Introduction to Critical Network Infrastructures

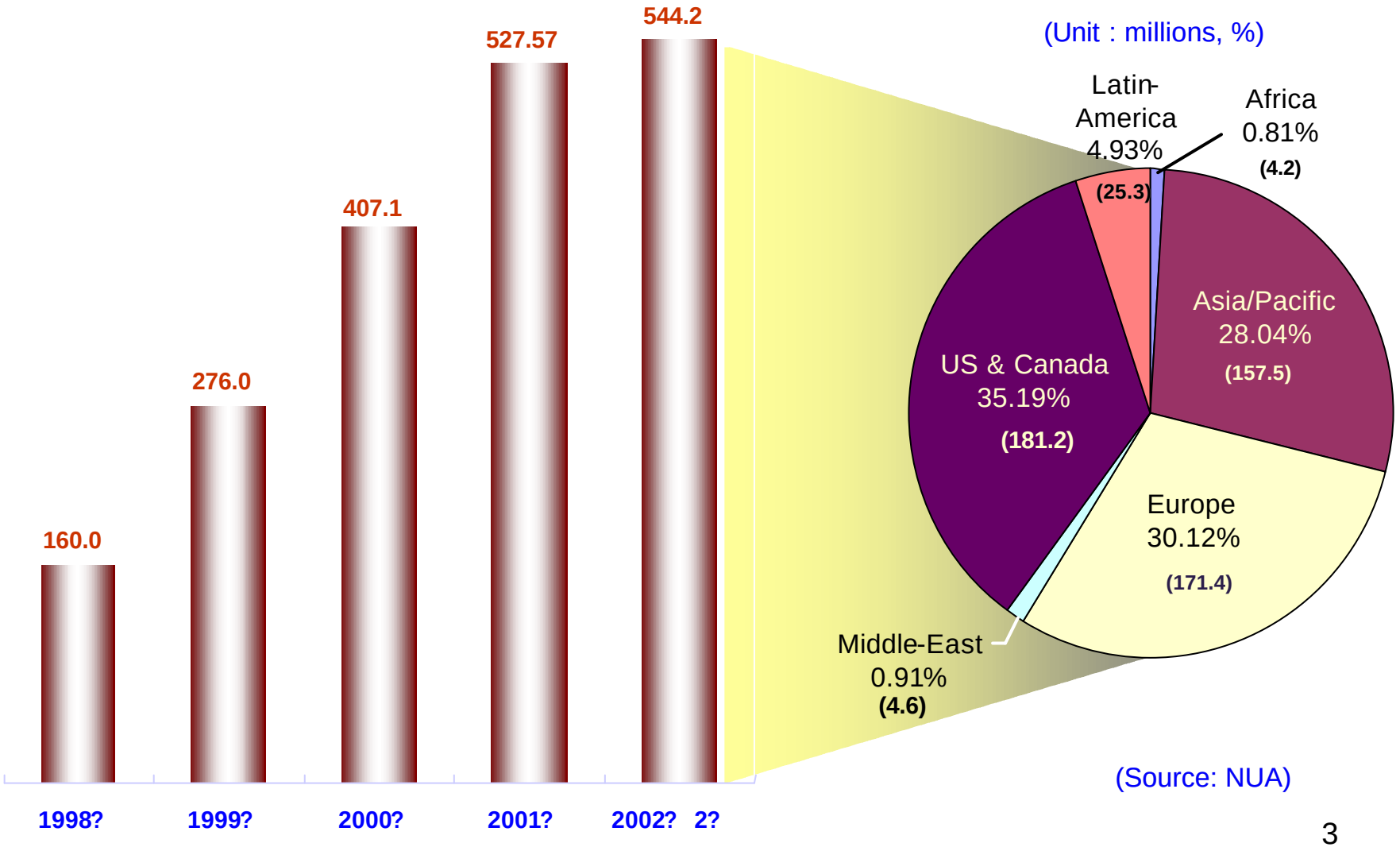
2002. 5. 20

Kijoon Chae
Ewha Womans University

Contents

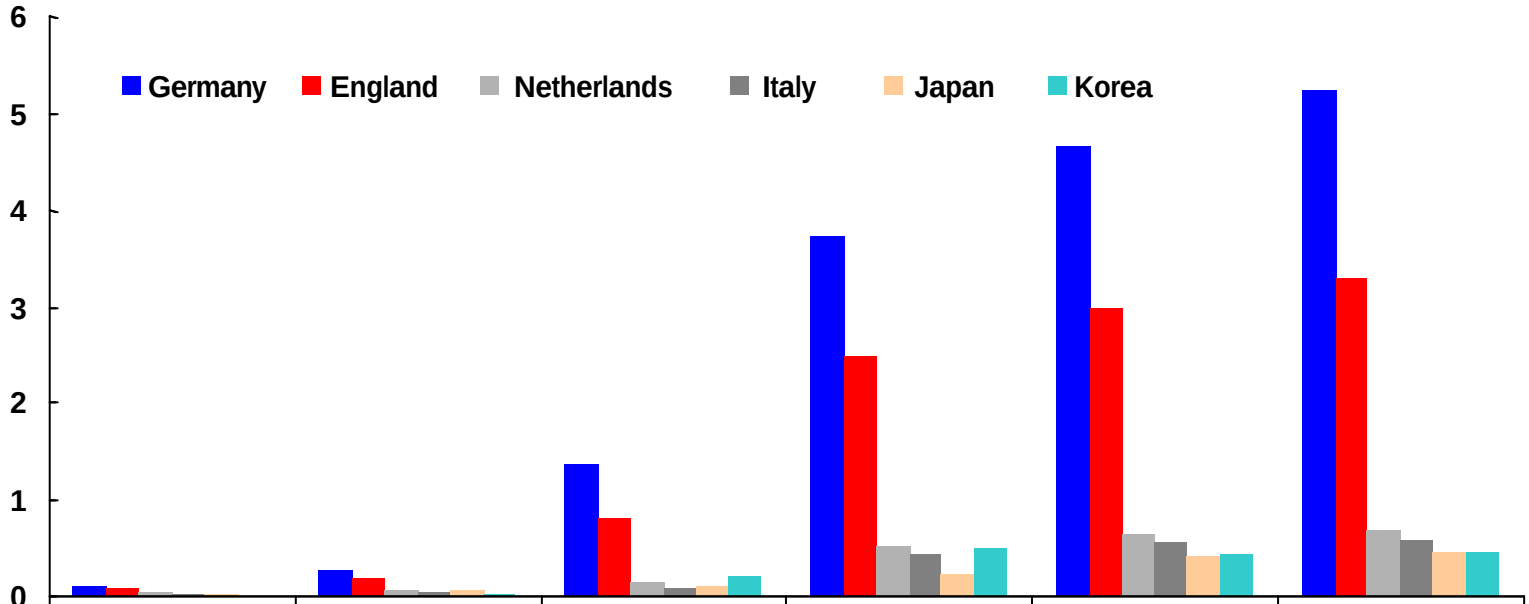
- Background
- Objective
- What is CNI?
- Network Trends and Vulnerabilities
- Current Problems for CNI
- Solutions for Security Problems
- Other Areas Impacting Infrastructures
- Suggestions and Conclusion

Worldwide Internet Users



(Source: NUA)

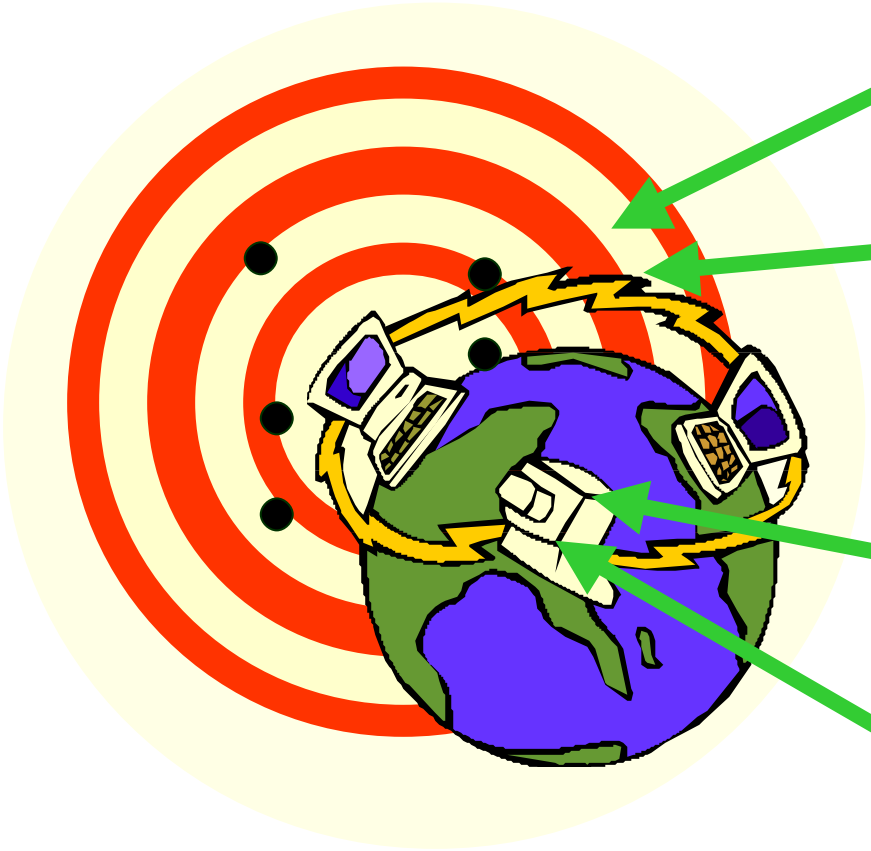
Number of Domains (Upper 6 countries)



	1997	1998	1999	2000	2001.6	2002.1
Germany	105,344	288,191	1,384,361	3,738,732	4,658,764	5,254,281
England	95,151	196,753	807,487	2,506,589	2,977,535	3,295,442
Netherlands	40,000	65,000	160,000	530,000	643,638	702,854
Italy	21,658	45,819	93,279	437,322	569,143	594,452
Japan	33,739	58,549	124,573	234,294	417,013	473,539
Korea	8,045	26,166	207,023	517,354	454,799	465,323

(Source: KRNIC)

Why is the Internet vulnerable?



Millions of entry points world-wide

Tens of thousands of interconnected networks

Open systems culture

Ease of use of intruder tools

What is a Security Vulnerability?

- Security Vulnerability : flaw or weakness in a system's design, implementation or operation that could be exploited to violate the system's security (RFC 2828)

- Threat: action or event to do harm to security

Vulnerability + Threat → Risk

Protocol Vulnerabilities

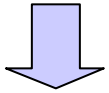
- Standards bodies have accepted protocols with serious vulnerabilities.
- Security depends on the whole protocol.
- Protocol vulnerabilities last a long time.
- Threats change over time.
- Implicit assumptions are often violated.
- Application layer protocols also have security vulnerabilities.
- Inattention to security issues creates vulnerable protocols.

(Source: Dr. Greg Shannon at Lucent Technologies

ITU-T Workshop on Security, Seoul, 13-14 May 2002)

Objective

- The great variety of vulnerabilities and threats exist on the network.
- Most IT-based network infrastructures are not secure.
- International cooperation is needed to secure CNIs.



- Identify the explicit significance of the CNIs
- Provide possible solutions to resolve CNI security problems
- Find methods to collaborate and cooperate among countries

What is CNI?

- ## Logical aspect

  A public or private network that carries information relevant to national security and safety or information of high financial value

- ## Physical aspect

  The whole network or a part of the network that exchanges information of high significance

Network Trends: Internet

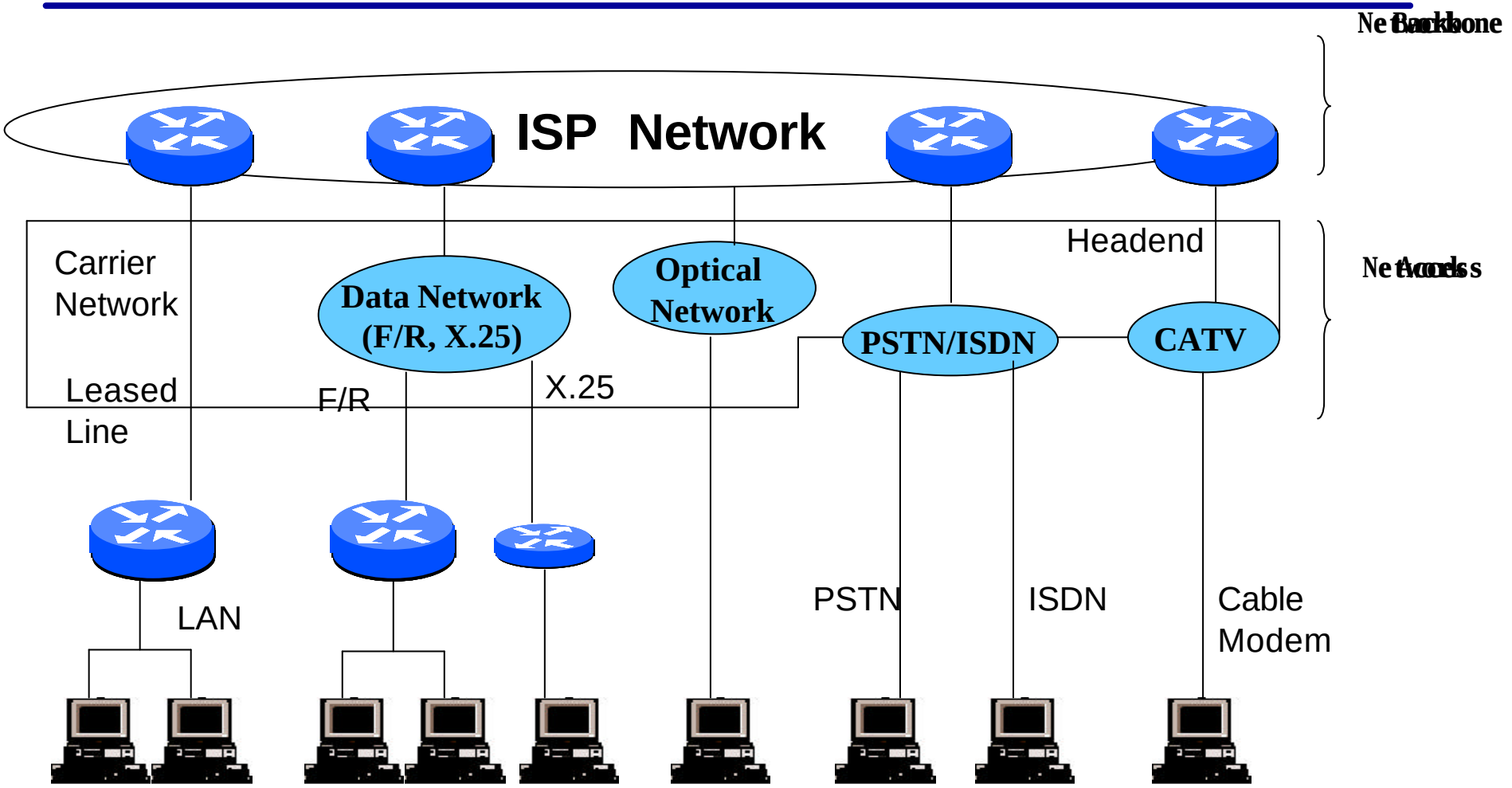
- The twenty-first century is the era of the Internet.
- Internet has been helpful to combine techniques of traditional industry and info-communication.

Problems of Internet

- Inefficient communications
- High cost and low transmission speeds to end-users
- “Bottleneck” impediments to the construction of high-speed networks
- Unfair network access policies
- Inefficient network extension
- Excessive waiting times
- Service with no guarantee of the bandwidth between end users and QoS for a real-time service
- Poor of security provision

⇨ Need to develop Next-Generation Internet (NGI)

Hierarchical Architecture of Internet

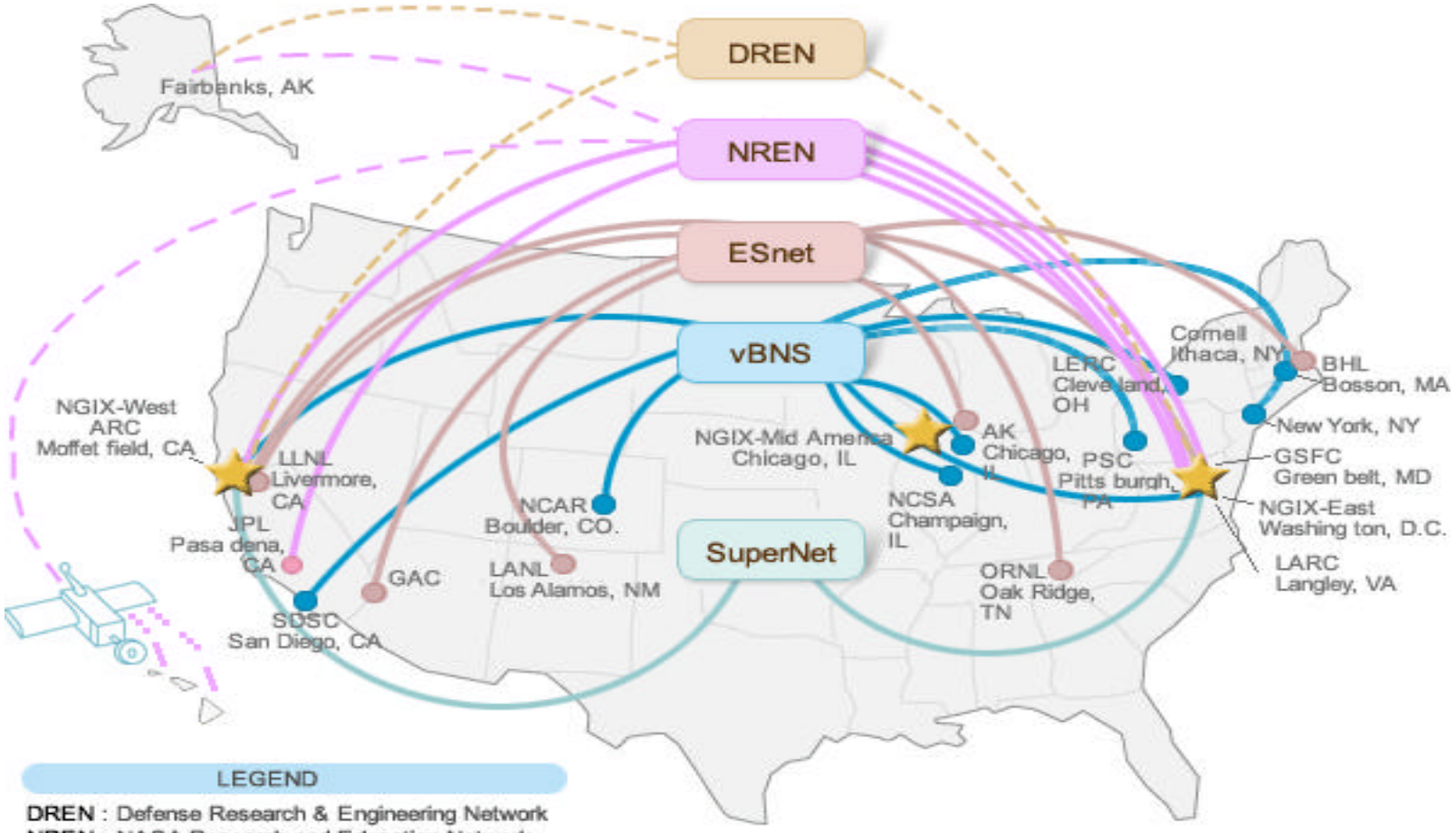


May cause "Bottlenecks"

Next Generation Internet

- Resolve today's Internet problems
- Adjust to changes in demand as society becomes more information-oriented
- Present potential solutions to the problems of network congestion, service delay, lack of addresses, expensive charges, etc.
- Support multimedia and mobile services of a high speed and performance with guaranteed qualities

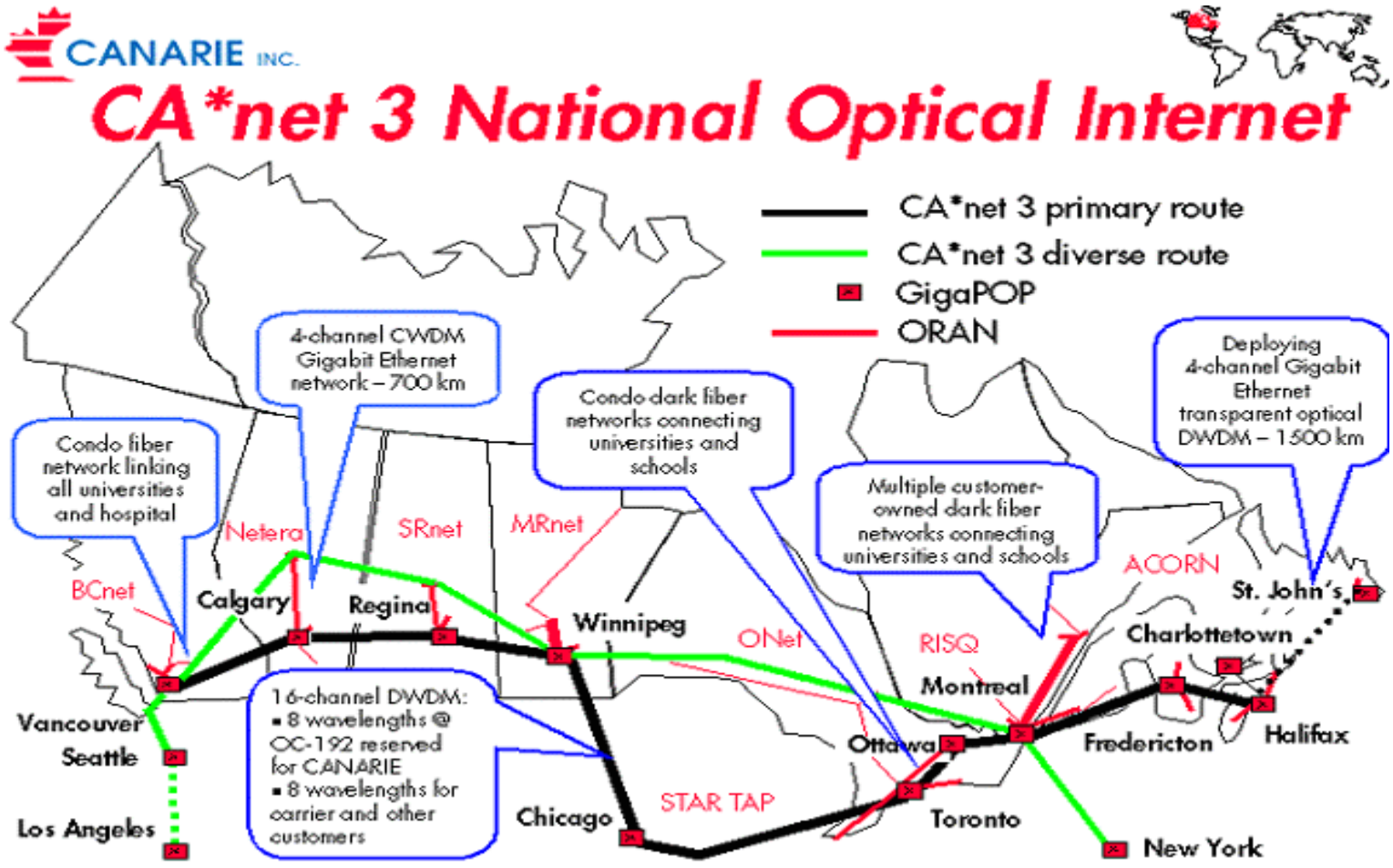
NGI (United States)



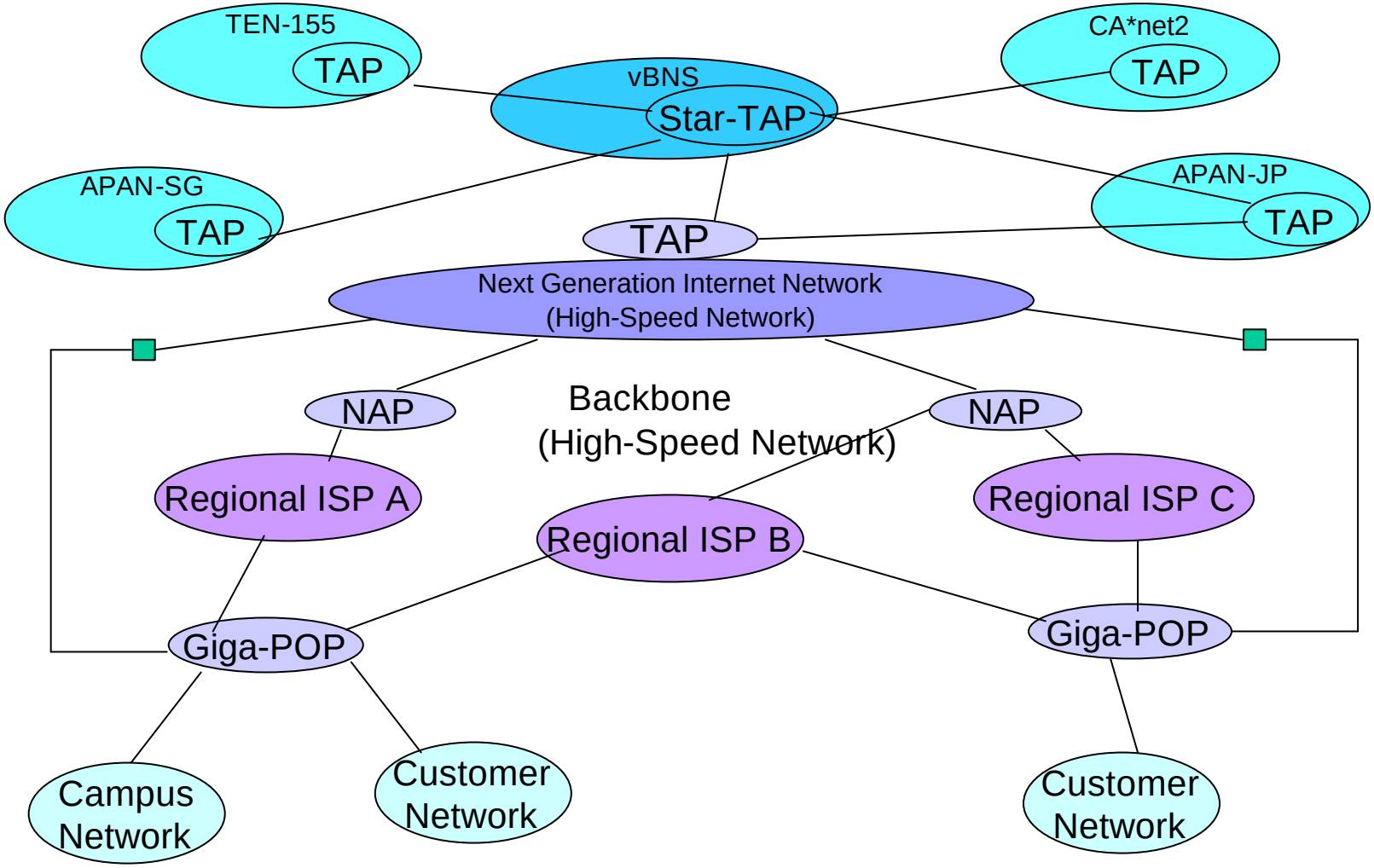
LEGEND

DREN : Defense Research & Engineering Network
NREN : NASA Research and Education Network
ESnet : Energy Sciences Network (DOE)
vBNS : Very High Speed Backbone Network Service (NSF)
NOTE : vBNS will support initial Internet 2 community
SuperNet : Terabit Research Network (DARPA)

NGI (Canada: CANARIE)



Hierarchical Architecture of NGI



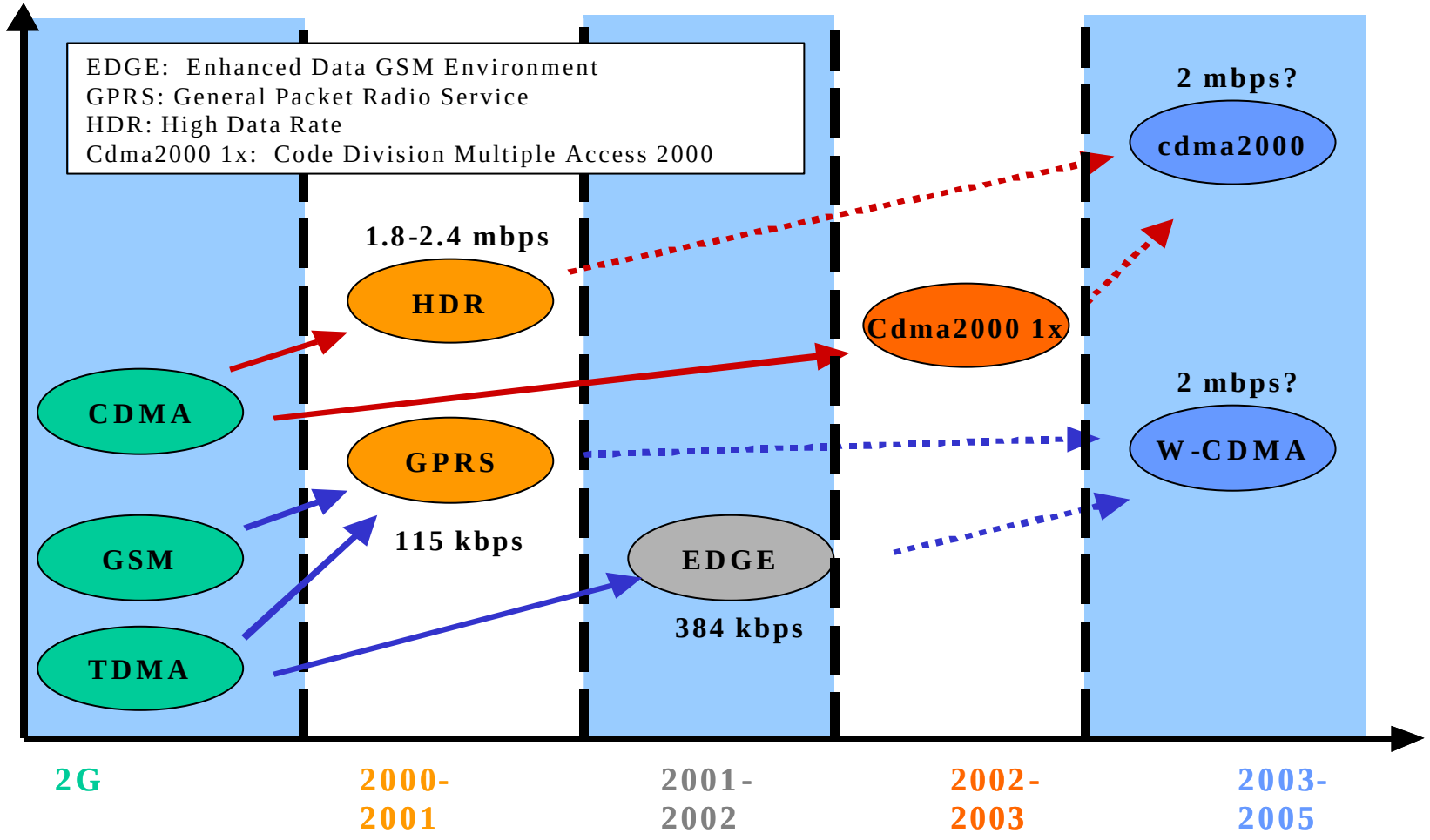
Security of Internet / NGI

- Security services are applied to individual systems, networks of a particular nation.
- Necessary to apply security system at the intermediate access point
- Interoperability among individual security systems should be provided.
- Secure network techniques should be introduced.

Mobile Communication

- Anywhere, anytime, anyplace communication systems
- Next-generation mobile systems foresee the convergence of mobile, fixed and IP networks towards future high-speed services.
- International Trends of Mobile Systems
  - Evolved from the 1st generation to the 2nd generation (2G)
    - From analogue to digital system
    - Provide better quality and higher capacity at a lower cost
    - 2G (CDMA, GSM, TDMA)
  - 2.5G system
    - HDR, GPRS, EDGE
  - The 3rd generation (3G) system
    - Called IMT-2000 or FPLMTS
    - Integrated applications and services
      - multimedia messaging, infotainment, location-based services, etc,.
    - cdma2000, W-CDMA
  - The 4th generation (4G) system
    - Various internetworking and integrating technologies
    - IP and high-speed packet wireless transmission
    - Provide mobile multimedia services over tens of Mbps at low cost

From 2G to 3G mobile systems

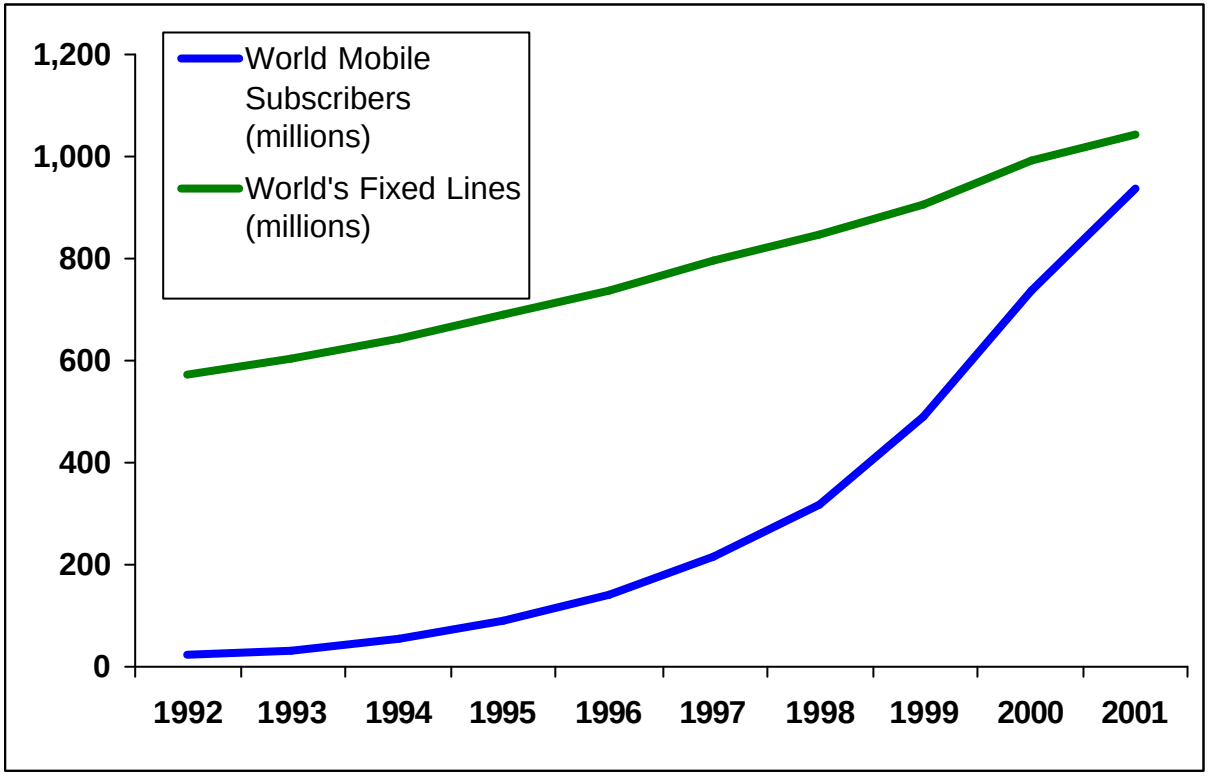


Source: **ITU IMT-2000 and Beyond Study Group.**

Mobile Communication Technologies

- Migrate mobile traffic onto an all-IP network
  - IP is scalable and can tolerate a variety of radio protocols.
  - Translate into enhanced data transmission services for Internet-enabled devices
  - Stimulate the innovation of diversified services for consumers
  - More flexible for application development than current networks
  - Support a wide array of access technologies
    - 802.11b, W-CDMA, Bluetooth, HyperLAN, etc.

Mobile and fixed-line users worldwide



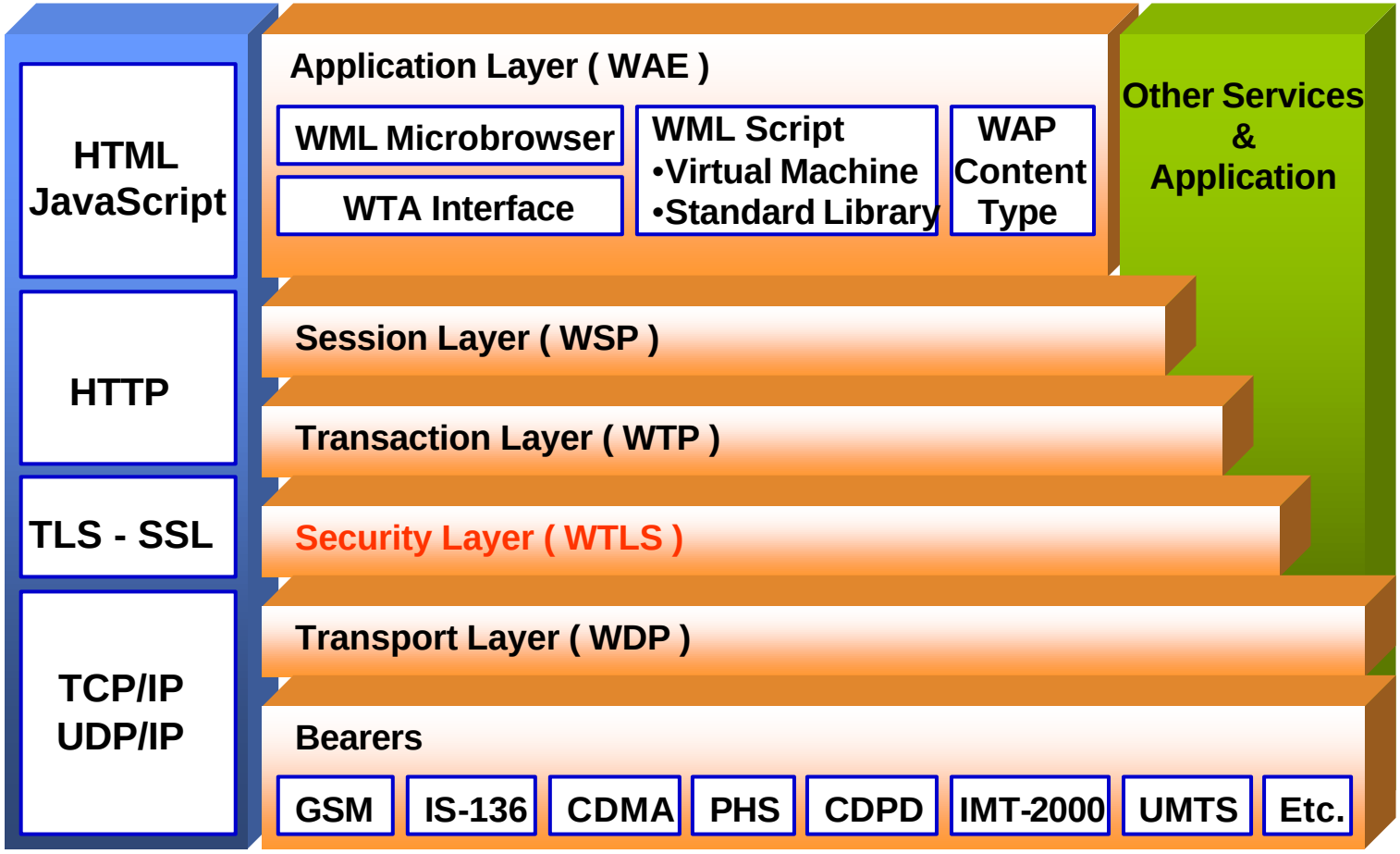
Source: **ITU World Telecommunication Indicators Database.**

- By the end of 2001, almost one in every six of the world's inhabitants had a mobile phone.
- During 2002, mobile subscribers will overtake the number of fixed lines worldwide.

Vulnerability on Mobile Systems

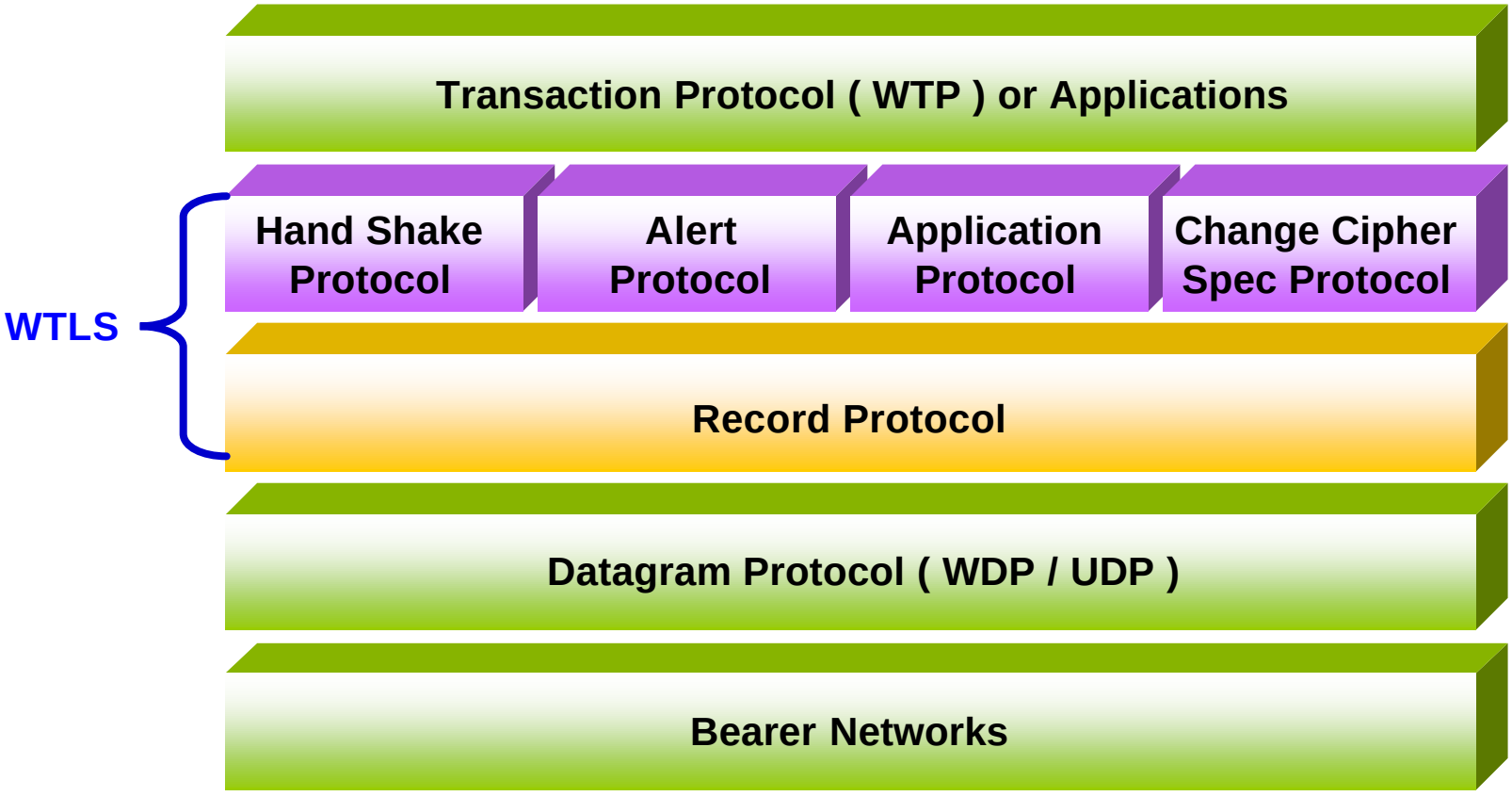
- **Data stores and data transmissions are becoming increasingly vulnerable to interception, hacking and viruses.**
- **The main vulnerabilities occur at the translation point between the wireless protocols and the wireline (fixed) protocols.**
- **Strong authentication procedures are required to prevent security breaches.**
  - WAP (Wireless Application Protocol) 2.0 protocol
    - Ericsson, Motorola, Nokia, and Unetworkired Planet organized WAP Forum.
    - Employs WTLS (Wireless Transport Layer Security)
  - I-mode
    - Developed by NTT DoCoMo
    - Employs SSL communication just between I-mode gateway and server

WAP Protocol Stack



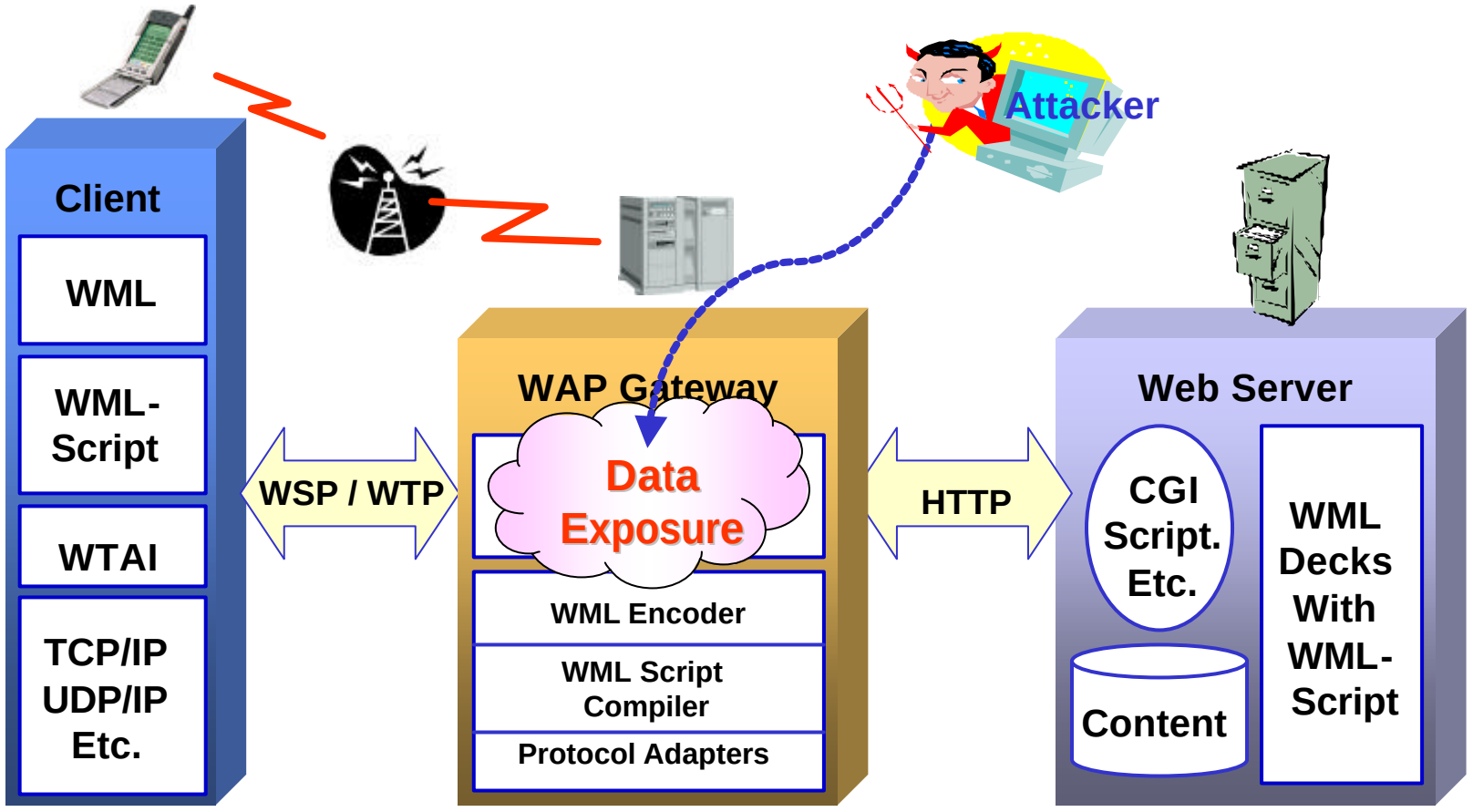
Source : WAP Forum, http://www.wapforum.org

WTLS Protocol Stack



Source : WAP Forum, http://www.wapforum.org

Vulnerability of Wireless Internet Service



End–to–end communication is not secure !!!

Transaction Security

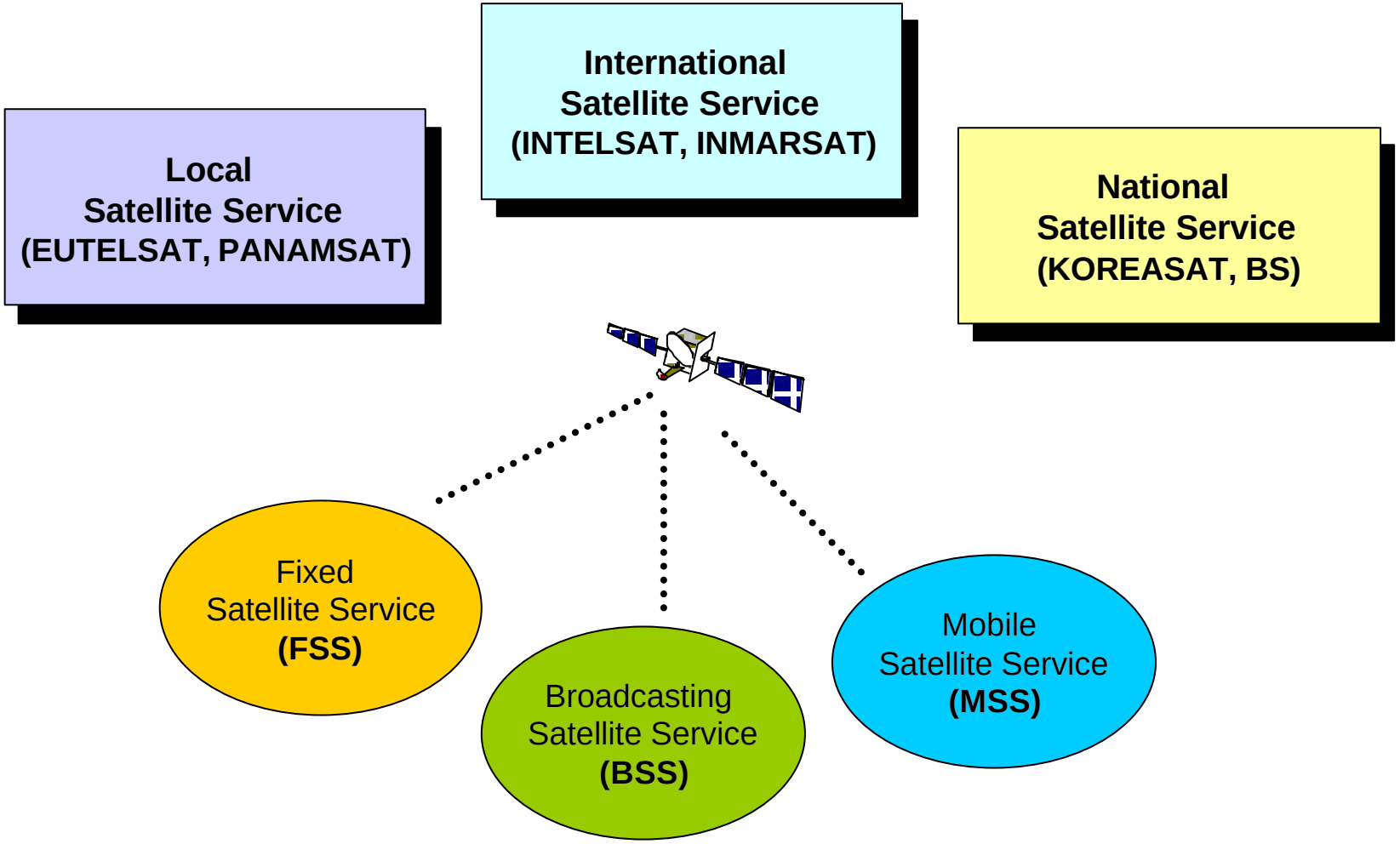
- In relation to transaction security, the privacy firm Meconomy makes the following recommendations:

1. The use of an open platform for devices, in order to enable users to apply their own privacy and security technologies

2. Separation of personal identifiers from transactional data, to increase privacy and security.

3. Use of data collected for a transaction should be limited to the specific transaction in question.

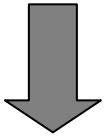
Satellite Communication Service



Satellite Communication Services

Traditional Services

Low-speed data communication
Long-distance telephone transmission
International TV broadcasting services



Enhanced Services

High-speed data communication
Satellite ISDN service
Satellite mobile communication
High quality of broadcasting
Low costs

Types of Satellite Communication

Geostationary Satellite

36,000km above the ground ⇒270msec delay

International calls

Broadcasting services

Trans-ocean, land, aeronaut communication

e.g. INTELSAT

LEO-Satellite

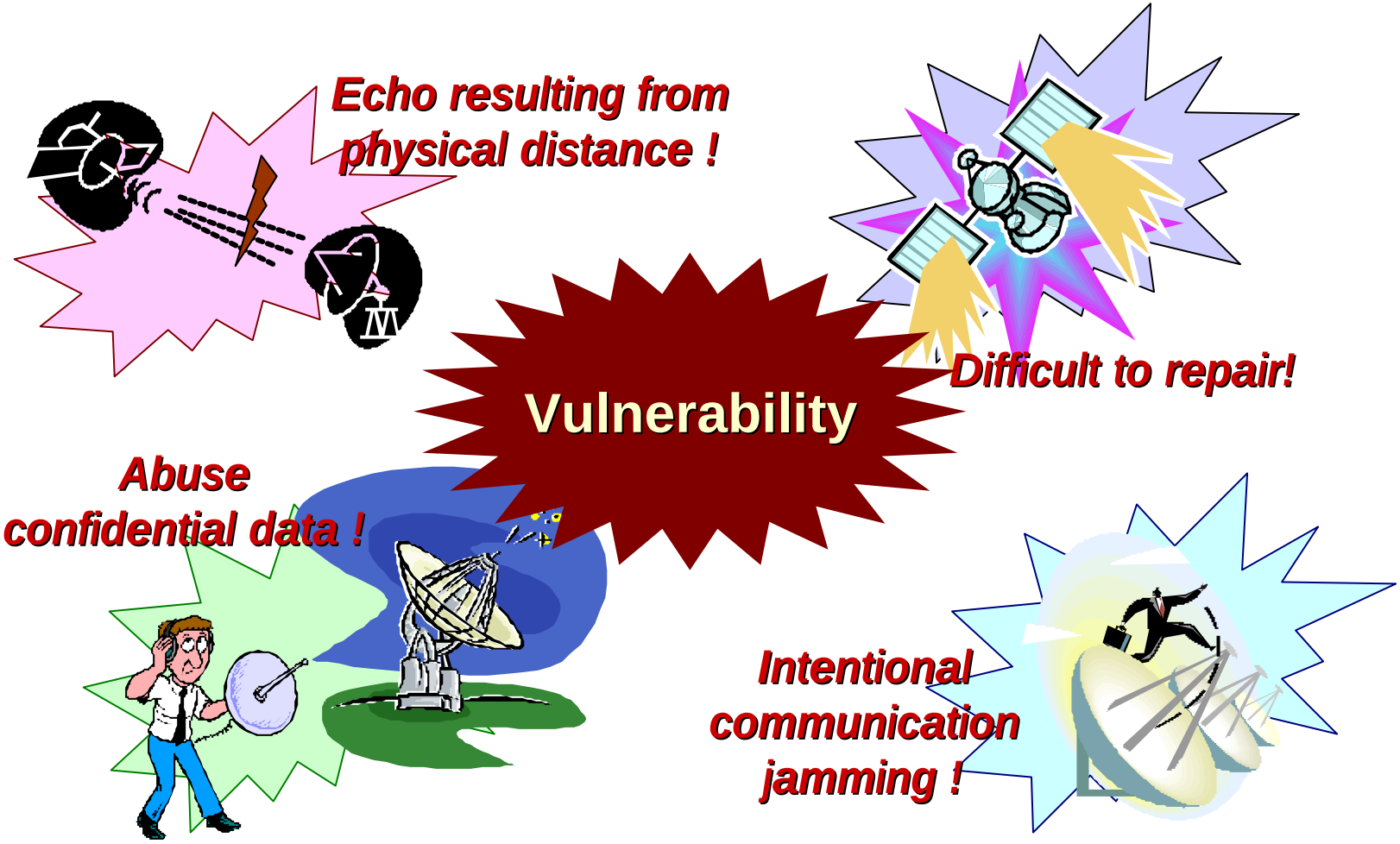
1,000km above the ground

Communication anywhere in the world

Mobile Internet

e.g. Iridium, Globalstar, INMARSAT's IOC plan

Vulnerabilities on Satellite Communication



Current Problems associated with CNI

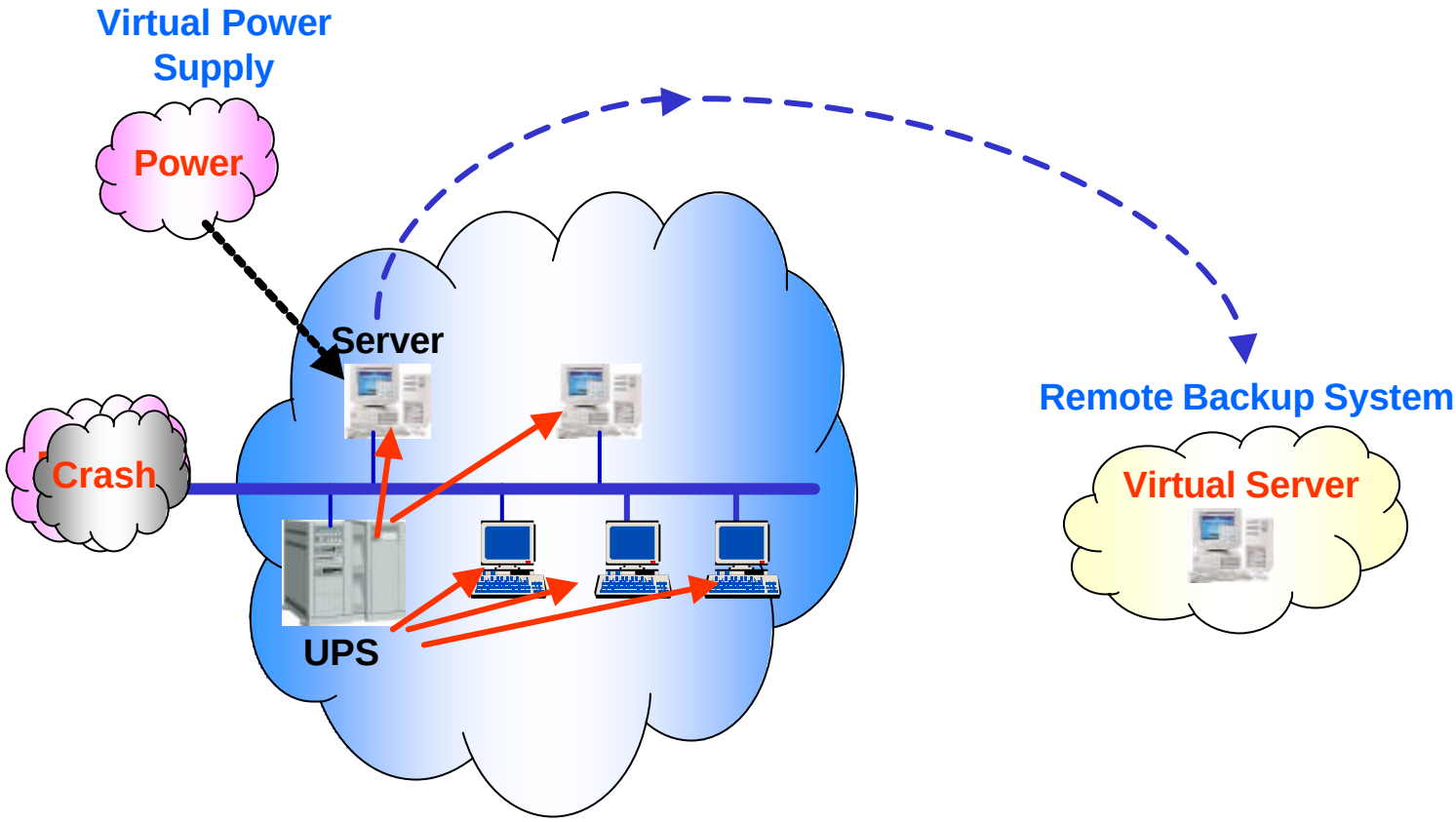
- As networks become more global, more and more people have access to critical data.
- Networks involved in CNI are vulnerable to many dangerous threats:
  - Physical damages on the infrastructure by natural factors or unintentional troubles

    e.g. Natural disaster, power outage, network failure, etc.
  - Security factors in network systems operating the infrastructure

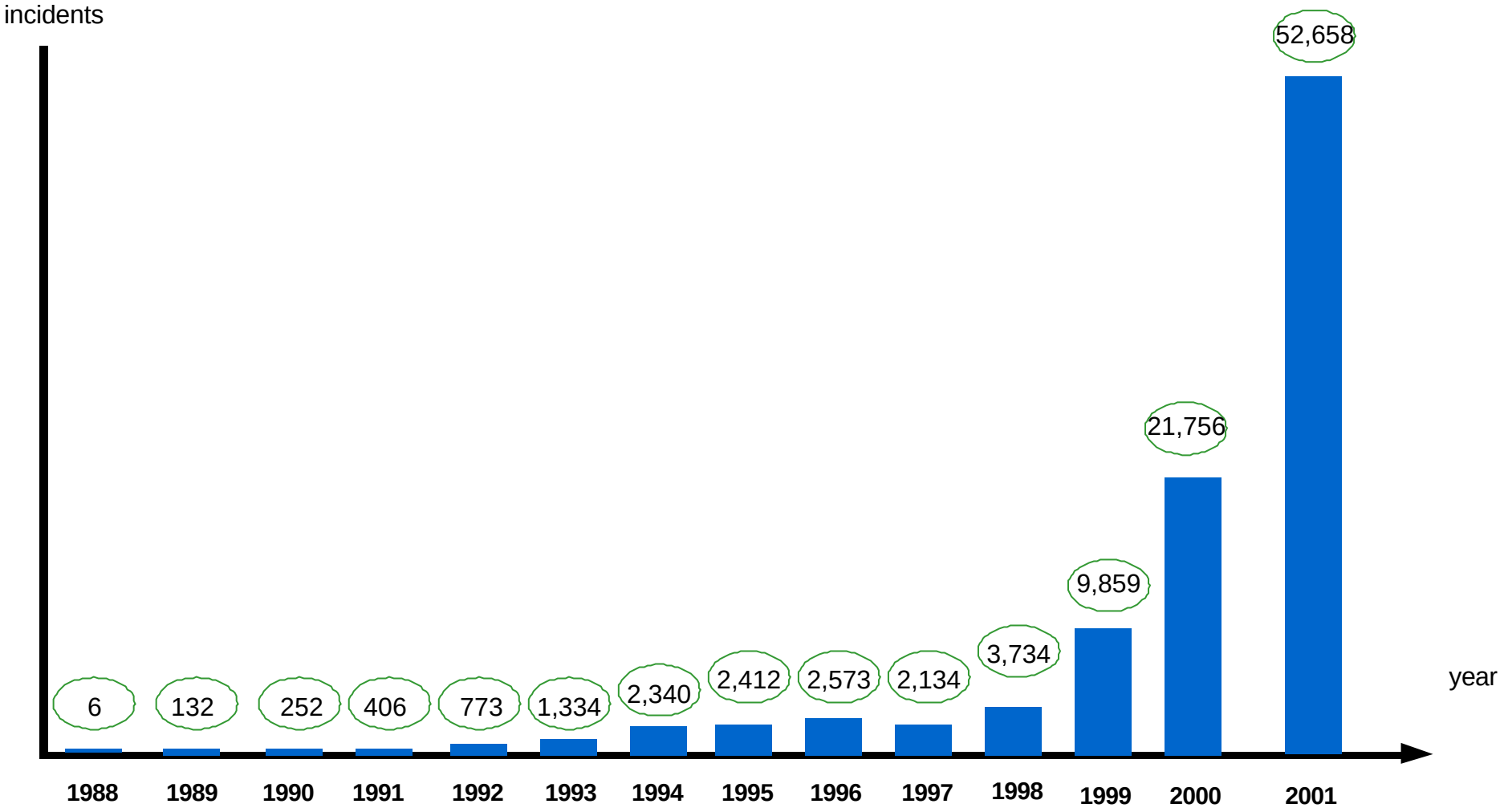
    e.g. Unauthorized access, intrusions, network disruptions, malicious software, etc.
  - Attacks through weak points in network components such as operating systems, routers, switches, name servers, etc.

⇨ Developing policies and technologies to resolve the problems and enhance confidence for CNI is required.

Power Attack



Number of Incidents Reported



Source : CERT (http://www.cert.org/)

Solutions for Security Problems

- Reasons for CNI security to become a significant issue
  - data protection, economic dependency, national security, e-commerce, etc.
- Need for international cooperation for CNI security
  - Resolving CNI security problems is an urgent priority.
  - Grades of security capability vary greatly between different networks.
  - No common policy or system to guarantee reliability
  - Since IT industries evolve very fast, CNIs cannot be secured indefinitely using existing security tools.
- Major types of policy
  - Providing systematic legal solutions
  - Awareness-raising regarding the necessity of CNI security

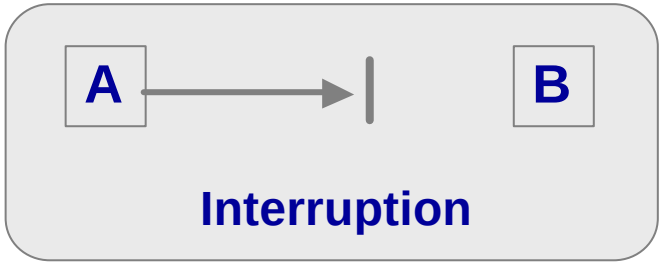
Security Schemes & Policies for CNI(1/2)

- Building a theoretical framework for understanding and predicting the nature of the CNI securities and their effects as a whole
- Developing the capability to model and simulate in real time the behavior of the CNI by developing an architecture and related enabling technologies
- Developing a set of quantitative metrics for measuring the scale of impacts of CNI disruptions
- Developing new technologies and techniques to contain, mitigate, and defend against the effects of CNI disruptions

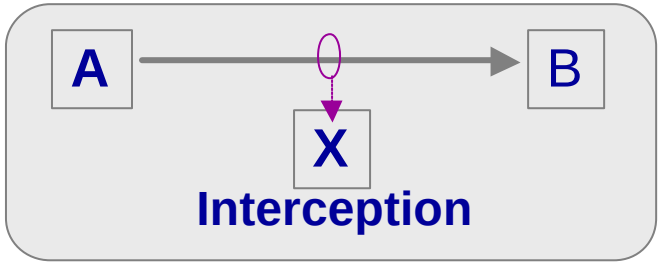
Security Schemes & Policies for CNI(2/2)

- Developing capabilities to adequately and realistically test new methodologies, techniques, and technologies.
- Defining a set of tasks for further work on specific CNI policy issues that could be analyzed using tools and methodologies.
- Developing the ability to characterize and incorporate new critical infrastructures into the models and methodologies as such infrastructures develop.

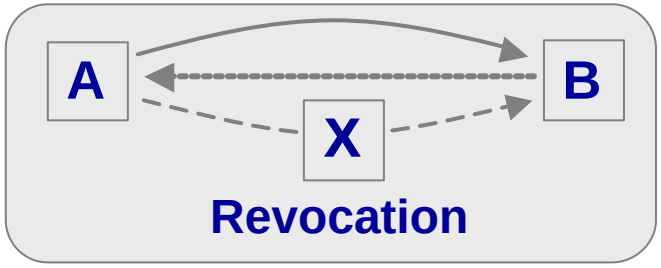
Security Services



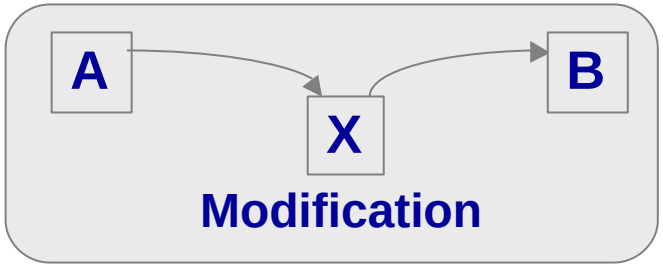
AVAILABILITY



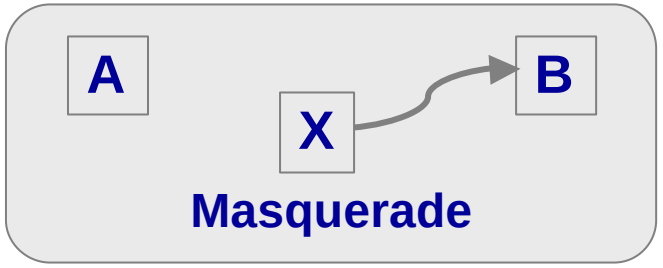
CONFIDENTIALITY



Non - REPUDIATION

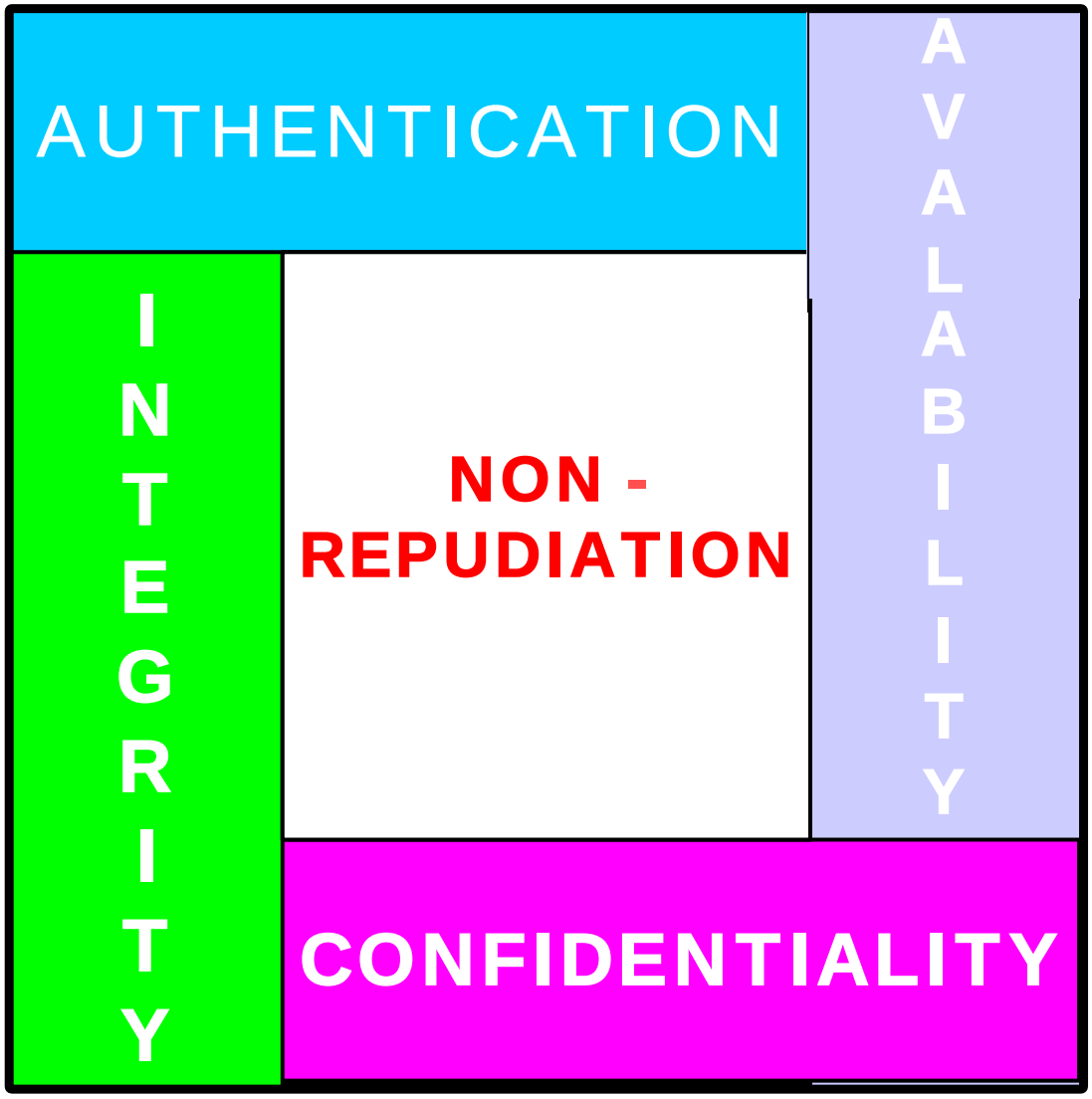


INTEGRITY

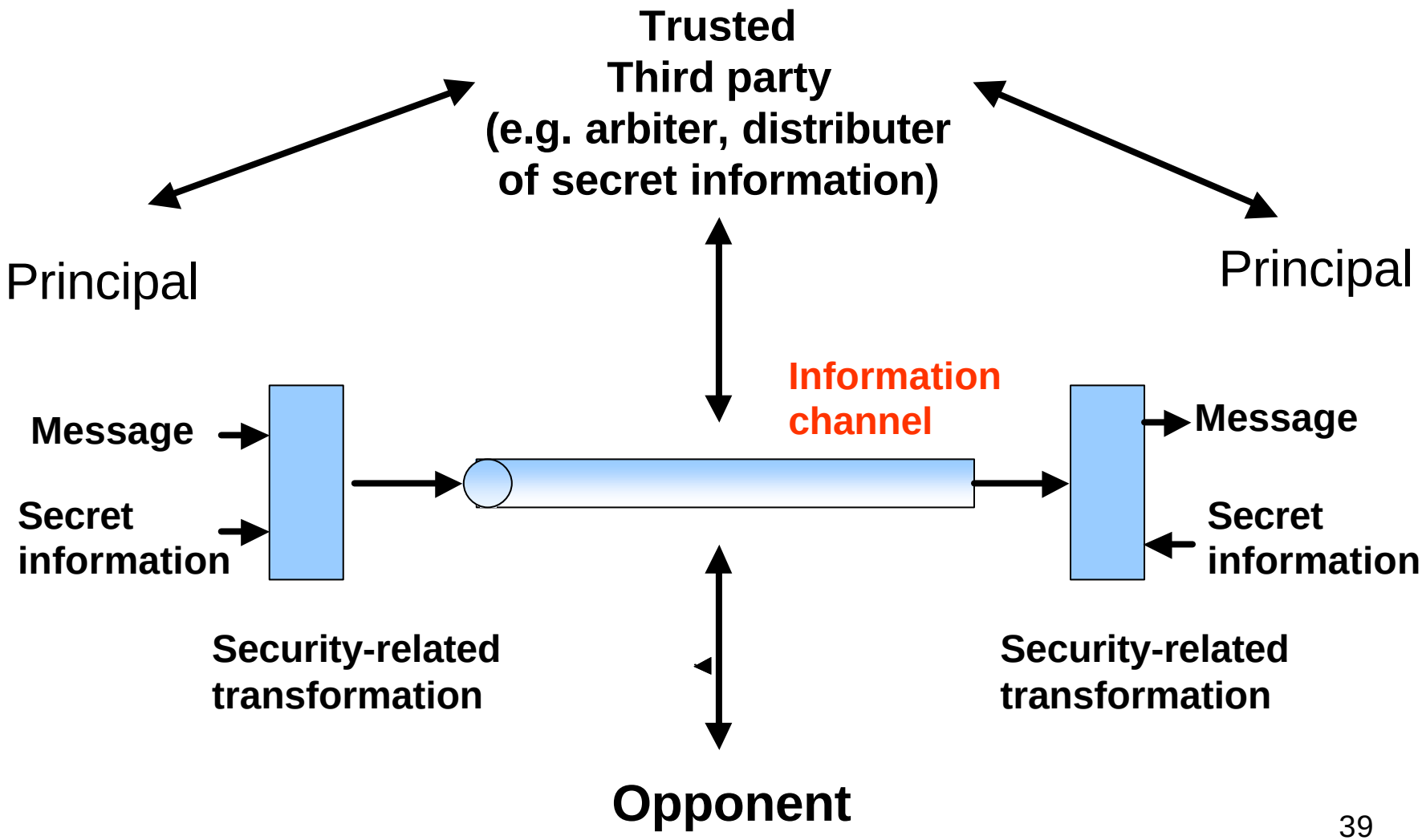


AUTHENTICATION

Security Services



Network Security Model



Cooperation Mechanisms for CNI

❖ Scopes of CNI concerns

- ➢ National scope
  - Concern the main security or government network in a particular nation
  - Considered impossible to ensure the security of important data or strategic functions of a nation on the public Internet
    - → A separate network is required.
  - US Govnet
    - ✓ Independent government administrative network that is planned to be a private voice and data network based on the IP protocol
    - ✓ But, with no connectivity to commercial or public networks
    - ✓ Must perform functions with no risk of penetration or disruption from users on other networks

Cooperation Mechanisms for CNI

- International scope
  - Mainly focus on trade and financial networks over the world
  - SWIFT
    - ✓ Global data communication system
    - ✓ Operate for the exchange financial information among international banks for many years
  - EDI (Electronic Data Interchange)
    - ✓ Allow the easy processing of customs documents in the trading world

Cooperation Mechanisms for CNI

- Need of international cooperation for CNI
  - Security problems of International network increase.
  - Although a network of a particular nation may provide a high degree of reliability or security, the security of total networks may still depend on lower level's interconnected networks.

- In spite of the fact that cooperation for CNI security on the international level is regarded as essential, few of the existing international CNI security systems have been standardized.

⇒ International standard organizations, such as ITU, could play an important role in standardizing policies and technologies for CNI security.

Cooperation Mechanisms for CNI

- International cooperation for CNI security
  - OECD (Organization for Economic Co-operation and Development)
    - Security guidelines recommend a policy that limits its member from individual data distribution processes when a particular member is not equipped with a security system at the “same” level as that of other members.
  - EU
    - Cooperate with US to improve the security of critical infrastructures,
    - Made all possible research efforts on CERTs (Computer Emergency Response Teams)
  - EC
    - Cooperate with G8, OECD, UN, etc.
  - Global Business Dialogue on E-Commerce / Global Internet Project
    - Forums for discussion about security problems between private sector players with regard to e-commerce

Other Areas Impacting Infrastructure

- Possible constructive steps to protect CNI from other networks:
  - Complete separation of CNI from other network areas
    - US Govnet, CIA, Pentagon, Korean Military Networks
    - Advantage : maximize the security of critical data
    - Disadvantage : limitation to user access depending on the location and situation
  - Heightened security for other network areas related to CNI
    - CNI co-exists with the Internet or is interconnected with other networks for optimal data access.
    - Impossible to set up separate networks for every CNI
    - ⇒ Ensure further security by applying security policies and technologies at access point level or end-to-end level

Suggested Principles to Enhance Trust in CNI

- Establish detailed standards to distinguish between CNIs and non-CNIs
- Classify CNI infrastructures, analyzing those CNI systems in operation in order to understand their status and to assign them to a particular category
- Analyse the vulnerable aspects in CNIs by category and prepare possible steps to enhance security for each category
- Legislate an internationally certified warranty policy for CNI security and establish a specific standard for the security being applied for particular CNIs in order to guarantee a certain lever of service for users

Suggestions for Possible Role by the ITU

- Establish security management standards at the international level in order to apply general security principles for CNI
- Establish standards for security policies and technologies in order to guarantee the reliable and efficient operation of networks, both for independent and interconnected CNIs
- Identify examples of CNI best practice

Conclusion

- CNI is a public or private network that carries information relevant to national security and safety or information of high financial value.
- Roughly classified into two categories:
  - Completely independent and separate
  - Connected to other networks
- There is a lack of awareness of CNIs, a lack of investment in CNI security and a lack of standardization.
- It is urgent that common security issues be analyzed, and solutions be developed through international support and cooperation.