HUMAN

The Human ingredient includes human involvement throughout the entire lifecycle of activities related to the communications infrastructure (design, implementation, operation, maintenance and de-commissioning), intentional and unintentional behaviours, limitations, education and training, human-machine interfaces, and ethics and values.

HUMAN VULNERABILITY
physical (limitations, fatigue)
cognitive (distractibility, forgetfulness, ability to deceive, confusion)
ethical (divided loyalties, greed, malicious intent)
user environment (user interface, job function, corporate culture)
human-user environment interaction

## POLICY

The policy ingredient includes behaviours between entities, namely agreements, standards, policies and regulations (ASPR), national and international scopes, as well as Federal, State and local levels, other legal issues, and any other arrangement between entities, including industry cooperation and other interfaces.

POLICY VULNERABILITY
lack of ASPR (agreements, standards, policies, regulations)
conflicting ASPR
outdated ASPR
unimplemented ASPR (complete or partial)
interpretation of ASPR (mis- or multi-)
inability to implement ASPR
enforcement limitations
boundary limitations
pace of development
information leakage from ASPR processes
inflexible regulation
excessive regulation
predictable behaviour due to ASPR

ASPR dependence on misinformed guidance
ASPR ability to stress vulnerabilities
ASPR ability to infuse vulnerabilities
inappropriate interest influence in ASPR

### Conclusion

The systematic identification of the vulnerabilities within a communications infrastructure is an important tool in improving its reliability and security. While it is essential to utilise multiple approaches to protect communications infrastructure, the vulnerability analysis approach is fundamentally distinct from the traditional threat-based protection methods. A threat-based approach is based on knowledge of the things or people that threaten the network and what drives them. While engineers do not know what drives a terrorist, they do know the equipment that comprises the network and what vulnerabilities it may have. Vulnerability analysis utilises that knowledge to protect against unimagined and unknown attacks. By identifying the finite number of vulnerabilities within a system, we can effectively protect the communications network from threats we have already seen, and from those that we have not yet seen.

The eight ingredients of communications infrastructure have been successfully used over the past several years by various corporations, and national and government advisory groups. These groups were chartered to analyze the performance of the network and provide guidance on improving network reliability and performance. Hundreds of best practices have been developed with this method. They now stand as the most authoritative collection of guidance for the industry, developed by the industry, in the areas of reliability, interoperability, physical security, cyber security and emergency services. These best practices have been internationally recognised as a cornerstone in the reliable and secure operation of communications networks. The development of these best practices has its foundation in the use of the eight ingredients and has affirmed that the eight ingredients provide comprehensive coverage of critical infrastructure.

## C. THREAT SCENARIOS

### 1 Introduction

The following is a description of the ITU-T X.805<sup>7</sup> network security framework. This framework is at the heart of security threat analysis. X.805 is based almost entirely on the Bell Labs Network Security Framework.<sup>8</sup> This powerful framework was also subsequently standardised as ISO/IEC 18028-2.<sup>9</sup> The framework therefore covers telecom and enterprise networks via the two standards and all three are referred to as X.805 in this Annex.

The current focus of network security is mostly concerned with securing individual components and preventing unauthorised access to network services by deploying a basic firewall to protect the perimeter of a network from outside attackers. In many cases security is an after thought. While these are necessary concerns, they do not represent a complete view of network security. It is critical to design and create security solutions from an end-to-end perspective for networks that cross the public telephone network, the Internet, or any Internet Protocol (IP) network. X.805 provides a comprehensive, top-down, end-to-end perspective on network security that can be applied to network elements, services, and applications including detecting, correcting, and preventing security vulnerabilities. It can be applied to all types of networks and across all layers of the protocol stack. Networks developed with attention to the framework will have a much more secure and comprehensive security architecture.

As more products and services are combined in increasingly complex ways to provide network solutions, it becomes more difficult to address the security of the solution and the end-user data for which the solution was developed. Not only must security be a concern for each product or service, the overall solution must be developed in a manner that promotes end-to-end security.

Network security is a constant task of evaluating new threats, maintaining the present organisational security, and incorporating new techniques where needed. Network security should be designed around a strong security framework, available tools, standardised protocols, and, where available, easily configured software and hardware. In addition, an end-to-end network security solution must take into account the three types of activities that occur on a network: network management activities, network control or signalling activities, and end-user activities. Naturally, in a multi-vendor environment, no end-to-end security solution can be achieved without standards. Thus, service providers need to understand the balance of price, features, and the ease of use for various security technologies and solutions.

The Bell Labs Network Security Framework was created to address the global security challenges of service providers, enterprises, and consumers for wireless, optical, and wireline voice, data, and converged networks. This security framework addresses security concerns for the management information, control/signalling information, and end-user data used and transported by the network infrastructure, network services, and network-based applications. X.805 should be used over the entire lifetime of a network security program. It should be used to assist in the development of network security policies and requirements, as well as to form the basis for a network security assessment

7 International Telecommunication Union, Telecommunication Standardization Sector, "Security Architecture for Systems Providing End-to-End Communications," ITU-T Rec. X.805, October 2003.

8 A. McGee, S. R. Vasireddy, C. Xie, D. Picklesimer, U. Chandrashekhar, and S. Richman, "A Framework for Ensuring Network Security," Bell Labs Technical Journal, Volume 8, Issue 4, Pages 7 – 27, February 5, 2004.

9 International Standards Organization, "Information Technology - Security Techniques - IT Network Security - Part 2: Network Security Architecture," ISO/IEC 18028-2: September 2005.

## 2 Security Threats

X.805 describes a security structure for an end-to-end network security solution. It identifies security issues that need to be addressed in order to detect, correct, and prevent both intentional and accidental threats originating from inside or outside the network. The five types of security threats to a network that can be caused by intentional or unintentional actions are destruction, corruption, removal, disclosure and interruption. ITU-T Recommendation X.800 addresses these five threats to telecommunications networks.<sup>10</sup> These are depicted in Figure C-1.

- *Destruction* of information and/or other resources is an attack on availability and data integrity. Examples include malicious destruction of network equipment, erasure of a software program or data file, cutting of a communication line, and malfunction of an operating system file manager so that it cannot find a particular disk file.
- *Corruption* or modification is an attack on data integrity and authentication. An unauthorised party tampers with information and/or an asset. Examples include changing the network configuration information in a database (e.g., the addition of records to an authentication database) and modifying data being transmitted in a network.
- *Removal*, theft or loss is an attack on access control and confidentiality. An unauthorised party gains access to and removes information and/or other assets. The outside party can be a person, a program, or a computing system. Examples of this type of attack are wiretapping to obtain data in a network and passive listening to a wireless radio transmission.
- *Disclosure* of information is an attack on privacy and confidentiality. An unauthorised party gains access to an asset and its information. Examples include unauthorised data capture (e.g., data sniffing) and discovery of unprotected WLAN access points.
- *Interruption* of an asset or service temporarily where it becomes lost, unavailable, or unusable is an attack on availability. An example is flooding a network element with calls or data (e.g., denial of service) which degrade throughput or cause delay so that the connection, session or service becomes unusable, malicious destruction of a network element (e.g., cutting of a communications facility), and malfunction of an operating system file manager so that it cannot find a particular disk file.

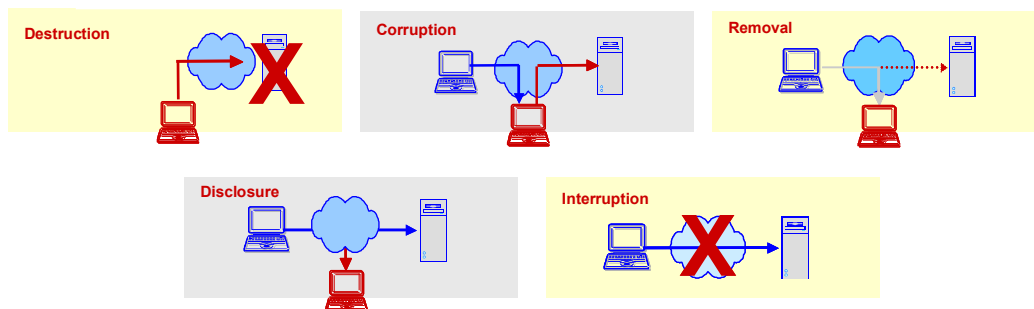


Figure C-1: Threat Model

## 3 Security Layers

X.805 includes the concept of security layers that consist of a hierarchy of network equipment and facility groupings. The three security layers, which build on one another to provide comprehensive, end-to-end security solutions, are:

<sup>10</sup> International Telecommunication Union, Telecommunication Standardization Sector, "Data Communication Networks: Open Systems Interconnection (OSI); Security, Structure and Applications," ITU-T Rec. X.800, 1991.

- The *infrastructure layer*, which consists of the network transmission facilities as well as individual network elements and hardware platforms, including the hardware and software comprising the network elements and platforms. The infrastructure layer also includes the offices or physical facilities in which the transmission facilities, network elements, and platforms reside. The infrastructure layer represents the fundamental building blocks of networks, their services, and their applications. Examples of components that belong to the infrastructure layer are individual routers, switches, and servers as well as the communication links between them.
- The *services layer*, which consists of services that customers receive from service providers. These services include basic transport and basic IP connectivity (e.g., Internet access), IP service enablers such as authentication, authorisation, and accounting (AAA) services, dynamic host configuration services, and domain name services to value-added services such as voice over IP (VoIP), quality of service (QoS), virtual private networks (VPNs), location services, Toll-Free-services, and instant messaging (IM). Note that at this layer the end-users (i.e., service provider customers) as well as the service provider itself are potential targets of security threats. For example, an attacker may attempt to deny the service provider's ability to offer the service, or the attacker may attempt to disrupt service for an individual customer of the service provider (e.g., a large corporation).
- The *applications layer*, which focuses on network-based applications accessed by service provider customers, as well as end-user applications that require network services. These applications are enabled by network services and include basic applications such as file transport (e.g., file transfer protocol [FTP]) and Web browsing applications, fundamental applications such as directory assistance (e.g., 411), network-based voice messaging, and e-mail, as well as high-end applications such as customer relationship management, human resource systems (e.g., PeopleSoft<sup>11</sup>), electronic/mobile-commerce, network-based training, and video collaboration. Network-based applications may be provided by third-party application service providers (ASPs), service providers acting as ASPs, or by enterprises hosting them in their own (or leased) data centres. At this layer, there are four potential targets for security attacks: the application user, the application content provider, the middleware provided by third-party integrators (e.g., web-hosting services), and the service provider.

Figure C-2 depicts the security layers as a series of enablers for secure network solutions: the infrastructure layer enables the services layer, and the services layer enables the applications layer.

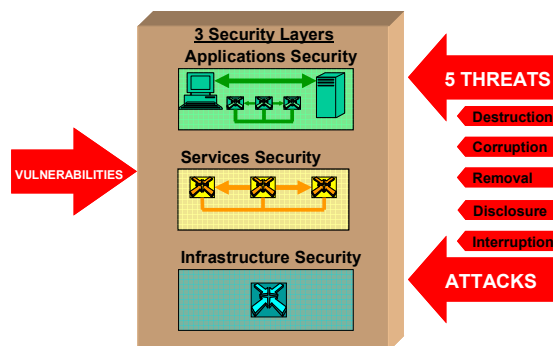


Figure C-2: Security Layers

In addition, the Network Security Framework recognises that each layer has unique security vulnerabilities, which result in potential security threats and attacks if they are not

<sup>11</sup> PeopleSoft is a registered trademark of PeopleSoft, Inc.

addressed. The network security layers represent a separate category from the layers of the Open Systems Interconnection (OSI) Reference Model.<sup>12</sup> As will be shown below, all three security layers can be applied to each layer of the OSI reference model.

The security layers identify where security must be addressed in products and solutions by providing a sequential perspective of network security. For example, first security vulnerabilities are addressed for the infrastructure layer, then security vulnerabilities are addressed for the services layer, and finally they are addressed for the applications layer.

#### 4 Security Planes

The security planes represent the three types of activities that take place on a network. By defining these planes—the management plane, the control plane, and the end-user plane—we are able to focus on the unique security needs associated with network management activities, network control or signalling activities, and end-user activities.

- The *management plane* facilitates the operations, administration, maintenance, and provisioning (OAM&P) of the network elements, transmission facilities, back-office systems (e.g., operations support systems, business support systems, customer care systems), and data centres. This plane supports the fault, configuration, accounting, performance, and security (FCAPS) functions. It should be noted that the network carrying the traffic for these activities may be in-band or out-of-band with respect to the service provider's user traffic.
- The *control plane* is concerned with enabling the efficient delivery of information, services, and applications across the network. It typically involves machine-to-machine communications containing information that allows the machines (e.g., switches or routers) to determine how to best route or switch traffic across the underlying transport network. This type of information is sometimes referred to as control or signalling information. The network carrying these types of messages may be in-band or out-of-band with respect to the service provider's user traffic. For example, IP networks carry their control information in-band, whereas the public switched telephone network (PSTN) carries its control information in a separate out-of-band signalling network (the Signalling System 7 [SS7] network). Example traffic of this type includes routing protocols (e.g., OSPF, BGP), DNS, SIP, SS7.
- The *end-user plane* addresses how service provider customers access and use the service provider's network. This plane also represents actual end-user data flows. End-users may use the service provider's network to only provide connectivity, to benefit from value-added services such as VPN's, or to access network-based applications.

Service provider networks should be designed such that events on one security plane are kept totally isolated from the other security planes. For example, a flood of DNS lookups, originating from activity on the end-user plane, should not lock out the OAM&P interface in the management plane, preventing an administrator from correcting the problem.

Figure C-3 demonstrates the need to isolate the different security planes and shows how the concept of security planes fits into the Network Security Framework.

---

<sup>12</sup> International Organization for Standardization, "Information Technology—Open Systems Interconnection—Basic Reference Model: The Basic Model," ISO/IEC Standard 7498-1, 1994.

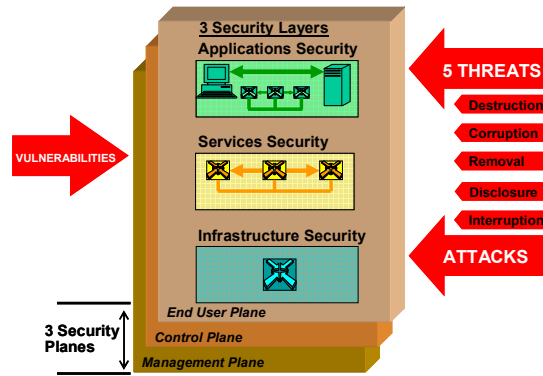


Figure C-3: Applying Security Planes to Security Layers

This framework recognises that each plane imposes its own unique security concerns and techniques to address these concerns on each of the security layers discussed previously. Consider, for example, a VoIP Service, which is addressed by the services security layer. Securing the management of the VoIP service (e.g., provisioning users) raises issues that are independent of securing the control of the service (e.g., protocols such as SIP) and also of securing the end-user data being transported by the service (e.g., the user's voice).

## 5 The Network Security Framework

The Network Security Framework uses standard security services and mechanisms found in the ITU-T Recommendation X.800 to define eight basic dimensions of security that must be addressed in order to thwart attempts to exploit network vulnerabilities. These dimensions are not limited to the network, but extend to applications and end-users as well. In addition, the security dimensions apply to service providers or enterprises offering security services to their customers. The security dimensions are:

- *Access management* or *access control*, which protects against unauthorised use of network resources. Access management ensures that only authorised personnel or devices are allowed access to network elements, stored information, information flows, services, and applications. In addition, role-based access control provides different access levels to guarantee that individuals and devices can only gain access to and perform operations on the network elements, stored information, and information flows for which they are authorised. The access management security dimension addresses the interception and fabrication security threats.
- *Authentication*, which is used to confirm the identities of communicating entities. Authentication ensures the validity of the claimed identities of the entities participating in communication (e.g., person, device, service, or application) and provides assurance that an entity is not attempting a masquerade or unauthorised replay of a previous communication. The authentication security dimension addresses the fabrication security threat.
- *Non-repudiation*, which provides proof of the origin of data or the cause of an event or an action. It ensures the availability of evidence that can be used to prove that some kind of event or action has taken place so that the cause of the event or action cannot be repudiated later. The non-repudiation security dimension addresses the fabrication security threat.
- *Data confidentiality* or *data security*, which protects data from unauthorised disclosure. Data confidentiality ensures that data is kept private from unauthorised access or viewing. Encryption, coupled with access management techniques, is often used to keep data secure. This security dimension addresses the interception threat.
- *Communication security*, which ensures that information flows only between the authorised endpoints. The information flow is not diverted or intercepted as it flows between these endpoints. The concept of communication security is an extension to

Recommendation X.800 in that it is currently not included in the recommendation. The recommendation does discuss a routing control mechanism that could be used to provide communication security at the IP layer and above. This security dimension addresses the interception threat.

- *Data integrity*, which ensures the correctness or accuracy of data against unauthorised modification, deletion, creation, and replication and provides an indication of unauthorised activities in these areas. The data integrity security dimension addresses the modification and fabrication security threats.
- *Availability*, which ensures that there is no denial of authorised access to network elements, stored information, information flows, services, and applications due to events impacting the network. Disaster recovery solutions are included in this category. The availability dimension is an extension to Recommendation X.800. The availability security dimension addresses the interruption security threat.
- *Privacy*, which provides for the protection of information that might be derived from the observation of network activities. This dimension also includes protection of information associated with individual users, service providers, enterprises, or the network infrastructure that might be obtained either by direct or covert means. Examples of this information include Web sites that a user has visited, a user's geographic location, and the IP addresses and DNS names of devices in a service provider network. Recommendation X.800 includes traffic flow confidentiality, which addresses some aspects of the privacy dimension. The privacy security dimension addresses the interception security threat.

Figure C-4 completes the Network Security Framework by including security dimensions to address security vulnerabilities at each security plane of each security layer to provide a comprehensive viewpoint of a network's security requirements.

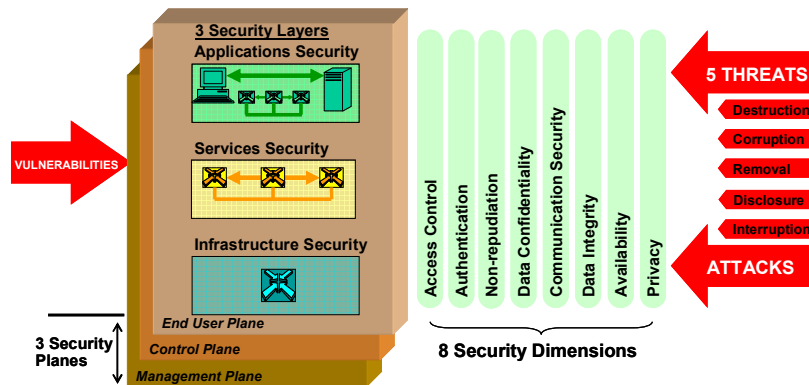


Figure C-4: The Network Security Framework

For a given network's desired security posture, it may not be required to address each security dimension. It also may not be required to address each security plane and each security layer for a specific network's desired security posture.

X.805 can be applied to any type of network residing at any level of the protocol stack. For example, in an IP network, which resides at layer 3 of the protocol stack, the infrastructure layer refers to the individual routers, the point-to-point communications links between the routers (e.g., SONET, ATM PVCs), and server platforms used to provide the support services required by an IP network. The services layer refers to the basic IP service itself (e.g., Internet connectivity), the IP support services (e.g., AAA, DNS, DHCP), and advanced value-added services offered by the service provider (e.g., VoIP, QoS, VPN). Finally, the applications layer refers to the applications the user is using the IP network to access, such as e-mail.

Likewise, for an ATM network, which resides at layer 2 of the protocol stack, the infrastructure layer refers to the individual switches and the point-to-point communications links between the switches. The services layer refers to the different classes of transport provided by an ATM service offering (constant bit rate, variable bit rate–real time, variable bit rate–non-real time, available bit rate, and unspecified bit rate).<sup>13</sup> Finally, the applications layer refers to the applications the end-user is using the ATM network to access, such as a video conferencing application.

Figure C-5 shows how the Network Security Framework is converted into tabular form to provide a methodical approach to securing service provider networks.

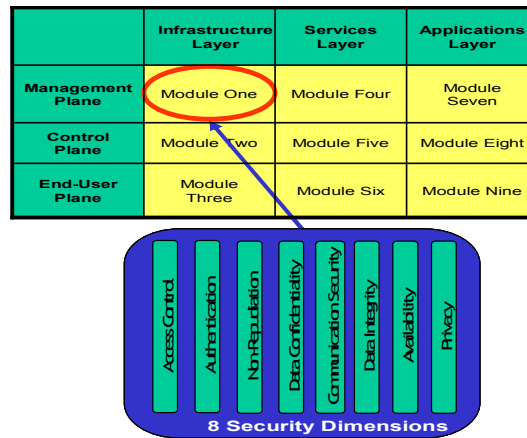


Figure C-5: Tabular Form of Network Security Framework

As can be seen from the figure, the intersection of a security layer with a security plane represents a unique perspective for consideration of the eight security dimensions.

Each of the nine perspectives has unique security issues that result in unique security requirements for each perspective, and these issues must be addressed. The following subsections identify the types of issues that must be addressed for each security layer.

### 5.1 Securing the Infrastructure Layer

Securing the management plane of the infrastructure layer is concerned with securing the Operations, Administration, Maintenance and Provisioning (OAM&P) of the individual network elements, communication links, and server platforms that constitute the network. We consider the configuration of network devices and communications links to be a management activity as well. An example of infrastructure management that needs to be secured is the configuration of an individual router or switch by network operations personnel.

Securing the control plane of the infrastructure layer consists of securing the control or signalling information that resides in the network elements and server platforms that constitute the network, as well as securing the receipt and transmission of control or signalling information by the network elements and server platforms. For example, the switching tables residing in network switches need to be protected from tampering or unauthorised disclosure. In another example, routers need to be protected from receiving and propagating bogus routing updates or responding to bogus routing requests originating from spoofed routers.

<sup>13</sup> International Organization for Standardization, "Information Technology–Open Systems Interconnection–Basic Reference Model: The Basic Model," ISO/IEC Standard 7498-1, 1994.

Securing the end-user plane of the infrastructure layer consists of securing user data and voice as it resides in or is transported through network elements, as well as while it is being transported across communications links. Protecting user data resident on server platforms is of concern here as well as protecting user data against unlawful interception as it is transported through network elements or across communication links.

### **5.2 Securing the Services Layer**

Securing the services layer is complicated because services may build upon one another in order to satisfy customer requirements. For example, in order to provide a VoIP service, a service provider must first provide basic IP service, with its requisite enabling services such as AAA, DHCP, and DNS. The service provider may also need to deploy a VPN service in order to meet customer QoS and security requirements for the VoIP service. Therefore, the service offering under consideration must be decomposed into its composite services before evaluating its overall security.

Securing the management plane of the services layer is concerned with securing the OAM&P of network services. We consider the configuration of network services to be a management activity as well. An example of service management that needs to be secured is the provisioning of authorised users of an IP service by network operations personnel.

Securing the control plane of the services layer consists of securing the control or signalling information used by the network service. Using a VoIP service as an example, issues surrounding the securing of the SIP protocol used to initiate and maintain VoIP sessions would be addressed here.

Securing the end-user plane of the services layer consists of securing user data and voice as it uses the network service. For example, the confidentiality of a user's conversation must be protected in a VoIP service. Likewise, a DNS service must ensure the confidentiality of users of the service.

### **5.3 Securing the Applications Layer**

Securing the management plane of the applications layer is concerned with securing the OAM&P of network-based applications. We consider the configuration of network-based applications to be a management activity as well. For an e-mail application, an example management activity that would need to be secured is the provisioning and administration of user mailboxes.

Securing the control plane of the applications layer consists of securing the control or signalling information used by the network-based application. This type of information typically causes the application to alter the way it executes in response to receiving the information. Using an e-mail application as an example, issues surrounding the securing of the simple mail transfer protocol (SMTP) and the post office protocol (POP) used to control the delivery of e-mail would be addressed here.

Securing the end-user plane of the applications layer consists of securing user data provided to the network-based application. For example, the confidentiality of a user's credit card number must be protected by an electronic commerce application.

## **6 The Security Framework Applied to Service Provider Networks**

Network-based IP VPN service is used as an illustrative example to demonstrate how the security framework is used in a service provider environment

### 6.1 Brief Overview of IP VPN Service Architecture

Figure C-6 shows the functional architecture for a network-based IP VPN service,<sup>14</sup> which consists of four key building blocks:

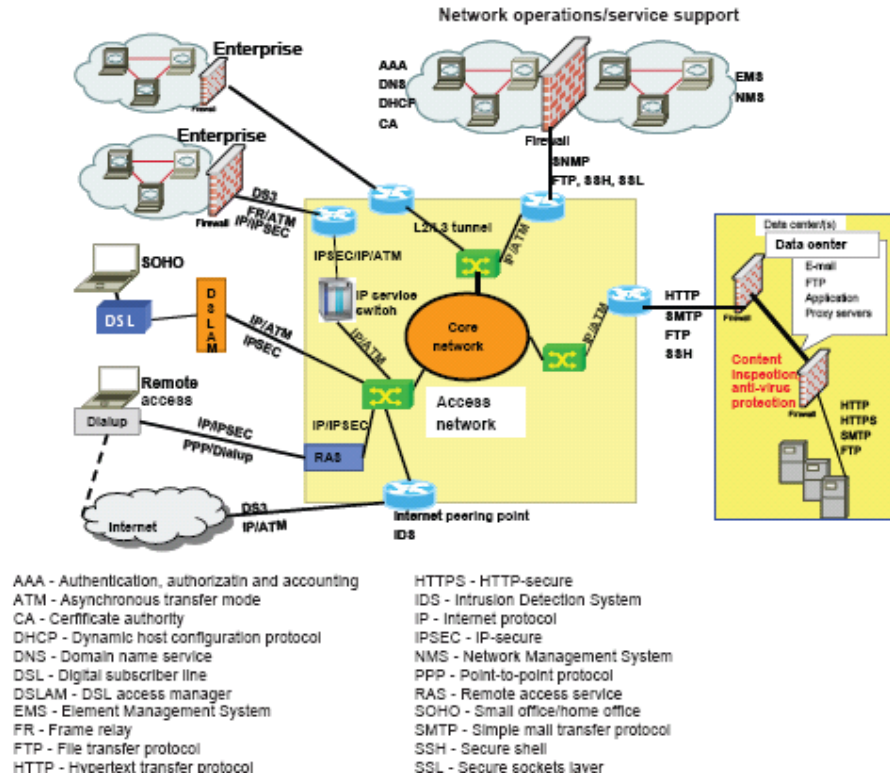


Figure C-6: Example Network Based IP VPN Service

- *Customer premises equipment (CPE)*, which can be located at an enterprise location or at a remote dial-up site. It can also be located at a small office/home office (SOHO) with broadband access. The customer traffic is concentrated through a firewall/access gateway in the access network. The type of CPE determines the demarcation between the service provider and the customer. For example, it could be a firewall WAN interface or a DSL/dial modem's PSTN interface. A customer may be required to implement certain features in the CPE to facilitate IP VPN interoperability.
- The *access network*, which comprises various systems to support access to the IP VPN service. These systems include RAS devices, access routers, and IP service switches, which function as firewalls, authentication system/proxies, and access concentrators for IP VPN traffic. These network elements can also initiate layer 2/layer 3 tunnels based on the customer's profile.
- *Network operations/service support systems*, which reside in the network operations centre and are used to configure the network elements in order to provide IP VPN service. This configuration is done using protocols such as SNMP, TFTP, and SSH. AAA servers, policy servers, and certificate authority servers support the IP VPN AAA functions. There are numerous other systems supporting FCAPS functions.
- A *data centre*, which can be located in either a service provider network or in an enterprise network. For the sake of simplicity, we consider the case where the data centre is part of the service provider network. Data centres house

14 D. Fowler, Virtual Private Networks: Making the Right Connection, Morgan Kaufman, San Francisco, CA, 1999.

applications such as e-mail, Web hosting, and other information sources. The protocols used in the data centre applications include SMTP, FTP, HTTP, and HTTPS. An IP VPN may be used to provide access to these applications.

### 6.2 Using X.805 to Address IP VPN Security Issues

This section demonstrates how X.805 is used to identify security threat scenarios. IP VPN service is used as an example. Additional future network vulnerabilities could be derived from considering the X.805 framework.

An IP VPN service is found at the services layer of the security framework. Therefore, the key entities that need to be secured for an IP VPN service are the network elements, network element protocols and configurations, OSS/BSS systems, and user data that are being transported by the service. Table C-1 shows categories of network elements, protocols, and services that need to be assessed under our security framework.

**Table C-1: Assigning IP VPN systems and components to layers**

Infrastructure Layer Systems and Components	Services Layer Systems and Components
<ul style="list-style-type: none"> <li>• Individual network elements</li> <li>• VPN/firewall appliances</li> <li>• OSS/BSS systems</li> <li>• Platform operating systems.</li> <li>• SNMP management information bases</li> </ul>	<ul style="list-style-type: none"> <li>• Remote access service</li> <li>• VPN service</li> <li>• VPN management systems</li> <li>• Intrusion detection systems</li> </ul>

BSS – Business support system  
OSS – Operations support system  
SNMP – Simple network management protocol  
VPN – Virtual private network

The systems and components listed in this table are categorised as belonging to either the infrastructure layer or the services layer of the security framework; the applications layer does not play a role. In addition, for the sake of simplicity, end-user devices, such as laptop computers, are not included in the table.

Table C-2 indicates which components and services listed in Table V have security issues that need to be addressed in the management plane, control plane, and/or end-user plane.

**Table C-2: Identifying security Planes for IP VPN service components**

	Infrastructure Layer Systems and Components	Services Layer Systems and Components
Management Plane	<ul style="list-style-type: none"> <li>• Individual network elements</li> <li>• VPN/firewall appliances</li> <li>• OSS/BSS systems</li> <li>• Platform operating systems</li> <li>• SNMP MIBs</li> </ul>	<ul style="list-style-type: none"> <li>• Remote access service</li> <li>• VPN service</li> <li>• VPN management systems</li> <li>• Intrusion detection systems</li> </ul>
Control Plane	<ul style="list-style-type: none"> <li>• Individual network elements</li> <li>• VPN/firewall appliances</li> <li>• OSS/BSS systems</li> </ul>	<ul style="list-style-type: none"> <li>• Remote access service</li> <li>• VPN service</li> </ul>
End-User Plane	<ul style="list-style-type: none"> <li>• Individual network elements</li> <li>• VPN/firewall appliances</li> <li>• OSS/BSS systems</li> </ul>	<ul style="list-style-type: none"> <li>• Remote access service</li> <li>• VPN service</li> </ul>

BSS – Business support system  
OSS – Operations support system  
SNMP – Simple network management protocol  
VPN – Virtual private network

The security issues for each of the cells in Table II are evaluated to assess the overall security of the IP VPN service.

Next, we analyze the IP VPN service components for security issues associated with their relevant security planes as identified in Table VI. The objective is to assess the possible threats and their impact on the IP VPN service and to impose requirements to address those threats. This analysis uses the security dimensions to identify the possible threats to various IP VPN functions. An example of an IP VPN function is the authentication of users and network elements. Security assessment of the IP VPN authentication function will focus on the different layers and planes of network elements or systems in the IP VPN authentication function and examine ways to address issues relevant to each security dimension. Table C-3 provides sample security requirements imposed by each security dimension on the management plane of the IP VPN service's infrastructure layer and potential security threats to the IP VPN service if the requirements are not satisfied.

**Table 3: Sample security requirements for the IP VPN service infrastructure layer, management plane**

<b>IP VPN Service Infrastructure Layer, Management Plane</b>		
<b>Security Dimension</b>	<b>Security Requirements</b>	<b>Potential Threats</b>
<b>Access Control</b>	<ul style="list-style-type: none"> <li>Verify unauthorised packets are not allowed to enter the network element.</li> <li>Verify unnecessary services are disabled on network elements.</li> <li>Deploy IDS systems.</li> <li>Address known policy server, syslog, and management protocol vulnerabilities.</li> <li>Prevent easy outside discovery of the network elements.</li> <li>Address vulnerabilities in service activation for network element interfaces.</li> </ul>	<ul style="list-style-type: none"> <li>DoS attacks</li> <li>Session hijacking, lost data</li> <li>Network downtime</li> <li>Unauthorised resource utilisation</li> <li>Virus propagation</li> </ul>
<b>Authentication</b>	<ul style="list-style-type: none"> <li>Address known login, password, and shared secret vulnerabilities.</li> <li>Deploy certificate authority servers.</li> <li>Implement anti-spoofing capabilities.</li> </ul>	<ul style="list-style-type: none"> <li>Password/login compromise</li> <li>Theft of service</li> <li>Session hijacking, loss of data</li> </ul>
<b>Non-Repudiation</b>	<ul style="list-style-type: none"> <li>Deploy certificate authority servers.</li> <li>Deploy logging servers.</li> <li>Deploy backup/storage systems.</li> </ul>	<ul style="list-style-type: none"> <li>No administrative/management accountability</li> <li>Audit failures</li> <li>Possible violation of regulations.</li> </ul>
<b>Data Confidentiality</b>	<ul style="list-style-type: none"> <li>Implement data encryption.</li> </ul>	<ul style="list-style-type: none"> <li>Incorrect network element configurations, management data, or billing data</li> <li>Loss of proprietary information</li> <li>Password/login compromise</li> <li>Theft of service</li> </ul>
<b>Communication Security</b>	<ul style="list-style-type: none"> <li>Address known management protocol vulnerabilities.</li> <li>Verify management network topology.</li> <li>Verify firewall configuration.</li> </ul>	<ul style="list-style-type: none"> <li>Unauthorised network administration/management activities</li> <li>Unauthorised management traffic</li> <li>DoS attacks</li> </ul>
<b>Data Integrity</b>	<ul style="list-style-type: none"> <li>Implement data hashing techniques.</li> </ul>	<ul style="list-style-type: none"> <li>Incorrect network element configurations, management data, or billing data</li> <li>Session hijacking</li> </ul>
<b>Availability</b>	<ul style="list-style-type: none"> <li>Deploy IDS systems.</li> <li>Deploy firewalls.</li> </ul>	DoS attacks
<b>Privacy</b>	<ul style="list-style-type: none"> <li>Prevent the discovery of the DNS names and IP addresses of network elements and ports.</li> <li>Hide the source, destination IP addresses of management packets that are sent and received.</li> </ul>	Targeting information visible to potential attackers

DNS – Domain name service  
DoS – Denial of service

IDS – Intrusion detection system  
IP – Internet protocol

Once the security requirements are identified, other tools and techniques are used to satisfy them, gather data, and verify the implementation. Results from these activities provide information about the actual security posture of the service provider's IP VPN service. The implementation and testing of security requirements is beyond the scope of this paper.

## D. COMMUNICATIONS NETWORKS INTERDEPENDENCIES

The European Commission has addressed European Critical Infrastructure (ECI) in a European Programme on Critical Infrastructure Protection (EPCIP) since 2004.<sup>15</sup> The ECI is defined as a critical infrastructure that, if disrupted or destroyed, would significantly affect two or more Member States or a single Member State if the critical infrastructure is located in another Member State. The eleven ECI sectors are currently defined as:

- I. Energy
- II. Nuclear Industry
- III. Information, Communication Technologies, ICT
- IV. Water
- V. Food
- VI. Health
- VII. Financial
- VIII. Transport
- IX. Chemical Industry
- X. Space
- XI. Research Facilities

Public and Legal Order and Safety, and Civil Administration are two sectors which are normally considered in the United States, Japan and Canada. They are not in the European Commission list.

### **Interdependence with Other Member State Infrastructures**

Although the European Commission has its ECI list, each Member State also categorises and addresses its own National Critical Infrastructures (NCIs) and there are critical infrastructure programmes existing at various stages of development, within each Member State. Therefore, it is important for to insure the interdependence between infrastructures at the European Level with the Member state level. Table D-1 shows the NCIs defined for a sample of Member States compared with the ECIs in the first column.

---

<sup>15</sup> Green Paper, On a European Programme for Critical Infrastructure Protection, Commission of the European Communities, COM(2005) 576 final, Brussels, BE, 17 November 2005.

Table D-1: Example National Critical Infrastructures (CIs) Compared to the European CIs

EP-CIP	France	Austria	Netherlands	Italy	Finland	Germany
I-Energy	• Energy & Electricity • Nuclear Power Stations	• Energy	• Energy (Electricity, Natural Gas, & Oil)	• Energy (Gas, Oil)	• Energy Networks & Supply	• Energy Supply (Electricity, Oil, Gas) • Nuclear Power Stations
II-Nuclear		• Chemical & Nuclear	• Chemical & Nuclear			
III-Information & Communication Technology (ICT)	• (Tele) Communication	• Information & Communication Technology (ICT)	• (Tele) Communications (Fixed, Mobile, Radio Communication & Navigation, Satellite Communication, Broadcast, Internet Access, Postal & Courier)	• (Tele) Communication	• Information & Communication Technology (ICT)	• ICT/(Tele) Communication
IV-Water	• Water	• Water	• Water Supply • Retaining & Managing Surface Water • Utilities	• Water • Utilities	• Water • Utilities	• Water
V-Food		• Food Supply	• Food (Supply & Safety)		• Food Supply	• Food Supply
VI-Health	• Health	• Health	• Health	• Health	• Health • Social Services	• Health
VII-Finance	• Banking & Finance	• Finance	• Financial (Services, Public & Private Infrastructure)	• Banking & Finance	• Banking & Finance • Payment Systems/ Currency Supply	• Banking, Finance & Insurance
VIII-Transport	• Transport	• Transport	• Transport	• Transport	• Transport	• Transport
IX-Chemical	• Chemical & Biotechnology	• Chemical & Nuclear	• Chemical & Nuclear			• Hazardous Materials (Chemical & Biological)
X-Space		• Space • Research				
XI-Research Facilities						• Research Institutions
	• Public Safety & Order	• Public & Legal Order and Safety	• Public Safety & Order • Legal Order	• Public Safety & Order		• Civil Protection
		• Civil Administration	• Public Administration	• Public Administration • eGovernment		• Public Administration/ Justice
				• Emergency Services		• Emergency Services
					• Electronic & Print Media	• Broadcasting • Media
					• Defense Industry	
						• Icons/ Symbolic Buildings

The table shows the variation across Member States and the European Union. We have found that sector boundaries exist and that the sectors normally operate in an almost entirely “stove pipe” manor. Each sector normally ensures its own integrity. Therefore, even though Member States rightly should have sovereignty (based on their best knowledge of the people, institutions, geography, etc. within their respective Nations) and sectors best understand the issues within their respective sectors, there should be an effort to either further align the European Commission view of critical infrastructure sector definitions or additional efforts for Member State interactions for common national critical infrastructures, so that the interdependencies can be better understood and addressed. Cross sector planning, assessment, resolution and notification should be sought. This is in alignment with the recent EPCIP memo.<sup>16</sup>

### **Interdependence within Sectors**

Interdependencies also exist within each sector. For example, within the Energy sector there are Electric, Oil and Gas infrastructures which exist. Electric power generation can depend on oil and gas and in turn oil and gas production can depend on electricity. These and other infrastructures (e.g., water) have networks for surveillance, command and control which are called SCADA (Supervisory Control and Data Acquisition) networks. The SCADA networks are also interdependent.

Examples within the Banking sector include cash machine networks, on-line banking, check processing centers and banks. Transport includes railroads, airports and seaports. Communications plays a key role within all of these. For example, communications effects not only seaport operations, but also the employment and economics in and around the seaport.

The Communications sector includes end offices, switching offices, power and fuel. Within communications, there also exist the interdependencies between network types (e.g., VoIP networks interfacing with the PSTN/IN networks) and between multiple network operators and multiple Member States. So for example, an outage or virus in one network can cascade to other networks. Thus, the interdependencies need to be understood and controlled.

### **Other Infrastructure Interdependencies**

A number of types of other infrastructure interdependencies exist. For example, there are **Physical interdependencies**, such as the material output of one infrastructure used by another. Examples are communications depending on electricity for operation and back up electricity depending on oil. **Cyber interdependencies** depend on electronic interfaces and informational linkages, such as databases and applications servers. An example of **Geographic interdependence** is common corridors, such as tunnels and bridges. Critical facilities are often concentrated within these corridors. Finally, Logical interdependence exists. For example, the sectors are often dependent on financial markets. Figure D-2 depicts the infrastructure physical dependencies within sectors, across sectors and across Member State boundaries.

---

<sup>16</sup> “The European Programme for Critical Infrastructure Protection (EPCIP)”, Memo 06/477, 12 December 2006, Brussels.

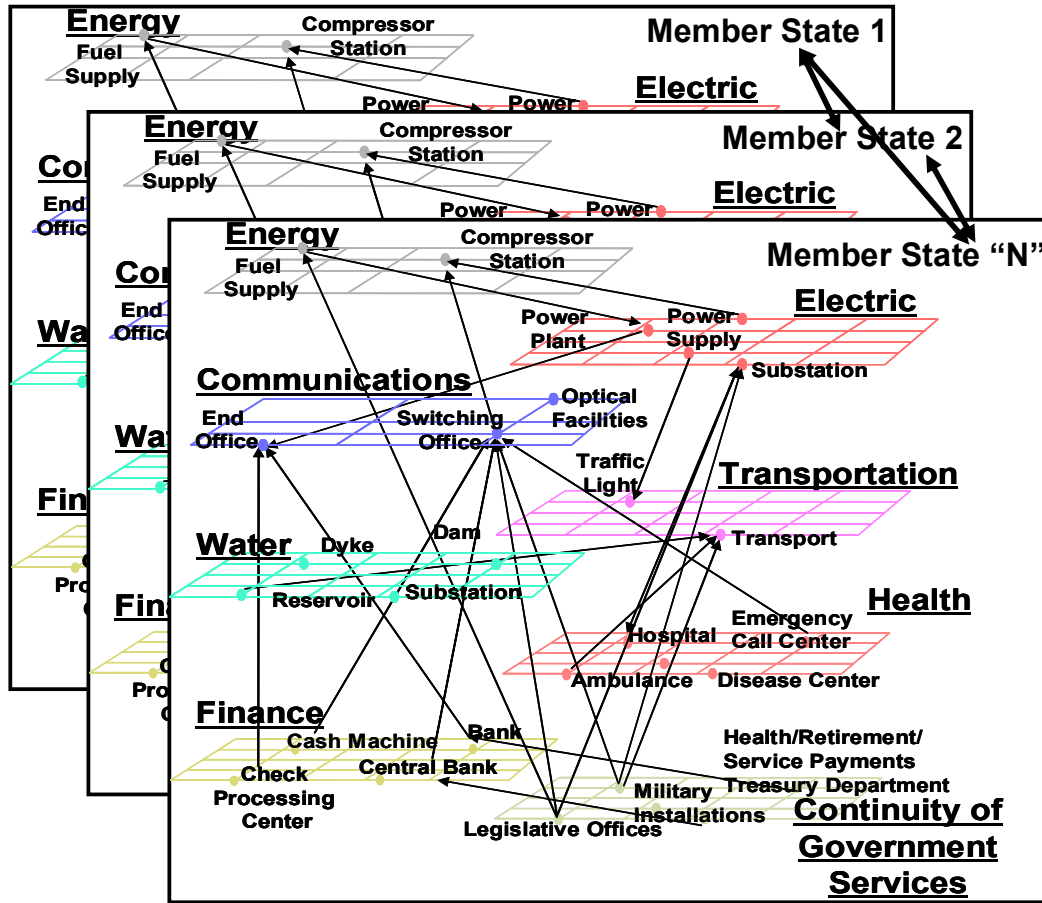


Figure D-2: Concept of Infrastructure Physical Dependencies

The highest degree of interdependence is Communications and Electric Power. All of the sectors depend on both of these and Communications depends on a number of the other sectors as in Figure D-3.

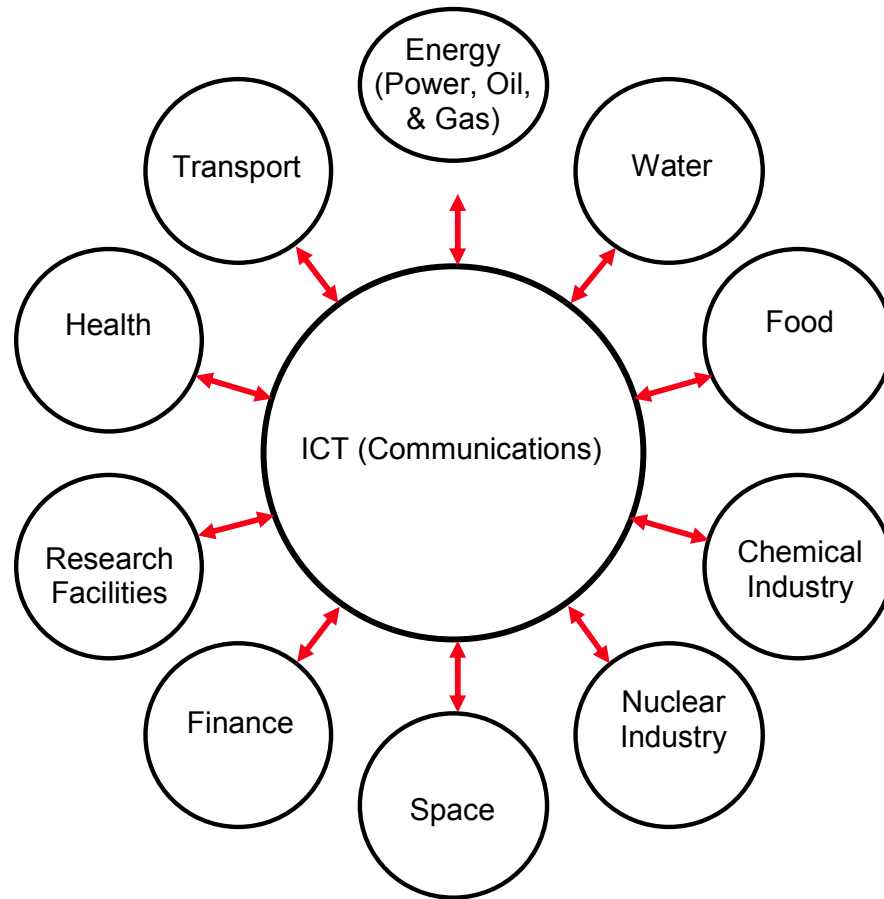


Figure D-3: Infrastructure Dependence on Communications

### Cascading Outage Concerns

These interdependencies, as well as the interconnection and interfacing of similar infrastructures across Member State boundaries, create the concern for cascading outages, when one or more of the infrastructures become unavailable. For example, a power outage may immediately, or after a period of time, cause telecommunications unavailability. This in turn, could cause a disruption in emergency services and response (see Figure D-4). The November 2006 European power outage, which started locally and spread regionally, is an example of cascading within a sector.<sup>17</sup>

<sup>17</sup> An overload in Germany's power network on November 4, 2006, triggered outages, leaving millions without electricity. Power failed first in Cologne, Germany, before shutting down across parts of France, Italy, Spain and Austria. Belgium, the Netherlands and Croatia were also affected.

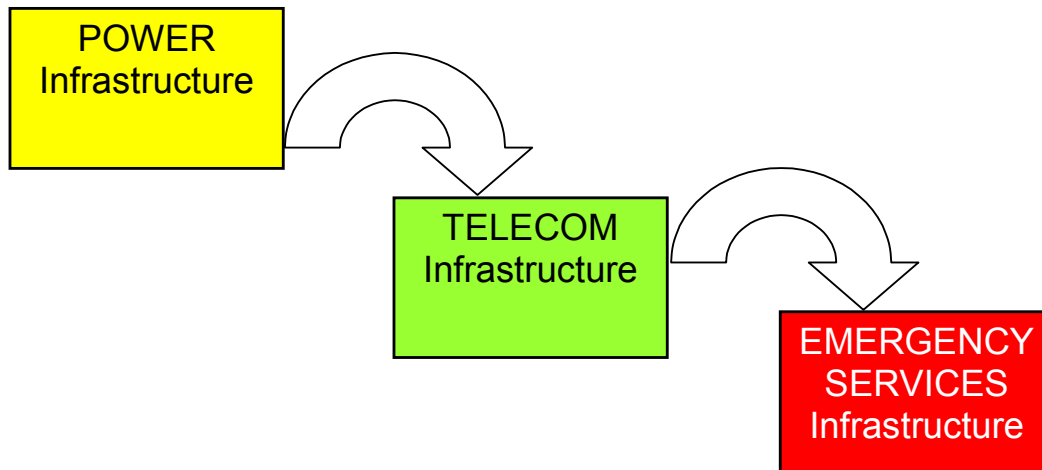


Figure D-4: Example Cascading of Outage

The national critical infrastructures will be evolving to the use of and support by the future networks. These networks will have multiple access media, such as mobile radio, wireline DSL, and cable. This distributed access will depend largely on power supplied from commercial sources in combination with battery reserve when the commercial power is off.

Powering with only commercial infrastructure is becoming more and more common. Users are much more likely to access their voice service using cordless phones, which need power to operate. Often, they do not have line-powered (i.e. powered via the telecommunications facility) phones at all. Moreover, the new VoIP phones are not line-powered.

Access using wireless service only is becoming much more prevalent, especially with younger people. It is estimated that about 8% of households in 2006 have wireless only service (i.e. no wireline service). This is expected to grow rapidly because of the economic incentive to do so.<sup>18</sup>

Access via voice over cable telephony service is also being offered by the cable companies as part of their triple play strategy. The cable modems need power to operate. These modems also support data and video. Moreover, other broadband access (e.g., DSL) is also highly dependent on commercial power. The DSL modem within the home or office and DSLAMs located in malls, apartment complexes and roadsides are examples.

The increased dependence on commercial, AC power therefore makes the critical infrastructures more susceptible to power blackouts and cascading outages.

The cascading effects and plans for addressing the more likely cascading outages can be driven by an understanding of the infrastructure interdependencies, as well as the modelling of the infrastructure reliability. Thus, an effort should be made to determine the degree of dependencies. A numerical weighting, such as in Figure D-5, could be used<sup>19</sup> where hypothetical weighting is shown for example purposes.

<sup>18</sup> New York Times, "Dangling Broadband from the Phone Stick", Business section, March 19, 2005.  
<sup>19</sup> Hypothetical interdependencies shown as an example.

Critical Infrastructure Interdependency*	Energy	ICT	Water	Food	Health	Financial	Public Safety	Civil Admin.	Transport	Chemical, Nuclear	Space, Research
Energy		4*									
Nuclear		4									
Information, Communication Technologies (ICT)	5	5	2	1	1	1	3	2	2	1	3
Water		4									
Food		2									
Health		3									
Finance		5									
Transport		4									
Chemical		4									
Space		5									
Research Facilities		5									

(\*0=None, 1=Very Low, 2=Low, 3=Medium, 4=Strong, 5=Very Strong)

Figure D-5: Example only. Sample Infrastructure Interdependence

### Emergency Contacts

Another factor which affects the cascading nature of outages, as well as the ability to respond quickly and effectively in emergency situations is based on prior knowledge of who to contact for support in specific situations. This information is also useful for conducting preparedness exercises.

At best, informal knowledge and agreements exist between limited sets of people, organisations or governments. The contacts and arrangements are often only known to the specific people. As staffing changes, the knowledge and agreements are easily lost. A more formal database of contact information, a Responsibility Data Base, would be very beneficial to develop.

Examples of categories to consider for the Responsibility Data Base include:

- Country Level
- Entity Level
- Time of Day
- Day of Week
- Holiday
- Type
  - Physical, Cyber, Geographic, Logical
  - Mutual Aid
  - Recovery
  - Testing
- Primary, Secondary Contact
- Telephone Numbers
- Email addresses and URLs

Table D-6 shows a conceptual construct for the Responsibility Data Base.

Table D-6: Example of Critical Infrastructure Responsibility Matrix

Critical Infrastructure Interdependency	Austria	Finland	France	Germany	Italy	Netherlands
Energy						
Nuclear						
Information, Communication Technologies (ICT)						
Water						
Food						
Health						
Finance						
Transport						
Chemical						
Space						
Research Facilities						

- Country Level
- Entity Level
- Time of Day
- Day of Week
- Holiday
- Type
  - Physical, Cyber, Geographic, Logical
  - Mutual Aid
  - Recovery
  - Testing
- Primary, Secondary Contact
- Telephone Numbers
- Email addresses and URLs

**Conclusion**

The dependencies surrounding the critical infrastructures lead us to conclude that the European Commission should encourage and support Communication (and other critical infrastructure) engagements for:

- Rationalizing the critical infrastructure categories across Member States
- Understanding and representing the interdependencies between Communications (and other critical infrastructure sectors) and the other critical infrastructures through modelling
- Identifying and modelling the dynamic nature and quantifying the magnitude of interdependence
- Development and use of standard information (e.g., for a Responsibility Matrix)